# Лекция 4: отношения и их графы

Дискретная математика, ВШЭ, факультет компьютерных наук

(Осень 2014 – весна 2015)

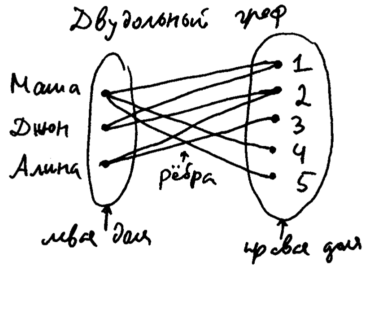
## 1 Отношения

Мы уже говорили, что в естественном языке множествам соответствуют свойства. Часто эти свойства выражаются прилагательными. Например, прилагательное «красный» соответствует множеству объектов, которые мы считаем красными. Лингвисты говорят о «предикатах» как свойствах, которыми может обладать (или не обладать) субъект — математики говорят о соответствующих множествах, которые могут содержать (или не содержать) этого самого субъекта (он может быть их элементом или не быть). Как мы видели, этот перевод может быть продолжен — пересечению множеств соответствует союз «и», объединению — союз «или» (понимаемый в неисключительном смысле).

Но сейчас нас интересует другая конструкция языка и её формализация: когда после контрольной говорят, что «Маша решила задачу 4», это означает, что Маша и задача 4 находятся в некотором *отношении*, в котором они могут находиться или не находиться. Математики видят в этой фразе два множества $G$ (все студенты группы, где была контрольная) и $P$ (все задачи, предлагавшиеся на контрольной), и — как они говорят — «бинарное отношение» между множествами, которое указывает, кто чего решил. Это отношение можно представлять себе разными способами. Можно в списке группы у каждой фамилии написать номера решённых задач. Можно (хотя и менее привычно) у каждой задачи написать студентов, которые её решили. Можно составить таблицу наподобие такой:

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| Маша | + | | + | + | + |
| Джон | + | + | | | |
| Алина | | + | + | | |

А можно нарисовать картинку, называемую *двудольным графом*: слева (в левой *доле*) точками (*вершинами*) изобразить студентов, в правой доле вершинами считать задачи, и провести линии (*рёбра*), соответствующие успеху при решении задач:



**Задача 1.** На этой картинке есть ошибка — точнее, есть несоответствие между картинкой и таблицей с плюсами выше. Найдите его. Как надо исправить таблицу или картинку, чтобы его устранить?

Во всех случаях мы представляем (разными способами) одну и ту же информацию (считаем, что несоответствие, о котором шла речь в задаче, исправлено). Различие в способах представления становится важным, если нас интересует удобство хранения и обработки этой информации — соответствующий раздел в программировании изучает различные «структуры данных» для представления множеств, отношений и других абстрактных объектов.

## 2 Отношения с точки зрения математики

С точки зрения математики, наше отношение задаётся (как мы уже говорили) множествами $G$, $P$ и некоторым подмножеством *декартова произведения* $G \times P$ множеств $G$ и $P$. Надо только объяснить, что за множество мы называем декартовым произведением. В нашем случае оно состоит из 15 элементов. В него входят следующие *упорядоченные пары*:

$$\begin{gathered}\langle \text{Маша}, 1\rangle, \langle \text{Маша}, 2\rangle, \langle \text{Маша}, 3\rangle, \langle \text{Маша}, 4\rangle, \langle \text{Маша}, 5\rangle,\\ \langle \text{Джон}, 1\rangle, \langle \text{Джон}, 2\rangle, \langle \text{Джон}, 3\rangle, \langle \text{Джон}, 4\rangle, \langle \text{Джон}, 5\rangle,\\ \langle \text{Алина}, 1\rangle, \langle \text{Алина}, 2\rangle, \langle \text{Алина}, 3\rangle, \langle \text{Алина}, 4\rangle, \langle \text{Алина}, 5\rangle.\end{gathered}$$

Мы перечислили их в этом порядке, но порядок не играет роли — множество $G \times P$ состоит из этих 15 элементов. Если вспомнить нашу таблицу, то элементы множества $G \times P$ соответствуют клеточкам таблицы: в каждой клеточке понятно, о каком студенте и о какой задаче идёт речь. Отношение, задаваемое нашей таблицей, состоит из 8 элементов, соответствующих плюсам в таблице:

$$\langle \text{Маша}, 1\rangle, \langle \text{Маша}, 3\rangle, \langle \text{Маша}, 4\rangle, \langle \text{Маша}, 5\rangle, \langle \text{Джон}, 1\rangle, \langle \text{Джон}, 2\rangle, \langle \text{Алина}, 2\rangle, \langle \text{Алина}, 3\rangle.$$

В предыдущем абзаце много терминов, о которых стоит поговорить подробнее. Что такое «упорядоченная пара», например? Упорядоченная пара $\langle a, b\rangle$ составляется из объектов $a$ и $b$. Слово «упорядоченная» означает, что мы различаем пару $\langle a, b\rangle$ и пару $\langle b, a\rangle$. В нашем примере это было не так важно, так как студентов трудно перепутать с задачами, но в принципе множества $G$ и $P$ могут иметь общие элементы, и тогда это существенно. Другими словами, мы считаем, что

$$\langle a, b\rangle = \langle a', b'\rangle,$$

если $a = a'$ и $b = b'$. Это отличает упорядоченные пары от неупорядоченных: для любых двух объектов $a$, $b$ можно определить множество $\{a, b\}$, состоящее из этих двух элементов (если $a = b$, в нём будет только один элемент). Но в этом случае $\{a, b\} = \{b, a\}$, поэтому такое множество называют *неупорядоченной парой*.

**Задача 2.** Польский математик Куратовский в первой половине XX века придумал, как определить формально упорядоченные пары: он предложил считать, что

$$\langle a, b\rangle = \{\{a\}, \{a, b\}\}.$$

Проверьте (аккуратно разобрав случаи), что при таком определении равенство $\langle a, b\rangle = \langle a', b'\rangle$ возможно, лишь если $a = a'$ и $b = b'$.

Можно ещё объяснить, откуда берутся слова «декартово» и «произведение» в названии для множества $A\times B$, состоящего из всех упорядоченных пар вида $\langle a, b\rangle$ при всевозможных $a \in A$, $b \in B$. Это называют произведением, потому что в арифметике произведение чисел возникает как раз при подсчёте пар. Если множество $A$ содержит $m$ элементов, а множество $B$ содержит $n$ элементов, то с каждым из $m$ элементов множества $A$ можно составить $n$ пар, спаривая его с каждым из $n$ элементов множества $B$. Всего получается $m \times n$ элементов.

Слово «декартово» происходит от фамилии французского математика и философа Рене Декарта.[1] Он придумал, что на плоскости можно ввести систему «декартовых координат», проведя две перпендикулярные ориентированные прямые, оси координат. После этого каждая точка плоскости задаётся упорядоченной парой чисел $\langle x, y\rangle$, своих координат по оси абсцисс и оси ординат. Заметим, что пара именно упорядоченная: точки $\langle 1, 2\rangle$ и $\langle 2, 1\rangle$ — это совсем разные точки. Можно сказать, что декартовы координаты устанавливают взаимно однозначное соответствие между плоскостью (ими снабжённой) и декартовым произведением $\mathbb{R} \times \mathbb{R}$ множества действительных чисел на себя.

После всех этих разговоров мы можем кратко сказать: *бинарным отношением на множествах $A$ и $B$* называется любое подмножество $R$ декартова произведения $A \times B$. Мы говорим, что элементы $a \in A, b \in B$ находятся в отношении $R$, если $(x, y) \in R$. Есть несколько вариантов обозначения для этого: пишут, например $aRb$ или $R(a, b)$. Скажем, в нашем примере можно ввести имя *Решил* для рассмотренного отношения, и сказать, что *Решил*(Маша, 3) истинно, а *Решил*(Джон, 4) ложно.

Слово «бинарное» подчёркивает, что речь идёт об отношении между элементами двух множеств. Наряду с бинарными отношениями мы можем рассмотреть отношения и любой другой «валентности», или «арности». Назовём *$k$-арным отношением на множествах* $A_1, \ldots, A_k$ любое подмножество множества $A_1 \times A_2 \times \ldots \times A_k$. При $k = 1$ говорят об *унарных* отношениях — это уже знакомые нам свойства, при $k = 3$ получаются *тернарные*. Одно и то же слово русского языка может использоваться для обозначения отношений разной валентности. Скажем, «Маша бьёт Джона» сообщает об элементе бинарного отношения, а в более подробном сообщении «Маша бьёт Джона веником» то же самое слово «бьёт» описывает тернарное отношении (как сказали бы лингвисты, «имеет три актанта»). Последнее сообщение можно было бы записать как *Бьёт*(Маша, Джон, веник).

Если множества $A$ и $B$, на которых определено бинарное отношение, совпадают, то говорят просто о бинарном отношении на множестве $A$. Аналогично определяются $k$-арные отношения. Например, можно рассмотреть тернарное отношение «быть суммой» на множестве целых чисел: оно состоит из троек $\langle a, b, c\rangle$, для которых $a = b + c$.[2]

В современных информационных системах используют так называемые «реляционные базы данных» — возможно, многие слышали о языке запросов SQL, который используют

[1]Как философ он попал в «Маскарад» к Лермонтову: один из игроков, предвосхищая современных экономистов, говорит Арбенину: «Что ни толкуй Волтер или Декарт — // Мир для меня — колода карт,// Жизнь — банк; рок мечет, я играю,// И правила игры я к людям применяю.» Декарт-философ также известен латинским изречением Cogito ergo sum (мыслю, следовательно, существую).

[2]Тут возникает вопрос, как определять тройки. Мы хотим, чтобы $\langle a, b, c\rangle = \langle a', b', c'\rangle$ означало, что $a = a'$, $b = b'$ и $c = c'$. Этого можно добиться, положив $\langle a, b, c\rangle = \langle\langle a, b\rangle, c\rangle$ или $\langle a, b, c\rangle = \langle a, \langle b, c\rangle\rangle$; оба варианта годятся, так что можно выбрать какой-то один. Множество всех троек $\langle a, b, c\rangle$ при $a \in A$, $b \in B$, $c \in C$ называется *декартовым произведением* трёх множеств $A, B, C$ и обозначается $A \times B \times C$.

для обращения к таким базам. Слово «реляционные» (relational) происходит от английского слова “relation”, означающего «отношение». В реляционной базе данных информация (о мире) хранится в виде отношений: скажем, понятие «место жительства» рассматривается как отношение между множеством людей и множеством жилых помещений, и т. д. Это оказалось достаточно удобным и универсальным подходом к представлению различной информации.

**Задача 3.** Представим себе, что проверяющие контрольную ставят за каждую задачу один из знаков $0, -, \mp, \pm, +$. Как можно представить результаты контрольной в виде тернарного отношения?

## 3 Свойства бинарных отношений

Мы будем в первую очередь говорить о бинарных отношениях. Унарные отношения — это просто множества, мы их уже обсуждали, а бинарные отношения сложнее, в них уже есть какая-то внутренняя структура, и тут есть о чём поговорить.

Бинарное отношение $R$ на множестве $X$ называют *симметричным*, если из $R(x, y)$ следует $R(y, x)$. Многие слова русского языка такую симметрию подразумевают: скажем, отношение «$x$ — родственник $y$» на множестве всех людей обычно считают симметричным (хотя, конечно, может случиться и так, что А считает Б своим родственником, а Б и знать А не желает). Примерно то же самое можно сказать об отношении «$x$ знаком с $y$», или отношении «$x$ и $y$ — соседи». Другие отношения, скажем «$x$ посылал $y$ письмо» или «$x$ — мать $y$», не симметричны. В последнем примере $R(x, y)$ вообще несовместно с $R(y, x)$.

**Задача 4.** Докажите, что если отношение знакомства между людьми симметрично, то количество людей, имеющих нечётное число знакомых, чётно.

**Задача 5.** Является ли отношение «$x$ — брат $y$» (в самом простом, генеалогическом смысле) симметричным?

Другое свойство бинарных отношений на некотором множестве: отношение $R$ *транзитивно*, если из $R(x, y)$ и $R(y, z)$ следует $R(x, z)$. Например, отношение «быть предком» на множестве всех людей транзитивно: если А — предок Б, а Б — предок В, то А — предок В. А отношение «быть отцом» не транзитивно. Классическая фраза «вассал моего вассала не мой вассал» (не будем вдаваться в уточнение того, что это значит и в каких странах и когда так было) теперь может быть сформулирована научно: «отношение вассалитета не обязано быть транзитивным».

**Задача 6.** Будет ли отношение $x$ знаком с $y$ на множестве людей транзитивным?

Много транзитивных отношений возникает в процессе сравнений: естественно считать, что отношения «$x$ выше $y$», «$x$ сильнее $y$», «$x$ красивее $y$» и т. п. подразумевают транзитивность — её отсутствие воспринимается как парадокс (как в игре камень–ножницы–бумага, когда камень сильнее ножниц, ножницы сильнее бумаги, а бумага сильнее камня).

**Задача 7.** Является ли отношение «быть делителем» на множестве положительных целых чисел симметричным? транзитивным? Тот же вопрос для отношения «быть взаимно простым» (не иметь общих делителей, кроме 1) на том же множестве.

**Задача 8.** Будем говорить, что одна прямоугольная коробка «меньше» другой, если одно из трёх измерений первой коробки меньше одного из трёх измерений второй (если их можно поставить на пол так, чтобы первая коробка была ниже второй). Будет ли это отношение транзитивным?

**Задача 9.** В ходе турнира каждая команда сыграла с каждой по одному разу, причём ничьих не было и каждая команда хоть кому-то да проиграла. Докажите, что найдутся три команды А, Б, В, нарушившие транзитивность: А выиграла у Б, Б выиграла у В, а В выиграла у А.

**Задача 10.** Педанты заметят, что в предыдущей задаче мы неявно предполагаем, что в турнире участвовало конечное число команд. Почему это предположение существенно?

Будет ли отношение «$x$ — родственник $y$» транзитивным? Хочется сказать, что да и что родственник твоего родственника — твой родственник. С другой стороны, есть опасность таким образом распространить родство на всех ныне живущих людей (даже если и не считать, что все они потомки Адама — и без этого родственных связей довольно много). Это — типичная ситуация «парадокса кучи» — добавление одной песчинки не может превратить в кучу то, что раньше кучей не было, но тем не менее кучи бывают.

Третье свойство бинарного отношения, *рефлексивность*, означает, что $R(x,x)$ для любого $x$. (Слово «рефлексия» означает размышления о самом себе.) Интересно, что наша языковая интуиция не всегда отчётлива в этом месте: будет ли, например, отношение «$x$ знаком с $y$ рефлексивным»? Знаком ли человек с самим собой? Это уже вопрос с философским оттенком: совет «Познай самого себя» ничего не говорит о том, была ли эта попытка познания успешной. Скорее, видимо, нет — когда человек говорит, что у него есть трое знакомых, вряд ли он включает в них себя. Является ли человек своим собственным однофамильцем? своим собственным родственником? своим собственным соседом?

В математике, конечно, такая неопределённость недопустима, и говоря о бинарном отношении, мы должны заранее решить, что мы думаем по поводу отношения объекта с самим собой. Скажем, отношение $x \le y$ будет рефлексивным (поскольку $x \le x$ для любого $x$), а отношение $x < y$ не будет.

Заметим, что если мы хотим считать отношение «быть родственником» симметричным и транзитивным, то придётся считать его рефлексивным: если А родственник Б, то по симметрии Б будет родственником А, и по транзитивности (ведь мы же не говорили, что все три элемента разные!) получаем, что А будет родственником самому себе.

Повторим, что все эти свойства (транзитивность, рефлексивность, симметричность) не имеют смысла для бинарных отношений между элементами $A$ и $B$ при $A \ne B$.

## 4 Отношения эквивалентности

Отношение на некотором множестве, которое одновременно рефлексивно, симметрично и транзитивно, называют *отношением эквивалентности*. Например, отношение «быть однофамильцем» (иметь одинаковую фамилию; мы сейчас считаем каждого человека своим собственным однофамильцем) или «быть одноклассником» (с той же оговоркой).

Вообще, если множество $X$ разбито на непересекающиеся подмножества, то отношение «попасть в одно подмножество» будет отношением эквивалентности. Немного другой пример: пусть для каждого элемента множества $X$ определена какая-то характеристика, скажем, «цвет» из какого-то заранее выбранного множества цветов. Тогда отношение «быть одного цвета» является отношением эквивалентности.

Оказывается, что это общая ситуация:

**Теорема 1.** *Любое отношение $R$, являющееся отношением эквивалентности на множестве $A$, делит $A$ на классы эквивалентности — непересекающиеся подмножества множества $X$, при этом любые два элемента одного класса находятся в отношении $R$, а любые два элемента разных классов не находятся в отношении $R$.*

*Доказательство.* Пожалуй, тут сложнее понять, что тут вообще надо доказывать (и почему это не очевидно), чем доказать — но в качестве образца проведём подробно формальное рассуждение.

Для каждого $x \in A$ рассмотрим множество тех $y$, для которых верно $R(x, y)$. Обозначим его через $[x]$. Его можно было бы назвать «классом эквивалентности элемента $x$» — собственно говоря, так его и называют, но само по себе это название не гарантирует разбиения на классы, это ещё надо доказывать. А именно, надо доказать, что

- объединение всех множеств вида $[x]$ совпадает с множеством $A$;
- два множества $[x]$ и $[y]$ либо не пересекаются, либо совпадают;
- наконец, надо ещё доказать, что $[x] = [y]$ в том и только том случае, когда $R(x, y)$, то есть $R$ совпадает с отношением «принадлежать одному классу».

Как это доказать?

(1) В силу рефлексивности множество $[x]$ содержит $x$ в качестве своего элемента: $x \in [x]$, поскольку $R(x, x)$. Отсюда следует, что объединение всех этих множеств совпадает с $A$. (Выйти за пределы $A$ они не могут, так как мы рассматриваем отношение на множестве $A$ и элементы множества $A$.)

(2) Пусть для двух элементов $x, y \in A$ их классы $[x]$ и $[y]$ пересеклись. Это означает, что есть такой $z \in A$, что $R(x, z)$ и $R(y, z)$. Симметричность даёт $R(z, y)$, после чего мы применяем транзитивность к $R(x, z)$ и $R(z, y)$ и заключаем, что $R(x, y)$. Выведем отсюда, что $[x] = [y]$. В самом деле, если произвольный элемент $t$ принадлежит $[y]$, то $R(y, t)$. Вспоминая, что $R(x, y)$и применяя транзитивность, получаем $R(x, t)$, то есть $t \in [x]$. Мы доказали, таким образом, что $[y] \subset [x]$. Аналогично доказывется, что $[x] \subset [y]$, так что $[x] = [y]$.

(3) Если для каких-то $x, y$ верно $R(x, y)$, то $x$ и $y$ оба лежат в одном классе, а именно, в $[x]$. Обратно, если $x$ и $y$ лежат в каком-то $[z]$, то по определению имеем $R(z, x)$ и $R(z, y)$, симметричность даёт $R(x, z)$ и после этого транзитивность даёт $R(x, y)$. □

Интересные вещи, связанные с этой теоремой, рассказывают биологи. Попытаемся разделить живые существа на виды, объединяя в один вид тех, которые скрещиваются. (Конечно, речь идёт о популяциях, а не об отдельных особях.) Возможность такого деления предполагает, что это отношение транзитивно. Однако так бывает не всегда. Рассказывают (см., например, статью про Ring species в википедии; русский вариант называется «Кольцевые виды»), что когда птицы живут вокруг некоторого препятствия (скажем, пустыни), может оказаться так, что они образуют незамкнутое кольцо: всюду, кроме точки разрыва, соседи скрещиваются, но встречающиеся с разных сторон точки разрыва птицы уже не скрещиваются, хотя живут рядом. Русская статья пишет, что «такие примеры, обладающие промежуточными характеристиками между видом и более низкими таксономическими рангами, противоречат классическому представлению о дискретности видов», а английская статья не стесняется назвать вещи своими именами: «the issue is that interfertility (ability to interbreed) is not a transitive relation — if A can breed with B, and B can breed with C, it does not follow that A can breed with C — and thus does not define an equivalence relation. A ring species is a species that exhibits a counterexample to transitivity» (R. Brown, "Same species" vs. "Interfertile": concise wording can avoid confusion when discussing evolution).

В математике отношение эквивалентности используется, например, при формальном определении рациональных чисел. Допустим, мы уже определили целые числа. Рассмотрим дроби, то есть упорядоченные пары $\langle m, n\rangle$, где $m$ и $n$ — целые числа и $n > 0$. Первый элемент пары будем называть числителем, второй — знаменателем, и записывать пару для наглядности как $\frac{m}{n}$ (не придавая пока разделяющей черте никакого смысла — просто решили так записывать пару, и всё). Определим отношение на множестве пар, считая, что $\frac{m}{n}$ находится в этом отношении с $\frac{u}{v}$, если произведения $mv$ и $nu$ равны. (Хочется сказать: если частные $m/n$ и $u/v$ равны, но мы пока не определили рациональных чисел и частного.) Обозначение для этого отношения: $\frac{m}{n} \sim \frac{u}{v}$.

Проверим, что это отношение эквивалентности. В самом деле, $\frac{m}{n} \sim \frac{m}{n}$ (рефлексивность), потому что $mn = nm$. Симметричность тоже сразу следует из определения. А вот транзитивность немного сложнее: если $\frac{m}{n} \sim \frac{u}{v}$ и $\frac{u}{v} \sim \frac{k}{l}$, то по определению $mv = nu$ и $ul = vk$. Домножая равенства на $l$ и $n$ и применяя транзитивность для обычного равенства чисел, получаем $mvl = nul = nvk$. Теперь надо воспользоваться таким свойством целых чисел: на ненулевое число (в нашем случае $v$) можно сокращать. Получится $ml = nk$, то есть $\frac{m}{n} \sim \frac{k}{l}$. Транзитивность проверена.

Имея отношение эквивалентности, можно рассмотреть соответствующие классы эквивалентности и назвать их рациональными числами. Класс дроби $\frac{m}{n}$ после этого можно назвать рациональным числом, получающимся при делении $m$ на $n$. Например при делении 2 на 3 и при делении 4 на 6 получается одно и то же рациональное число, множество всех пар $\frac{m}{n}$, где $2n = 3m$ (или $4n = 6m$, это то же самое).

После этого надо аккуратно (долго и занудно) определять арифметические операции над рациональными числами и доказывать их свойства. Скажем, чтобы сложить два рациональных числа, нужно выбрать их представители, скажем, $\frac{m}{n}$ и $\frac{u}{v}$, и рассмотреть рациональное число (класс эквивалентности), содержащий $\frac{mv+nu}{nv}$.

**Задача 11.** Проверьте, что это определение корректно, то есть что получившийся класс (сумма) не зависит от того, какие именно представители выбраны в двух классах-слагаемых.

## 5 Связные компоненты в неориентированных графах

Неориентированным графом называется картинка из нескольких точек (вершин), в которой некоторые пары точек соединены линиями (рёбрами). Будем считать, что между данными двумя точками может быть только одно ребро (или не быть ребра), тогда такой граф можно представлять себе как симметричное бинарное отношение $E$ на множестве вершин $V$. (Вершинам $x$, для которых $E(x, x)$, соответствуют петли на картинке, ведущие из $x$ в себя. Иногда такие рёбра запрещают, но нам сейчас это не важно.)

Имея такой граф, можно определить на множестве вершин отношение достижимости: $R(x, y)$ истинно, если из вершины $x$ можно добраться до вершины $y$, передвигаясь по рёбрам графа. Можно представлять себе вершины как города, а рёбра как дороги, тогда достижимость означать возможность проехать по этим дорогам из одного города в другой. Ясно, что отношение достижимости является отношением эквивалентности:

- чтобы попасть из вершины $x$ в неё саму, даже не нужно никуда идти (рефлексивность)
- если мы можем пройти по рёбрам графа из вершины $x$ в вершину $y$, то, пройдя по тем же рёбрам в обратном порядке, мы попадем из вершины $y$ в вершину $x$ (симметричность);
- если мы можем пройти из вершины $x$ в вершину $y$, а из вершины $y$ в вершину $z$, то можно пройти из вершины $x$ в вершину $z$: сначала по первому маршруту идём в вершину $y$, а затем по второму маршруту в вершину $z$ (транзитивность).

Следовательно, вершины графа разбиваются на классы эквивалентности относительно отношения достижимости. Эти классы эквивалентности называются *компонентами связности* графа. При этом две вершины лежат в одной компоненте тогда и только тогда, когда из одной можно дойти до другой по ребрам графа.

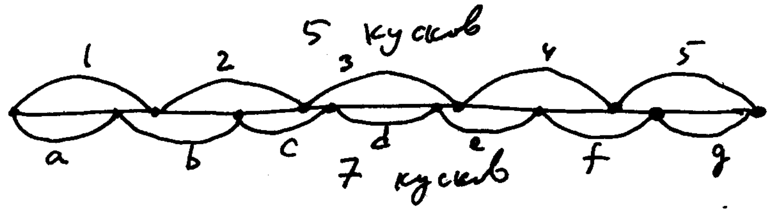
Граф называется *связным*, если в нём только одна компонента связности, то есть если из любой вершины можно пройти в любую, идя по рёбрам.

Всё это выглядит бессмысленным переливанием из пустого в порожнее, но на самом деле не так уж и бессмысленно. Например, понятие компоненты связности позволяет легко доказать такое утверждение:

**Теорема 2.** *В связном графе с $n$ вершинами не меньше $n-1$ рёбер.*

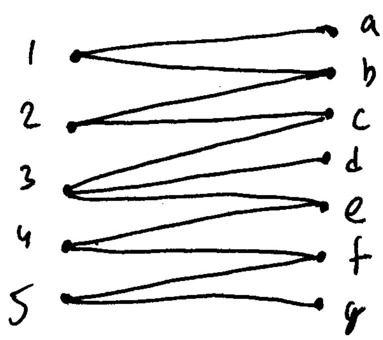
*Доказательство.* Будем добавлять рёбра по одному. Вначале нет ни одного ребра, и есть $n$ связных компонент (каждая вершина — своя компонента). Добавление одного ребра либо не меняет числа компонент (если это ребро соединяет две вершины одной компоненты), либо уменьшает это число на единицу (если ребро соединяет две вершины разных компонент, то эти компоненты сливаются в одну). В конце — когда все рёбра добавлены и получился связный граф — у нас только одна связная компонента. Значит, число связных компонент уменьшалось не меньше $n-1$ раз. □

Эта теорема в свою очередь позволяет решить такую красивую задачу. Допустим, что нам надо заранее разрезать торт на несколько кусков, готовясь к приходу гостей — так, чтобы его можно было раздать поровну $m$ людям, а также чтобы его можно было (с теми же разрезами, только перегруппировав куски) раздать поровну $n$ людям. Какое минимальное число кусков понадобится? Пусть, скажем, $m = 5$ и $n = 7$; сколько надо кусков, чтобы можно было раздать торт поровну и пяти, и семи людям? Наивный способ состоит в том, чтобы разделить торт на части по $1/35$ и потом группировать куски по 5 и по 7. Но легко понять, что это не оптимально (с точки зрения числа кусков) — представим себе торт отрезком и наметим точки разреза на 5 и на 7 равных частей. В первом случае будет 4 точки разреза, во втором 6, всего 10 точек разреза, то есть 11 кусков. Сделав все эти разрезы заранее, мы решим задачу, то есть 11 кусков достаточно. (В общем случае достаточно $m + n - 1$ кусков.)




Как доказать, что это оптимальный способ, то есть что 10 кусков недостаточно? Можно разбирать разные варианты и случаи и это установить, но есть такое рассуждение (которое легко обобщается на произвольные взаимно простые $m$ и $n$).

Нарисуем схему раздачи в виде графа. Слева изобразим 5 гостей, справа изобразим 7 гостей, а куски изобразим рёбрами, соединяющими тех, кому они попали при том и другом варианте раздачи. Получится двудольный граф, соответствующий бинарному отношению *иметь общий кусок*[3]. На картинке показан граф, изображающий ту же самую раздачу, но, разумеется, возможны и другие варианты.




Нам надо доказать, что в этом графе не менее 11 рёбер. Заметим, что в нём 12 вершин. Значит, если рёбер меньше 11, то граф будет несвязен (вот где нужна предыдущая теорема!), и куски разбиваются на несколько групп. Спросим себя, какой может быть вес кусков в одной из групп. Все эти куски в каждом из вариантов идут каким-то гостям, и больше эти гости ничего не получают (иначе эти новые куски вошли бы в ту же связную компоненту). Значит, общий вес кусков в группе должен быть кратен 1/5 торта и 1/7 торта одновременно, а это невозможно, кроме того случае, когда общий вес равен 1, то есть группа только одна. Получаем искомое противоречие.

## 6 Композиция отношений

Все знают, что тёща — это мать жены, но не все знают, как это научно сформулировать. С точки зрения математика, тут есть два отношения

$$W(x, y) = y \text{ — жена } x$$

[3] Строго говоря, это не совсем так: может случиться, что на картинке будет два ребра, соединяющих одну и ту же пару вершин, чего в графе бинарного отношения быть не может. Впрочем, это означает, что какие-то два куска в двух вариантах раздачи остаются вместе, и тогда их можно было бы объединить в один, уменьшив число кусков.

и

$$M(y, z) = z \text{ — мать } y$$

и мы применяем к ним операцию, называемую *композицией.*

Формальное определение композиции выглядит так. Пусть даны два отношения $R \subset A \times B$ и $S \subset B \times C$. Их *композицией* называется отношение $S \circ R \subseteq A \times C$, определяемое так:

$$(x, z) \in S \circ R \Leftrightarrow \text{существует такой } y \in B, \text{ что } (x, y) \in R \text{ и } (y, z) \in S.$$

В нашем примере $A, B, C$ — это одно и то же множество, а именно, множество всех людей, $M \circ W(x, z)$ как раз и означает, что $z$ — тёща $x$: определение композиции в данном случае читается как

$$\text{существует такой } y, \text{ что } W(x, y) \text{ и } M(y, z),$$

то есть что найдётся такой человек $y$, что $y$ — жена $x$ и $z$ — мать $y$. Заметим ещё, что это определение вполне имеет смысл и в странах, где разрешено иметь много жён — тогда у одного человека может быть и много тёщ.

Обратите внимание, что композиция двух отношений может быть определена только в том случае, когда у них общее множество $B$. Если вас спросят на экзамене, чему равна композиция отношения $R(x, y)$, означающего, что человек $y$ — отец человека $x$, и отношения $S(y, z)$, означающего, что число $z$ на единицу больше числа $y$, то это скорее всего «проверка на вшивость» — если экзаменуемый начинает что-то вычислять, то на этом экзамен можно заканчивать. (Хороший студент в этот момент смотрит на экзаменатора как на идиота, и удовлетворённый экзаменатор переходит к следующему вопросу.)

Можно рассмотреть и более научный пример. Пусть $A, B, C$ равны множеству действительных чисел, $R(x, y)$ означает, что $y = x^2$, а $S(y, z)$ означает, что $z = y + 1$. Тогда $S \circ R(x, z)$ означает, что найдётся $y$, для которого $y = x^2$ и $z = y + 1$, то есть что $z = x^2 + 1$.

Заметим, что для обозначения переменных можно использовать любые буквы: можно было бы сказать, например, что $R(y, z)$ означает, что $z = y^2$, а $S(x, y)$ означает, что $y = x + 1$. Это бы означало ровно то же самое: что $R$ есть множество всех пар, в которых второе число равно квадрату первого, а $S$ есть множество всех пар, в которых второе число на единицу больше первого. Но в таких обозначениях проще вычислить композицию в другом порядке $R \circ S$: она состоит из пар $(x, z)$, для которых

$$\exists y (y = x + 1) \wedge (z = y^2).$$

Мы использовали здесь стандартное обозначение $\wedge$ для «и», а также «квантор существования» $\exists y$ вместо слов «существует $y$». Так или иначе, это означает, что $z = (x + 1)^2$. Видно, что композиция может зависеть от порядка, даже если и в том, и в другом порядке она имеет смысл. Что, впрочем, и по жизни ясно: отец брата — совсем не то же, что брат отца.

**Задача 12.** Закончить предложение: отношение $R$ на множестве $A$ транзитивно тогда и только тогда, когда композиция $R \circ R \ldots$

**Задача 13.** Рассмотрим на множестве $\mathbb{R}$ бинарное отношение $R(x, y)$, означающее, что $y = x + 1$. Чему равно $R \circ R$?

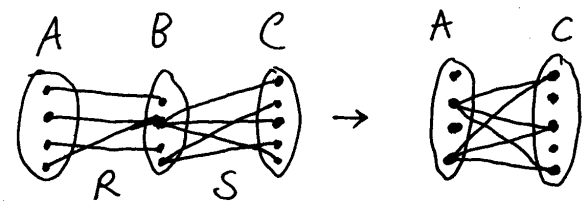
**Задача 14.** Тот же вопрос, если $R(x, y)$ означает $x + y = 1$.

**Задача 15.** Тот же вопрос, если $R(x, y)$ означает $xy = 1$.

**Задача 16.** Тот же вопрос, если $R(x, y)$ означает $xy > 1$.

По существу та же операция композиции встречается в реляционных базах данных под названием операции JOIN, применяемой к двум отношениям. Разница в обозначениях: там, говоря об отношениях, говорят не о первом или втором члене пары, а дают этим членам имена. Скажем, можно рассматривать отношение ПРОЖИВАТЬ между множеством людей и множеством помещений, и говорить, что оно имеет атрибуты ЖИЛЕЦ и ЖИЛЬЁ, а также отношение НАХОДИТЬСЯ между множеством помещений и множеством улиц, имеющее атрибуты ЖИЛЬЁ и УЛИЦА. Применяя операцию JOIN по атрибуту ЖИЛЬЁ, мы получаем отношение ПРОЖИВАТЬ-НА-УЛИЦЕ с атрибутами ЖИЛЕЦ и УЛИЦА (между множеством людей и множеством улиц). Ясно, что это та же самая композиция отношений, но в других обозначениях.

Можно описать операцию композиции и в терминах графов. Представим два отношения $R \subset A \times B$ и $S \subset B \times C$ в виде двудольных графов с общей долей $B$ (правой долей для $R$ и левой долей для $S$). Тогда их композиция будет двудольным графом с левой долей $A$ и правой долей $C$: ребро $a$–$c$ в таком графе означает, что найдётся $b$, для которого $a$ соединено с $b$ ребром, и $b$ соединено с $c$ ребром, то есть что из $a$ в $c$ можно пройти за два шага:




Для знакомых с линейной алгеброй композицию отношений можно описать ещё одним способом. Будем изображать отношение матрицей, как мы делали, только вместо плюсов будем писать положительные числа, а вместо пустых клеток — нули. Тогда композиция отношений будет изображаться произведением матриц. Понятно, почему?

## 7 Функции

Школьники знают, что функция $f$ — это когда каждому элементу $x$ из некоторого множества, *области определения* функции, поставлен в соответствие какой-то элемент $f(x)$ другого множества, *области значений*, причём только один. Для программиста функция — это алгоритм, который получает на вход аргумент некоторого типа (скажем, целое число) и возвращает результат некоторого типа (может быть, другого). Скажем, функция «возведение в квадрат», которая определена для каждого целого $x$, и ставит в соответствие этому $x$ его квадрат (ещё говорят: отображает $x$ в $x^2$), записывается так:

```
function square(x:integer): integer;
begin square:= x*x; end;
```

(Мы привели программу на паскале, потому что там используется как раз слово function,[4] но аналогичные конструкции есть и в других языках программирования.)

[4]В этом примере математики и программисты находят общий язык — но когда математик слышит, что «функция зацикливается» или (хуже того) у ней есть «побочный эффект», из-за которого $f(x)+f(x)$ может быть не равно $2f(x)$, он невольно вздрагивает.

Используя понятие бинарного отношения, можно определить понятие функции как частный случай. А именно, отношение $F \subseteq A \times B$ называется *функцией из $A$ в $B$* , если каждый элемент множества $A$ находится в отношении $F$ не более чем с одним элементом множества $B$. Другими словами: если в $F$ нет двух пар с одинаковой первой компонентой и разными вторыми. Поскольку понятие функции важное, потренируемся в искусстве переформулировок: $F$ — функция, если для любых $x \in A$ и $y_1, y_2 \in B$ с $y_1 \neq y_2$ хотя бы одна из пар $(x, y_1)$ и $(x, y_2)$ не лежит в $F$. (Понятно, почему это то же самое?)

Мы не требуем, чтобы всякий элемент $x \in A$ находился в отношении $F$ с каким-то элементом в $B$, важно только, чтобы он не находился в отношении $F$ с двумя разными элементами $B$. Так что для данного $x \in A$ может либо не быть никакого элемента в $B$, находящегося с $x$ в отношении $F$, либо быть ровно один такой элемент $y$. Во втором случае говорят, что $x$ входит в *область определения* функции $F$, а этот самый единственный элемент $y$, находящийся в отношении $F$ с $x$, называют *значением функции $F$ на $x$* и обозначают $F(x)$. Элементы $F(x)$ для всех $x$ из области определения функции $F$ образуют *множество значений* функции $F$. Другими словами, множество значений функции $F$ — это множество элементов в $B$, находящихся в отношении $F$ с некоторым элементом в $A$.

Если область определения функции совпадает с $A$, то пишут $f\colon A \to B$. Такие функции еще называют *всюду определенными*, а иногда *тотальными* (по-английски total) в отличие от общего случая *частичных* (или частично определенных, англ. partial) функций.

Ещё немного терминологии.

Функция $f\colon A \to B$ называется *инъекцией*, если её значения в различных точках различны, то есть разным элементам из $A$ ставятся в соответствие разные элементы $B$. Иначе говоря, $f$ — инъекция, если $f(x_1) = f(x_2)$ влечет $x_1 = x_2$. (Переформулировка: если $x_1 \neq x_2$ влечёт $f(x_1) \neq f(x_2)$.

**Задача 17.** Незадачливый студент перепутал определение инъекции и сказал: «если $f(x_1) \neq f(x_2)$ влечёт $x_1 \neq x_2$». Что за свойство функции он определил?

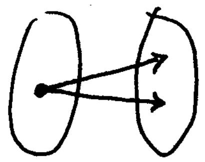
Функция $f\colon A \to B$ называется *сюръекцией*, если её область значений совпадает со всем множеством $B$, то есть если для всякого элемента $y \in B$ найдётся элемент $x \in A$, для которого $f(x) = y$.

Функция $f\colon A \to B$ называется *биекцией*, если она одновременно является и инъекцией, и сюръекцией. Другими словами, функция является биекцией, если всякому элементу из $B$ соответствует ровно один элемент из $A$.

**Задача 18.** Требование «ровно один» состоит из двух: не более одного и не менее одного. Что из этого соответствует инъективности, а что — сюръективности?

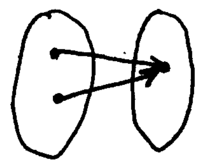
Напомним, что все эти три определения относятся к случаю, когда функция $f$ тотальна (её область определения совпадает с $A$); это подразумевается записью $f\colon A \to B$.

Что означают для отношения, представленного как двудольный граф, все эти свойства? Быть функцией означает, что из каждой вершины в левой доле выходит не более одного ребра. Те вершины слева, из которых выходит одно ребро, образуют область определения. Те вершины, куда входят рёбра, образуют область значений функции. (Мы говорим «выходят» и «входят», считая, что рёбра идут слева направо; для функций это естественно.) На первой картинке показано, чего у функции не должно быть.



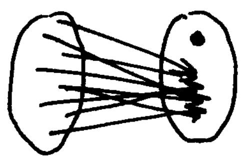
не функция

Инъективность означает, что нет двух стрелок, ведущих из разных точек в одну:



не инъекция

Сюръективность — точнее, её нарушение — на рисунке изобразить сложнее: для сюръективной функции не должно быть точек справа, в которые не ведёт ни одной стрелки.



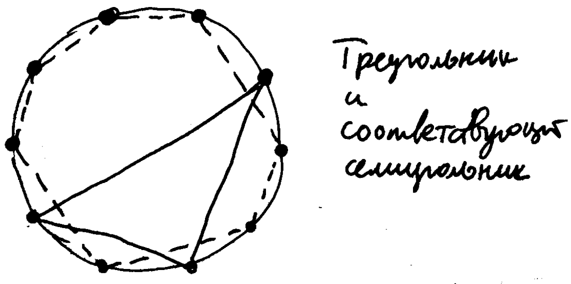
не сюръекция

В биекции каждая вершина с одной стороны соединена ровно с одной вершиной с другой стороны, поэтому их ещё называют *взаимно однозначными соответствиями*: соединённые вершины, то есть аргумент функции и её значение, *соответствуют* друг другу при этой биекции.

**Задача 19.** Пусть $A$ и $B$ — конечные множества, состоящие из $a$ и $b$ элементов. При каком условии на $a$ и $b$ существует инъекция $f\colon A \to B$? Тот же вопрос для сюръекций и биекций.

**Задача 20.** При каких условиях на действительные числа $a, b, c$ функция $f\colon \mathbb{R} \to \mathbb{R}$, задаваемая равенством $f(x) = x^3 + ax^2 + bx + c$, является инъекцией, при каких сюръекцией и при каких биекцией?

Установление взаимно однозначного соответствия (биекции) часто является удобным способом показать, что в двух множествах одинаковое количество точек. Пусть, скажем, на окружности выбрано 10 точек. Чего больше: треугольников с вершинами в этих точках или выпуклых семиугольников с вершинами в этих точках? Их поровну, так как есть взаимно однозначное соответствие: треугольнику соответствует выпуклый семиугольник, соединяющий остальные вершины




На самом деле, конечно, треугольник и семиугольник тут только для рисунка, а речь идёт о трёх- и семиэлементных подмножествах десятиэлементного множества и равенстве $\binom{10}{3} = \binom{10}{7}$.

**Задача 21.** На окружности выбрано несколько чёрных точек и одна белая. Чего больше: треугольников с чёрными вершинами или выпуклых четырёхугольников с тремя чёрными и одной белой вершиной? выпуклых многоугольников, у которых все вершины чёрные, или выпуклых многоугольников, у которых все вершины, кроме одной, чёрные, а одна белая?

Инъекции, сюръекции и биекции можно использовать для сравнения бесконечных множеств на предмет выяснения того, «где больше элементов». Но тут надо быть осторожным. Ещё Галилей (тот самый, которому приписывают фразу «а всё-таки она вертится» после допросов «компетентными органами») заметил, что точные квадраты натуральных чисел ($0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 9, \ldots$) составляют лишь небольшую часть натуральных чисел, но находятся с ними во взаимно однозначном соответствии ($x \mapsto x^2$), и что маленький отрезок в этом смысле содержит столько же точек, сколько большой.

**Задача 22.** Как установить взаимно однозначное соответствие между отрезками разной длины?

Галилей заключил, что про бесконечные множества нет смысла спрашивать, какое из них больше, и единственное, что мы можем сказать, что они бесконечны. Лишь через три с лишним века Георг Кантор понял, что это не так и что для бесконечных множеств такое сравнение тоже имеет смысл, только нужно быть аккуратным. В частности, он понял, что на отрезке больше точек, чем натуральных чисел в натуральном ряду. Мы этим ещё займёмся, но можно немного потренироваться уже сейчас.

**Задача 23.** Пусть $A$ и $B$ — два множества. Покажите, что свойства

- существует функция $f\colon A \to B$, являющая инъекцией
- существует функция $f\colon B \to A$, являющаяся сюръекцией

равносильны. (Если выполнено любое из этих свойств, то говорят, что в $A$ не больше элементов, чем в $B$.)

Раньше (и до сих пор это осталось в «школьной математике») предполагалось, что аргумент функции — это число (пара чисел для функций двух переменных, тройка чисел для функции трёх переменных) и т. д., а функции с нечисловыми аргументами назывались *отображениями* или *преобразованиями*. Сейчас слова «функция», «отображение» и «преобразование» обычно употребляются как синонимы.

Для функции $f$, аргументами и значениями которой являются действительные числа, можно нарисовать на плоскости её *график* — множество всех точек с координатами $(x, f(x))$. Собственно, в нашей терминологии, когда функция рассматривается как отношение, то есть множество пар, разница между функцией и её графиком невелика: в одном случае мы рассматриваем пары чисел, а в другом точки с такими координатами.

## 8 Подсчёты

Чтобы освоиться с терминологией, посмотрим, как разные комбинаторные задачи можно сформулировать на языке отношений и функций.

Пусть $A$ состоит из $m$ элементов, а $B$ состоит из $n$ элементов. Сколько всего бывает отношений $R \subset A \times B$? Поскольку отношения — это просто подмножества этого множества, то ответ $2^{mn}$.

Посчитаем теперь, сколько есть разных функций $f\colon A \to B$. Для каждой точки $x \in A$ (для каждого элемента $x \in A$) есть $n$ возможных значений для $f(x)$ (это значение может быть любым элементом множества $B$). Они выбираются независимо, так что всего есть $n^m$ функций. Упомянем кстати, что множество всех всюду определённых функций $A \to B$ часто обозначается как раз $B^A$.

Раньше мы считали слова длины $m$, составленные из букв $n$-элементного алфавита. Это в сущности тот же самый подсчёт, поскольку каждое такое слово есть отображение множества из $m$ позиций в алфавит.

Можно подсчитать и не всюду определённые функции из $A$ в $B$. Теперь для каждого $f(x)$ есть $n+1$ вариантов: это значение может быть не определено, а может быть любым элементом множества $B$. Соответственно получаем ответ $(n+1)^m$.

Сколько есть биекций $A \to B$? Если $m \neq n$, то нет ни одной. А если $m = n$? Будем снова выбирать значения по очереди, расположив все $n$ элементов $A$ в каком-то порядке. Для первого элемента допустимы все $n$ значений, для второго — все, кроме одного (уже использованного раньше), для третьего — $(n-2)$ и так далее, всего получается $n! = 1 \cdot 2 \cdot \ldots \cdot n$. Собственно говоря, мы повторили рассуждение о перестановках; биекции — это просто научное название для тех же перестановок.

Аналогично можно подсчитать инъекции. Если $m > n$, то их нет (большее множество не может быть инъективно отображено в меньшее). Если $m \leq n$, то аналогичное рассуждение даёт $n(n-1)(n-2) \cdot \ldots \cdot (n-m+1)$ (или $n!/m!$).

А вот для сюръекций дела немного хуже, и формула содержит суммирование. (Впрочем, и факториал тоже скрывает в себе много операций, так что принципиально разница невелика.)

**Теорема 3.** *Количество сюръекций $m$-элементного множества в $n$-элементное при $m \geq n$ равно*

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^m.$$

*(и равно нулю при $m < n$).*

Напомним, что сюръекции должны быть определены на всех $m$ элементах.

*Доказательство.* Надо воспользоваться формулой включений и исключений. Пусть $B$ состоит из $n$ элементов $b_1, \ldots, b_n$. Не-сюръекции $A \to B$ — это те функции, область значений которых не содержит одного из элементов $b_1, \ldots, b_n$, то есть объединение множеств

$$A(b_1) \cup A(b_2) \cup \ldots \cup A(b_n),$$

где через $A(b)$ обозначается множество тех функций, которые не принимают значения $b$. Легко понять, что все множества $A(b)$ имеют размер $(n-1)^m$ (мы просто выбросили одно значение). Более того, столь же легко посчитать размер их пересечений: если $b \neq b'$, то $A(b) \cap A(b')$ — это функции, не принимающие значений $b$ и $b'$, их будет $(n-2)^m$. Остаётся воспользоваться формулой включений и исключений: из всех функций ($n^m$) надо вычесть $n$ множеств вида $A(b_i)$, то есть $n(n-1)^m$, затем посокрушаться, что мы вычли лишнее и вернуть обратно $\binom{n}{2}$ их попарных пересечений, всего $\binom{n}{2}(n-2)^m$, затем снова вычесть тройные пересечения, которых $\binom{n}{3}$ и каждое из которых имеет размер $(n-3)^m$, и так далее. $\square$

С точки зрения программирования эта формула даёт быстрый — по сравнению с перебором всех сюръекций — алгоритм нахождения их количества.

Можно сразу же заметить, что подсчитанное нами число сюръекций делится на $n!$, поскольку сюръекцию можно строить в два шага: сначала разбить $m$ элементов на $n$ непустых групп, решив отнести в одну группу те элементы, у которых одинаковый образ, а затем решить, как соотносятся эти группы с элементами $B$ (выбрав одну из $n!$ биекций). Количество разбиений $m$ элементов на $n$ непустых группы ($=$ количество отношений эквивалентности на $m$-элементном множестве, имеющих $n$ классов эквивалентности) называется иногда *числом Стирлинга второго рода* — в честь того же Стирлинга, что и приближённая формула $n! \approx \sqrt{2\pi n}(n/e)^n$. Оно обозначается $S(m,n)$ или $\left\{ {m \atop n} \right\}$ и вычисляется по той же формуле, только надо поделить на $n!$ в конце.

## 9 Композиции функций

Мы уже определили композицию для произвольных отношений. Частным случаем этого определения является композиция для функций, нужно только доказать, что *композиция двух функций является функцией.*

В самом деле, пусть $F \subset A \times B$ и $G \subset B \times C$ – функции. Рассмотрим отношение $G \circ F \subset A \times C$. Чтобы проверить, что это функция, достаточно убедиться, что никакие две пары $(x, z_1)$ и $(x, z_2)$ с $z_1 \neq z_2$ не лежат одновременно в $G \circ F$. Предположим противное: $(x, z_1), (x, z_2) \in G \circ F$. По определению композиции это означает, что существуют $y_1, y_2 \in B$, для которых $(x, y_1), (x, y_2) \in F$ и $(y_1, z_1), (y_2, z_2) \in G$. Если $y_1 \neq y_2$, получаем противоречие с тем, что $F$ — функция. Если $y_1 = y_2$, получаем противоречие с тем, что $G$ — функция.

Говоря по-простому, если в двудольном графе, изображающем отношение $F$, нет двух стрелок слева направо, выходящих из одной точки, и то же самое верно для графа, изображающего $G$, то при последовательном движении слева направо у нас ни в какой момент нет выбора и мы можем прийти только в одну точку (если вообще можем).

Можно и прямо определить композицию функций, не вспоминая про отношения. Если $F$ есть функция из $A$ в $B$, а $G$ есть функция из $B$ в $C$, то $G \circ F(x)$ определена на тех $x$ из области определения $F$, для которых $F(x)$ принадлежит области определения $G$, и равна $G(F(x))$.

Обратите внимание, что в записи $G \circ F$ мы сначала пишем ту функцию, которая применяется второй — просто потому, что такой же порядок в записи $G(F(x))$. Если бы мы обозначали значение функции $F$ на $x$ не $F(x)$, а $xF$ или $(x)F$ (чему ничего не препятствует, кроме традиции), то и в обозначении для композиции было бы логично писать $F$ и $G$ в другом порядке.

**Задача 24.** Какое преобразование плоскости является композицией двух осевых симметрий? (Тут есть два случая: когда оси симметрий пересекаются и когда они параллельны.)

**Задача 25.** Какое преобразование является композицией двух центральных симметрий?

**Задача 26.** Какое преобразование является композицией двух поворотов вокруг разных точек, если повороты на один и тот же угол, но в разные стороны (один по часовой стрелке, другой против)?

**Задача 27.** Докажите, что любое движение плоскости (преобразование, сохраняющее расстояния) является композицией двух или трёх осевых симметрий.

С точки зрения программиста композицию можно описать так:

```
function GoF(a:A):C;
  var b:B;
begin b:=F(a); GoF:=G(b); end;
```

Здесь $A, B, C$ задают типы соответствующих переменных; мы для наглядности упомянули переменную типа $B$, но можно было бы просто написать

```
function GoF(a:A):C;
begin GoF:=G(F(a)); end;
```

Композиция отношений (и, в частности, функций) обладает свойством *ассоциативности*

$$(R \circ S) \circ T = R \circ (S \circ T).$$

Здесь мы предполагаем, что множества, для которых определены отношения, выбраны согласованно, то есть $R \subset A \times B$, $S \subset B \times C$ и $T \subset C \times D$ (иначе композиции нельзя определить).

Это проще понять, чем объяснить: обе части равенства задают отношение $M$, для которого $M(a, d)$ равносильно тому, что найдутся такие $b \in B$ и $c \in C$, что одновременно $R(a, b)$, $S(b, c)$ и $T(c, d)$:

$$M(a, d) \Leftrightarrow (\exists\, b \in B)(\exists\, c \in C)[R(a, b) \wedge S(b, c) \wedge T(c, d)].$$

(Композиция заменяет два шага по рёбрам графов на один; теперь у нас три графа, и всё равно, в каком порядке их склеивать.)

**Задача 28.** Дробно-линейной функцией называют функцию вида $f(x) = (ax + b)(cx + d)$, где $a, b, c, d$ — некоторые вещественные числа (константы). Покажите, что композиция двух дробно-линейных функций почти дробно-линейна (и объясните, почему «почти»).

Знающие линейную алгебру могут заметить, что коэффициенты композиции дробно-линейных функций вычисляются так же, как при умножении матриц $2 \times 2$ (и объяснить, почему).

Тождественной функцией на множестве $A$ называется функция $\mathrm{id}_A\colon A \to A$, которая отображает всякий элемент $x \in A$ в себя: $\mathrm{id}_A(x) = x$. При композиции тождественные функции ведут себя, как единица при умножеии: для любой функции $f\colon A \to B$ выполнены равенства

$$\mathrm{id}_B \circ f = f \circ \mathrm{id}_A = f.$$

(Обратите внимание, что здесь две тождественные функции — одна на $A$, другая на $B$, иначе композицию нельзя определить.)

Если функция $f\colon A \to B$ является биекцией (взаимно однозначным соответствием), то можно определить обратную функцию $f^{-1}$: если $f$ отображает $x$ в $y$, то обратная функция $f^{-1}$ отображает $y$ в $x$. Инъективность $f$ гарантирует, что это действительно функция, а сюръективность $f$ гарантирует, что эта функция определена на всём $B$.

Обозначение $f^{-1}$ для обратной функции не случайно: мы сравнили композицию с умножением, а тождественную функцию с единицей. Продолжая эту линию, можно заметить, что для биекции $f\colon A \to B$ выполнены равенства

$$f^{-1} \circ f = \mathrm{id}_A \text{ и } f \circ f^{-1} = \mathrm{id}_B\,.$$

**Задача 29.** Покажите, что если для функций $f\colon A \to B$ и $g\colon B \to A$ выполнены два равенства $g \circ f = \mathrm{id}_A$ и $f \circ g = \mathrm{id}_B$, то функция $f$ является биекцией и $g$ обратна к $f$.

**Задача 30.** Иногда эти два требования разделяют и говорят, что $g\colon B \to A$ является *левой обратной* (сооответственно *правой обратной*) к $f$, если $g \circ f = \mathrm{id}_A$ (соответственно $f \circ g = \mathrm{id}_B$).

- Приведите примеры, когда левая обратная не является правой обратной и когда правая обратная не является левой.
- Может ли такое случиться для конечных множеств?
- Может ли быть так, что у одной функции есть и левая, и правая обратные, но они различны?
- Для каких функций существует левая обратная?
- Для каких функций существует правая обратная?

Заметим, что определение обратной функции симметрично: если $g$ обратна к $f$, то и $f$ обратна к $g$.

Если функция $f$ отображает множество $A$ в себя, то можно рассмотреть её композицию с собой, получится функция $f \circ f$, которую обозначают ещё $f^2$. Надо только не путать с обычным возведением в квадрат, поскольку $\sin^2$ может обозначать и функцию $x \mapsto \sin(\sin(x))$, и функцию $(\sin x)^2$. Аналогично определяется и $f^3(x) = f(f(f(x)))$, и вообще $f^k(x)$, называемая также *$k$-й итерацией* функции $f$.

**Задача 31.** Рассмотрим функцию $f\colon [0,1] \to [0,1]$, заданную формулой $f(x) = 4x(1 - x)$. (Коэффициент подобран так, чтобы областью значений был как раз отрезок $[0,1]$.) Сколько решений имеют уравнения $f(x) = x$? $f(f(x)) = x$? $f^n(x) = x$? (В последнем случае мы имеем в виду композицию $n$ копий функции $f$, а не возведение числа в степень $n$.)

**Задача 32.** Докажите, что для любой функции $f\colon A \to A$, отображающей конечное множество $A$ в себя, найдутся различные целые положительные $m, n$, при которых $f^m$ и $f^n$ совпадают.

**Задача 33.** Докажите, что для любой биекции $f\colon A \to A$ конечного множества $A$ в себя существует целое положительное $n$, при котором $f^n = \mathrm{id}_A$.

Биекции конечного множества называют перестановками этого множества, а минимальное $n$ с указанным в задаче свойством называют *порядком* перестановки.

**Задача 34.** Покажите, что порядок любой перестановки $n$-элементного множества делит нацело число $n!$.

**Задача 35.** Циклом $(a_1 a_2 \dots a_n)$ называется перестановка (биекция на конечном множестве), при котором элемент $a_1$ переходит в $a_2$, в свою очередь $a_2$ переходит в $a_3$ и так далее до $a_n$, которое переходит в $a_1$. (При $n = 2$ получается обмен двух элементов, или, как говорят, *транспозиция*; при $n = 1$ можно считать, что получится тождественная перестановка.) Покажите, что всякую перестановку можно представить как композицию нескольких циклов, не содержащих общих элементов.

Композицию перестановок называют также их *произведением* и говорят о *группе перестановок*. Группу перестановок $n$-элементного множества называют также *симметрической группой* и обозначают $S_n$.

**Задача 36.** Покажите, что каждую перестановку можно представить в виде произведения некоторого числа транспозиций, причём чётность этого числа будет одинаковой во всех представлениях. (Скажем, любое разложение тождественной перестановки в произведение транспозиций содержит чётное число транспозиций.)

**Задача 37.** Мы уже определили $f^n$ при целом $n \geq 2$, а также $f^{-1}$ для биекций. Как надо определить $f^0$, $f^1$ и отрицательные степени (для биекций), чтобы выполнялось равенство

$$f^{m+n} = f^m \circ f^n$$

(при любых целых $m$ и $n$)?

## 10 Теорема Кантора–Бернштейна

В заключение мы приведем доказательство теоремы, которую обычно называют *теоремой Кантора–Бернштейна*, хотя исторически это не вполне точно: первые её доказательства были опубликованы Шрёдером (1896) и Бернштейном (1897). Обычно ее формулируют в терминах мощности множеств, позже мы увидим, что такая стандартная формулировка непосредственно вытекает из следующего утверждения.

**Теорема 4.** *Если для множеств $A$ и $B$ существует инъекция из $A$ в $B$ и инъекция из $B$ в $A$, то существует и биекция между $A$ и $B$.*

*Доказательство.* Пусть $f\colon A \to B$ и $g\colon B \to A$ – инъекции. Рассмотрим (возможно, бесконечный) ориентированный граф с вершинами $A \cup B$ (для простоты обозначений предположим, что $A$ и $B$ не пересекаются). Для точек $x \in A$ и $y \in B$ мы проводим из $x$ в $y$, если $f(x) = y$, и ребро из $y$ в $x$, если $g(y) = x$. Если нарисовать множество $A$ слева, а множество $B$ справа, то можно сказать, что мы проводим рёбра слева направо согласно функции $f$ и справа налево согласно функции $g$.

По построению из каждой точки выходит ровно одно ребро. А сколько рёбер входит? Поскольку функции инъективны, то не больше одного (но может не входить не одного).

Разобьем граф на компоненты связности (забыв для этого об ориентации рёбер) и рассмотрим каждую компоненту отдельно. Как устроены эти компоненты? Есть три возможности. Связная компонента может быть

- циклом из стрелок;
- бесконечной цепочкой стрелок, начинающейся в некоторой вершине (в которую ничего не входит);
- бесконечной в обе стороны цепочкой стрелок.

В самом деле, вперёд всегда можно идти по единственной стрелке, а назад либо можно пойти единственным образом, либо нельзя пойти вовсе. Если, идя вперёд, мы дважды попадём в одну вершину, то образуется цикл (и это возможно, лишь если мы вернёмся в начальную вершину). Если нет, то образуется бесконечная цепочка вперёд; её можно однозначно продолжать назад, при этом либо мы упрёмся в вершину, где назад не пройти, либо получим двустороннюю цепочку.

**Задача 38.** Проведите это рассуждение более подробно.

Это верно для любого ориентированного графа, в котором из каждой вершины выходит ровно одна стрелка и в каждую вершину входит не больше одной стрелки. В нашем конкретном случае есть дополнительная структура: вершины бывают левые и правые (из $A$ и из $B$). Они чередуются, поэтому цикл может быть только чётной длины и содержит поровну вершин из $A$ и из $B$. Любое из отображений $f$ и $g$ может быть использовано, чтобы построить биекцию между $A$- и $B$-вершинами цикла (так что есть два варианта биекции). То же самое верно для бесконечной в обе стороны цепочки (два варианта). Если же цепочка бесконечна только в одну сторону, то для построения биекции годится только одно из отображений. Скажем, если она начинается с элемента $a \in A$, то годится только функция $f$ (при которой $a$ соответствует $f(a)$, затем $g(f(a))$ соответствует $f(g(f(a)))$ и так далее). Но в любом случае одна из функций $f$ и $g$ годится, так что внутри каждой связной компоненты у нас есть биекция, и остаётся их объединить для всех связных компонент. □

В доказательстве теоремы Кантора–Бернштейна искомая биекция $h$ строится только из тех пар, которые отвечают двум инъекциям. В результате множество $A$ разбивается на части $A_1$ и $A_2$, а множество $B$ разбивается на части $B_1$ и $B_2$, при этом $f$ осуществляет биекцию между $A_1$ и $B_1$, а $g$ осуществляет биекцию между $B_2$ и $A - 2$.

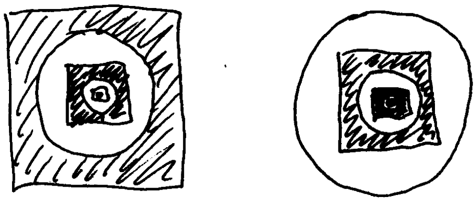
Это позволило предложить по существу теорему Кантора–Бернштейна в качестве задачи на одной из школьных олимпиад, сформулировав её так:

**Теорема 5.** *Квадрат и круг можно разбить на пары взаимно подобных частей.*

(Квадрат разбивается в объединение непересекающихся фигур $A_1$ и $A_2$, круг разбивается в объединение непересекающихся фигур $B_1$ и $B_2$, при этом $A_1$ подобно $B_1$, а $A_2$ подобно $B_2$.)

*Доказательство.* Возьмём преобразование подобия, которое отображает квадрат внутрь круга, оно будет инъекцией. (Бывает же внутри круга маленький квадрат!) Аналогично можно поместить круг в квадрат с помощью другого преобразования подобия. Остаётся применить доказательство теоремы Кантора–Бернштейна к этим двум инъекциям. □

Можно, конечно, сказать, что это нечестно — давать на олимпиаде задачу, использующую стандартный результат из «высшей математики». С другой стороны, можно решить эту задачу, не ссылаясь на Кантора и Бернштейна, а просто вдумчиво рассматривая картинку с чёрным квадратом — но не просто как у Малевича, а с кругом внутри.



(Две видеокамеры смотрят на круглый и квадратный экраны, показывая на них перекрёстно свои изображения).

## 11 Что дальше?

В этой лекции у нас почти не было интересных теорем, речь больше шла об определениях, соглашениях, обозначениях и т. д. Цель наша была в том, чтобы привыкнуть к некоторому языку (множества, отношения, функции, композиция,...) — и для этого поговорить на этом языке о чём-то сравнительно простом и знакомом. (Никто не ждёт откровений от диалогов в учебнике английского языка.)

Этот язык будет нам постоянно встречаться — будем ли мы говорить о логических операциях и кванторах, или о графах, или об упорядоченных множествах, или о вычислимых функциях и перечислимых свойствах. Да и не только нам — пытаясь уточнить смысл понятия падежа, Колмогоров и Зализняк предлагали считать падежом класс эквивалентности некоторого отношения.[5]. Умение увидеть какие-то из рассмотренных нами структур часто бывает полезно, даже если на первый взгляд ничего подобного не скажешь. Например, есть такая задача, которую может понять даже семиклассник: в десятизначном числе, составленном из разных цифр, можно вычеркнуть шесть цифр, чтобы оставшиеся четыре шли в возрастающем или в убывающем порядке. Однако (по-видимому, самое простое) её решение состоит в том, что на множестве цифр рассматривается подходящее бинарное отношение порядка («стоять левее и одновременно быть меньше» — мы разберём этот пример в разделе об упорядоченных множества).

[5] И при этом в русском языке обнаруживается больше падежей, чем традиционнные шесть — именительный, родительный, дательный, винительный, творительный и предложный. Скажем, в обороте «в лесу» этот самый «лес» считают стоящим в «местном» падеже. См. подробности в `http://www.kolmogorov.info/uspensky-k_opredeleniyu_padezha_po_kolmogorovu.html`