

Уральский федеральный университет
Институт естественных наук и математики

Департамент математики, механики и
компьютерных наук

При поддержке компаний



Введение в математику

Екатеринбург, 2019

Авторы: А.Г. Гейн, П.А. Гейн, И.А. Михайлова

Курс предназначен для ознакомления с базовой терминологией математических дисциплин: множества и операции над ними, отношения на множестве, графы и их свойства, отображения множеств и их свойства, операции на множестве и их свойства, метод математической индукции, основные комбинаторные схемы, элементы математической логики. Для каждой темы приведён комплект заданий для самопроверки.

Предисловие

Уважаемые первокурсники! Вы начинаете (по крайней мере, большинство из вас) изучать математику, поскольку то, что изучалось вами в школе, так же далеко от математики, как танцы на вечеринке от балета. И прежде, чем осваивать математический ландшафт, надо выучить язык, посредством которого вы будете это делать. Мы предлагаем вам триединый путь:

1. Видеолекции, которые вы должны прослушать во внеаудиторном режиме.
2. Работа с учебным пособием, которые вы сейчас читаете.
3. Работа на практических занятиях.

Помните при этом, что «спасение утопающих – дело рук самих утопающих»: со всеми возникающими вопросами и затруднениями в понимании материала не стесняйтесь обращаться к преподавателям на консультациях.

Каждая тема в этом пособии представлена отдельной лекцией. В ней приведены определения основных терминов, базовые утверждения с доказательствами и примеры, иллюстрирующие используемые понятия. Определяемые термины выделены *курсивом*.

Текст каждой лекции разбит на отдельные логически законченные пункты. А внутри пунктов текст разрывается небольшими заданиями для самопроверки, которая позволит вам оценить, насколько хорошо вы усвоили прочитанный материал. Эти задания размещены на цветной плашке и помечены символом . Старайтесь выполнить эти задания, прежде чем продолжите чтение. Разумеется, если его выполнение вызвало затруднение – это не повод не читать материал дальше. Надо только обязательно разобраться с этим заданием либо на консультации с преподавателем, либо привлекая другие информационные средства.

В некоторых местах вы встретите текст, отмеченный символом . Он означает, что данный фрагмент текста (тоже размещённый на цветной плашке) при первом чтении можно пропустить: он направлен на расширение вашего кругозора, и читать его лучше в свободное от выполнения обязательных заданий время.

В конце каждой лекции есть раздел «Задания для самостоятельной работы». Это обязательные задания, которые вы должны выполнить до того, как придёте на практическое занятия по теме лекции. Если какое-то из них не получается,

надо информировать об этом преподавателя. Выполнение этих заданий будет контролироваться.

Ответы к некоторым заданиям вы будете вводить в тестовую систему проверки. Около номера таких заданий стоит буква Т.

Мы настоятельно вам советуем после того, как вы посмотрите и прослушаете видеолекцию и/или прочитаете тот же материал в этом пособии, написать «шпаргалку» по теме лекции. В ней не место пространным рассуждениям, примерам и т.п. Соберите в ней основные сведения, которые будут вам в помощь при работе на практических занятиях. При этом на каждое практическое занятие полезно иметь с собой все «шпаргалки», которые к этому моменту уже были вами созданы.

Лекция 1. Множества и логика

В школьном курсе математики вы, конечно, употребляли слово «множество». Но что такое множество? Академическая группа студентов – это множество. И стадо слонов – это тоже множество. Стая птиц – множество. И косяк рыб – тоже множество... Но что же такое множество?

Понятие множества. Способы задания множества

Математика – одна из немногих честных наук, которая признаёт, что в ней есть неопределяемые понятия. Хотя есть они, конечно, в любой науке. Ведь что значит дать определение? Это значит объяснить новое понятие через другие, уже известные понятия. Ясно, что такая цепочка не может разворачиваться бесконечно (чтобы не получилось замкнутого круга), поэтому где-то там, в самом начале, расположились неопределяемые понятия. *Множество* (как, впрочем, и алгоритм) является в математике неопределяемым понятием.



Приведите примеры неопределяемых понятий из геометрии.

Но это вовсе не означает, что нельзя понять, что такое множество. По словам основателя теории множеств Георга Кантора множество надо понимать как совокупность объектов, называемых элементами данного множества, которую мы можем представлять себе как единое целое. И вовсе не обязательно, чтобы это были материальные объекты, – герои мультфильма «Маша и медведь» тоже образуют множество.

Как математики поступают с неопределяемыми понятиями? Они устанавливают между ними взаимосвязи. Вот примеры: точка лежит (или не лежит) на прямой; через две различные точки проходит прямая и только одна и т. п. Так же и с множествами: каждый объект может быть элементом того или иного множества, а может им не быть. Быть или не быть – вот в чём вопрос! Будем говорить, что множество задано, если для любого объекта можно определить, является он элементом этого множества или нет.



Здесь мы снова сталкиваемся с принципиальной трудностью – что означают слова «определить, является элементом или нет»? Означают ли они, что имеется алгоритм, дающий ответ на этот вопрос? Как вы узнаете несколько позже, всё не так-то просто.

Договоримся обозначать множества заглавными латинскими буквами, а их элементы – строчными. Заметим, что элементами множества могут быть другие множества. Это легко понять, если представить себе множество некой сумкой, а

его элементы – тем, что в ней содержится, тогда ничто не мешает положить внутрь сумки еще одну сумку. Будем писать $x \in M$, если x принадлежит множеству M (т. е. является его элементом), и $x \notin M$, если не принадлежит.

Оказывается весьма полезным среди самых разнообразных множеств иметь особое множество – *пустое*. Так называют множество, вообще не содержащее элементов. Его обозначают $\emptyset$.



А вот множества, которое содержало бы в себе всевозможные объекты, в том числе и все множества, не существует. И не только потому, что человеку невозможно представить себе всё-всё на свете как единую совокупность. Само понятие множества, содержащего в себе все множества, является противоречивым. Это один из так называемых парадоксов Рассела (желающие, конечно, могут найти его описание в интернете).

Как же задавать множества? Чтобы узнать, стал ли абитуриент элементом множества первокурсников, надо просто заглянуть в список зачисленных. Так что самый простой способ задания множества – перечисление всех его элементов. И в программировании такая структура данных, как множество, задаётся перечислением всех его элементов. Мы такое перечисление договоримся записывать так: $\{a_1, a_2, \dots, a_n\}$. Конечно, $a_1, a_2, \dots, a_n$ – это не сами элементы, а их имена, так же, как в списке зачисленных не сами абитуриенты, а их фамилии, имена и отчества, хотя само множество зачисленных состоит, конечно, из живых людей.

Впрочем, многие из вас в описанной ситуации воспользовались, наверно, другим способом. Зная проходной балл, вы сравнили его со своими баллами и сделали вывод. В этом случае попадание объекта в множество обеспечивается некоторым условием: если оно выполнено, объект множеству принадлежит, если нет, то – увы... Записывать задание множества условием договоримся так: $\{x \mid P(x)\}$, где $P(x)$ – формулировка того самого условия (другими словами, свойства элемента x), которые обеспечивают попадание x в множество.

Например: $\{1, 2\}$, $\{0, 2, 4, 6\}$, $\{x \mid x \text{ – целое четное неотрицательное число, меньшее } 8\}$, $\{x \mid x \text{ является корнем уравнения } x^2 - 3x + 2 = 0\}$.



Если немного подумать, то окажется, что человеку довольно часто приходится по описанию множества посредством указания свойства находить его элементы. По цене и качеству или ещё каким-то свойствам покупатель ищет в магазине нужный ему товар, следователь по уликам ищет преступника, конструктор ищет материал, свойства которого дадут ему возможность реализовать свою идею и т.п. Иногда, конечно, множество может оказаться

пустым. Само доказательство, что множество, заданное указанием свойств его элементов, не пусто, может оказаться весьма сложной задачей. В математике вы неоднократно будете доказывать теоремы о том, что объекты с заданными свойствами существуют (т. е. что не пусто соответствующее множество). Такие теоремы называются *теоремами существования*. Они могут быть двух видов. Скажем, когда перед авиаконструктором стоит задача создать самолёт с заданными характеристиками, он «доказывает» теорему существования тем, что создаёт проект такого самолёта, т. е. приводит алгоритм построения нужного объекта. И в математике многие теоремы существования доказываются описанием алгоритма, позволяющего построить нужный объект. Такие теоремы (как и их доказательства) называют *конструктивными*. Но математики (в основном великие) придумали способы доказательства теорем существования без предъявления алгоритма. Такие теоремы называют *теоремами чистого существования*. Оказалось, что и они играют немаловажную роль в решении программистских задач. Но об этом позже...

В множестве, как и в реальной жизни, каждый элемент уникален. Конечно, среди людей встречаются полные тёзки, у которых совпадают фамилии, имена и отчества, но паспортные данные у них всё-таки различны. Поэтому перечисляя элементы во множестве, мы будем считать, что они все попарно различны, и у каждого из них уникальное имя. Это позволяет сказать, что два множества равны, если они состоят из одних и тех же элементов. Вот более строгая формулировка.

Определение 1.1. Множество X равно множеству Y , если для каждого x из утверждения $x \in X$ следует, что $x \in Y$ и, наоборот, для каждого y из утверждения $y \in Y$ следует, что $y \in X$.

Пусть $A = \{1, 2\}$, $B = \{0, 2, 4, 6\}$, $C = \{x \mid x - \text{целое четное неотрицательное число, меньшее } 8\}$, $D = \{x \mid x \text{ является корнем уравнения } x^2 - 3x + 2 = 0\}$. Нетрудно убедиться, что $A = D$ и $B = C$.



Объясните, почему верны указанные равенства.

Для некоторых числовых множеств существуют стандартные обозначения:

N – множество натуральных чисел,

Z – множество целых чисел,

Q – множество рациональных чисел,

R – множество действительных чисел или числовая прямая.

Пусть $a, b \in R$ такие, что $a < b$. Тогда

$(a, b) = \{x \in \mathbf{R} \mid a < x < b\}$ – интервал на числовой прямой;
 $(a, b] = \{x \in \mathbf{R} \mid a < x \leq b\}$, $[a, b) = \{x \in \mathbf{R} \mid a \leq x < b\}$ – полуинтервалы;
 $[a, b] = \{x \in \mathbf{R} \mid a \leq x \leq b\}$ – отрезок;
 $(-\infty, b] = \{x \in \mathbf{R} \mid x \leq b\}$, $[a, +\infty) = \{x \in \mathbf{R} \mid a \leq x\}$ – лучи.

Подмножества

Определение 1.1. Множество A называется *подмножеством* множества B , если из того, что $x \in A$ следует $x \in B$ (т. е. если каждый элемент множества A является элементом множества B).

Тот факт, что множество A является *подмножеством* множества B , записывают так: $A \subseteq B$ или $B \supseteq A$. Ясно, что всякое множества является своим подмножеством, т. е. утверждение $A \subseteq A$ истинно для любого множества A . Если же $A \subseteq B$, но при этом $A \neq B$, то A называется *собственным подмножеством* множества B . Этот факт записывают как $A \subset B$ или $B \supset A$.

Пример 1.

1) $\mathbf{N} \subset \mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R}$.

2) $(-2, 5) \subset (-2, 5] \subset [-2, 5] \subset (-\infty, 5]$.

Теорема 1.1. Для любого множества M выполняется $\emptyset \subseteq M$.

Доказательство. Предположим, что это не так. Тогда должен найтись элемент из множества $\emptyset$, который не принадлежит множеству M . Однако такого элемента в множестве $\emptyset$ нет, значит, наше предположение неверно, и теорема доказана. $\square$

Теорема 1.2. Множества A и B равны тогда и только тогда, когда $A \subseteq B$ и $B \subseteq A$.



Докажите эту теорему самостоятельно.

Пусть M – некоторое множество.

Определение 1.2. Множество всех подмножеств множества M называется *булеаном* множества M .

Булеан множества M обозначают $\mathcal{B}(M)$ (другое обозначение $\mathcal{P}(M)$). Можно записать: $\mathcal{B}(M) = \{X \mid X \subseteq M\}$. Ясно, что в булеане непустого множества M всегда есть, по крайней мере, два элемента: $\emptyset$ и само M .



Найдите $\mathcal{B}(\emptyset)$.

Пример. Пусть $M = \{a, b, c\}$. Тогда $\mathcal{B}(M) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$. Как видите, в $\mathcal{B}(M)$ содержится 8 элементов, а $8 = 2^3$. Как будет

доказано позже, булеан множества, содержащего n элементов, всегда состоит из 2^n элементов.

Элементы математической логики

Скорее всего, вас не смутило предложение доказать теорему 1.2 – ведь доказывать теоремы вас учили ещё в школе. Да и родители не раз пытались доказать вам свою правоту, а иногда и вы – им. И всё же, вступая на тропу математики и компьютерных свершений, давайте обсудим, что мы доказываем и как.

Доказываем мы всегда истинность какого-либо утверждения, иначе говоря, высказывания. Под *высказыванием* обычно понимают повествовательное предложение, про которое можно наверняка сказать, истинно оно или ложно.

Вот несколько примеров:

1. Число $\sqrt{2}$ иррационально.
2. Число $\sqrt{2}$ рационально.
3. Любое натуральное число x рационально.
4. Любое действительное число x рационально.
5. Существует действительное число x , которое рационально.
6. Число x рационально.
7. В записи числа $\sqrt{2}$ обязательно встретятся 20 записанных подряд цифр 9.
8. Число называется рациональным, если оно равно отношению целого числа к натуральному.
9. Верно ли, что число $\sqrt{2}$ иррационально?
10. Докажите, что число $\sqrt{2}$ иррационально.

Первые пять предложений, очевидно, являются высказываниями, причем 1-е, 3-е и 5-е – истинны, а 2-е и 4-е – ложны. Два последних предложения не являются высказываниями, поскольку они вовсе не повествовательные предложения: одно из них вопросительное, а другое – побудительное. Предложение 8 не является высказыванием, поскольку об его истинности говорить бессмысленно — оно лишь определяет новое понятие через ранее введенные.

В повествовательном предложении 6 истинность заключенной в нем информации зависит от значения переменной x : при одних ее значениях утверждение оказывается истинным, при других — ложным. Так что это предложение нельзя отнести к высказываниям. Мы рассмотрим подобные утверждения немного позже.

Об утверждении 7 мы вряд ли можем прямо сейчас сказать, истинно оно или ложно. Но ситуация такова, что в реальности оно либо истинно, либо ложно. Так что это высказывание.

Возвращаясь к вопросу, поставленному в начале этого пункта, можно сказать, что доказательство – это некоторый способ получения одних истинных высказываний из других, истинность которых уже была установлена ранее. Эти способы и начал изучать в IV веке до н.э. древнегреческий учёный Аристотель, заложив основы формальной логики. Подчеркнём, что устанавливать истинность исходных утверждений – это задача конкретных наук: физики, химии, биологии, истории и т.д. В математике истинность исходных утверждений – их, как вы знаете, называют аксиомами – принимается без доказательства. А вот все остальные утверждения должны (по мере возможностей) получаться по правилам формальной логики.

В школьном курсе информатики вы уже изучали основные операции над высказываниями. В таблице 1.1 воспроизведены их названия и обозначения. Те, которые будут преимущественно использоваться в нашем курсе, записаны первыми. В другой учебной литературе могут использоваться другие термины и обозначения.

Таблица 1.1

Логическая операция	Обозначение	Смысл в обычном языке
Конъюнкция, логическое умножение	$\&$, $\cdot$, $\wedge$	Союзы <i>и, а, но</i>
Дизъюнкция, логическое сложение	$\vee$, $+$	Союз <i>или</i>
Отрицание, инверсия	$\neg$, $-$	Частица <i>не</i>
Импликация, следование	$\Rightarrow$, $\rightarrow$	Оборот <i>если ..., то ...</i>
Эквиваленция	$\Leftrightarrow$, $\leftrightarrow$, $\equiv$,	Обороты <i>тогда и только тогда, необходимо и достаточно</i>

В математической логике логические операции называются *логическими связками*.

Договоримся обозначать высказывания заглавными латинскими буквами. Например, высказывание «у слона есть уши» можно обозначить буквой *X*, а высказывание «у слона есть хобот» – буквой *Y*.

В математике принято считать, что истинное высказывание имеет логическое значение 1, а ложное – 0. В некоторых языках программирования

True и False соответственно (хотя внутри компьютера они всё равно кодируются как 1 и 0).

Во всех логических операциях, кроме операции отрицания, участвуют два аргумента. Поэтому применение, например, конъюнкции к высказываниям X и Y обычно записывают как $X \& Y$, а применение импликации к тем же высказываниям – как $X \Rightarrow Y$. Отрицание высказывания X записывают в виде $\neg X$.

Значения логических операций задаются, как вы знаете, с помощью *таблиц истинности*. В них для всевозможных комбинаций значений аргументов записывается результат применения операции. Для всех операций эти таблицы истинности собраны в одну таблицу 1.2.

Таблица 1.2

X	Y	$X \& Y$	$X \vee Y$	$\neg X$	$X \Rightarrow Y$	$X \Leftrightarrow Y$
1	1	1	1	0	1	1
1	0	0	1	0	0	0
0	1	0	1	1	1	0
0	0	0	0	1	1	1

Как видно из таблицы, истинность высказывания, полученного применением дизъюнкции, имеет место, когда истинно либо одно высказывание, либо другое, либо оба одновременно. К примеру, истинность высказывания «Идет дождь *или* дует ветер» означает, что на улице имеет место одна из трех ситуаций: идет дождь и нет ветра; нет дождя, но дует ветер; одновременно идет дождь и дует ветер. Поэтому, записывая данную фразу средствами математической логики, естественно представить ее в виде $X \vee Y$, где X – это высказывание «Идет дождь», а Y – высказывание «Дует ветер».

Возможно, вас удивила таблица истинности для операции следования. Многим почему-то кажется, что утверждение «Если X , то Y » истинно в том и только том случае, когда X и Y истинны одновременно, т. е. совпадает с конъюнкцией этих высказываний. Но давайте подумаем: когда ложно высказывание «Если X , то Y » и когда ложно высказыванием « X и Y »? Ведь если они одновременно истинны, то и ложными они должны быть одновременно. Легко понять, что высказывание « X и Y » ложно тогда и только тогда, когда ложно хотя бы одно из высказываний X или Y . А ложность высказывания «Если X , то Y » означает, что, хотя высказывание X истинно, высказывание Y ложно. Отсюда и вытекает то формальное определение импликации, которое приведено в таблице 1.2. В частности, высказывание «Если $2 \times 2 = 5$, то $2 \times 2 = 4$ » истинно.

Как, впрочем, истинно и высказывание «Если $2 \times 2 = 5$, то $2 \times 2 = 3$ ». Нередко отмеченное свойство импликации формулируют так: из истины следует истина, а из лжи – что угодно.

Если у вас имеются какие-то высказывания $X_1, X_2, \dots, X_n$, то, применяя логические связи, вы можете конструировать высказывание с довольно сложной записью. Например, $\neg(X_1 \vee X_2) \& (\neg X_1 \vee X_3)$. Такие записи мы будем называть *формулами* и обозначать их тоже заглавными латинскими буквами – ведь в конечном счёте это тоже высказывания.

В записи формулы мы использовали скобки, чтобы показать, в каком порядке следует выполнять операции. Но в формуле $\neg X_1 \vee X_3$ какую операцию выполнять раньше – отрицание или дизъюнкцию? Конечно, из школьного курса информатики вы знаете о приоритетах логических операций, напомним их: наивысший приоритет имеет отрицание (если она есть, то выполняется первой), второй приоритет у конъюнкции, третий – у дизъюнкции, а у импликации и эквиваленции самый низкий приоритет.

Определение 1.3. Две формулы, содержащие в своей записи один и тот же набор высказываний $X_1, X_2, \dots, X_n$, будем называть *равносильными*, если они принимают одно и то же логическое значение при любом наборе значений высказываний $X_1, X_2, \dots, X_n$.

Равносильность формул будем обозначать знаком $=$.

Чтобы определить, равносильны ли две формулы, достаточно для каждой из них составить таблицы истинности и убедиться, что они одинаковы.

Пример 2. Покажем равносильность формул $X \Rightarrow Y$ и $\neg X \vee Y$.

Таблица 1.3

X	Y	$\bar{X}$	$X \Rightarrow Y$	$\neg X \vee Y$
1	1	0	1	1
1	0	0	0	0
0	1	1	1	1
0	0	1	1	1

Всем видно, что столбцы для $X \rightarrow Y$ и $\neg X \vee Y$ совпадают. Значит, формулы равносильны, т. е. можно записать $X \rightarrow Y = \neg X \vee Y$.

Отметим, что в языках программирования также есть логические операции, которые в точности соответствуют логическим связкам конъюнкции, дизъюнкции и отрицанию. Но операций импликации и равносильности нет – именно потому, что их можно заменить тремя указанными выше связками. Для

импликации мы только что это показали, а для равносильности убедитесь в этом самостоятельно, выполнив следующее упражнение.



Проверьте равносильность следующих формул: $X \Leftrightarrow Y$, $(X \Rightarrow Y) \& (Y \Rightarrow X)$ и $(X \& Y) \vee (\neg X \& \neg Y)$.

Равносильность некоторых формул настолько важна, что их называют законами математической логики. Вот список этих законов с их названиями.

1. Идемпотентности: $X \vee X = X$, $X \& X = X$;
2. Коммутативности: $X \vee Y = Y \vee X$, $X \& Y = Y \& X$;
3. Ассоциативности: $(X \vee Y) \vee Z = X \vee (Y \vee Z)$, $(X \& Y) \& Z = X \& (Y \& Z)$;
4. Поглощения: $X \vee (X \& Y) = X$, $X \& (X \vee Y) = X$;
5. Дистрибутивности: $X \vee (Y \& Z) = (X \vee Y) \& (X \vee Z)$,
 $X \& (Y \vee Z) = (X \& Y) \vee (X \& Z)$;
6. Двойного отрицания: $\neg \neg X = X$;
7. Де Моргана: $\neg(X \vee Y) = \neg X \& \neg Y$, $\neg(X \& Y) = \neg X \vee \neg Y$;
8. Исключённого третьего: $X \vee \neg X = 1$;
9. Противоречия: $X \& \neg X = 0$;
10. Свойства нуля: $X \vee 0 = X$, $X \& 0 = 0$;
11. Свойства единицы: $X \vee 1 = 1$, $X \& 1 = X$.
12. $\neg 1 = 0$, $\neg 0 = 1$.
13. Монотонности: если $X \Rightarrow Y$, то $X \& Z \Rightarrow Y \& Z$ и $X \vee Z \Rightarrow Y \vee Z$ для любого высказывания Z .



Проверьте самостоятельно справедливость каждого из указанных законов.

Определение 1.4. Формула, содержащая в своей записи набор высказываний $X_1, X_2, \dots, X_n$, называется *тождественно истинной*, если она принимает значение 1 при любом наборе значений высказываний $X_1, X_2, \dots, X_n$.

Вот два примера тождественно истинных формул: $X \vee \neg X$ и $X \Rightarrow X$.



Проверьте, что эти формулы тождественно истинны.

Определение 1.5. Формула, содержащая в своей записи набор высказываний $X_1, X_2, \dots, X_n$, называется *тождественно ложной*, или *противоречием*, если она принимает значение 0 при любом наборе значений высказываний $X_1, X_2, \dots, X_n$.

Вот пример тождественно ложной формулы: $X \& \neg X$.

Понятия равносильности и тождественной истинности тесно связаны.

Теорема 1.3. Формулы F и G равносильны тогда и только тогда, когда формула $F \Leftrightarrow G$ тождественно истинна.

Доказательство. Пусть F и G равносильны. Если при каком-либо наборе логических значений высказываний $X_1, X_2, \dots, X_n$, входящих в запись формулы F , она принимает значение 1, то и G принимает значение 1 при том же наборе логических значений высказываний $X_1, X_2, \dots, X_n$. Значит, на этом наборе значений высказываний $X_1, X_2, \dots, X_n$ формула $F \Leftrightarrow G$ имеет значение 1. Аналогично формула $F \Leftrightarrow G$ имеет значение 1, если формула F принимает значение 0 при каком-либо наборе логических значений высказываний $X_1, X_2, \dots, X_n$. Следовательно, формула $F \Leftrightarrow G$ тождественно истинна.

Обратно. Поскольку формула $F \Leftrightarrow G$ принимает значение 1 на любом наборе логических значений высказываний $X_1, X_2, \dots, X_n$, формулы F и G принимают одинаковые значения на этом наборе. Это означает, что F и G равносильны. $\square$

Ясно, что из формул (а не только непосредственно из высказываний) можно получать новые формулы, используя логические связки. Надо только аккуратно следить за приоритетами операций и по мере необходимости ставить скобки. Например, если F – это $X \vee Y$, а G – это $X \& Z$, то $F \& G$ – это $(X \vee Y) \& X \& Z$. Впрочем, если, применяя логические связки к формулам, вы всегда будете заключать формулы в скобки, хуже не будет, а вот от ошибок это вас защитит.

Поскольку каждая формула – это в конечном счёте высказывание, то, подставляя в формулы законов логики вместо X , Y и Z любые формулы, вы снова получите тождественно истинную формулу.

В следующей теореме приведён ещё один способ получения истинных формул математической логики.

Теорема 1.4. Если формулы $F \Rightarrow G$ и $G \Rightarrow H$ истинны на некотором наборе логических значений высказываний $X_1, X_2, \dots, X_n$, входящих в записи этих формул, то и формула $F \Rightarrow H$ тоже истинна на этом наборе.

Доказательство. Рассмотрим набор логических значений высказываний $X_1, X_2, \dots, X_n$, входящих в записи формул $F \Rightarrow G$ и $G \Rightarrow H$, для которого эти формулы истинны. Если логическое значение формулы F на этом наборе оказалось равным 0, то, по определению импликации, логическое значение формулы $F \Rightarrow H$ равно 1 независимо от логического значения формулы H . Если же логическое значение формулы F оказалось равным 1, то, снова по определению импликации, логическое значение формулы G равно 1 ввиду истинности формулы $F \Rightarrow G$. По той же причине логическое значение формулы H равно 1. А тогда и логическое значение формулы $F \Rightarrow H$ тоже равно 1. $\square$

Поскольку истинность формулы $F \Leftrightarrow G$ равносильна тому, что одновременно истинны формулы $F \Rightarrow G$ и $G \Rightarrow F$, мы получаем следующее

Следствие 1.5. Если формулы $F \Leftrightarrow G$ и $G \Leftrightarrow H$ истинны на некотором наборе логических значений высказываний $X_1, X_2, \dots, X_n$, входящих в записи этих формул, то и формула $F \Leftrightarrow H$ тоже истинна на этом наборе.

Это следствие вместе с теоремой 1.3 позволяет осуществлять равносильные преобразования формул в виде единой цепочки.

Пример 3. Вася писал программу и в одном из операторов ветвления получил следующее условное выражение: $(A \vee B) \& \neg(\neg A \& C)$. Помогите Васе упростить свою запись так, чтобы осталось как можно меньше логических операторов.

Воспользуемся законами логики высказываний:

$$\begin{array}{ccccccc} & \textcircled{7} & & \textcircled{6} & & & \textcircled{5} \\ (A \vee B) \& \neg(\neg A \& C) & = & (A \vee B) \& (\neg\neg A \vee \neg C) & = & (A \vee B) \& (A \vee \neg C) = A \vee (B \& \neg C). \end{array}$$

Значит, Вася смело может писать условие в виде $A \vee (B \& \neg C)$.

И снова вернёмся к вопросу о доказательстве. Мы объявили, что это некий способ получения одних истинных высказываний из других, истинность которых уже была установлена ранее. И способ этот весьма прост: если известно, что истинно высказывание A и истинно высказывание $A \Rightarrow B$, то истинным будет и высказывание B . Это прямо следует из определения импликации. А само правило называют *móduſ rónens* (в переводе с латинского – правило вывода).

Определение 1.6. Доказательством утверждения B называют цепочку высказываний $A_1, A_2, \dots, A_n = B$, где каждое A_k либо аксиома, либо ранее доказанное высказывание, либо получено из предыдущих элементов цепочки применением *modus ponens*.

Напомним, что *аксиомами* называют исходные высказывания, принимаемые без доказательства, а высказывания, которые могут быть получены посредством доказательства, называются *теоремами*. Обычно теорему можно представить в виде $A \Rightarrow B$. В этом случае высказывание A называется *посылкой* теоремы, а высказывание B – её *заключением*.

Конечно, теорема не всегда прочитывается в канонической форме «Если A , то B », человеческий язык намного богаче. Но фактически такая форма всегда подразумевается. Например, теорема «В прямоугольнике диагонали равны» является высказыванием «Если четырёхугольник является прямоугольником, то его диагонали равны». Иногда, чтобы избежать громоздкости формулировки, её

разбивают на отдельные части. Например: «Пусть прямая перпендикулярна одной из двух параллельных прямых. Тогда она перпендикулярна и второй». Ясно, что это другая формулировка теоремы «Если прямая перпендикулярна одной из двух параллельных прямых, то она перпендикулярна и второй».

Иногда теоремы формулируют в виде $A \Leftrightarrow B$. Вы должны понимать, что здесь «спрятались» две теоремы: $A \Rightarrow B$ и $B \Rightarrow A$.

Операции над множествами

Определение 1.7. *Пересечением* множеств A и B называется множество $\{x \mid x \in A \text{ и } x \in B\}$.

Множество, являющееся пересечением множеств A и B , обозначают $A \cap B$.

Определение 1.8. *Объединением* множеств A и B называется множество $\{x \mid x \in A \text{ или } x \in B\}$.

Множество, являющееся объединением множеств A и B , обозначают $A \cup B$.

Определение 1.9. *Разностью* множеств A и B называется множество $\{x \mid x \in A \text{ и } x \notin B\}$.

Множество, являющееся разностью множеств A и B , обозначают $A \setminus B$.

Если A и B – некоторые множества точек плоскости, то на рисунке 1 закрашены а) пересечение, б) объединение, в) разность этих множеств.

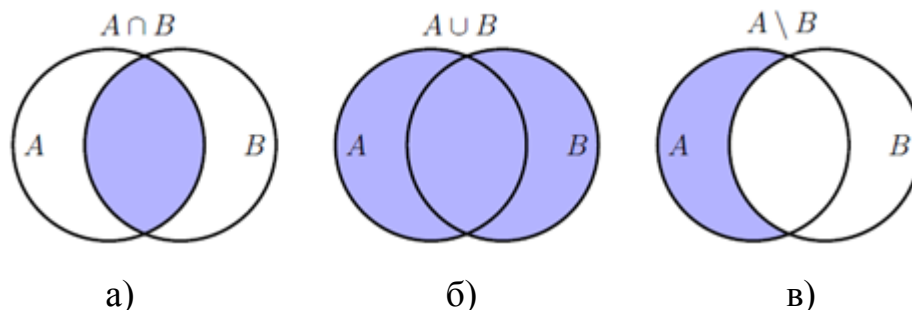


Рис. 1. Пересечение, объединение и разность двух множеств

Если множество $A = \{x \mid P(x)\}$, а множество $B = \{x \mid Q(x)\}$, то легко понять, что $A \cap B = \{x \mid P(x) \& Q(x)\}$, а $A \cup B = \{x \mid P(x) \vee Q(x)\}$.



Докажите два равенства. Запишите, используя $P(x)$ и $Q(x)$, множество $A \setminus B$.

Когда написано, что $x \notin M$, мы понимаем, что в множестве M объекта, обозначенного буквой x , нет. Но так, чтобы объект вообще не принадлежал никакому множеству, в реальной жизни представить себе трудно. В своей деятельности человек, как правило, оперирует с объектами из того или иного множества. Такое множество принято называть *предметной областью*. Предметная область может быть очень широкой и не обязательно однородной.

Например, для учёного-химика его предметная область – химические элементы и их соединения, химические реакции и методы анализа вещества и многое другое. А животные и растения в его предметную область не входят.

В математике вместо расплывчатого термина «предметная область» говорят *универсальное множество*. Так, обсуждая те или иные свойства чисел, вы довольно часто будете в качестве универсального множества рассматривать множество действительных чисел.

Будем обозначать универсальное множество буквой U .

Определение 1.10. Дополнением множества A называется множество $U \setminus A$.

Дополнение множества A обозначают $\bar{A}$.

Для любых множеств A, B, C выполняются тождества:

1. Идемпотентности: $A \cap A = A$; $A \cup A = A$;
2. Коммутативности: $A \cap B = B \cap A$; $A \cup B = B \cup A$;
3. Ассоциативности: $(A \cap B) \cap C = A \cap (B \cap C)$; $(A \cup B) \cup C = A \cup (B \cup C)$;
4. Поглощения: $A \cap (A \cup B) = A$; $A \cup (A \cap B) = A$;
5. Дистрибутивности: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$,
 $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;
6. Двойного дополнения: $\bar{\bar{A}} = A$;
7. Законы де Моргана: $\overline{A \cap B} = \bar{A} \cup \bar{B}$; $\overline{A \cup B} = \bar{A} \cap \bar{B}$;
8. $A \cap \bar{A} = \emptyset$;
9. $A \cup \bar{A} = U$;
10. $A \cap \emptyset = \emptyset$; $A \cup \emptyset = A$;
11. $A \cap U = A$; $A \cup U = U$;
12. $\bar{U} = \emptyset$; $\bar{\emptyset} = U$;
13. Монотонности: если $A \subseteq B$, то $A \cap C \subseteq B \cap C$ и $A \cup C \subseteq B \cup C$ для любого множества C .



Если сравнить законы логики и первые 12 тождеств для множеств, то мы увидим, что стоит заменить $\vee$ на $\cup$, $\&$ на $\cap$, $\neg$ на $\bar{}$, $\Leftrightarrow$ на $=$, 0 на $\emptyset$, 1 на U как эти два списка совпадут. Это, конечно, не случайно. Попытайтесь объяснить подмеченный феномен.

Приведём в качестве примеров доказательства трёх из указанных законов.

Пример 1. $A \cup (A \cap B) = A$.

Доказательство. Надо проверить, что каждый элемент из множества, записанного в левой части равенства, содержится в множестве из правой части и наоборот.

Пусть $x \in A \cup (A \cap B)$. Тогда, по определению объединения множеств, $x \in A$, и нужное нам уже получено, или $x \in A \cap B$. Во втором случае, по определению пересечения множеств, $x \in A$ и $x \in B$, т. е. и в этом случае $x \in A$. Таким образом, любой элемент из $A \cup (A \cap B)$ принадлежит A .

Обратно. Пусть $x \in A$. Тогда, по определению объединения множеств, $x \in A \cup (A \cap B)$. $\square$

В следующем примере мы воспользуемся методом равносильных преобразований.

Пример 2. $\overline{A \cap B} = \bar{A} \cup \bar{B}$.

Доказательство. Высказывание $x \in \overline{A \cap B} \Leftrightarrow \neg(x \in A \cap B) \Leftrightarrow \neg(x \in A \& x \in B) \Leftrightarrow \neg(x \in A) \vee \neg(x \in B) \Leftrightarrow (x \notin A) \vee (x \notin B) \Leftrightarrow (x \in \bar{A}) \vee (x \in \bar{B}) \Leftrightarrow x \in \bar{A} \cup \bar{B}$. По следствию 1.5 высказывания $x \in \overline{A \cap B}$ и $x \in \bar{A} \cup \bar{B}$ равносильны, а их равносильность означает равенство множеств $\overline{A \cap B}$ и $\bar{A} \cup \bar{B}$. $\square$

Пример 3. Если $A \subseteq B$, то $A \cup C \subseteq B \cup C$ для любого множества C .

Доказательство. Заметим, что высказывания $X \subseteq Y$ и $(x \in X) \Rightarrow (x \in Y)$ равносильны для любых множеств X и Y .

Высказывание $x \in A \cup C \Leftrightarrow (x \in A) \vee (x \in C) \Rightarrow (x \in B) \vee (x \in C) \Leftrightarrow x \in B \cup C$. По теореме 1.4 $x \in A \cup C \Rightarrow x \in B \cup C$. Значит, $A \cup C \subseteq B \cup C$. $\square$



Укажите, какое свойство операций над высказываниями позволяет записать $(x \in A) \vee (x \in C) \Rightarrow (x \in B) \vee (x \in C)$.

Ассоциативность операций $\cup$ и $\cap$ позволяет не писать скобки, если несколько множеств подряд соединены какой-либо одной из этих операций. Если же используется разные операции, то операции над множествами выполняются в соответствии с их приоритетом: высший приоритет имеет операция дополнения, следующий приоритет имеет операция пересечения, затем операция объединения. У операции разности самый низкий приоритет.

Декартово произведение множеств

Определение 1.11. *Кортежем длины n называется упорядоченный набор $(a_1, a_2, \dots, a_n)$ из n необязательно различных элементов. В случае $n = 2$ такой кортеж называют упорядоченной парой.*

Два кортежа $(a_1, a_2, \dots, a_n)$ и $(b_1, b_2, \dots, b_n)$ одинаковой длины *равны* тогда и только тогда, когда $a_i = b_i$ для всех $1 \leq i \leq n$.

Сравните: для $a \neq b$ двухэлементные множества $\{a, b\}$ и $\{b, a\}$ равны, в то время как упорядоченные пары (a, b) и (b, a) различны.

Определение 1.12. Декартовым произведением множеств $M_1, M_2, \dots, M_n$ называется множество всевозможных кортежей $(a_1, a_2, \dots, a_n)$, где $a_i \in M_i$ для всех $1 \leq i \leq n$. Декартово произведение множеств $M_1, M_2, \dots, M_n$ обозначают $M_1 \times M_2 \times \dots \times M_n$. Если $M_1 = M_2 = \dots = M_n = M$, то $M_1 \times M_2 \times \dots \times M_n$ обозначают M^n и называют *декартовой степенью* множества M .

Пример 1. Пусть $A = \{a, b, c\}$, $B = \{1, 2\}$. Тогда $A \times B = \{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)\}$, а $B \times A = \{(1, a), (2, a), (1, b), (2, b), (1, c), (2, c)\}$.

Этот пример показывает, что $A \times B \neq B \times A$.

Пример 2. Каждая точка на плоскости имеет две координаты, каждая из которых является действительным числом, поэтому координатную плоскость можно считать $\mathbf{R}^2$.

Пример 3. Декартово произведение отрезков $[a, b] \times [c, d]$ задает на координатной плоскости прямоугольник со сторонами, параллельными осям координат, и противоположными вершинами в точках с координатами (a, c) и (b, d) .



Укажите две другие вершины прямоугольника $[a, b] \times [c, d]$.

Пример 4. Множество всех кортежей длины n , составленных из нулей и единиц, — это $\{0, 1\}^n$.

Ещё раз о математической логике. Предикаты

Немного раньше мы обсуждали, что повествовательное предложение «Число x рационально» не может быть признано высказыванием, поскольку при одних значениях x утверждение окажется истинным, при других — ложным. Такие предложения называют *предикатами*, или, по-другому, *высказывательными формами*, потому что после подстановки вместо x конкретного числа оно превращается в высказывание. Фактически любой предикат является функцией от одной или нескольких переменных, принимающих только два значения: 1 (истина) или 0 (ложь). Например, предикат «сумма x и y равна z » от трех аргументов x , y и z , рассматриваемый на множестве натуральных чисел, принимает значение 1 при $x = 3, y = 4, z = 7$ и значение 0 при $x = 2, y = 2, z = 5$. Мы ещё будем обсуждать понятие функции, но пока будем опираться на то представление об этом математическом понятии, которое сформировалось у вас

в школе. Функцию от аргументов $x_1, x_2, \dots, x_n$ принято в математике обозначать $f(x_1, x_2, \dots, x_n)$. Предикаты, следуя этой традиции, обозначают почти также, например, $P(x_1, x_2, \dots, x_n)$ – вместо функционального символа f пишут заглавную латинскую букву. Она, разумеется, может быть любой. Например, предикат «сумма x и y равна z » можно обозначить как $S(x, y, z)$. Как мы видели, $S(3, 4, 7) = 1$, а $S(2, 2, 5) = 0$.

В предикате $S(x, y, z)$ переменные x, y и z *свободны*, в том смысле, что каждая из них может принимать любое значение из множества натуральных чисел. Но давайте рассмотрим такой предикат: «существует x , для которого сумма x и y равна z ». На первый взгляд здесь тоже присутствуют три переменных, но реально подставлять числа можно только вместо y и z . В таблице 1.4 приведены значения этого предиката для некоторых наборов значений аргументов y и z .

Таблица 1.4

y	z	Значение предиката	Комментарий
1	2	1	Подходит $x = 1$
2	2	0	Не существует подходящего x
3	5	1	Подходит $x = 2$
5	3	0	Не существует подходящего x

Переменная x в таком предикате называется *связанной*. При этом говорят, что переменная x связана *квантором существования*. Для него есть специальное обозначение: $\exists$. Происхождение этого знака простое: в английском слове «Exist» – существовать – взята первая буква и симметрично отражена относительно вертикальной оси. С помощью этого символа и уже обозначенного ранее предиката $S(x, y, z)$ наш новый предикат запишется так: $\exists x (S(x, y, z))$. А можно и просто написать $\exists x (x + y = z)$.

Для предиката $\exists x (x + y = z)$, рассматриваемого на множестве слов русского языка, найдите его значение, если

- а) $y = \text{ель}, z = \text{газель}$;
- б) $y = \text{гель}, z = \text{газель}$;
- в) $y = \text{газель}, z = \text{газель}$.

Здесь, как и во многих языках программирования, символ $+$ обозначает операцию соединения (конкатенации) строк.

Впрочем, переменная может быть связанной и по-другому. Рассмотрим для примера предикат «для любого y выполнено неравенство $x + y > z$ » на множестве натуральных чисел. Здесь связанной переменной является y . В таблице 1.5 указаны значения этого предиката для нескольких наборов значений аргументов x и z .

Таблица 1.5

x	z	Значение функции	Комментарий
1	1	1	При любом y верно $1 + y > 1$
1	2	0	Не подходит $y = 1$
3	5	0	Не подходит, например, $y = 2$
5	3	1	При любом y верно $5 + y > 3$

В этом случае говорят, что переменная связана *квантором общности* (иногда говорят *всеобщности*), который обозначают символом $\forall$. Его происхождение аналогично происхождению символа $\exists$: от слова «All» – все – взята первая буква и симметрично отражена относительно горизонтальной оси. С помощью этого квантора рассматриваемый предикат записывается так: $\forall y (x + y > z)$.

В предикате могут оказаться связанными не одна, а несколько переменных. Например, можно рассмотреть предикат $\exists x \forall y (x + y = z)$ – существует x такой, что для любого y выполняется равенство $x + y = z$. Или другой предикат: $\forall y \exists x (x + y = z)$ – для любого y существует x такой, что выполняется равенство $x + y = z$. Каждый из них является предикатом от одной переменной z , но это разные предикаты. Скажем, на множестве целых чисел первый из них при любом значении переменной z принимает значение 0, в то время как второй предикат тоже при любом значении переменной z принимает значение 1. Как видите, порядок кванторов имеет принципиальное значение.

Если в предикате все переменные оказались связанными, то такой предикат является высказыванием. Например, предикат $\forall z \forall y \exists x (x + y = z)$ — это высказывание, утверждающее, что для любых чисел z и y существует их разность (она обозначена переменной x). Это высказывание истинно на множестве целых чисел, но ложно на множестве натуральных чисел. Поэтому, обсуждая свойства того или иного предиката, надо всегда указывать множество, на котором он рассматривается.

Если в записи один и тот же квантор употребляется подряд несколько раз, то для более краткой записи его пишут один раз. Так, вместо $\forall z \forall y \exists x (x + y = z)$

можно написать $\forall z, y \exists x (x + y = z)$, а вместо $\forall z \exists y \exists x (x + y = z)$ – написать $\forall z \exists y, x (x + y = z)$

Какими именами будут названы связанные переменные, совершенно неважно, но очень важно, чтобы имена свободных переменных не совпадали с именами связанных переменных! Иначе этим переменным свободы не видать.



Не надо думать, что связанные переменные присутствуют только в математической логике. Под другими названиями, но исполняя ту же роль, они встречаются в различных областях математики и программирования. Вот, например, выражение: $\sum_{i=1}^n x^i$. Здесь x и n – свободные переменные, они могут принимать любые значения, каждая, разумеется, из своего множества: $x \in \mathbf{R}$ и $n \in \mathbf{N}$. Конечно, в этой записи ещё присутствует переменная i , но от неё результат не зависит – он, как, быть может, вы помните, равен $x \frac{x^n - 1}{x - 1}$, если $x \neq 1$, и n , если $x = 1$. Переменная i называется *индексом суммирования*. Попробуйте вспомнить, как называется переменная x в выражении $\int_0^1 x^2 dx$. Без неё не обойтись при вычислении этого интеграла, но результатом является число $\frac{1}{3}$ и никакой переменной даже близко не видно.

В программировании такое наблюдается, как только вы используете подпрограмму или процедуру. Входные и выходные параметры – это, по сути, свободные переменные, а вот локальные переменные данной подпрограммы / процедуры конкретно связаны только с ней. До начала исполнения подпрограммы / процедуры о них можно не знать, и после окончания – тоже.

Над предикатами можно выполнять все те же логические операции, которые рассматривались нами для высказываний. Ведь для того, чтобы вычислить значение такого «составного» предиката, достаточно знать логические значения предикатов, из которых он составлен. Например, предикат $\neg P(x_1, x_2, \dots, x_n)$ принимает значение 1 тогда и только тогда, когда предикат $P(x_1, x_2, \dots, x_n)$ принимает значение 0.

Построение отрицания к какому-либо утверждению можно выполнить добавлением словосочетания «Неверно, что...». Например, отрицание высказывания «Я пошел в кино» можно выразить так: «Неверно, что я пошел в кино». Правда, в обычной речи свою мысль таким образом выражают крайне редко. Обычно говорят: «Я не пошел в кино» или «Не я пошел кино», или «Я пошел не в кино». Как определить, какая фраза является отрицанием исходного высказывания? В каждом конкретном случае своя.

В математической логике с построением отрицания к какому-либо предикату всё проще. Обозначим через $P(x)$ предикат «у студента x есть ноутбук». Высказывание «у каждого студента есть ноутбук» запишется как $\forall x (P(x))$. Отрицание данного высказывания, очевидно, звучит так: «существует студент, у которого нет ноутбука». Такое высказывание запишется как $\exists x (\neg P(x))$. Другой пример. Пусть теперь $R(x)$ – это предикат «студент x , поступивший в университет, набрал на ЕГЭ по информатике меньше 80 баллов». Высказывание «существует поступивший в университет студент, который набрал на ЕГЭ по информатике меньше 80 баллов» будет записано как $\exists x (R(x))$. Его отрицание – это высказывание «все студенты, поступившие в университете, набрали на ЕГЭ по информатике не меньше 80 баллов». Оно будет записано как $\forall x (\neg R(x))$. Таким образом, действует следующее общее правило построения отрицания предикатов с кванторами.

Пусть предикат имеет вид $Q_1x_1 Q_2x_2 \dots Q_kx_k (P(x_1, x_2, \dots, x_k, y_1, y_2, \dots, y_n))$, где $Q_1, Q_2, \dots, Q_k$ – символы $\forall$ или $\exists$, $x_1, x_2, \dots, x_k$ – связанные переменные, $y_1, y_2, \dots, y_n$ – свободные переменные предиката P . Для построения отрицания нужно каждый квантор общности заменить квантором существования и наоборот, а предикат P заменить его отрицанием.

Напомним, что всякая теорема является высказыванием, т.е. её формулировка не может содержать свободных переменных. Это наше высказывание может кому-то показаться ложным. Ведь читаем же мы в учебниках формулировки теорем типа «В прямоугольнике диагонали равны» или «В равнобедренном треугольнике высота, опущенная на основание, является медианой и биссектрисой». В первом предикате переменная имеет имя «прямоугольник», во втором – «равнобедренный треугольник». И никаких кванторов! Но каждому со школьной скамьи ясно, что здесь подразумевается квантор общности – первое высказывание в духе математической логики надо читать: «В любом прямоугольнике диагонали равны», второе – «В любом равнобедренном треугольнике высота, опущенная на основание, является медианой и биссектрисой». Это общепринятая договорённость: если в формулировке теоремы есть переменные, кажущиеся свободными, это означает, что они связаны квантором общности.

Определение 1.13. Пусть $P(x_1, x_2, \dots, x_n)$ – некоторый предикат, заданный на множестве M . Множество $\{(x_1, x_2, \dots, x_n) \mid P(x_1, x_2, \dots, x_n) = 1\}$ Называется *областью истинности* предиката $P(x_1, x_2, \dots, x_n)$.

Таким образом, область истинности предиката – это подмножество декартовой степени множества M . В частности, одноместный предикат – это задание некоторого подмножества множества M . Поэтому нередко одноместный предикат называют свойством, определяющим данное подмножество.

Область истинности предиката $P(x_1, x_2, \dots, x_n)$ будем обозначать $I(P(x_1, x_2, \dots, x_n))$.

Докажите, что для любых предикатов $P(x_1, x_2, \dots, x_n)$ и $Q(x_1, x_2, \dots, x_n)$, определённых на множестве M , выполняются равенства



- а) $I(P(x_1, x_2, \dots, x_n) \& (Q(x_1, x_2, \dots, x_n))) = I(P(x_1, x_2, \dots, x_n)) \cap I(Q(x_1, x_2, \dots, x_n))$;
- б) $I(P(x_1, x_2, \dots, x_n) \vee (Q(x_1, x_2, \dots, x_n))) = I(P(x_1, x_2, \dots, x_n)) \cup I(Q(x_1, x_2, \dots, x_n))$;
- в) $I(P(x_1, x_2, \dots, x_n) \Rightarrow (Q(x_1, x_2, \dots, x_n))) = I(P(x_1, x_2, \dots, x_n)) \subseteq I(Q(x_1, x_2, \dots, x_n))$.

Даже в школьной математике запись многих утверждений языком математической логики будет весьма громоздкой и трудной для понимания. Чтобы до некоторой степени упростить запись и облегчить её понимание используют так называемые ограниченные кванторы. Дело в том, что нередко нас интересуют случаи, когда переменная принимает не произвольные значения, а из некоторого конкретного подмножества того множества, на котором рассматривается предикат в целом. Например, высказывание «Для любого действительного числа $y > 0$ существует действительное число $z > 0$, такое, что $yz = 1$ », как вы понимаете, истинно. Но его нельзя просто записать в виде $\forall y \exists z (yz = 1)$ – такое высказывание заведомо ложно.



Объясните почему.

Надо как-то отразить в записи средствами математической логики, что числа y и z принадлежат множеству положительных чисел.



Попытайтесь записать высказывание «Для любого действительного числа $y > 0$ существует действительное число $z > 0$, такое, что $yz = 1$ » средствами математической логики.

Вот возможный вариант:

$$\forall y (y > 0 \Rightarrow \exists z (z > 0 \& yz = 1)).$$

Гораздо проще и естественнее выглядела бы запись

$$\forall y > 0 \exists z > 0 (yz = 1),$$

которая, к тому же, легко читается.

Давайте разберёмся, что мы сделали. Принадлежность чисел y и z множеству положительных чисел мы записали с помощью одноместного предиката « $x > 0$ ».

Пусть $P(x)$ – произвольный предикат от переменной x . Теперь видно, что запись $\forall P(x) (Q(x, x_1, x_2, \dots, x_n))$ – это сокращение записи $\forall x (P(x) \Rightarrow Q(x, x_1, x_2, \dots, x_n))$, а запись $\exists P(x) (Q(x, x_1, x_2, \dots, x_n))$ – это сокращение для $\exists x (P(x) \& Q(x, x_1, x_2, \dots, x_n))$.



Проверьте, что $\neg \forall P(x) (Q(x, x_1, x_2, \dots, x_n)) = \exists P(x) (\neg Q(x, x_1, x_2, \dots, x_n))$ и $\neg \exists P(x) (Q(x, x_1, x_2, \dots, x_n)) = \forall P(x) (\neg Q(x, x_1, x_2, \dots, x_n))$

Выражения $\forall P(x)$ и $\exists P(x)$ называются *ограниченными кванторами общности и существования*, соответственно.

Задания для самостоятельной работы

1. Докажите, что $[-\frac{1}{n+1}, \frac{1}{n+1}] \subset (-\frac{1}{n}, \frac{1}{n})$ при любом натуральном n .
2. Найти множество $\mathcal{B}(A)$ всех подмножеств множества A , если
 - а) $A = \{1; 2; \{3\}\}$; б) $A = \{1; \{2; 3\}\}$; в) $A = \{\emptyset\}$.
3. Для произвольных высказываний X, Y и Z докажите равносильность высказываний
 - а) $X \Rightarrow Y$ и $\neg Y \Rightarrow \neg X$;
 - б) $X \Rightarrow (Y \Rightarrow Z)$ и $(X \Rightarrow Y) \Rightarrow (X \Rightarrow Z)$;
 - в) $X \& Y \vee \neg X \& Y \vee X \& \neg Y$ и $X \vee Y$.
4. Через A, B и C обозначены некоторые множества. Среди ниже приведённых равенств укажите верные и докажите их. Для неверных равенств обоснуйте свою точку зрения.
 - а) $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$; в) $(A \cap B) \setminus C = (A \setminus C) \cap (B \setminus C)$;
 - б) $C \setminus (A \cup B) = (C \setminus A) \cup (C \setminus B)$; г) $C \setminus (A \cap B) = (C \setminus A) \cap (C \setminus B)$.
5. Пользуясь свойствами операций, докажите, что
 - а) $\overline{\overline{A} \cup B} \cup B = A \cup B$; б) $\overline{\overline{A} \cap \overline{B}} = \overline{A} \cup (A \cap B)$.
6. Пусть $A = [-1, 4) \times [0, 2)$, $B = (-1, 1) \times \mathbf{R}$, $C = \mathbf{R} \times [-1, 1]$. Изобразите на координатной плоскости множества $A \cup B \cap \overline{C}$ и $(A \setminus B) \cap C$.
- 7.^T Рассмотрите предикаты, заданные на множестве натуральных чисел:
 - а) « x — нечетное число и для любого простого числа y выполнено неравенство $x \leq y$ »;
 - б) « x — простое число и для любого простого числа y выполнено неравенство $x \leq y$ ».

Для каждого из этих предикатов укажите все те значения аргумента x , для которого данный предикат истинен.

8. Пусть предикат $P(x, y)$ означает «фигура x вписана в фигуру y ». Пусть x пробегает множество всех треугольников, расположенных на некоторой плоскости, а y — множество всех окружностей на той же плоскости.

а) Для высказываний $\forall x \forall y (P(x, y))$, $\forall x \exists y (P(x, y))$, $\exists x \forall y (P(x, y))$, $\exists x \exists y (P(x, y))$, $\forall y \forall x (P(x, y))$, $\forall y \exists x (P(x, y))$, $\exists y \forall x (P(x, y))$, $\exists y \exists x (P(x, y))$ запишите каждое из них предложением русского языка.

б) ^T Определите, какие из этих высказываний истинны.

9. ^T Для каждого из приведенных ниже предикатов укажите свободные переменные.

а) $\forall x \exists y ((x + y = z) \& (z > 0) \vee (xz < y) \& (y < 0))$;

б) $\forall x ((x + y = z) \& (z > 0) \vee \exists y ((xz < y) \& (y < 0)))$;

в) $\forall x (\exists y ((x + y = z) \& (z > 0)) \vee \exists z ((xz < y) \& (y < 0)))$.

10. ^T Пусть область допустимых значений переменных x , y и z — множество целых чисел. Вычислите значение предиката

$$\forall x (\exists y ((x + y = z) \& (z > 0)) \vee \exists z ((xz < y) \& (y < 0)))$$

а) при $y = 0$ и $z = 1$;

в) при $y = -1$ и $z = 2$;

б) при $y = 1$ и $z = 0$;

г) при $y = -1$ и $z = -1$.

11. ^T Пусть $M(x, y, z)$ — предикат от трех переменных x , y , z , означающий, что точка y является серединой отрезка, концами которого служат точки x и z ; если же x и z совпадают (т. е. $x = z$), то $y = x$. Имеется ровно восемь вариантов связывания всех переменных x , y , z (в указанном порядке) кванторами общности и существования.

а) Вот три из этих вариантов: $\exists x \forall y \forall z (M(x, y, z))$; $\forall x \exists y \forall z (M(x, y, z))$; $\forall x \forall y \exists z (M(x, y, z))$. Укажите, какие из этих высказываний являются истинными.

б) Вот ещё три варианта: $\exists x \exists y \forall z (M(x, y, z))$; $\forall x \exists y \exists z (M(x, y, z))$; $\exists x \forall y \exists z (M(x, y, z))$. Укажите, какие из этих высказываний являются истинными.

12. Пусть $f(x)$ — некоторая функция, определённая на множестве действительных чисел.

а) Приведите пример функции $f(x)$, для которой истинно высказывание $\forall x > 0 \exists y > 0 (f(x) > f(y))$.

б) Постройте отрицание к высказыванию, записанному в пункте а), и приведите пример функции $f(x)$, для которой оно истинно.

13. ^T Найдите $\left(\bigcap_{n>2} \left(-\frac{1}{n}; 1 + \frac{1}{n} \right) \right) \setminus \left(\bigcup_{n>2} \left[\frac{1}{n}; 1 - \frac{1}{n} \right] \right)$.

Лекция 2. Графы

Теория графов, как и теория множеств, знает имя своего создателя – Леонард Эйлер. Именно он предложил для решения задачи о кёнигсбергских мостах использовать конфигурацию из точек, соединённых линиями. Желая узнать эту историю подробнее легко разыщут её в интернете.

Графы являются важным инструментом моделирования транспортных сетей, сетей трубопроводов, компьютерных сетей и вообще любых коммуникационных сетей.

Понятие графа. Простейшие свойства графов

Определение 2.1. *Неориентированным графом G называется пара множеств (V, E) , где V – множество вершин графа, а E – множество рёбер, каждое из которых представлено парой $\{u, v\}$, где $u, v \in V$.*

Обычно вершины неориентированного графа изображают точками, а рёбра – линиями, соединяющими какие-либо из этих точек. Разумеется, нам неважно, какой именно линией – прямой или кривой – соединяются вершины графа. При таком изображении отчётливо видно, что любое ребро описывается той парой вершин, которые оно соединяет. Вполне может случиться так, что ребро соединяет вершину саму с собой. Отметим ещё, что для неориентированного графа не важен порядок в указании вершин, которое данное ребро соединяет.

Далее везде будем писать $G = (V, E)$ и называть неориентированный граф просто графом. Кроме того, в этой лекции, да и в большинстве других, рассматриваются только конечные графы, т.е. такие, у которых множества V и E конечны.

На рисунке 1 в графе, изображённом слева, ребра e_2 и e_8 пересекаются, но точка их пересечения не является вершиной. В графе, изображённом справа, эти ребра нарисованы так, что они не пересекаются, но ясно, что обе картинki изображают один и тот же граф.

В русскоязычной литературе ребро e , соединяющее вершины u и v , чаще всего обозначают как (u, v) , а в англоязычной – принято обозначение uv . По умолчанию буква n используется для обозначения числа вершин графа, а m – для числа его рёбер.

Если ребро e соединяет вершины u и v , то говорят, что эти вершины *смежные*, а ребро e *инцидентно* вершинам u и v . На рисунке 1 вершины v_1 и v_2 смежные, а ребро e_2 им инцидентно.

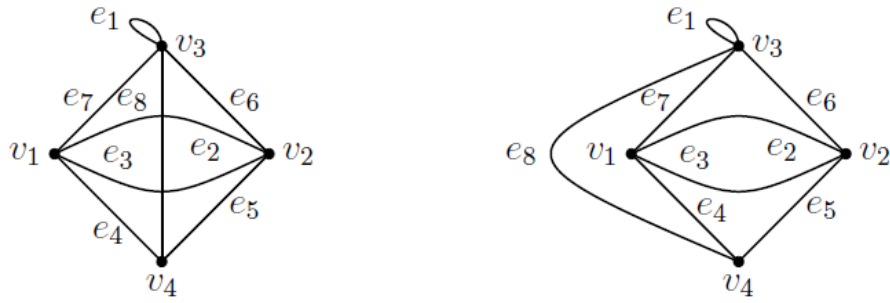


Рис. 1 Разные изображения одного графа

Ребра называются *кратными*, если они инцидентны одной и той же паре вершин.¹ Ребро, инцидентное ровно одной вершине, называется *петлёй*. На рисунке 1 ребра e_2 и e_3 кратные, а ребро e_1 является петлёй.

Степенью вершины называют количество инцидентных ей рёбер. Степень вершины v обозначают $\deg(v)$. При этом петля считается дважды, потому что она инцидентна этой вершине как одним своим концом, так и другим. Например, для графа на рисунке 1 $\deg(v_1) = \deg(v_2) = 4$, а $\deg(v_3) = 5$.

Одно из важных свойств любого графа сформулировано в следующей теореме.

Теорема 2.1. Сумма степеней всех вершин графа равна удвоенному количеству рёбер.

Доказательство. У каждого ребра, даже если это петля, есть две вершины – по одной на каждом его конце (для петли они просто совпали). Поэтому, находя сумму степеней вершин, мы каждое ребро подсчитываем дважды – один раз вершиной с одного конца ребра, другой раз вершиной с другого его конца. $\square$

Если $G = (V, E)$ – граф с m рёбрами, то утверждение теоремы можно записать следующей формулой:

$$\sum_{v \in V} \deg(v) = 2m.$$

Следствие 2.2. В любом графе число вершин нечетной степени чётно.

Доказательство. Пусть $G = (V, E)$ – произвольный граф, имеющий m рёбер. Обозначим через V_n множество вершин нечетной степени, а через V_c множество вершин четной степени. Тогда по теореме 2.1

$$2m = \sum_{v \in V} \deg(v) = \sum_{v \in V_c} \deg(v) + \sum_{v \in V_n} \deg(v),$$

где $\sum_{v \in V_c} \deg(v)$ – четное число. Следовательно, $\sum_{v \in V_n} \deg(v)$ также четно. Так как в $\sum_{v \in V_n} \deg(v)$ каждое слагаемое нечетно, то таких слагаемых должно быть

¹ При наличии кратных рёбер обозначение ребра его концами уже, конечно, невозможно. Но в данном вводном курсе графы с кратными ребрами будут встречаться редко, и в этих ситуациях будут даны соответствующие разъяснения.

четное число. □

Это утверждение обычно называют «Леммой о рукопожатиях». Такому названию она обязана следующему утверждению: в любой момент времени число людей, совершивших нечётное число рукопожатий, чётно.



Объясните этот феномен человеческих отношений.

Маршруты в графе и связность

Определение 2.2. *Маршрутом* в графе $G = (V, E)$ называется последовательность вершин и рёбер $v_0, e_1, v_1, v_2, \dots, v_{n-1}, e_n, v_n$ такая, что ребро e_i инцидентно вершинам v_{i-1} и v_i для всех $1 \leq i \leq n$. При этом вершина v_0 называется *начальной*, а v_n — *конечной*. Маршрут, в котором начальная и конечная вершины совпадают, называется *циклом*.

Договариваются также, что одна отдельно взятая вершина тоже является маршрутом, который начинается и заканчивается в этой вершине (не путайте с маршрутом, который состоит из вершины, петли и той же вершины!).

Если некоторый маршрут является циклом, то ясно, что в качестве начальной вершины можно выбрать любую из вершин этого маршрута. Мы далее будем считать, что все такие маршруты представляют один и тот же цикл.

Посмотрите на граф, изображенный на рисунке 2 (на цветовое различие рёбер и вершин пока внимания не обращайте). В нём есть несколько маршрутов из вершины v_1 в v_2 . Это, например, маршрут p_1 , равный v_1, e_1, v_2 , а также маршрут p_2 , равный $v_1, e_2, v_3, e_4, v_4, e_6, v_5, e_5, v_3, e_4, v_4, e_3, v_2$. В маршруте p_2 выделенные жирным шрифтом вершины и ребра повторяются. В обычной жизни при поиске пути из одного пункта в другой маршруты с повторяющимися вершинами и рёбрами, как правило, не рассматриваются.

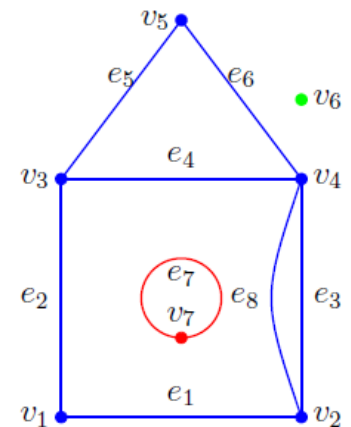


Рис. 2

Определение 2.3. *Длиной маршрута* называется количество входящих в него рёбер.

Например, маршрут p_3 , равный $v_4, e_8, v_2, e_3, v_4, e_6, v_5$, имеет длину 3.

Определение 2.4. *Цепью* называется маршрут, в котором любое его ребро входит ровно один раз. *Путем* (или *простой цепью*) называется цепь, в которой нет повторяющихся вершин.

Например, на рисунке 2 маршрут p_3 , равный $v_4, e_8, v_2, e_3, v_4, e_6, v_5$ является цепью и не является путем. Маршрут p_1 из примера выше является путем.



Что нужно сделать, чтобы превратить маршруты p_2 и p_3 в пути?

Лемма 2.3. Если в графе G есть маршрут из вершины u в вершину v , то существует и путь из вершины u в вершину v .

Доказательство. Из всех маршрутов из вершины u в вершину v выберем маршрут наименьшей длины (если таких несколько, возьмём любой из них). Покажем, что этот маршрут является путём. Допустим, что это не так. Тогда есть вершина w , которая на этом маршруте встречается, по крайней мере, дважды. Рассмотрим первое появление этой вершины на маршруте при движении от вершины u и её последнее появление. Тогда весь фрагмент маршрута от первого появления вершины w на маршруте до её последнего появления может быть удалён из маршрута, а вершина w обозначена на маршруте только один раз (в месте «склейки» двух частей маршрута). Получился маршрут из вершины u в вершину v меньшей длины, что противоречит исходному выбору маршрута. $\square$

Отметим, что в любом конечном графе обязательно существует самый длинный путь, а вот самого длинного маршрута может не существовать.

Определение 2.5. Цикл называется простым, если каждая его вершина (за исключением той, которая в записи цикла назначена начальной и конечной) содержится в нём один раз.

На рисунке 2 маршрут $v_4, e_3, v_2, e_8, v_4, e_4, v_3, e_5, v_5, e_6, v_4$ является циклом, который состоит из двух простых циклов v_4, e_3, v_2, e_8, v_4 и $v_4, e_4, v_3, e_5, v_5, e_6, v_4$.

Если граф моделирует какую-либо городскую транспортную сеть, то дорожное происшествие на какой-либо узкой улице блокирует движение по ней транспорта. Тем самым из графа надо удалить соответствующее ребро. Хуже, если это произошло на перекрёстке: тогда из графа надо удалить не только вершину, обозначающую перекрёсток, но и все инцидентные ей рёбра.

Пусть $G = (V, E)$ – граф, e – его ребро. Про граф $G' = (V, E \setminus \{e\})$ говорят, что он получен из графа G удалением ребра e . Результат такой операции над графом G обозначают $G - e$.

Пусть $G = (V, E)$ – граф, v – его вершина. Про граф G'' говорят, что он получен из графа G удалением вершины v , если множество его вершин равно $V \setminus \{v\}$, а множество рёбер получено удалением из E всех рёбер, инцидентных вершине v . Результат такой операции над графом G обозначают $G - v$.

Более общая ситуация описывается следующим определением.

Определение 2.6. Пусть $G = (V, E)$ – граф. Граф $G' = (V', E')$ называется подграфом графа G , если

- 1) $V' \subseteq V$;
- 2) $E' \subseteq E$;
- 3) если $e = \{u, v\} \in E'$, то $u, v \in V'$.

Ясно, что графы $G - e$ и $G - v$ являются подграфами графа G . Нетрудно понять, что любой подграф может быть получен из исходного графа некоторой последовательностью применения операций удаления вершин и рёбер.



Пусть G – граф, изображенный на рисунке 2. Изобразите граф $((G - v_7) - e_5) - e_6) - e_8$.

Нетрудно понять, что любой маршрут в графе является подграфом.

Для любой транспортной сети весьма желательно, чтобы из любой точки можно было проехать в любую другую точки этой сети. Иными словами, граф такой сети должен обладать так называемым свойством связности.

Определение 2.7. Вершина u графа G *связана* с вершиной v , если существует маршрут из u в v .

В силу высказанной ранее договорённости каждая вершина всегда связана сама с собой. Также отметим, что если в графе существует маршрут из u в v , то, конечно же, существует маршрут из v в u (надо просто маршрут из u в v записать в обратном порядке). Значит, если вершина u связана с вершиной v , то и вершина v связана с вершиной u . Кроме того, если вершина u связана с вершиной v , а вершина v связана с вершиной w , то маршрут от вершины u до вершины v можно продолжить до вершины w , просто приписав к нему маршрут от v до w . Значит, в этом случае вершина u связана с вершиной w .

Определение 2.8. Граф называется *связным*, если любые две его вершины связаны.

Иными словами, граф *связен*, если существует путь из любой его вершины в любую другую.

Рассмотрите ещё раз граф, изображённый на рисунке 2. Он не *связен*. Но у него есть подграфы, которые *связны*: скажем, подграф, изображенный синим цветом. А ни одна из оставшихся двух вершин не связана с какой-либо вершиной этого подграфа.

Определение 2.9. Пусть $G = (V, E)$ – граф. Его подграф $G' = (V', E')$ называется *компонентой связности* графа G , если G' *связен*, каждое ребро,

инцидентное вершинам из V' , принадлежит E' и для любых вершин $u \in V'$ и $v \in V \setminus V'$ в графе G нет маршрута из u в v .

У графа на рисунке 2 три компоненты связности; они обозначены синим, красным и зелёным цветами. Красная и зеленая компоненты связности содержат ровно одну вершину, такие вершины называются *изолированными*. В некоторых алгоритмах, с которыми вы дальше будете иметь дело, требуется, чтобы рассматриваемый граф был связным. Но такие алгоритмы можно применять для произвольных, не обязательно связных графов, сведя задачу к рассмотрению каждой конкретной компоненты связности графа.

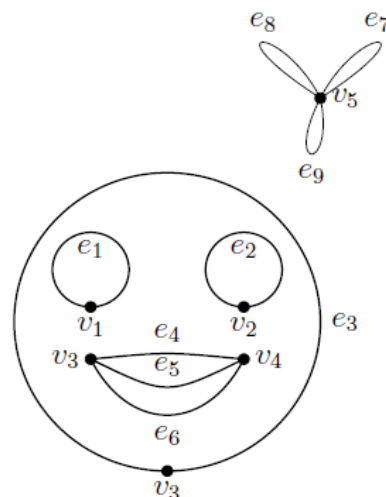


Рис. 3

У графа, изображенного на рисунке 3, найдите компоненты связности, а также укажите кратные рёбра и петли.

Обыкновенные графы и деревья

В задачах поиска пути важным является сам факт наличия ребра между двумя вершинами, поэтому в таких задачах имеет смысл рассматривать граф без кратных рёбер и петель.

Определение 2.10. Граф без петель и кратных рёбер называется *обыкновенным*.

Пусть в обыкновенном графе n вершин. Минимальное число рёбер в таком графе равно нулю, соответствующий граф состоит из n изолированных вершин. Он называется *пустым* графом и обозначается через O_n . В таком графе любые две вершины не смежны, так что он имеет n компонент связности.

Обыкновенный граф с n вершинами, любые две вершины которого смежны, называется *полным* графом и обозначается K_n . На рисунке 4 изображен граф K_5 .

Граф K_n , очевидно, связан. Нетрудно понять, что любой другой обыкновенный граф, имеющий n вершин, можно получить из K_n удалением некоторого числа рёбер.

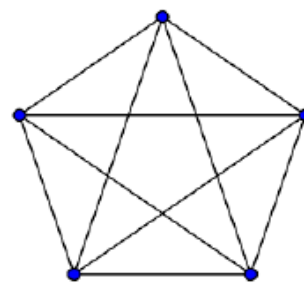


Рис. 4. Граф K_5 .

Используя теорему 2.1, нетрудно подсчитать количество рёбер в графе K_n . Степень каждой вершины равна $n - 1$, всего n вершин, значит, $n(n - 1) = 2m$, откуда $m = \frac{n(n-1)}{2}$.

Пусть имеется некоторый обыкновенный связный граф. Тогда при удалении некоторого числа рёбер может получиться некоторый «экстремальный» связный граф, в котором при удалении любого ребра он перестанет быть связным. Такие графы имеют специальное название и обладают интересными свойствами.

Определение 2.11. Связный граф без циклов называется *деревом*.

Три дерева изображены на рисунке 5.



Рис. 5. Молекула этана C_2H_6 и деревья с одной и двумя вершинами.

У графа без циклов (необязательно связного) каждая компонента связности – дерево, то есть граф без циклов – это набор деревьев, и называется такой граф, естественно, *лесом*.

Отметим важные свойства деревьев.

Теорема 2.4. Пусть G – дерево.

- 1) G – обыкновенный граф;
- 2) для любой пары вершин графа G существует и притом единственный путь, соединяющий эти две вершины;
- 3) если в графе G удалить ребро, то он перестанет быть связным;
- 4) если в графе G добавить одно ребро, то появится единственный цикл.

Доказательство. Утверждение 1 очевидно, так как петля является циклом длины 1, а пара кратных рёбер – циклом длины 2.

Благодаря пункту 1 каждая пара смежных вершин дерева однозначно определяет соединяющее их ребро. Поэтому, записывая для дерева тот или иной путь, нам достаточно фиксировать только последовательность вершин.

Пусть u, v – две различные вершины дерева. Так как граф связан, то по лемме 2.3 существует путь из u в v . Допустим, что существуют два различных пути p_1 и p_2 из u в v . Вершина u является общей для путей p_1 и p_2 . Возможно, что для них существуют другие общие вершины, поэтому обозначим через w_1 вершину, для которой путь из u в w_1 является наидлиннейшей общей частью

путей p_1 и p_2 . Через w_2 обозначим следующую общую вершину путей p_1 и p_2 на пути из w_1 в v (такая существует, так как v – общая вершина). Следовательно, вершины w_1 и w_2 различны, и в графе существует два непересекающихся пути из w_1 в w_2 , которые вместе образуют цикл. Полученное противоречие доказывает утверждение 2 этой теоремы.

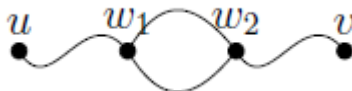


Рис. 6. К доказательству утверждения 2 теоремы 2.4.

Для доказательства утверждения 3 рассмотрим произвольное ребро $e = \{u, v\}$. В дереве, согласно утверждению 2, существует единственный путь из u в v . Очевидно, это путь u, e, v . Рассмотрим граф $G - e$ и предположим, что он связан. Тогда в нём существует путь p из вершины u в v , не содержащий ребра e . Заметим, что p также является путем в графе G . Значит, в дереве G нашлись два пути из u в v , что противоречит утверждению 2.

Перейдем к доказательству утверждения 4. Рассмотрим граф G' , полученный из дерева G добавлением нового ребра e , инцидентного вершинам u и v . В графе G существует путь из u в v , который, конечно, не содержит ребро e . Тогда при добавлении к этому пути ребра e мы получаем цикл в графе G' .

Допустим, что в графе G' существует два различных цикла C_1 и C_2 . Отметим, что оба эти цикла содержат ребро e , так как в противном случае в дереве $G = G' - e$ уже был бы цикл. Пусть $p_1 = C_1 - e$, $p_2 = C_2 - e$, тогда p_1 и p_2 – два различных пути из u в v в дереве G . Получено противоречие. $\square$

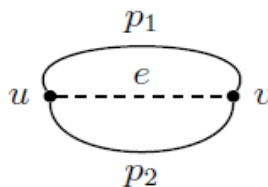


Рис. 7. К доказательству утверждения 4 теоремы 2.4.

Так как в дереве существует единственный путь между любыми двумя вершинами, то назовем *расстоянием* между ними длину этого пути.

На рисунке 8 два изображения одного и того же дерева. Картинка справа называется *корневым изображением* дерева или *подвешенным деревом*. Подобное изображение знакомо любому, кто пользовался проводником Windows. В большинстве алгоритмов, которые используют деревья, под деревом как раз подразумевают подвешенное дерево. Вершина v_3 здесь – *корень* дерева, она находится на расстоянии 0 от самой себя, поэтому будем считать, что она на нулевом уровне дерева. На следующем уровне изображены все

вершины, которые непосредственно смежны с корнем, на уровне 2 – те, которые находятся на расстоянии два от корня и т. д. Вершины степени один такие, как v_1, v_6, v_9 , называются *листьями*. Наибольшее из расстояний от корня до листьев называется *высотой* дерева, она совпадает с количеством уровней в корневом изображении. Высота дерева, изображенного на рисунке 8 равна 3.

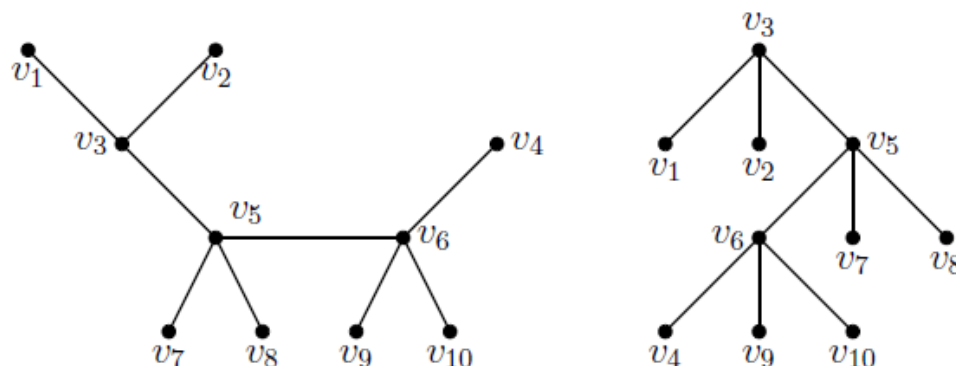


Рис. 8. Дерево и его корневое изображение из вершины v_3 .

Из свойств корневого изображения дерева следует еще один примечательный факт о деревьях.

Теорема 2.5. Пусть G – дерево, имеющее n вершин и m рёбер. Тогда $m = n - 1$.

Доказательство. Рассмотрим корневое изображение дерева G с произвольным корнем, имеющее высоту h . Тогда пусть n_s – число вершин на уровне s , причем $n_0 = 1$. Заметим, что каждая вершина на уровне s смежна ровно с одной вершиной с предыдущего уровня, поэтому $n_1 + n_2 + \dots + n_h = m$. Сумма слева равна $n - n_0 = n - 1$, откуда $m = n - 1$. $\square$

Следствие 2.6. Минимальное число рёбер в связном графе с n вершинами равно $n - 1$.

Двудольные графы

Каждый болельщик футбола знает, что у футболистов есть право, определённое его контрактом, выбирать клуб, за который он будет играть в том или ином сезоне. В итоге между множествами футболистов и клубов складываются отношения, которые на языке графов можно выразить так: множество вершин разбито на два подмножества – футболистов и клубов – и каждая вершина первого подмножества соединена ребром с теми вершинами второго подмножества, которые обозначают клубы, за который когда-нибудь играл этот футболист. Мы не приводим получающуюся картинку, поскольку

футболистов и клубов слишком много, чтобы они могли уместиться хотя бы на одной странице данного пособия.

Подобные ситуации отношений между объектами разного вида возникают довольно часто, поэтому такого типа графы заслуживают внимания.

Определение 2.12. Граф $G = (V, E)$ называется *двудольным*, если множество его вершин можно разбить на два непустых непересекающихся подмножества X и Y , называемых *долями*, так, что если вершины в графе G смежны, то они принадлежат разным долям.

Двудольные графы обозначают также $G = (X, Y, E)$.



Могут ли в двудольном графе быть петли? А кратные ребра?

Обыкновенный двудольный граф, у которого каждая вершина одной доли смежна со всеми вершинами другой доли, называется *полным двудольным графом*. Полный двудольный граф, доли которого содержат r и s вершин обозначают $K_{r,s}$.

Доли двудольного графа принято изображать либо вертикальными рядами, либо одну над другой (рис. 9).

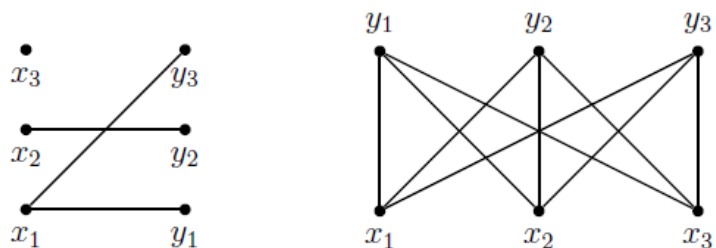


Рис. 9. Некоторый двудольный граф и полный двудольный граф $K_{3,3}$.

Отметим, что если в графе, изображённом на рисунке 9 слева, долями считать множества $\{x_1, x_2\}$ и $\{x_3, y_1, y_2, y_3\}$, то соответствующий граф также будет двудольным. Справа на рисунке изображен граф $K_{3,3}$, который еще называют «три дома, три колодца». Это название возникло в связи со следующей задачей. На некотором участке есть три дома и три колодца. Можно ли проложить по дорожки от каждого дома к каждому колодцу так, чтобы никакие две дорожки не пересекались? Иными словами, можно ли граф $K_{3,3}$ изобразить так, чтобы его рёбра не пересекались нигде, кроме вершин? Ответ отрицательный, но это совсем другая история, выходящая за рамки нашего вводного курса.



Подсчитайте, сколько рёбер в графе $K_{r,s}$.

Ориентированные графы

До сих пор мы считали, что если в графе есть ребро $e = \{u, v\}$, то по нему можно пройти как от вершины u к v , так и наоборот. Но в жизни бывает так, что одно из направлений закрыто (например, в городе одностороннее движение по улице, невозможно начать разработку проекта без сформулированного на него технического задания и т. п.). В этом случае можно считать, что у ребра есть направление или, по-другому, ориентация.

Определение 2.13. *Ориентированным графом G называется пара (V, E) , где V – множество вершин, а E – множество рёбер вида $(u, v) \in V \times V$.*

Для рёбер ориентированного графа применяют и другое обозначение: $\overrightarrow{uv}$. Для краткости ориентированный граф часто называют *орграфом*.

Пусть $e = (u, v) \in E$, тогда говорят, что ребро e *выходит* из вершины u и *заходит* в вершину v . Соответственно, у каждой вершины есть две степени: *степень исхода*, обозначаемая $\overrightarrow{\deg}(u)$ или $\deg^-(u)$, – это число рёбер, выходящих из вершины u , и *степень захода*, обозначаемая

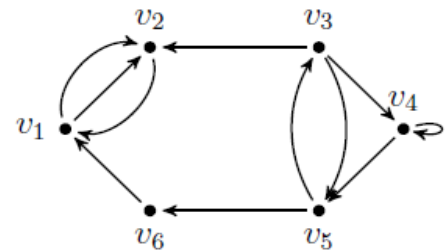


Рис. 10. Орграф

$\overleftarrow{\deg}(v)$ или $\deg^+(v)$, – это число рёбер, входящих в вершину v .

Для орграфов выполняется утверждение, аналогичное теореме 2.1.

Теорема 2.7. Сумма степеней исхода всех вершин орграфа равна сумме степеней захода всех его вершин.



Докажите теорему 2.7 самостоятельно.

Утверждение теоремы 2.7 можно записать следующей формулой:

$$\sum_{v \in V} \overrightarrow{\deg}(v) = \sum_{v \in V} \overleftarrow{\deg}(v).$$

Определение подграфа ориентированного графа почти дословно повторяет соответствующее определение для неориентированного.



Сформулируйте это определение.

Определение маршрута, который в этом случае называется *ормаршрутом*, аналогично неориентированному случаю: это последовательность вершин и рёбер $v_0, e_1, v_2, \dots, v_{n-1}, e_n, v_n$, где каждое ребро e_i выходит из вершины v_{i-1} и заходит в вершину v_i для всех $1 \leq i \leq n$. Для пути соответствующий термин *орпуть*, для цикла – *орцикл* или, по-другому, *контур*.

В то же время для неориентированных и ориентированных графов принципиально отличаются понятие связности. Мысленно уберите ориентацию рёбер у орграфа на рисунке 10, и соответствующий неориентированный граф окажется связным. Однако в исходном орграфе есть орпуть v_4 в v_1 , но нет орпути из v_1 в v_4 . В этом причина появления для орграфов понятия сильной связности.

Определение 2.14. Вершины u и v орграфа G называются *сильно связанными*, если существуют ормаршруты из u в v и из v в u . Договоримся также считать, что каждая вершина сильно связана сама с собой.

На рисунке 10 вершины v_1 и v_2 сильно связаны, а вершина v_6 сильно связана только сама с собой.



Докажите, что для сильно связанных вершин u и v существуют орпути из u в v и из v в u .

Определение 2.15. Орграф называется *сильно связным*, если любые две его вершины сильно связаны.

Если орграф не является сильно связным, то в нём можно выделить несколько компонент сильной связности.

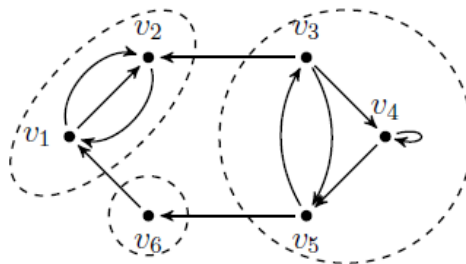


Рис. 11. Компоненты сильной связности в орграфе

Определение 2.16. Пусть $G = (V, E)$ – орграф. Его подграф $G' = (V', E')$ называется *компонентой сильной связности* графа G , если G' сильно связан, каждое ребро, инцидентное вершинам из V' , принадлежит E' и существует вершина $u \in V'$ такая, что для любой вершины $v \in V \setminus V'$ в графе G нет ормаршрута из u в v или из v в u .

На рисунке 11 каждая компонента сильной связности обведена пунктирной линией.

Есть ещё одно принципиальное отличие компонент связности неориентированного графа от компонент сильной связности орграфа. Теоретико-множественное объединение компонент связности неориентированного графа совпадает со всем исходным графом, а для

компонент сильной связности орграфа это, как правило, оказывается не так (см. рис. 11).

Представление графа матрицей смежности

Изображение графа рисунком удобно для восприятия человеком. Однако, если для решения задачи надо применить компьютер, такой способ представления уже малопригоден. Поэтому используют другие способы представления графов. Здесь мы расскажем только об одном из них.

Пусть у нас имеется некоторый орграф, имеющий n вершин $v_1, v_2, \dots, v_n$. Составим для него таблицу, имеющую n строк и n столбцов по следующему правилу: если в орграфе есть ребро (v_i, v_j) , то в клетке таблицы, стоящей на пересечении i -й строки и j -го столбца, пишется 1, в остальных клетках таблицы пишутся нули. Получившаяся таблица называется *матрицей смежности* данного орграфа (но в отличие от таблицы в матрице нет линий, расчерчивающей её на клетки, а сама матрица обычно заключается в круглые скобки).

Если имеются кратные рёбра (как, например, у орграфа на рисунке 10), то в матрице смежности в соответствующем месте пишут не 1, а количество ребер. Так, для орграфа на рисунке 10 матрица смежности выглядит следующим образом:

$$\begin{pmatrix} 0 & 2 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$



Составьте матрицу смежности для орграфа, изображённого на рисунке 11.

Если граф неориентированный, то для него матрица смежности строится так, как если бы каждое его ребро представляло два противоположно ориентированных ребра. У неориентированного графа матрица смежности всегда симметрична относительно диагонали, идущей из левого верхнего угла в правый нижний. Эту диагональ матрицы называют *главной*.



Составьте матрицу смежности для графа, изображённого на рисунке 2.

Раз уж зашла речь о матрицах, дадим общее определение.

Определение 2.16. *Матрицей* над множеством M называется прямоугольная таблица, составленная из элементов множества M . Если в матрице m строк и n

столбцов, то говорят, что матрица имеет размеры $m \times n$. Если $m = n$, то матрица называется *квадратной*.

Элементы матрицы обозначаются обычно малыми латинскими буквами с индексами: первый индекс – это номер строки, в которой расположен элемент множества M , второй – номер столбца, в котором расположен этот элемент. Например, a_{ij} . Часто в этом случае говорят, что элемент располагается на пересечении i -й строки и j -го столбца.

Задания для самостоятельной работы

1. Пусть $\mathcal{B}(A)$ — множество всех подмножеств трехэлементного множества $A = \{1; 2; 3\}$.

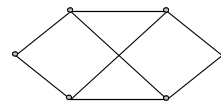
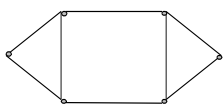
а) Изобразите граф, вершинами которого являются элементы $\mathcal{B}(A)$, причем вершины X и Y соединены ребром тогда и только тогда, когда $X \cap Y = \emptyset$.

б)^T Составьте список степеней вершин графа, построенного в пункте а).

2. Существует ли связный граф с 5-ю вершинами и следующим распределением степеней вершин а) 0, 1, 2, 3, 4; б) 1, 1, 2, 3, 4; в) 1, 1, 2, 2, 4; г) 1, 1, 2, 3, 3? При ответе «Да», надо предъявить изображение такого графа, ответ «Нет» надо обосновать.

3. Выясните, одинаковы ли графы, изображенные на рис. 13 а); на рис. 13 б). (В каждом графе 6 вершин, обозначенных точками на концах рёбер, пересечения рёбер вершинами не считаются.)

а)



б)

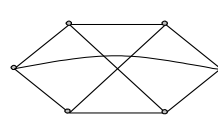
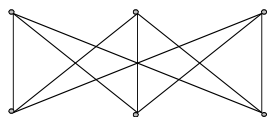


Рис. 12. Графы к заданию 3

4. Может ли в государстве, в котором из каждого города выходит ровно три дороги, быть ровно 100 дорог?

5.^T Ученые двух стран, Пингвинии и Дельфинии, переписываются между собой. Каждый пингвинский ученый переписывается с тремя дельфинскими, а

каждый дельфинский — с четырьмя пингвинскими. В Пингвинии 1000 ученых. Сколько ученых в Дельфинии?

6. Изобразите все различные деревья, имеющие а) 5 вершин; б) 6 вершин.

7. Сколько рёбер в лесе, имеющем n вершин и k компонент связности?

8.^T В некотором государстве 2000 городов. Решено соединить их непересекающимися дорогами так, чтобы из каждого города можно было проехать в любой другой, возможно проезжая при этом через несколько других городов. Какое наименьшее число дорог нужно проложить?

9. Пусть $V = \{2; 3; 4; 6; 8; 9\}$. Элементы a и b из V соединены ребром, идущим от a к b , если $a - b \in V$.

а) Изобразите полученный орграф, рассматривая V как множество его вершин.

б)^T Укажите степени захода и исхода для каждой вершины этого графа.

10. Пусть $\mathcal{B}(A)$ — множество всех подмножеств трехэлементного множества $A = \{1; 2; 3\}$.

а) Изобразите граф, вершинами которого являются элементы $\mathcal{B}(A)$, причем вершины X и Y соединены ребром тогда и только тогда, когда $X \subseteq Y$.

б)^T Укажите степени захода и исхода для каждой вершины этого графа.

11.^T Укажите компоненты сильной связности следующих орграфов, перечислив для каждой из них входящие в неё вершины.

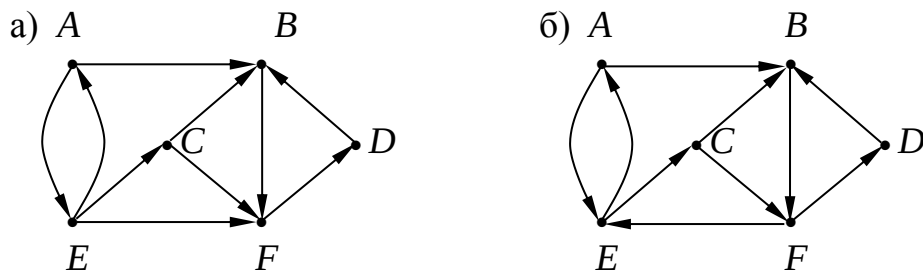


Рис. 13. Графы к заданию 11

12. Изобразите орграф, заданный следующей матрицей смежности:

$$\begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 2 & 0 & 1 \\ 2 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 2 & 0 \\ 0 & 1 & 0 & 3 & 0 \end{pmatrix}.$$

Лекция 3. Бинарные и другие отношения

Мы уже обсудили, что множества играют фундаментальную роль в самой математике и многообразных её приложениях. Однако описывая окружающий мир, мы не только перечисляем интересующие нас объекты, т.е. задаём множество, но и указываем отношения, которыми эти объекты могут быть связаны. Такие связи могут быть весьма разнообразными, но мы начнем с наиболее общего представления об отношениях элементов множеств.

В отношениях могут находиться элементы самых разнообразных множеств. Например, могут быть родственные отношения между людьми, скажем, один человек другому является братом; между числами – одно число меньше другого; между геометрическими объектами – некоторая точка принадлежит той или иной прямой и т.д.

Совсем не обязательно, чтобы отношение связывало равно два объекта – человека с человеком, число с числом, точку и прямую. Например, отношение точка A лежит между точками B и C связывает, как мы видим, 3 объекта.



Придумайте ещё примеры отношений, которые связывают а) два объекта, б) три объекта; в) четыре объекта.

Определение отношения

Как нередко фиксируются отношения в обыденной жизни? Например, что два человека стали мужем и женой. Идут в ЗАГС, и там им выдают бумагу, в которой так и написано, что эти два человека – муж и жена. Как фиксируется, что такой-то является сыном или дочерью таких-то двух человек? То же самое – выдаётся бумага, в которой фигурируют эти три человека. Как фиксируется, что данный человек принят на работу в такое-то предприятие? Заключается договор между этим человеком и уполномоченным представителем предприятия. Что общего во всех этих примерах? В каждом из них просто фиксируется, кто именно (или что именно) находится в рассматриваемом отношении. Если отвлечься от того, о чём эти отношения, то становится понятно, что задать отношение – это записать те объекты, которые находятся в данном отношении. Такую запись удобно представлять кортежем, а список всех таких записей и есть описание данного отношения. Каждый кортеж в свою очередь – это элемент декартова произведения тех множеств, откуда берутся элементы кортежа. Тем самым мы приходим к следующему определению.

Определение 3.1. Пусть $M_1, M_2, \dots, M_n$ – некоторые множества. *Отношением* на совокупности этих множеств называется любое подмножество декартова произведения этих множеств. Если $M_1 = M_2 = \dots = M_n = M$, то говорят об отношении на множестве M .

Определение 3.2. Количество множителей в декартовом произведении (т.е. количество компонентов в каждом кортеже) называют *арностью*, или *местностью*, данного отношения.

Таким образом, отношения бывают двуместные, или бинарные, трёместные, четырёхместные и т.д. Отношение «меньше» на множестве чисел бинарное, отношение «точка лежит внутри треугольника» тоже бинарное на совокупности из двух множеств – множества точек и множества треугольников; отношение «лежать между» на множестве точек трёместное, отношение «четыре точки лежат на одной окружности» на множестве точек плоскости четырёхместное.

Определите арность отношений

- а) точки A, B и C лежат на одной прямой;
- б) точки A, B и C лежат на прямой l .

Отношение мы будем обычно обозначать буквой R (от английского relation – отношение). Тогда факт, что некоторая совокупность объектов $a_1, a_2, \dots, a_n$ находится в отношении R , можно записать так: $(a_1, a_2, \dots, a_n) \in R$. Правда, такая запись довольно непривычна для бинарных отношений – никто не пишет $(x, y) \in <$ для чисел x и y (здесь символ $<$ – стандартное обозначение отношения «меньше»), или $(l, m) \in \parallel$ для прямых l и m (здесь символ $\parallel$ – стандартное обозначение отношения «быть параллельными»). Все привыкли писать $x < y$ и $l \parallel m$. Поэтому и мы для бинарных отношений позволим себе (и вам) писать $a_1 R a_2$.

Можно ли, по вашему мнению, говорить об унарном (одноместном) отношении? Если нет, то почему, Если да, то как понимать, что означает такое отношение.

Среди всевозможных отношений на совокупности множеств $M_1, M_2, \dots, M_n$ есть два особых отношения. Одно из них совпадает с $M_1 \times M_2 \times \dots \times M_n$ и называется *универсальным*, другое – пустое множество, которое естественно называть *пустым* отношением.

Поскольку отношение – это по определению некоторое множество, то его можно задавать так же, как задают множества: списком или с указанием свойства. По существу задание отношения списком мы обсудили, когда вводили само понятие отношения. Ясно, что такой способ продуктивен, когда множества, на которых рассматривается отношение, конечны. Если же среди множеств имеются бесконечные, то в этом случае отношение задаётся свойством. На самом деле с этим вариантом задания отношения мы тоже уже встречались: отношение «меньше» на множестве чисел списком не задашь и отношение «лежать между» на множестве точек плоскости тоже.



На числовой прямой заданы точки с координатами $-2, 0, 3, 5, 8$. Отношение R на множестве, состоящем из этих точек, задано свойством: $(x, y, z) \in R$, если точка с координатой y лежит строго между точками с координатами x и z . Запишите отношение R списком.

Операции над отношениями

Поскольку отношения – это подмножества $M_1 \times M_2 \times \dots \times M_n$, для них определены теоретико-множественные операции объединения и пересечения. Они называются соответственно операциями *объединения* и *пересечения* отношений. Можно также брать дополнение заданного отношения до универсального отношения. Обозначения этих операций такие же, как и для любых множеств.



На множестве прямых в пространстве заданы следующие бинарные отношения: $(l, m) \in R_1$, если прямые l и m параллельны; $(l, m) \in R_2$, если прямые l и m пересекаются. Каким общим свойством на множестве всех прямых пространства можно описать отношение $R_1 \cup R_2$? Каким общим свойством на множестве всех прямых пространства можно описать отношение $\overline{R_1} \cap \overline{R_2}$

Для отношений определена ещё одна особая операция, которую принято называть произведением отношений.

Определение 3.3. Пусть отношение $R_1 \subseteq L_1 \times L_2 \times \dots \times L_k \times M_1 \times M_2 \times \dots \times M_s$, а отношение $R_2 \subseteq M_1 \times M_2 \times \dots \times M_s \times N_1 \times N_2 \times \dots \times N_t$. Тогда отношение $R_3 \subseteq L_1 \times L_2 \times \dots \times L_k \times N_1 \times N_2 \times \dots \times N_t$ называется *произведением* отношений R_1 и R_2 , если кортеж $(a_1, a_2, \dots, a_k, c_1, c_2, \dots, c_t) \in R_3$ в том и только том случае, когда существуют такие элементы $b_1 \in M_1, b_2 \in M_2, \dots, b_s \in M_s$, для которых

$(a_1, a_2, \dots, a_k, b_1, b_2, \dots, b_s) \in R_1$ и $(b_1, b_2, \dots, b_s, c_1, c_2, \dots, c_t) \in R_2$. Множества $M_1, M_2, \dots, M_s$ называются *связывающими* отношения R_1 и R_2 . Если связывающие множества отсутствуют, произведение R_1 и R_2 совпадает с $R_1 \times R_2$.

Операцию умножения отношений будем обозначать символом $\circ$. Из определения произведения отношений видно, что произведение отношения арности $k + s$ на отношение арности $s + t$ даёт отношение арности $k + t$.

Множества $M_1 = M_2 = M_3 = \{-2, 0, 3, 5, 8\}$. Отношения $R_1 \subseteq M_1 \times M_2 \times M_3$ и $R_2 \subseteq M_2 \times M_3 \times M_1$ заданы свойством: $(x, y, z) \in R_i, i \in \{1; 2\}$, если $x < y < z$.

а) Вычислите произведение $R_1 \circ R_2$, если связывающие множества – это M_2 и M_3 . Каким свойством задано отношение $R_1 \circ R_2$?

б) Вычислите произведение $R_2 \circ R_1$, если связывающее множество – это M_1 .

Из недавнего прошлого в довольно скорое будущее: несколько слов о базах данных

Раз вы учитесь на компьютерной специальности, значит, ещё недавно сдавали ЕГЭ по информатике. Есть там задание 4, которое начинается словами: «Ниже представлены два фрагмента таблиц из базы данных о...». Нам не так уж важно, о чём эта база данных. Допустим, это база данных некоторого оператора сотовой связи. Одна из таблиц этой базы вполне может выглядеть так:

Номер звонившего	Дата звонка	Код региона	Продолжительность звонка
111-22-33	01.01.2020	77	7
111-22-33	02.01.2020	28	9
111-33-44	01.01.2020	13	20
111-33-44	02.01.2020	66	17
111-33-44	02.01.2020	77	7
111-33-45	01.01.2020	13	11
...	...	...	...

Таких номеров телефонов, конечно, не существует, так что нас нельзя

обвинить в разглашении персональных данных.

Данная таблица фактически представляет собой четырёхместное отношение: каждая строка – это кортеж из $M_1 \times M_2 \times M_3 \times M_4$, где M_1 – множество телефонных номеров, M_2 – множество дат, M_3 – множество кодов субъектов РФ и зарубежных стран, M_4 – множество натуральных чисел.

Эта таблица постоянно обновляется: в неё добавляются новые строки, а какие-то по истечению срока хранения (например, месяца) удаляются. Но есть таблицы, т.е. отношения, которые в меньшей степени подвержены изменениям. Скажем, такая:

Фамилия И.О.	Номер телефона
Иванов М.С.	111-22-33
Иванов М.С.	111-33-45
Петров К.Л.	111-33-44
...	...

Ясно, что эта информация хранится столько времени, сколько данный абонент будет клиентом данного оператора.

Как получить информацию, сколько времени суммарно Иванов пользовался услугами данного оператора? Ясно, что надо перемножить эти два отношения по связывающему множеству «Номер телефона».

Конечно, теория баз данных не сводится к использованию операции умножения многоместных отношений. В ней используются и другие операции, но это всё равно некоторые операции над отношениями.

Частный случай: бинарные отношения. Свойства бинарных отношений

Бинарные отношения занимают особое место среди всех отношений, поскольку многие из наиболее важных отношений бинарные. Даже среди рассмотренных выше примеров бинарных отношений больше, чем отношений других арностей. Напомним, что для бинарных отношений мы договорились записывать символ отношения между элементами, находящимися в данном отношении. Запись aRb обычно читают «элемент a находится в отношении R с элементом b ». Например, запись $a < b$ читают «число a меньше числа b ». ☺

Как и отношение произвольной арности, бинарные отношения можно задавать списком или указанием свойства. Но для бинарных отношений есть и другие

способы задания. Например, бинарное отношение $R \subseteq A \times B$ можно изобразить двудольным орграфом: стрелка, ведущая из вершины a_i в вершину b_j , означает, что $a_i R b_j$. Нетрудно понять, что задание отношения списком пар – это в точности задание соответствующего ему орграфа списком рёбер.

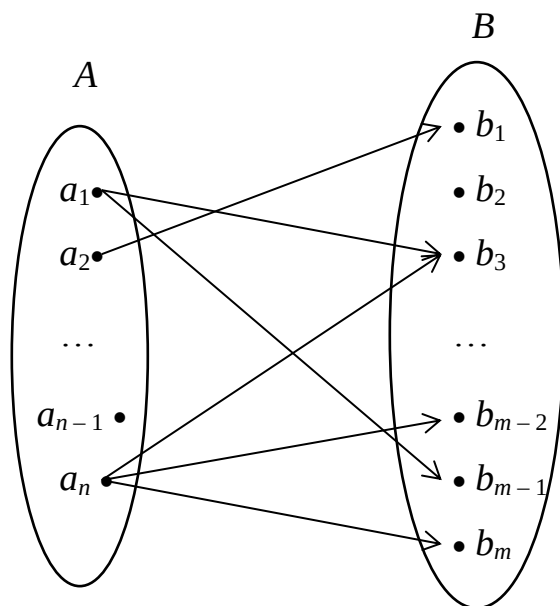


Рис. 3.1. Изображение отношения R в виде двудольного орграфа

Любое бинарное отношение можно записать матрицей: если $a_i R b_j$, то на пересечении i -й строки и j -го столбца пишется 1, остальные элементы – нули.

Теоретико-множественные операции над бинарными отношениями выполняются так же, как и над любыми другими. А вот об умножении поговорим подробнее. Прежде всего, хотелось бы, чтобы произведение бинарных отношений снова было бинарным отношением. Поэтому, говоря об умножении бинарных отношений R_1 и R_2 , обычно договариваются, что $R_1 \subseteq A \times B$, а $R_2 \subseteq B \times C$, и множество B выступает в роли связывающего. Мы тоже будем придерживаться этой договорённости.

Проиллюстрируем умножение бинарных отношений небольшим примером.

Пример. Пусть

$$A = \{1; 2; 3; 4\},$$

$$B = \{u; v; w; x; y; z\},$$

$$C = \{\alpha; \beta; \gamma; \delta\},$$

$$R_1 = \{(1; w); (1; y); (2; u); (4; w); (4; x); (4; z)\},$$

$$R_2 = \{(u; \beta); (v; \gamma); (v; \delta); (w; \alpha); (x; \alpha); (x; \delta)\}.$$

Найти $R_1 \circ R_2$.

Ответ: $R_1 \circ R_2 = \{(1; \alpha); (2; \beta); (4; \alpha); (4; \delta)\}$.

На рисунке 3.2 красным цветом отмечены те рёбра орграфов, изображающих отношения R_1 и R_2 , благодаря которым в произведении этих отношений присутствуют указанные в ответе пары.

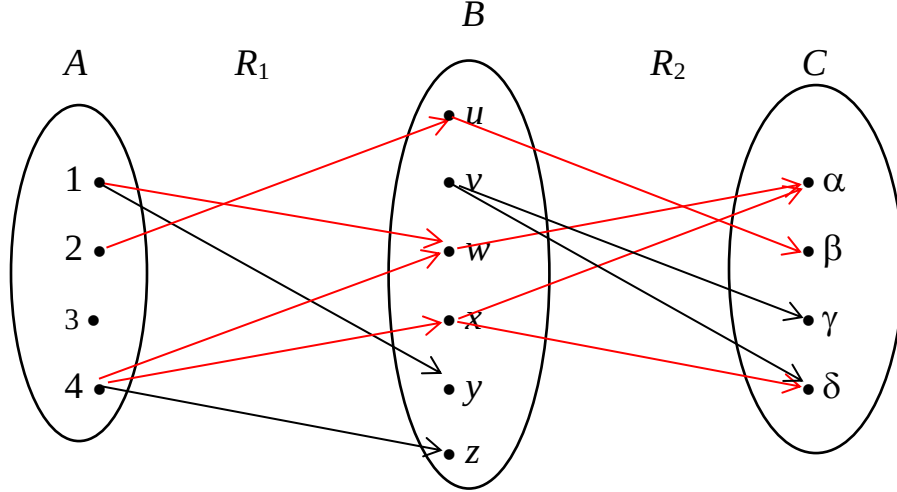


Рис. 3.2. Вычисление произведения отношений R_1 и R_2 .

Разумеется, вы должны научиться находить произведение отношений, не прибегая к помощи изображения их орграфами.

Операция умножения бинарных отношений обладает очень важным свойством, которое в математике называется *ассоциативностью*, а в школе – сочетательным законом.

Теорема 3.1. Для любых бинарных отношений $R_1 \subseteq A \times B$, $R_2 \subseteq B \times C$ и $R_3 \subseteq C \times D$ справедливо равенство $(R_1 \circ R_2) \circ R_3 = R_1 \circ (R_2 \circ R_3)$.

Доказательство. Нам требуется доказать равенство двух множеств: $(R_1 \circ R_2) \circ R_3$ и $R_1 \circ (R_2 \circ R_3)$. Заметим, прежде всего, что $R_1 \circ R_2 \subseteq A \times C$, $R_2 \circ R_3 \subseteq B \times D$, а оба множества $(R_1 \circ R_2) \circ R_3$ и $R_1 \circ (R_2 \circ R_3)$ – это подмножества множества $A \times D$.

Пусть $(a, d) \in (R_1 \circ R_2) \circ R_3$. Это значит, что существует такой элемент c из множества C , что $(a, c) \in R_1 \circ R_2$ и в то же время $(c, d) \in R_3$. Условие $(a, c) \in R_1 \circ R_2$ означает, что существует такой элемент $b \in B$, для которого $(a, b) \in R_1$ и $(b, c) \in R_2$. Поскольку для найденных нами элементов $b \in B$ и $c \in C$ выполнено условие $(b, c) \in R_2$ и $(c, d) \in R_3$, можно сделать вывод, что $(b, d) \in R_2 \circ R_3$. Учитывая $(a, b) \in R_1$, получаем, что $(a, d) \in R_1 \circ (R_2 \circ R_3)$. Значит, $(R_1 \circ R_2) \circ R_3 \subseteq R_1 \circ (R_2 \circ R_3)$.



Включение $R_1 \circ (R_2 \circ R_3) \subseteq (R_1 \circ R_2) \circ R_3$ докажете самостоятельно.

Следовательно, $(R_1 \circ R_2) \circ R_3 = R_1 \circ (R_2 \circ R_3)$. □

Введём для бинарных отношений ещё одну операцию: обращение отношения.

Определение 3.4. Отношение $S \subseteq B \times A$ называется обратным к отношению $R \subseteq A \times B$, если bSa тогда и только тогда, когда aRb .

Например, обратным к отношению «точка лежит на прямой» на множестве прямых в пространстве является отношение «прямая проходит через точку».



Какое отношение на множестве действительных чисел является обратным к отношению «меньше»?

Отношение, обратное к отношению R , будем обозначать R^{-1} .



Пусть для бинарного отношения R построен соответствующий ему орграф.

Как по этому орграфу построить орграф отношения R^{-1} ?

Пусть бинарное отношение R представлено матрицей. Какой матрицей будет представлено отношение R^{-1} ?



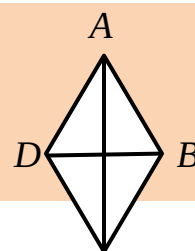
Особое внимание к бинарным отношениям объясняется ещё и тем, что любое n -арное отношение R при $n > 2$ можно формально рассматривать как бинарное. Для этого произведение $M_1 \times M_2 \times \dots \times M_k \times M_{k+1} \times \dots \times M_n$ представим в виде $(M_1 \times M_2 \times \dots \times M_k) \times (M_{k+1} \times \dots \times M_n)$ и обозначим множество $M_1 \times M_2 \times \dots \times M_k$ через N_1 , а множество $M_{k+1} \times \dots \times M_n$ через N_2 . Тогда кортеж $(a_1, a_2, \dots, a_k, a_{k+1}, \dots, a_n)$ из отношения R будет представлен кортежем $((a_1, a_2, \dots, a_k), (a_{k+1}, \dots, a_n))$ из бинарного отношения $R' \subseteq N_1 \times N_2$.

Бинарные отношения на множестве и их свойства

Теперь мы займёмся ещё более частным случаем: бинарными отношениями на множестве. В этом случае отношение можно изобразить орграфом другой структуры: вершинами считать элементы множества и соединять их стрелкой в том и только том случае, если соответствующие этим вершинам элементы находятся в данном отношении.



На рисунке 3.3 изображён ромб с проведёнными в нём диагоналями. Множество M – множество, состоящее из шести отрезков: AB , BC , CD , DA , AC и BD . Изобразите соответствующим орграфом каждое из перечисленных ниже



бинарных отношений на множестве M :

- а) отрезки пересекаются (т.е. имеют ровно одну общую точку);
- б) отрезки не пересекаются (т.е. не имеют общих точек);
- в) отрезки имеют хотя бы одну общую точку.

С
Рис. 3.3

Если R – некоторое бинарное отношение на множестве M , то для него определены отношения $R \circ R, R \circ R \circ R, \dots, \underbrace{R \circ R \dots \circ R}_{n \text{ раз}}$. Такие произведения мы

будем обозначать соответственно $R^2, R^3, \dots, R^n$.

Некоторые бинарные отношения на множестве обладают рядом важных свойств. Мы в этом пункте будем говорить только о четырёх из них: рефлексивности, симметричности, транзитивности и антисимметричности.

Определение 3.5. Отношение R на множестве M называется *рефлексивным*, если для любого элемента a из M справедливо, что aRa .

Вот несколько примеров рефлексивных отношений:

- на множестве целых чисел: меньше или равно;
- на множестве воздушных шаров: быть одного цвета;
- на множестве людей: быть одноклассником.

Определите, какие из следующих отношений рефлексивны:

- а) отношение подобия на множестве треугольников;
- б) отношение «делиться нацело» на множестве натуральных чисел;
- в) отношение перпендикулярности на множестве прямых;
- г) отношение «быть старше» на множестве людей.

Рефлексивным, очевидно, является универсальное отношение на любом множестве. Также очевидно, что пустое отношение рефлексивным не является. Для заданного множества M обозначим символом Δ множество пар вида (a, a) , построенных для всех элементов a из M . Отношение Δ на множестве M называется *отношением равенства*. Легко понять, что отношение Δ рефлексивно. Более того, для любого рефлексивного отношения R справедливо $\Delta \subseteq R$.

Верно ли обратное утверждение: если $\Delta \subseteq R$, то отношение R рефлексивно?

Определение 3.6. Отношение R на множестве M называется *симметричным*, если для любых элементов a и b множества M из выполнения утверждения aRb следует справедливость утверждения bRa .

Вот несколько примеров симметричных отношений:

- на множестве прямых: быть параллельными;
- на множестве целых чисел: быть одного знака;
- на множестве людей: быть одноклассниками.

Определите, какие из следующих отношений симметричны:

- а) отношение подобия на множестве треугольников;
- б) отношение «меньше» на множестве натуральных чисел;
- в) отношение перпендикулярности на множестве прямых;
- г) отношение «быть братом» на множестве людей.

Свойство симметричности отношения на множестве легко записать с помощью операций над отношениями: отношение R симметрично тогда и только тогда, когда $R^{-1} \subseteq R$.

Докажите это утверждение самостоятельно.

Если отношение изображено соответствующим ему орграфом, то легко увидеть, будет ли данное отношение симметричным: отношение симметрично тогда и только тогда, когда в соответствующем ему графе для каждой стрелки, ведущей из вершины a в вершину b , есть стрелка, ведущая из вершины b в вершину a . Фактически это означает, что граф является неориентированным.

Определение 3.7. Отношение R на множестве M называется *транзитивным*, если для любых элементов a , b и c множества M из выполнения утверждений aRb и bRc следует справедливость утверждения aRc .

Вот несколько примеров транзитивных отношений:

- на множестве кругов: лежать внутри;
- на множестве целых чисел: делиться нацело;
- на множестве вершин орграфа: быть сильно связанными;
- на множестве сотрудников одной организации: быть начальником.

Определите, какие из следующих отношений транзитивны:

- а) отношение подобия на множестве треугольников;
- б) отношение «меньше» на множестве натуральных чисел;
- в) отношение параллельности на множестве прямых;
- г) отношение «быть братом» на множестве людей.

Свойство отношения «быть транзитивным» также можно записать с помощью операций над отношениями.

Теорема 3.2. Отношение R на множестве M транзитивно тогда и только тогда, когда $R^2 \subseteq R$.

Доказательство. Пусть отношение R транзитивно. Проверим, что тогда из $(a, b) \in R^2$ следует $(a, b) \in R$. Действительно, $(a, b) \in R^2$ означает, что существует такой элемент $c \in M$, для которого $(a, c) \in R$ и $(c, b) \in R$. Ввиду транзитивности отношения R получаем $(a, b) \in R$. Тем самым, $R^2 \subseteq R$.

Обратно. Пусть $R^2 \subseteq R$ и для элементов a, b и c выполнено aRb и bRc . По определению умножения отношений это означает, что $(a, c) \in R^2$. Но тогда $(a, c) \in R$ и, следовательно, отношение R транзитивно. $\square$

Определение 3.8. Отношение R на множестве M называется *антисимметричным*, если для любых элементов a и b множества M из выполнения утверждений aRb и bRa следует, что элементы a и b совпадают.

Вот несколько примеров антисимметричных отношений:

- на множестве целых чисел: меньше или равно;
- на множестве всех подмножеств некоторого множества: быть подмножеством;
- на множестве натуральных чисел: делиться нацело.

С помощью операций отношение антисимметричности записывается так: отношение R на множестве M антисимметрично тогда и только тогда, когда $R \cap R^{-1} \subseteq \Delta$.



Докажите это утверждение самостоятельно.

Если отношение изображено соответствующим ему оргграфом, то и в этом случае легко увидеть, будет ли данное отношение антисимметричным: отношение антисимметрично тогда и только тогда, когда в соответствующем ему графе для каждой стрелки, ведущей из вершины a в другую вершину b , нет стрелки, ведущей из вершины b в вершину a .

Пусть в наборе некоторых бинарных отношений на одном и том же множестве каждое из них обладает некоторым свойством. Будет ли тогда этим свойством обладать результат применения к этим отношениям какой-либо операции? Ответ на это вопрос для операции пересечения отношений даёт следующая теорема.

Теорема 3.3. Пересечение любого набора рефлексивных (симметричных, транзитивных, антисимметричных) отношений является рефлексивным (соответственно симметричным, транзитивным, антисимметричным) отношением.

Доказательство. Рассмотрим произвольный набор транзитивных отношений R_i . Обозначим через R пересечение всех отношений данного набора. Пусть пары (x, y) и (y, z) принадлежат R . Тогда для каждого множества R_i обе эти пары принадлежат R_i . Поскольку каждое отношение R_i транзитивно, пара (x, z) принадлежит каждому множеству R_i , а, значит, принадлежит и их пересечению, т.е. отношению R . Следовательно, отношение R транзитивно. $\square$



Для остальных трёх свойств Теорему 3.2 докажите самостоятельно.

Для объединения отношений ситуация иная.



Исследуйте, для каких из четырёх рассматриваемых нами свойств объединение двух отношений, обладающих данным свойством, также обладает этим свойством.

Рассмотрим операцию обращения отношения.

Теорема 3.4. Отношение, обратное к рефлексивному (симметричному, транзитивному, антисимметричному) отношению является рефлексивным (соответственно симметричным, транзитивным, антисимметричным) отношением.



Докажите Теорему 3.4 самостоятельно для остальных трёх свойств.

Отношения эквивалентности

Среди всех бинарных отношений особую роль играют отношения двух видов: отношения эквивалентности и отношения порядка. В этом пункте мы рассмотрим отношения эквивалентности.

Определение 3.9. Отношение на множестве M называется *отношением эквивалентности*, если оно рефлексивно, симметрично и транзитивно.

Вот несколько примеров отношений эквивалентности:

- на любом множестве: отношение равенства;
- на множестве треугольников: отношение подобия;
- на множестве действительных чисел: иметь одинаковую целую часть;
- на множестве вершин графа: быть связанными;
- на множестве людей: быть одного года рождения.



Проверьте, что каждое из указанных отношений действительно является отношением эквивалентности. Приведите еще 2 – 3 примера отношений эквивалентности на различных множествах.

Понятие отношения эквивалентности связано с еще одним важным понятием теории множеств – разбиением.

Определение 3.10. Разбиением множества M называется его представление в виде объединения непустых непересекающихся подмножеств.

Вот, к примеру, два разбиения множества $M = \{\odot, \blacksquare, \blacksquare, \square, \frown\}$:

$$M = \{\odot, \frown\} \cup \{\blacksquare, \blacksquare, \square\} \text{ и } M = \{\blacksquare, \blacksquare\} \cup \{\odot, \square\} \cup \{\frown\}.$$



Объясните, почему для множества $M = \{1, 2, 3, 4, 5\}$ следующие записи нельзя считать разбиениями множества M :

- а) $\{1, 2, 3\} \cup \{5, 4, 3\}$;
- б) $\{1, 3\} \cup \{5, 4\}$;
- в) $\{1, 2, 3\} \cup \emptyset \cup \{5, 4\}$.

Теорема 3.5. (О разбиении множества) Каждое отношение эквивалентности задаёт разбиение множества, на котором оно определено. Любое разбиение множества задается некоторым отношением эквивалентности.

Доказательство. Рассмотрим первое утверждение теоремы. Пусть R – отношение эквивалентности на множестве M . Для каждого элемента a из M построим множество $M_a = \{x \mid x \in M \text{ и } xRa\}$. Среди этих множеств могут оказаться одинаковые. Соберём совокупность всех не совпадающих между собой множеств M_a и покажем, что их объединение образует разбиение множества M .

Во-первых, заметим, что каждое множество не пусто, поскольку $a \in M_a$ в силу рефлексивности отношения R .

Во-вторых, объединение всех выбранных нами множеств совпадает с M , поскольку каждый элемент из M попадает в подмножество, отмеченное им самим в роли индекса.

В третьих, покажем, что два различных множества M_a и M_b не пересекаются. Допустим противное: пусть $c \in M_a \cap M_b$. По построению множеств M_a и M_b это означает, что cRa и cRb . Ввиду симметричности отношения R имеем aRc . Выберем теперь произвольный x из M_a . Поскольку xRa и aRc , транзитивность отношения показывает, что xRc . Но при этом cRb . Применяя ещё раз свойство транзитивности, получаем xRb . Это означает, что $x \in M_b$. Поскольку x

выбирался произвольным, $M_a \subseteq M_b$. В то же время элементы a и b абсолютно равноправны, поэтому $M_b \subseteq M_a$. Значит, $M_a = M_b$ в противоречии с тем, что выбирались два различных множества.

Пусть теперь имеется некоторое разбиение множества M :

$$M = \bigcup_i \{M_i \mid M_i \neq \emptyset \text{ и } M_i \cap M_j = \emptyset \text{ при } i \neq j\}$$

Определим на M следующее отношение R :

aRb , если найдётся множество M_i , для которого $a \in M_i$ и $b \in M_i$.

Покажем, что R – отношение эквивалентности.

Во-первых, R рефлексивно. По определению объединения множеств каждый элемент a из M попадает хотя бы в одно подмножество M_i . Это означает, что aRa .

Во-вторых, R симметрично. Ясно, что если для пары (a, b) нашлось множество M_i , для которого $a \in M_i$ и $b \in M_i$, то это же множество годится для пары (b, a) .

В-третьих, R транзитивно. Пусть a, b и c – такие элементы, что aRb и bRc . Значит, найдётся такое множество M_i , для которого $a \in M_i$ и $b \in M_i$, и такое множество M_k , для которого $b \in M_k$ и $c \in M_k$. Мы видим, что b оказался общим элементом множеств M_i и M_k , а по определению разбиения разные его подмножества общих элементов не имеют. Следовательно, $M_i = M_k$, а тогда aRc .

Ясно также, что отношение R задаёт именно то разбиение, на основании которого оно было построено. $\square$

Пример. На множестве натуральных чисел определим отношение aRb условием $\frac{a-b}{3}$ – целое число (не обязательно положительное!). Проверим, что R – отношение эквивалентности.

Поскольку $\frac{a-a}{3} = 0$ – целое число, R рефлексивно.

Заметим, что $\frac{b-a}{3} = -\frac{a-b}{3}$, следовательно, R симметрично.

Наконец, $\frac{a-c}{3} = \frac{a-b}{3} + \frac{b-c}{3}$, так что из aRb и bRc следует aRc .

Построим разбиение множества натуральных чисел, определяемое этим отношением эквивалентности. Возьмём число 1 и построим множество M_1 . Легко понять, что $M_1 = \{1, 4, 7, \dots\} = \{3k + 1 \mid k \in \mathbb{N} \cup \{0\}\}$. Число 2 в M_1 не попало, поэтому построим $M_2 = \{2, 5, 8, \dots\} = \{3k + 2 \mid k \in \mathbb{N} \cup \{0\}\}$. Число 3 не

принадлежит $M_1 \cup M_2$, строим $M_3 = \{3, 6, 9, \dots\} = \{3k \mid k \in N\}$. Легко видеть, что $M_1 \cup M_2 \cup M_3 = M$. Тем самым, построено разбиение множества M .

Подмножества, фигурирующие в разбиении, нередко называют *классами эквивалентности*, а саму теорему называют теоремой о принципах классификации. Совокупность классов эквивалентности называют *фактор-множеством* множества M по отношению эквивалентности R и обозначают M/R . Класс эквивалентности, в который попадает элемент a обычно обозначают $\bar{a}$ или, если хотят точно указать отношение эквивалентности, a^R .



Какое разбиение произвольного множества задаёт отношение равенства? А универсальное отношение?

Среди примеров отношения эквивалентности фигурировало отношение связности для вершин графа.



Как для этого отношения называются классы эквивалентности?

Отношения порядка

Определение 3.11. Отношение на множестве M называется *отношением порядка*, если оно рефлексивно, транзитивно и антисимметрично.

Вот несколько примеров отношений порядка:

- на множестве прямоугольников: содержаться;
- на множестве действительных чисел: меньше или равно;
- на множестве сотрудников одного учреждения: быть начальником.



Проверьте, что каждое из указанных отношений действительно является отношением порядка. Приведите еще 2 – 3 примера отношений порядка на различных множествах.

Исторически сложилось так, что отношение порядка в литературе обычно называют отношением *частичного порядка*. Мы для краткости слово «частичного» будем опускать.

Определение 3.12. Множество M называется *упорядоченным*, если на нём определено некоторое отношение порядка.

Множество целых чисел упорядочено отношением «меньше или равно», множество подмножеств произвольного множества упорядочено отношением «быть подмножеством». Даже знаки для этих отношений похожи: $\leq$ и $\subseteq$. Удобно и для произвольного отношения порядка иметь какой-то похожий значок. Например, такой: $\trianglelefteq$.

Определение 3.13. Элементы a и b множества M , упорядоченного отношением $\leq$, называются *сравнимыми*, если $a \leq b$ или $b \leq a$.



Что можно сказать об элементах a и b , если одновременно $a \leq b$ и $b \leq a$?

В упорядоченном множестве нередко интересуются, так сказать, крайними элементами, т.е. такими, для которых уже нет меньших элементов или, наоборот, больших.

Определение 3.14. Элемент a множества M , упорядоченного отношением $\leq$, называется *минимальным*, если в M не существует элемента b , не равного a , для которого $b \leq a$.

Пример 1. В множестве неотрицательных действительных чисел, упорядоченном отношением $\leq$, минимальным элементом является число 0. В множестве положительных действительных чисел, упорядоченное отношением $\leq$, минимальных элементов нет.

Пример 2. Естественно считать точку окружностью нулевого радиуса – ведь это множество всех точек, удаленных от заданной точки на расстоянии 0. На множестве всевозможных окружностей (включая окружности нулевого радиуса) рассмотрим отношение «одна окружность лежит внутри другой или совпадает с ней». Легко проверить, что это отношение порядка и любая точка является минимальным элементом этого множества. Если это же отношение рассмотреть на множестве окружностей ненулевого радиуса, то такое множество минимальных элементов иметь не будет.

Эти примеры показывают, что упорядоченное множество может не иметь минимальных элементов, может иметь один минимальный элемент, а может иметь несколько (и даже бесконечно много) минимальных элементов.



Сформулируйте определение максимального элемента множества, упорядоченного некоторым отношением $\leq$. Приведите примеры упорядоченных множеств с максимальными элементами.

Определение 3.15. Элемент a множества M , упорядоченного отношением $\leq$, называется *наименьшим*, если для любого элемента b из M выполнено $a \leq b$.

Пример 3. В множестве неотрицательных действительных чисел, упорядоченном отношением $\leq$, число 0 является наименьшим элементом.

Пример 4. На множестве всевозможных окружностей (включая окружности нулевого радиуса), упорядоченном отношением «одна окружность лежит внутри другой или совпадает с ней», нет наименьшего элемента.

Пример 4 показывает различие понятий «минимальный элемент» и «наименьший элемент»: минимальные элементы в множестве есть, а наименьшего нет. Следующая теорема также свидетельствует о различии этих понятий.

Теорема 3.6. (О единственности наименьшего элемента) Если упорядоченное множество обладает наименьшим элементом, то только одним.

Доказательство. Пусть a – некоторый наименьший элемент множества M , упорядоченного отношением $\leq$. Предположим, что существует другой наименьший элемент; обозначим его b . По определению наименьшего элемента $a \leq b$ и $b \leq a$. В силу антисимметричности отношения $\leq$ получаем, что $a = b$ в противоречии с выбором элемента b . $\square$

Как видно из примера 2, минимальных элементов может быть сколько угодно.

Тем не менее, понятия «минимальный элемент» и «наименьший элемент», можно сказать, родственники.

Теорема 3.7. (О минимальности наименьшего элемента) Всякий наименьший элемент упорядоченного множества является минимальным.

Доказательство. Пусть a – некоторый наименьший элемент множества M , упорядоченного отношением $\leq$. Предположим, что он не является минимальным. Тогда существует элемент b , отличный от a , для которого $b \leq a$. В то же время по определению наименьшего элемента $a \leq b$. В силу антисимметричности отношения $\leq$ получаем, что $a = b$ в противоречии с выбором элемента b . $\square$



Сформулируйте определение наибольшего элемента множества, упорядоченного некоторым отношением $\leq$. Приведите примеры множеств, имеющих наибольший элемент. Сформулируйте и докажите для максимальных элементов теоремы, аналогичные теоремам 3.6 и 3.7.

Для отношений порядка тоже используют изображения в виде графа, но строят его для другого отношения, тесно связанного с заданным отношением порядка.

Определение 3.16. Говорят, что элемент a множества M , упорядоченного отношением $\leq$, *непосредственно предшествует* элементу b , если a и b различны, $a \leq b$ и не существует элемента c , также отличного от a и b , для которого $a \leq c$ и $c \leq b$.

Это отношение из четырёх рассматриваемых нами свойств обладает только одним – антисимметричностью, но именно его удобно использовать для построения наглядного представления отношения порядка. Совсем легко нужный граф строится, если множество M конечно. Сначала строят множество точек (вершин будущего графа), обозначенных максимальными элементами множества M . Ниже изображают ряд точек, обозначенных элементами, предшествующими элементам предыдущего ряда. Элементы, связанные отношением непосредственного предшествования, соединяют ребром. Ниже изображают ряд точек, обозначенных элементами, предшествующими элементам предыдущего ряда, и снова элементы, связанные отношением непосредственного предшествования, соединяют ребром. И так далее, пока не будут исчерпаны все элементы множества M . Построенный таким образом граф называют *диаграммой Хассе* данного отношения порядка.

Конечно, диаграмму Хассе можно строить не «сверху вниз», как это описано выше, а «снизу вверх», начиная с минимальных элементов.

Пример 5. Пусть $A = \{a, b, c\}$, множество $M = \mathcal{B}(A)$. На множестве M рассматривается отношение $\subseteq$. Минимальным (и даже наименьшим) элементом множества M , очевидно, является $\emptyset$. Оно непосредственно предшествует каждому из одноэлементных множеств $\{a\}$, $\{b\}$, $\{c\}$. Те в свою очередь непосредственно предшествуют двухэлементным множествам. И наконец, каждое двухэлементное множество непосредственно предшествует множеству A . Тем самым, диаграмма Хассе данного отношения будет выглядеть так, как показано на рисунке 3.4.

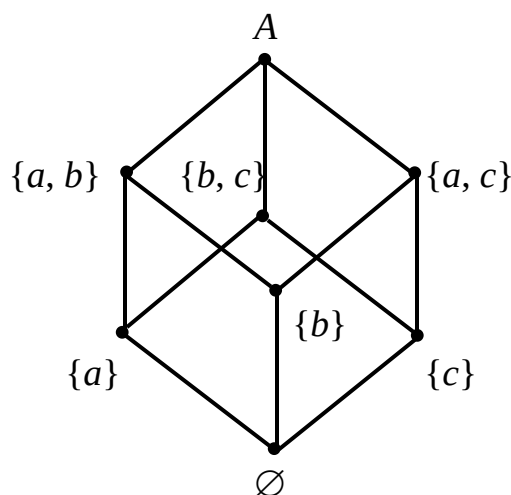


Рис. 3.4. Диаграмма Хассе для булеана трёхэлементного множества

Диаграмму Хассе естественно рассматривать как ориентированный граф, хотя направление на рёбрах этого графа обычно не указывают ввиду очевидности.



Сформулируйте, как по диаграмме Хассе (как орграфу) для разных элементов a и b данного упорядоченного множества определить,
а) находится ли элемент a с элементом b в данном отношении;
б) сравнимы ли элементы a и b .

Определение 3.17. Отношение порядка на множестве M называется *линейным*, если любые два элемента этого множества сравнимы.

Одним из важнейших примеров линейного порядка является отношение «меньше или равно» на любом подмножестве множества действительных чисел.



Как выглядит диаграмма Хассе линейно упорядоченного множества?

Взаимосвязь между отношениями и предикатами

Пусть на совокупности множеств $M_1, M_2, \dots, M_n$ задано некоторое отношение R . Тогда можно определить предикат $P(x_1, x_2, \dots, x_n)$ правилом

$$P(x_1, x_2, \dots, x_n) = 1 \text{ тогда и только тогда, когда } (x_1, x_2, \dots, x_n) \in R.$$

И наоборот, если есть некоторый предикат $P(x_1, x_2, \dots, x_n)$, определённый на $M_1 \times M_2 \times \dots \times M_n$, то множество $R = \{(x_1, x_2, \dots, x_n) \mid P(x_1, x_2, \dots, x_n) = 1\}$ является отношением на совокупности множеств $M_1, M_2, \dots, M_n$. Напомним, что множество R называют *областью истинности предиката* P .



Пусть P_1 и P_2 – предикаты на $M_1 \times M_2 \times \dots \times M_n$, а R_1 и R_2 – соответствующие им отношения. Запишите с помощью операций над R_1 и R_2 области истинности предикатов а) $P_1 \& P_2$; б) $P_1 \vee P_2$; в) $P_1 \rightarrow P_2$.

Как мы видим, что отношения и предикаты – родственные понятия. Говоря о предикате, всегда полезно иметь в виду связанное с ним отношение, и наоборот.

Задания для самостоятельной работы

1. Пусть $A = \{1; 2; 3\}$, $B = \{a; b; c; d\}$, $C = \{+; -; /\}$, $R_1 \subseteq A \times B$; $R_2 \subseteq B \times C$ такие, что $R_1 = \{(1; a); (1; d); (2; c); (3; d); (3; c)\}$, $R_2 = \{(a; +); (b; /); (d; -); (d; /)\}$. Вычислите $R_1 \circ R_2$ и $R_1 \circ R_1^{-1}$.

2.^T На множестве $\{1; 2; 3\}$ задано отношение $R = \{(1; 1); (1; 2); (2; 3)\}$. Вычислите а) $R \cup \Delta$, б) $R \cup R^{-1}$, в) $R \cap R^{-1}$, г) R^2 , д) R^3 .

3. На множестве $\{a; b; c\}$ найдите два бинарных отношения R_1 и R_2 , для которых $R_1 \circ R_2 \neq R_2 \circ R_1$.

4. В базе данных соревнования по метанию копья хранится в табличной форме отношение R_1 «Результаты жеребьевки», в котором указываются фамилия с инициалами и полученный при жеребьевке номер:

Константинов С.В.	1
Павлов У.Р.	2
Семенов М.С.	3
Туров Ф.П.	4
...	...

Результаты спортсменов после очередной попытки также фиксируется в виде отношения R_2 «Результаты попытки», в котором указываются номер спортсмена и его результат:

1	85,97 м
2	90,32 м
3	—
4	87,48
...	...

Каков смысл произведения отношений R_1 и R_2 ?

5. Верно ли каждое из следующих равенств

а) $(R_1 \cup R_2) \circ R_3 = (R_1 \circ R_3) \cup (R_2 \circ R_3)$;

б) $R_1 \circ (R_2 \cap R_3) = (R_1 \circ R_2) \cap (R_1 \circ R_3)$

для бинарных отношений R_1, R_2, R_3 , определённых на тех множествах, где можно выполнять соответствующие операции над этими отношениями? Ответ «Да» надо обосновать, ответ «Нет» аргументировать приведением примера.

6. Верно ли каждое из следующих равенств

а) $(R_1 \cup R_2)^{-1} = R_1^{-1} \cup R_2^{-1}$;

б) $(R_1 \cap R_2)^{-1} = R_1^{-1} \cap R_2^{-1}$

для бинарных отношений R_1 и R_2 , определённых на произвольном множестве M ? Ответ «Да» надо обосновать, ответ «Нет» аргументировать примером.

7. Докажите, что для бинарного отношения R на множестве M из $R^{-1} \subseteq R$ следует $R^{-1} = R$.

8. Верно ли, что для любого бинарного отношения R на множестве M

а) отношение $R^{-1} \cup R$ симметрично;

б) отношение $R^{-1} \cap R$ симметрично?

Ответ да, надо обосновать, ответ нет аргументировать приведением примера.

9.^Т Укажите, какими свойствами обладает каждое из отношений R_1 , R_2 и R_3 , заданных на множестве слов русского языка:

- а) $x R_1 y$ означает, что слова x и y не имеют ни одной общей буквы;
- б) $x R_2 y$ означает, что слова x и y имеют по крайней мере одну общую букву;
- в) $x R_3 y$ означает, что всякая буква, входящая в запись слова x , имеется в записи слова y .

10. На множестве $\{1; 2; 3; 4\}$ задано отношение $R = \{(1; 1); (1; 2); (2; 3), (1; 3); (4; 3)\}$.

- а)^Т Укажите какими свойствами обладает это отношение.
- б) Изобразите это отношение в виде орграфа.
- в) Запишите это отношение матрицей.

11. На множестве точек координатной плоскости задано отношение: $(a, b) R (c, d)$, если $a^2 + b^2 = c^2 + d^2$. Докажите, что R – отношение эквивалентности, и изобразите на координатной плоскости класс эквивалентности, которому принадлежит точка $(3, 4)$.

12. Изобразите орграф отношения эквивалентности, задающего разбиение множества M на следующие подмножества: $\{1; 4; 5\}$, $\{2; 6; 8\}$ и $\{3; 7\}$.

13. Корневое дерево можно рассматривать как диаграмму Хассе для множества его вершин. Какими элементами в этом множестве являются листья данного дерева? А корень?

Лекция 4. Отображения

Предыдущая лекция уже была посвящена различным аспектам связей между элементами одного или разных множеств. Эти связи описывались формализованно с помощью понятия «отношение». При этом все элементы в рассматриваемых отношениях были, можно сказать, равноправны. Говоря «число a меньше или равно числу b », мы ни одному из этих элементов не отдаём предпочтение. Но вот другая фраза: «Число b равно квадратному корню из числа a ». Конечно, здесь тоже речь идет об отношении между числами a и b , но воспринимается эта фраза так, что число a является как бы причиной появления числа b . В таком случае принято говорить, что число b является результатом некоторого отображения, применённого к числу a (здесь – извлечением корня), и тогда элемент a называют значением *аргумента* данного отображения, а элемент b – *значением* отображения на элементе a .

Определение отображения

Сформулируем определение отображения.

Определение 4.1. Пусть M_1 и M_2 – некоторые множества. *Отображением* множества M_1 в множество M_2 называют бинарное отношение, определённое на этих множествах, если первый компонент пары $(a, b) \in M_1 \times M_2$ рассматривается как аргумент, а второй – как значение для этого аргумента.

Отображения мы будем обозначать малыми буквами латинского алфавита (обычно f, g, h), а сам факт наличия отображения множества M_1 в множество M_2 записывать так:

$$f: M_1 \rightarrow M_2 \quad \text{или} \quad M_1 \xrightarrow{f} M_2.$$

Если элемент b оказался значением отображения f для аргумента a , то это будем записывать так: $b = f(a)$.

В связи с более пристальным вниманием к компонентам бинарного отношения возникают новые естественные вопросы о свойствах отображений:

– каждый ли элемент множества M_1 является значением аргумента данного отображения?

– каждый ли элемент из M_2 является значением отображения на каком-нибудь элементе из M_1 ?

– если некоторый элемент из M_1 является значением аргумента данного отображения, то могут ли у этого аргумента быть другие значения?

И т. д.

Определение 4.2. Пусть f – отображение множества M_1 в множество M_2 . *Областью определения* отображения f называется множество тех элементов a из M_1 , для которых в множестве M_2 существует элемент b такой, что $b = f(a)$.

Область определения отображения f обозначают $D(f)$, так что можно записать

$$D(f) = \{ a \mid a \in M_1 \ \& \ \exists b \in M_2 (b = f(a)) \}.$$

Определение 4.3. Пусть f – отображение множества M_1 в множество M_2 . *Областью значений* отображения f называется множество тех элементов b из M_2 , для которых в множестве M_1 существует элемент a такой, что $b = f(a)$.

Область значений отображения f обозначают $E(f)$, так что можно записать

$$E(f) = \{ b \mid b \in M_2 \ \& \ \exists a \in M_1 (b = f(a)) \}.$$

По-другому область значений называют *образом отображения* f .

Свойства отображений

Как и для отношений, для отображений есть важные свойства, которыми могут обладать (или не обладать) те или иные конкретные отображения.

Определение 4.4. Отображение f множества M_1 в множество M_2 называется *всюду определённым*, если $D(f) = M_1$.

Определение 4.5. Отображение f множества M_1 в множество M_2 называется *сюръективным*, если $E(f) = M_2$.

Пример 1. Пусть $M_1 = M_2 = \mathbf{R}$. Отображение, сопоставляющее числу квадратный корень из этого числа, не является всюду определённым, поскольку его область определения – множество неотрицательных действительных чисел. В то же время оно сюръективно – ведь каждое число является значением для подходящего аргумента. (Напомним: квадратным корнем из числа называется число, квадрат которого равен исходному числу. Так что у числа 9, например, при данном отображении два значения: 3 и -3 . Не путайте это отображение с понятием арифметического квадратного корня!)

Определение 4.6. Отображение f множества M_1 в множество M_2 называется *однозначным*, если каждого элемента a из $D(f)$ имеет ровно одно значения в множестве M_2 .

На языке математической логики это свойство отображения можно записать так:

$$\forall a \in M_1 \ \forall b \in M_2 \ \forall c \in M_2 (b = f(a) \ \& \ c = f(a) \Rightarrow b = c).$$

По-другому однозначные отображения называют *функциональными* или просто *функциями*.

Пример 2. Пусть $M_1 = M_2 = \mathbf{R}$. Отображение, сопоставляющее числу квадратный корень из этого числа, не является функциональным: для числа 9 при данном отображении два значения: 3 и -3 . Если же в качестве M_1 и M_2 взять множество положительных действительных чисел, то указанное отображение будет и всюду определённым, и однозначным.

Определите, какие из следующих отображений функциональны:

- а) $M_1 = M_2$ – множество точек одной прямой; отображение f сопоставляет точке A на этой прямой точку B , удалённую на расстояние 2 от точки A ;
- б) M_1 – множество пар точек плоскости, $M_2 = \mathbf{R}$; отображение f сопоставляет паре точек A и B расстояние между этими точками;
- в) M_1 – множество людей, M_2 – множество двухэлементных подмножеств множества M_1 ; отображение f сопоставляет человеку его родителей;
- г) $M_1 = M_2$ – множество вершин некоторого связного графа, $|M_1| > 2$; отображение f сопоставляет вершине u смежную с ней вершину v .

Определение 4.7. Отображение f множества M_1 в множество M_2 называется *инъективным*, если каждый элемент b из $E(f)$ является значением только одного элемента из M_1 .

На языке математической логики это свойство отображения можно записать так:

$$\forall b \in M_2 \forall a \in M_1 \forall c \in M_1 (b = f(a) \& b = f(c) \Rightarrow a = c).$$

Пример 3. Пусть $M_1 = M_2 = \mathbf{R}$. Отображение f , сопоставляющее числу квадратный корень из этого числа, инъективно.

Поскольку любое отображение – это по происхождению бинарное отношение, то его тоже нередко бывает удобно изображать орграфом.

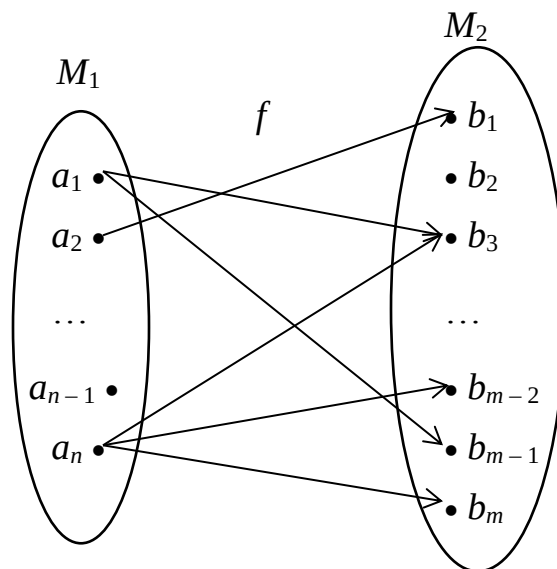


Рис. 4.1. Изображение отображения f в виде орграфа

Ясно, что $D(f)$ – это множество тех вершин, для которых есть исходящие рёбра, а $E(f)$ – это множество тех вершин, для которых есть входящие рёбра.



Как по орграфу, изображающему отображение, определить, является ли это отображение а) однозначным; б) инъективным?

Операции над отображениями

Прежде всего, речь идёт о тех двух операциях, которые играют особую роль именно для бинарных отношений: умножении и обращении. Определения для них остаются теми же самыми, только операцию умножения отображений обычно называют их композицией, а в совсем старых учебниках вы найдёте для неё название суперпозиция. Есть, однако, одна тонкость в принятых обозначениях. Пусть, например, $f : M_1 \rightarrow M_2$, а $g : M_2 \rightarrow M_3$. Записывая композицию отображений как умножение бинарных отношений, мы получим $f \circ g$. В то же время, если мы хотим записать, что элемент c из M_3 – это результат применения композиции этих отображений к элементу a из M_1 , то такая запись будет выглядеть так: $c = g(f(a))$. Получается не совсем естественная формула: $(f \circ g)(a) = g(f(a))$. Эта коллизия возникла исторически: понятие функции намного старше понятия отношения. Обозначение $f(a)$ придумал в 1718 году И. Бернулли, правда, аргумент в скобки он не заключал (мы и теперь иногда пишем без скобок, например, $\sin x$); скобки ввел в употребление в 1734 году Л. Эйлер. Теория бинарных отношений возникла практически одновременно с теорией множеств, т. е. в конце XIX века, когда менять обозначение для функций было уже поздно.

Из теоремы 3.1 следует, что операция композиции отображений ассоциативна.

Вторая операция – обращение функции – затруднений не доставляет: обратное отображение – это обратное отношение. И результат применения этой операции к отображению f , как и для отношений, обозначают f^{-1} . Надо только помнить, что если $f : M_1 \rightarrow M_2$, то обратное к нему отображение $f^{-1} : M_2 \rightarrow M_1$.



Объясните, почему $D(f^{-1}) = E(f)$, а $E(f^{-1}) = D(f)$, и докажите, что $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.

Важно знать, как те или иные свойства отображений ведут себя при применении операций к отображениям, обладающим этими свойствами. Ответ на этот вопрос содержат следующие две теоремы.

Теорема 4.1. Композиция всюду определенных (однозначных, сюръективных, инъективных) отображений является всюду определенным (соответственно, однозначным, сюръективным, инъективным) отображением.

Доказательство. Рассмотрим однозначные отображения $f: M_1 \rightarrow M_2$ и $g: M_2 \rightarrow M_3$ и предположим, что их композиция $f \circ g$ не является однозначным отображением. Это значит, что для некоторого элемента a из M_1 найдутся два разных элемента c_1 и c_2 из M_3 , для которых $c_1 = (f \circ g)(a)$ и $c_2 = (f \circ g)(a)$. По определению операции композиции найдутся такие элементы b_1 и b_2 из M_2 , для которых $b_1 = f(a)$ и $c_1 = g(b_1)$, а также $b_2 = f(a)$ и $c_2 = g(b_2)$. Поскольку f однозначное, $b_1 = b_2$; тогда из однозначности g следует, что $c_1 = c_2$ в противоречии с выбором элементов c_1 и c_2 . $\square$



Для остальных трёх свойств Теореме 4.1 докажите самостоятельно.

Теорема 4.2. Отображение, обратное всюду определенному отображению, сюръективно; отображение, обратное однозначному отображению, инъективно; отображение, обратное сюръективному отображению, всюду определенное; отображение, обратное инъективному отображению, однозначно.

Доказательство. Пусть f – инъективное отображение M_1 в M_2 . Допустим, что отображение f^{-1} не однозначно, т. е. существуют два таких элемента a_1 и a_2 из M_1 , которые являются значениями одного и того же элемента b при отображении f^{-1} . Но тогда, по определению, обратного отображения элемент b является значением для элементов a_1 и a_2 при отображении f – противоречие с определением однозначного отображения. $\square$



Для остальных трёх свойств Теореме 4.2 докажите самостоятельно.

Пусть f – всюду определённое однозначное отображение множества N в некоторое множество M . Тогда удобно представлять себе, что элементы множества M записываются в том порядке, в котором они фигурируют как значения функции f :

$$a_1, a_2, a_3, \dots, a_{n-1}, a_n, a_{n+1}, \dots$$

В этом случае говорят, что задана *последовательность* элементов из множества M . Этот факт записывают $a_n = f(n)$. Например, $a_n = \frac{n+1}{n}$ или $a_n = \sin n$. По-другому говорят, что последовательность – это функция натурального аргумента. Впрочем, иногда бывает удобно нумерацию членов последовательности начинать не с 1, а с 0. Конечно, от этого она не перестаёт быть последовательностью.

Взаимно-однозначные отображения. Равномощные множества

Особо важную роль играют отображения, обладающие одновременно всеми четырьмя свойствами: всюду определённые, однозначные, инъективные и сюръективные. Такие отображения называются *взаимно однозначными отображениями* множества M_1 на множество M_2 . По-другому их называют *взаимно однозначными соответствиями* множеств M_1 и M_2 . Для взаимно однозначных отображений из теорем 4.1 и 4.2 получается такое следствие.

Следствие 4.3. Композиция взаимно однозначных отображений является взаимно однозначным отображением. Отображение, обратное взаимно однозначному отображению, является взаимно однозначным.

Нетрудно сообразить, что если между множествами M_1 и M_2 установлено взаимно однозначное соответствие и множество M_1 конечно, то множество M_2 тоже конечно и в нём столько же элементов, сколько в множестве M_1 . Особенно легко это видеть, если взаимно однозначное отображение изобразить в виде графа (рис. 4.2): количество элементов в каждом множестве совпадает с количеством рёбер в этом графе.

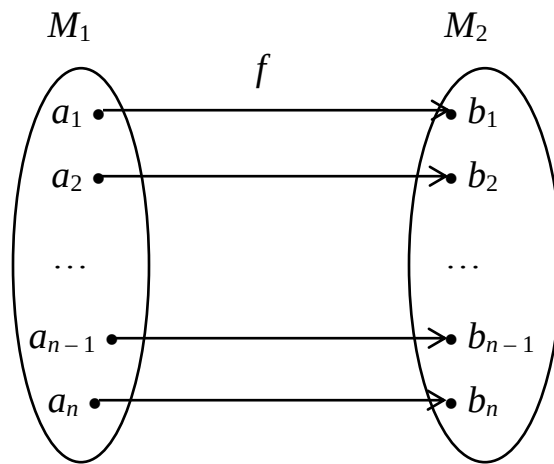


Рис. 4.2. Взаимно однозначное соответствие множеств

Ни для кого не будет открытием, что множество натуральных чисел бесконечно.

Определение 4.8. Множество M называется *счётным*, если существует взаимно однозначное отображение этого множества на множество натуральных чисел.

Термин «счётное» возник естественно, потому что взаимно однозначное отображение множества M на множество N фактически нумерует элементы множества M натуральными числами, т.е. как бы их пересчитывает.

Никакое конечное множество не позволит установить взаимно однозначное соответствие со своим собственным подмножеством. А для любого счётного множества это возможно. Но сначала мы докажем следующее утверждение.

Теорема 4.4. Множества положительных четных чисел, целых чисел и положительных рациональных чисел счётны.

Доказательство. Указать нужное отображение для множества положительных четных чисел совсем легко: для каждого чётного числа x полагаем $f(x) = \frac{x}{2}$.



Проверьте, что это отображение взаимно однозначно.

Для целых чисел построить нужное отображение немного сложнее. Определим отображение f таким правилом:

$$f(x) = \begin{cases} 2x, & \text{если } x \geq 0; \\ 2|x| - 1, & \text{если } x < 0. \end{cases}$$



Проверьте, что это отображение взаимно однозначно.

Чтобы доказать счётность множества положительных рациональных чисел, поступим следующим образом.

В первой строке запишем ряд натуральных чисел:

1, 2, 3, 4, 5, 6, 7, ...

Во второй строке запишем ряд рациональных чисел со знаменателем 2:

$\frac{1}{2}, \frac{3}{2}, \frac{5}{2}, \frac{7}{2}, \frac{9}{2}, \frac{11}{2}, \frac{13}{2}, \dots$

Заметьте: чтобы числа не повторялись, все числители нечётные. И дальше – каждое положительное рациональное число представлено несократимой дробью!

В третьей строке запишем ряд рациональных чисел со знаменателем 3:

$\frac{1}{3}, \frac{2}{3}, \frac{4}{3}, \frac{5}{3}, \frac{7}{3}, \frac{8}{3}, \frac{10}{3}, \dots$

В четвёртой строке запишем ряд рациональных чисел со знаменателем 4:

$\frac{1}{4}, \frac{3}{4}, \frac{5}{4}, \frac{7}{4}, \frac{9}{4}, \frac{11}{4}, \frac{13}{4}, \dots$

И так далее.

У нас получилась таблица, бесконечная вправо и вниз:

1, 2, 3, 4, 5, 6, 7, ...

$\frac{1}{2}, \frac{3}{2}, \frac{5}{2}, \frac{7}{2}, \frac{9}{2}, \frac{11}{2}, \frac{13}{2}, \dots$

$$\begin{array}{ccccccc} \frac{1}{3}, & \frac{2}{3}, & \frac{4}{3}, & \frac{5}{3}, & \frac{7}{3}, & \frac{8}{3}, & \frac{10}{3}, \dots \\ \frac{1}{4}, & \frac{3}{4}, & \frac{5}{4}, & \frac{7}{4}, & \frac{9}{4}, & \frac{11}{4}, & \frac{13}{4}, \dots \end{array}$$

.....

Проведём в этой таблице диагонали, как показано ниже, а затем пронумеруем рациональные числа вдоль диагоналей сверху вниз, переходя от одной диагонали к следующей.

$$\begin{array}{ccccccc} \textcircled{1} & \textcircled{2} & \textcircled{4} & \textcircled{7} & & & \\ 1, & 2, & 3, & 4, & 5, & 6, & 7, \dots \\ \textcircled{3} & \textcircled{5} & \textcircled{8} & & & & \\ \frac{1}{2}, & \frac{3}{2}, & \frac{5}{2}, & \frac{7}{2}, & \frac{9}{2}, & \frac{11}{2}, & \frac{13}{2}, \dots \\ \textcircled{6} & \textcircled{9} & & & & & \\ \frac{1}{3}, & \frac{2}{3}, & \frac{4}{3}, & \frac{5}{3}, & \frac{7}{3}, & \frac{8}{3}, & \frac{10}{3}, \dots \\ \textcircled{10} & & & & & & \\ \frac{1}{4}, & \frac{3}{4}, & \frac{5}{4}, & \frac{7}{4}, & \frac{9}{4}, & \frac{11}{4}, & \frac{13}{4}, \dots \end{array}$$

.....

Мы написали только первые 10 номеров, но надеемся, что алгоритм построения нумерации, т.е. взаимно однозначного отображения множества положительных рациональных чисел на множество натуральных чисел вам понятен. □



Допишите ещё два ряда этой таблицы и определите, какой номер будет у числа $\frac{7}{6}$ и какое рациональное число будет иметь номер 36.

Употребление слова «соответствие» вместо слова «отображение» уже намекает на то, чтобы рассмотреть следующее отношение между множествами.

Определение 4.9. Множество M_1 называется *равномощным* множеству M_2 , если существует взаимно однозначное отображение множества M_1 на множество M_2 .

Теорема 4.5. Отношение равномощности является отношением эквивалентности.

невозможно по построению числа с цифрами β_i . □

А теперь обещанное...

Теорема 4.7. Всякое счётное множество равномощно некоторому своему собственному подмножеству.

Доказательство. Для множества натуральных чисел утверждение следует, например, из теоремы 4.4: оно равномощно подмножеству чётных чисел. Это значит, что существует взаимно однозначное отображение f множества N на подмножество чётных чисел. Пусть M – произвольное счётное множество, и g – взаимно однозначное отображение M на N . Тогда композиция $g \circ f \circ g^{-1}$ является взаимно однозначным отображением множества M на его собственное подмножество. □

Рисунок 4.3 иллюстрирует доказательство теоремы, когда множество M записано как последовательность, а $f(x) = 2x$.

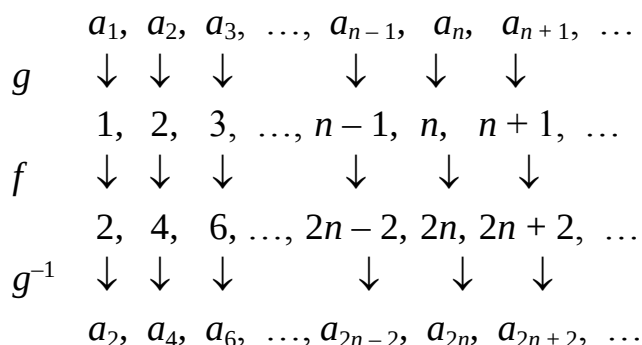


Рис. 4.3. Взаимно однозначное отображение множества M на собственное подмножество



Справедливо и более общее утверждение: всякое бесконечное множество равномощно некоторому своему собственному подмножеству. Поскольку для конечных множеств это не так, а понятие конечности, формально говоря, у нас не определено, то часто именно отрицание это свойства берут за определение конечности множества: множество называется *конечным*, если оно не равномощно никакому своему собственному подмножеству.

Особенности функциональных отображений

Хотя уже на 1-м курсе вам предстоит иметь дело и с нефункциональными отображениями, всё же основным объектом изучения будут функции. Поэтому уделим им немного больше внимания. Прежде всего, сформулируем необходимое и достаточное условие равенства функций.

Теорема 4.7. Функции $f: M_1 \rightarrow M_2$ и $g: M_1 \rightarrow M_2$ равны тогда и только тогда, когда $D(f) = D(g)$ и $f(x) = g(x)$ для любого элемента x из $D(f)$.

Доказательство. Пусть функции f и g равны, т.е. они равны как соответствующие бинарные отношения f и g , а значит, равны как подмножества множества $M_1 \times M_2$. Множество $D(f)$ – это по определению множество всех первых компонентов пар, принадлежащих f . Аналогично $D(g)$ – это множество всех первых компонентов пар, принадлежащих g . Раз f и g совпадают как множества пар, то и множества первых компонентов у них тоже совпадают.

В силу однозначности отображения f , в множестве пар, принадлежащих f как отношению, для каждого x из $D(f)$ есть только одна пара с первым компонентом x – это $(x, f(x))$. То же самое справедливо и для g . В силу равенства отношений это означает, что $(x, f(x)) = (x, g(x))$, т.е. $f(x) = g(x)$.

Обратно. Пусть $D(f) = D(g)$ и $f(x) = g(x)$ для любого элемента x из $D(f)$. Покажем, что тогда f и g равны как отношения, а потому равны и как отображения. Возьмем любую пару $(x, y) \in f$. В силу однозначности отображения f элемент y только один для каждого элемента x из $D(f)$, и он равен $g(x)$. Значит, пара $(x, y) \in g$. Импликация $(x, y) \in g \Rightarrow (x, y) \in f$ доказывается аналогично. Следовательно, $f = g$. $\square$

Пусть f – всюду определённая функция на множестве M_1 со значениями в множестве M_2 . На множестве M_1 определим отношение:

$$(x, y) \in R \Leftrightarrow f(x) = f(y).$$



Проверьте, что отношение R является отношением эквивалентности.

Это отношение называют *ядерной эквивалентностью* функции f . Как обычно, отношение эквивалентности разбивает множество M_1 на классы. На рисунке 4.4 схематично изображено такое разбиение множества M_1 .



Каждому ученику некоторой школы функция f сопоставляет номер класса, в котором он учится. Как называются учащиеся, попавшие в один класс разбиения по ядерной эквивалентности этой функции?

На рисунке 4.4 хорошо видно, что каждому классу ядерной эквивалентности ставится в соответствие ровно одно значение функции f . Иными словами, на фактор-множестве M_1 / R определена функция $\bar{f}$, сопоставляющая каждому классу ядерной эквивалентности функции f её значение на любом элементе этого класса. Выбор элемента не играет никакой роли, потому что на всех элементах из одного класса значение функции f одинаково.

Теорема 4.8. Пусть f – всюду определённая сюръективная функция из M_1 на M_2 , R – её ядерная эквивалентность. Тогда отображение $\bar{f}$ является взаимно-однозначным соответствием между фактор-множеством M_1 / R и M_2 .

Доказательство. Всюду определённая $\bar{f}$ и однозначность следует из определения. Сюръективность $\bar{f}$ следует из сюръективности функции f – у каждого элемента из M_2 есть прообраз, а значит, и непустой класс (возможно, одноэлементный) ядерной эквивалентности. Допустим, наконец, что есть два различных класса ядерной эквивалентности, образы которых при отображении $\bar{f}$ одинаковы. Выберем в одном классе элемент a , в другом – элемент b . По определению $\bar{f}$ на одном классе имеет значение $f(a)$, на другом – значение $f(b)$. По предположению $f(a) = f(b)$. Но тогда aRb , т. е. a и b принадлежат одному классу, что противоречит их выбору. Тем самым, доказано, что отображение $\bar{f}$ инъективно. $\square$

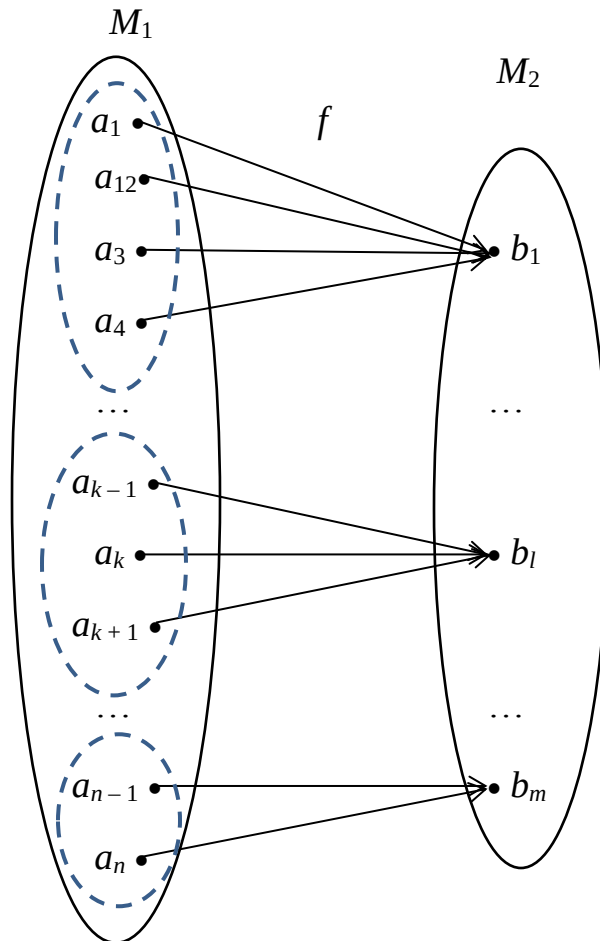


Рис. 4.4. Классы ядерной эквивалентности функции f .

Следствие 4.9. (Принцип Дирихле). Пусть f – всюду определённая функция из M_1 на M_2 . Функция f инъективна тогда и только тогда, когда её ядерная эквивалентность равна отношению Δ .

Доказательство почти очевидно, поскольку ядерная эквивалентность равна Δ тогда и только тогда, когда каждый класс этой эквивалентности одноэлементен. А тогда отображение $\bar{f}$ фактически совпадает с f .

В школьной олимпиадной математике принцип Дирихле формулируют обычно для конечных множеств следующим образом: если $n + 1$ зайцев рассадить в n клеток, то найдется клетка, в которой сидит не меньше двух зайцев. Отображение f – это, понятно, сопоставление каждому зайцу ту клетку, в которую его сажают. Поскольку f не взаимно-однозначно, ядерная эквивалентность отлична от отношения Δ , т. е. в каком-то её классе как минимум два зайца. Это именно те зайцы, которые сидят в одной клетке.

Несмотря на очень прозрачную и почти шуточную формулировку, принцип Дирихле оказался действенным инструментом доказательства многих важных теорем чистого существования.

Задания для самостоятельной работы

1.^T Между элементами множеств $X = \{-4; -3; -2; -1; 0; 1; 2; 3; 4\}$ и $Y = [-4; 4]$ задано отношение f правилом $x = y^2$, где $x \in X$, $y \in Y$. Рассматривая f как отображение множества X в множество Y , определите

- а) какова область определения f ;
- б) какова область значений f ;
- в) является ли f функцией;
- г) является ли f инъективным.

2. Пусть $X = \mathbf{N} \cup \{0\}$. Определим отображение $f: X \times X \rightarrow X \times X$ правилом $(a, b) \rightarrow (c, d)$, если c является частным при делении a на b , а d – остатком при делении a на b . Определите, какими свойствами обладает отображение f .

3.^T Пусть $X = \{x \mid x \in \mathbf{R} \text{ и } x > 0\}$. Рассмотрите отображение $f: X \rightarrow X$, заданное правилом $x \rightarrow \frac{1}{x^2+1}$.

- а) Определите свойства отображения f .
- б) Найдите обратное отображение f^{-1} и определите его свойства.

4.^T Рассмотрите отображение $f: \mathbf{R} \rightarrow \mathbf{R}$, заданное правилом $x \rightarrow \frac{1}{x^2+1}$.

- а) Определите свойства отображения f .
- б) Найдите обратное отображение f^{-1} и определите его свойства.

5. Докажите, что множество целых чисел, делящихся на 3, счётно.
6. Функция f ставит каждому четырехугольнику, лежащему в некоторой плоскости, его площадь. Как называются четырёхугольники, принадлежащие одному классу ядерной эквивалентности этой функции?
- 7.[†] Функция f множества $\mathbf{R}$ на множество $X = \{x \mid x \in \mathbf{R} \text{ и } x \geq 0\}$, заданная правилом $x \rightarrow x^2$. Укажите истинные высказывания о классах ядерной эквивалентности функции f :
- а) существует одноэлементный класс;
 - б) существует ровно один одноэлементный класс;
 - в) существует двухэлементный класс;
 - г) существует ровно один двухэлементный класс;
 - д) существует трёхэлементный класс;
 - е) существует класс, содержащий бесконечное число элементов.
8. Рассмотрите функцию $f: \mathbf{R} \times \mathbf{R} \rightarrow \mathbf{R}$, заданную правилом $(x, y) \rightarrow xy$. На координатной плоскости изобразите класс ядерной эквивалентности, соответствующий значению функции f , равному а) числу 3; б) числу -1 ; в) числу 0.

Лекция 5. Операции на множестве

Уже в первом классе, как только вы познакомились с натуральными числами, вас тут же стали учить выполнять над ними различные операции: находить сумму, разность, произведение и т.д. Расширялось множество чисел, и расширялся спектр операций: например, вы научились извлекать квадратные корни, а потом и корни произвольной степени. Появились многочлены и вообще произвольные функции, и вы снова учились выполнять операции над этими объектами... Но никто вам не объяснил (а вы и не спрашивали), что такое операция, выполняемая над элементами того или иного множества.

Определение операции на множестве

Определение 5.1. *Операцией* на множестве M называется всюду определённая функция из M^n в M . Число n называют *арностью*, или *местностью*, данной операции.

Вот несколько примеров операций:

- на множестве натуральных чисел: сложение двух чисел; это бинарная (двуместная) операция;
- на множестве целых чисел: нахождение числа, противоположного данному; это унарная (одноместная) операция;
- на множестве рациональных чисел: нахождение среднего арифметического n чисел; это n -арная (n -местная) операция;
- на множестве подмножеств данного множества: операция пересечения подмножеств; это бинарная операция.



Приведите ещё по одному примеру бинарной, унарной и n -арной операции.

Впрочем, в школе операцией иногда называют и то, что в смысле данного определения операцией не является, например, деление на множестве рациональных чисел.



Объясните, почему на множестве рациональных чисел деление не является операцией. Будет ли деление операцией на множестве положительных рациональных чисел?

Если функция на множестве M^n не является всюду определённой, то говорят, что задана *частичная операция*. Но мы частичные операции (кроме деления) будем рассматривать крайне редко.



Объясните, почему на множестве натуральных чисел вычитание является частичной операцией.

Бинарные операции и их свойства

Среди всех операций, с которыми обычно приходится иметь дело, наиболее часто используются унарные и бинарные операции. Для унарных операций используются самые разные способы записи символа операции: для операции перехода к противоположному числу знак « $-$ » пишется перед аргументом, для операции вычисления производной знак « $'$ » – справа от аргумента (в данном случае обозначения функции), для операции взятия дополнения к множеству знак « $\bar{}$ » – над аргументом. А ведь унарная операция – это всего лишь функция одного аргумента. И писать бы привычно $f(x)$...

Для бинарных операций, как и для бинарных отношений, вместо $f(x, y)$ пишут $x f y$. Например, $x + y$ для чисел или $A \cup B$ для множеств, или $f \circ g$ для функций. Символ $\circ$ мы и дальше будем использовать для обозначения произвольной бинарной операции (вместо буквы f между аргументами); если же нам в одной записи понадобится две произвольные операции, то в помощники возьмём символ $*$.



Запись операции между аргументами сложилась исторически и вошла в привычку. В 1920 году польский математик Ян Лукасевич предложил записывать знак операции до аргументов: $+ab$, $\cdot mn$, $/xy$. Тогда и скобки будут не нужны. Например, выражение $(2 + 3) / 5$ по Лукасевичу записывается как $/ + 2 3 5$, а выражение $5 / (2 + 3)$ записывается как $/ 5 + 2 3$. И без скобок совершенно ясно, как в каждом случае вычислять значение выражения. Не прижилось.

Но в 50-е годы прошлого века, отдавая дань Я. Лукасевичу, была предложена так называемая *обратная польская запись*, когда знак операции записывается после аргументов. В этом случае выражение $(2 + 3) / 7$ запишется как $2 3 + 7 /$, а $7 / (2 + 3)$ как $7 2 3 + /$. Оказалось, что обратная польская запись очень удобна для программистских целей, например, организации вычисления значения арифметического выражения с помощью такой структуры организации данных, как стек.

Возвращаясь к вашим школьным воспоминаниям, заметим, что, как только вы познакомились с операциями, сразу же начали изучать их свойства. Прежде всего, это переместительный и сочетательный законы сложения и умножения.



Попытайтесь вспомнить формулировки этих законов.

В математике эти законы называются свойствами *коммутативности* и *ассоциативности*.

Определение 5.2. Операция $\circ$, заданная на множестве M , называется *коммутативной*, если

$$\forall x, y \in M (x \circ y = y \circ x).$$

Можно сказать и без употребления x и y : операция называется коммутативной, если от перемены мест аргументов операции результат не меняется.

Определение 5.3. Операция $\circ$, заданная на множестве M , называется *ассоциативной*, если

$$\forall x, y, z \in M ((x \circ y) \circ z = x \circ (y \circ z)).$$

Можно сказать и без употребления имён переменных: операция называется ассоциативной, если от изменения расстановки скобок результат операции не меняется.

На множестве целых чисел операция сложения коммутативна и ассоциативна, операция вычитания некоммутативна и неассоциативна.



Проверьте, что на множестве рациональных чисел операция вычисления среднего арифметического двух чисел коммутативна, но не ассоциативна.

На множестве функций, отображающих множество действительных чисел в себя, операция композиции ассоциативна (по теореме 3.1), но не коммутативна:

$$\sqrt{} \circ \sin \neq \sin \circ \sqrt{}.$$



Запишите, чему равняется $(\sqrt{} \circ \sin)(x)$ и чему $(\sin \circ \sqrt{})(x)$ и убедитесь в неравенстве этих значений для какого-нибудь подходящего значения x .

Свойство ассоциативности позволяет расставлять скобки любым способом. Поэтому в выражениях, содержащих ассоциативную операцию и только её, скобки можно вообще не писать.

Определение 5.4. Пусть на множестве M задана операция $\circ$. Элемент e из M называется *нейтральным* относительно операции $\circ$, если

$$\forall x \in M (x \circ e = e \circ x = x).$$

На множестве натуральных чисел нейтральным элементом относительно операции умножения является число 1, нейтрального элемента относительно операции сложения это множество не имеет. На множестве целых чисел нейтральным элементом относительно операции умножения также является число 1, относительно операции сложения нейтральным элементом является

число 0. На множестве функций, отображающих множество M в себя, нейтральным элементом является *тождественное* отображение, т.е. такое f , для которого $f(x) = x$ при любом $x \in M$.

Договариваются, что если операция называется умножением, то нейтральный элемент называть единицей, а если операция называется сложением, то называть нулём.

Теорема 5.1. Если на множестве M существует нейтральный элемент относительно операции $\circ$, то только один.

Доказательство. Допустим, что это не так, и выберем какие-нибудь два различных нейтральных элемента e_1 и e_2 . По определению нейтрального элемента,

$$e_1 = e_1 \circ e_2 = e_2,$$

что противоречит выбору этих элементов. □

Определение 5.5. Пусть на множестве M задана операция $\circ$ и существует нейтральный элемент e относительно этой операции. Элемент $y \in M$ называется симметричным элементу $x \in M$ относительно операции $\circ$, если

$$x \circ y = y \circ x = e.$$

В множестве натуральных чисел относительно операции умножения симметричным элементом обладает только число 1. В множестве целых чисел относительно операции сложения каждый элемент обладает симметричным — это элемент, противоположный данному. В множестве рациональных чисел каждое ненулевое число имеет симметричное относительно операции умножения — это число, обратное данному. Для взаимно-однозначных отображений множества M на себя симметричным элементом относительно операции композиции является обратное отображение.



Докажите высказанное утверждение относительно композиции взаимно однозначных отображений.

Теорема 5.2. Если операция $\circ$ на множестве M ассоциативна, то для любого элемента x из M существует не более одного симметричного ему элемента.

Доказательство. Допустим, что для некоторого элемента найдётся два симметричных элемента y_1 и y_2 . Тогда по определению

$$y_1 = y_1 \circ e = y_1 \circ (x \circ y_2) = (y_1 \circ x) \circ y_2 = e \circ y_2 = y_2.$$

Полученное противоречие с выбором элементов y_1 и y_2 доказывает теорему. □

Если операция называется умножением, то симметричный элемент математики договорились называть обратным, если операция называется сложением, то договорились называть его противоположным.

Теорема 5.2 гласит, что если операция ассоциативна, то элемент, симметричный элементу x , однозначно определён исходным элементом. В этом случае его обычно обозначают x^{-1} , независимо от того, как называется операция. Исключение составляет случай, когда операция называется сложением. Тогда применяют обозначение $-x$.

Полугруппы и группы

Определение 5.6. Множество, на котором определена ассоциативная операция, называется *полугруппой*.

Вот важные примеры полугрупп:

- множество натуральных чисел как относительно операции сложения, так и операции умножения;
- множество отрицательных целых чисел относительно сложения;
- булеан множества M относительно операций объединения и пересечения;
- множество всюду определённых функций, отображающих множество M в себя, относительно операции композиции.

Отметим два важных свойства симметричных элементов в любой полугруппе.

Теорема 5.3. Если в полугруппе M элемент x обладает симметричным, то x симметричен элементу x^{-1} . Если элементы x и y обладают симметричными элементами, то элемент $y^{-1} \circ x^{-1}$ симметричен элементу $x \circ y$.

Доказательство. Чтобы доказать второе утверждение, достаточно проверить, что $(x \circ y) \circ (y^{-1} \circ x^{-1}) = (y^{-1} \circ x^{-1}) \circ (x \circ y) = e$. Вот нужные для этого цепочки равенств:

$$(x \circ y) \circ (y^{-1} \circ x^{-1}) = x \circ y \circ y^{-1} \circ x^{-1} = x \circ (y \circ y^{-1}) \circ x^{-1} = x \circ e \circ x^{-1} = x \circ x^{-1} = e.$$

$$(y^{-1} \circ x^{-1}) \circ (x \circ y) = y^{-1} \circ x^{-1} \circ x \circ y = y^{-1} \circ (x^{-1} \circ x) \circ y = y^{-1} \circ e \circ y = y^{-1} \circ y = e.$$



Докажите самостоятельно первое утверждение теоремы 5.3. □

Утверждение теоремы обычно записывают равенствами

$$(x^{-1})^{-1} = x \text{ и } (x \circ y)^{-1} = y^{-1} \circ x^{-1}.$$



Со второй половины XX века теория полугрупп приобрела особое значение как инструмент в теории формальных языков (а языки программирования, как

вы, наверно, знаете из курса школьной информатики, являются формальными) и в абстрактной теории автоматов, т.е. программируемых устройств, которые могут работать без вмешательства человека (не путать со всемирно известным автоматом Калашникова!).

Определение 5.7. Полугруппа с нейтральным элементом, в которой каждый элемент обладает симметричным, называется *группой*.

Вот важные примеры групп:

- множество целых чисел относительно операции сложения;
- множество положительных рациональных чисел относительно операции умножения;
- множество ненулевых действительных чисел относительно операции умножения;
- множество взаимно-однозначных отображений произвольного множества M на себя.

А два примера групп обсудим особо.

Пример 1. Группа подстановок.

Пусть M_n – множество первых n натуральных чисел. *Подстановкой* на множестве M_n называется взаимно однозначное отображение множества M_n на себя. Множество всех подстановок на множестве является группой и называется *группой подстановок* или, по-другому, *симметрической группой*. Обозначается эта группа S_n . Подстановки удобно записывать в виде таблицы из двух строк: в первой строке числа от 1 до n по порядку, во второй строке значения отображения на соответствующем элементе из первой строки:

$$f = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ a_1 & a_2 & \dots & a_{n-1} & a_n \end{pmatrix},$$

т.е. $a_k = f(k)$ для $1 \leq k \leq n$.

Обычно операцию композиции подстановок называют умножением и знак этой операции между подстановками не пишут. Например,

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} - \text{произведение двух подстановок из группы } S_3.$$



Найдите, чему равно это произведение. Найдите произведение этих же подстановок, поменяв местами сомножители. Коммутативна ли операция умножения подстановок?

Пример 2. Группа движений

Напомним, что движением называется такое всюду определённое однозначное отображение множества точек плоскости в себя, при котором расстояние между образами двух точек равно расстоянию между исходными точками.



Объясните, почему такое отображение обязательно инъективно.

Несколько труднее доказать, что всякое движение сюръективно. Зато легко понять, что композиция движений – это снова движение. Значит, движения плоскости образуют группу. Она называется *группой движений плоскости*. Аналогично можно определить *группу движений пространства*.

Определение 5.8. Группа с коммутативной операцией называется *коммутативной группой*.

По-другому коммутативные группы называют *абелевыми* в честь выдающегося норвежского математика Нильса Хенрика Абеля.

Симметрическая группа S_n при $n > 2$ и группа движений плоскости некоммутативны.

Понятие группы тесно связано с разрешимостью простейших уравнений.

Теорема 5.4. Пусть G – группа относительно операции $\circ$. Тогда для любых элементов a и b из G существуют и при том единственные такие элементы x и y , для которых $a \circ x = b$ и $y \circ a = b$.

Доказательство. Для элемента a существует симметричный a^{-1} . Положим $x_0 = a^{-1} \circ b$. Тогда

$$a \circ x_0 = a \circ (a^{-1} \circ b) = (a \circ a^{-1}) \circ b = e \circ b = b,$$

т. е. построенный нами элемент x_0 удовлетворяет требованиям теоремы.



Объясните каждое равенство в написанной выше цепочке равенств.

Покажем теперь, что любой элемент группы G , удовлетворяющий равенству $a \circ x = b$, совпадает с x_0 . Пусть x_1 таков, что $a \circ x_1 = b$. Тогда $a^{-1} \circ (a \circ x_1) = a^{-1} \circ b$. В то же время $a^{-1} \circ (a \circ x_1) = (a^{-1} \circ a) \circ x_1 = e \circ x_1 = x_1$. Следовательно, $x_1 = a^{-1} \circ b = x_0$.



Докажите, что элемент $y_0 = b \circ a^{-1}$ удовлетворяет равенству $y \circ a = b$ и любой другой элемент группы G , удовлетворяющий этому равенству, совпадает с y_0 . □

Замечание. Если операция $\circ$ не коммутативна, то элементы $a^{-1} \circ b$ и $b \circ a^{-1}$ могут и не совпадать.



Проверьте, что $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}^{-1}$.

Теорема 5.4 показывает, что в любой группе разрешимы уравнения первой степени. Уравнения более высоких степеней, скажем, квадратные, уже могут не иметь решений. Например, в группе положительных рациональных чисел относительно операции умножения уравнение $x^2 = 2$ решений не имеет.



Интересно, что верно и обратное утверждение.

Теорема 5.5. Если в полугруппе M с операцией $\circ$ для любых элементов a и b существуют такие элементы x и y , для которых $a \circ x = b$ и $y \circ a = b$, то M является группой относительно этой операции.

Доказательство. Сначала покажем, что полугруппе M есть нейтральный элемент. Выберем какой-нибудь элемент a из M и рассмотрим уравнение $a \circ x = a$. Обозначим через e_1 какое-либо его решение (нам не дано, что уравнение имеет единственное решение!). Покажем, что для любого элемента c из M выполнено равенство $c \circ e_1 = c$. Для этого рассмотрим уравнение $y \circ a = c$ и обозначим через c_1 какое-нибудь его решение. Напишем цепочку равенств:

$$c \circ e_1 = (c_1 \circ a) \circ e_1 = c_1 \circ (a \circ e_1) = c_1 \circ a = c.$$

Теперь рассмотрим уравнение $y \circ a = a$ и обозначим через e_2 какое-либо его решение. Аналогично доказывается, что для любого элемента c из M выполнено равенство $e_2 \circ c = c$.

Наконец, заметим, что $e_2 = e_2 \circ e_1 = e_1$. Следовательно, $e_1 = e_2 = e$ – нейтральный элемент полугруппы M .

Докажем теперь наличие симметричного у любого элемента a из M . Рассмотрим уравнения $a \circ x = e$ и $y \circ a = e$. Обозначим через x_0 и y_0 решения этих уравнений. Тогда $x_0 = e \circ x_0 = (y_0 \circ a) \circ x_0 = y_0 \circ (a \circ x_0) = y_0 \circ e = y_0$, т.е. элемент $x_0 = y_0$ симметричен элементу a . $\square$

Эта теорема показывает, что желание иметь в данном множестве решения для любого линейного уравнения при условии ассоциативности операции неизбежно приводит к понятию группы.

Следующее утверждение является ключом к доказательству многих математических утверждений.

Теорема 5.6. (Ключевая лемма) В группе G уравнение $x \circ x = x$ имеет единственное решение $x = e$, где e – нейтральный элемент группы.

Доказательство. Поскольку $e \circ e = e$, элемент e является решением уравнения $x \circ x = x$. Пусть x_0 – какое-нибудь решение этого уравнения. Тогда

$$x_0 = x_0 \circ e = x_0 \circ (x_0 \circ x_0^{-1}) = (x_0 \circ x_0) \circ x_0^{-1} = x_0 \circ x_0^{-1} = e.$$

□

Кольца и поля

Довольно часто на множестве бывает определена не одна, а несколько бинарных операций. Например, на множестве натуральных чисел – сложение и умножение, на множестве целых чисел – сложение, умножение и вычитание, на множестве положительных действительных чисел – сложение, умножение и деление. В этом случае важную роль играют совместные свойства этих операций. Одним из таких свойств является дистрибутивность одной операции относительно другой (в школе это свойство называют распределительным законом).

Определение 5.9. Пусть на множестве M определены бинарные операции $*$ и $\circ$. Говорят, что операция $*$ *дистрибутивна* относительно операции $\circ$, если

$$\forall x, y, z \in M (x * (y \circ z) = (x * y) \circ (x * z))$$

и

$$\forall x, y, z \in M ((y \circ z) * x = (y * x) \circ (z * x)).$$

Посмотрите, элемент x вместе с операцией $*$ как бы распределяется к каждому аргументу операции $\circ$.

Вот примеры некоторых пар операций, одна из которых дистрибутивна относительно другой:

- на множестве натуральных чисел: операция умножения дистрибутивна относительно операции сложения;
- на булеане множества M : операция объединения дистрибутивна относительно операции пересечения;
- на множестве действительных чисел: операция сложения дистрибутивна относительно операции выбора минимального числа из двух чисел.



Объясните, почему в последнем примере действительно выполнено свойство дистрибутивности.



В принципе дистрибутивное свойство бинарной операции можно рассматривать относительно операции произвольной аргументности:

$$x * f(y_1, y_2, \dots, y_n) = f(x * y_1, x * y_2, \dots, x * y_n) \text{ и}$$

$$f(y_1, y_2, \dots, y_n) * x = f(y_1 * x, y_2 * x, \dots, y_n * x).$$

Например, на множестве целых чисел бинарная операция умножения

дистрибутивна относительно унарной операции взятия противоположного элемента: $x \cdot (-y) = -(x \cdot y)$ и $(-y) \cdot x = -(y \cdot x)$.

Определение 5.10. *Кольцом* называется множество M , на котором определены две бинарные операции $\circ$ и $*$, удовлетворяющие следующим условиям:

- 1) относительно операции $\circ$ множество M является коммутативной группой;
- 2) операция $*$ дистрибутивна относительно операции $\circ$.

Какими бы ни были на самом деле операции $\circ$ и $*$ в кольце M , операцию $\circ$ принято называть сложением и обозначать символом $+$, операцию $*$ принято называть умножением и обозначать $\cdot$. Как и в школьной математике, этот символ обычно не пишут между аргументами данной операции.

«Школьные» примеры колец:

- множество целых чисел относительно операций сложения и умножения;
- множество действительных чисел относительно операций сложения и умножения;
- множество многочленов с действительными коэффициентами относительно операций сложения и умножения;
- множество функций из $\mathbf{R}$ в $\mathbf{R}$ относительно операций сложения и умножения.



Объясните, почему, несмотря на дистрибутивность операции пересечения множеств относительно операции объединения, булеан непустого множества M не является кольцом.



Если относительно операции $\circ$ множество является всего лишь коммутативной полугруппой, то такое множество с двумя операциями $\circ$ и $*$, где операция $*$ дистрибутивна относительно операции $\circ$, называется *полукольцом*. Ясно, что булеан любого множества является полукольцом относительно объединения и пересечения подмножеств, причём даже не важно, какую из двух операций считать $\circ$, а какую – $*$. Другой пример полукольца – множество положительных действительных чисел, где $x \circ y = \min \{x; y\}$, а $x * y = x + y$.

Напомним, что нейтральный элемент для операции сложения называется нулём и обозначается 0 , а нейтральный элемент относительно операции умножения (если он есть) называется единицей и обозначается 1 . Любое кольцо

обладает нулём и для каждого элемента существует и при том только один противоположный элемент.



Объясните почему.

Кроме того, в кольце по теореме 5.4 для любых элементов a и b однозначно разрешимы уравнения $a + x = b$ и $y + a = b$, причем в силу коммутативности сложения $x = (-a) + b = b + (-a) = y$.

Определение 5.11. Разностью элементов a и b называется такой элемент c , для которого $b + c = a$.

Как отмечено выше, такой элемент существует и определён однозначно для любых элементов a и b кольца. Тем самым, на любом кольце определена ещё одна бинарная операция, она называется, естественно, *вычитанием*.

Теорема 5.7. (Простейшие свойства колец) В кольце K

- 1) $\forall x (0 \cdot x = x \cdot 0 = 0)$ – свойство нуля;
- 2) $\forall x, y ((-x)y = x(-y) = -xy)$ – правило знаков;
- 3) $\forall x, y, z (x(y - z) = xy - xz \text{ и } (y - z)x = yx - zx)$ – дистрибутивность умножения относительно вычитания.

Доказательство.

- 1) Обозначим $0 \cdot x$ через a . Тогда

$$a + a = 0x + 0 \cdot x = (0 + 0)x = 0 \cdot x = a.$$

Согласно ключевой лемме $a = 0$. Равенство $x \cdot 0 = 0$ доказывается аналогично.

- 2) Для доказательства $(-x)y = -xy$ достаточно проверить, что $xy + (-x)y = 0$. Это очевидно в силу дистрибутивности умножения относительно сложения и пункта 1):

$$xy + (-x)y = (x + (-x))y = 0y = 0.$$

Равенство $x(-y) = -xy$ доказывается аналогично.



Напишите доказательства равенств $x \cdot 0 = 0$ и $x(-y) = -xy$. Докажите самостоятельно пункт 3) теоремы 5.7. □

Определение 5.11. Кольцо называется *коммутативным*, если операция умножения коммутативна. Кольцо называется *ассоциативным*, если операция умножения ассоциативна.

Все кольца из «школьных» примеров коммутативны и ассоциативны.

Приведём ещё два важных примера колец.

Пример 1. Кольцо вычетов по модулю n .

Пусть $M = \{0, 1, 2, \dots, n - 1\}$. Определим на M операции сложения и умножения следующими правилами:

$x \oplus y$ – остаток при делении на число n обычной суммы чисел x и y ;

$x \odot y$ – остаток при делении на число n обычного произведения чисел x и y .

Ясно, что оба правила действительно задают операции на множестве M и что 0 – нейтральный элемент для операции $\oplus$. Противоположный нулю элемент – он сам. Если же $x \neq 0$, то противоположный ему элемент вычисляется по правилу $n - x$ (здесь символ « $-$ » обозначает обычную операцию вычитания на множестве целых чисел).



Докажите коммутативность и ассоциативность операции $\oplus$ на множестве M . Тем самым, будет обосновано, что M является коммутативной группой относительно операции $\oplus$.

Коммутативность операции $\odot$ на множестве M с очевидностью следует из коммутативности обычного умножения чисел. Поэтому из двух формул, обосновывающих дистрибутивность, достаточно доказать только одну.



Докажите дистрибутивность операции $\odot$ относительно операции $\oplus$. Проверьте также, что операция $\odot$ на множестве M ассоциативна. Тем самым, будет обосновано, что M является коммутативным и ассоциативным кольцом относительно операций $\odot$ и $\oplus$.

В дальнейшем мы, следуя договорённости, будем обозначать операции $\odot$ и $\oplus$ обычными знаками $\cdot$ и $+$. Это кольцо называют *кольцом вычетов по модулю n* и обозначают $\mathbb{Z}_n$.



В кольце $\mathbb{Z}_6$ вычислите $2 + 5$ и $2 \cdot 5$. Какой элемент в этом кольце противоположен элементу 4? А какой элемент противоположен элементу 3?

Пример 2. Кольцо квадратных матриц размера 2×2 .

В конце лекции о графах было дано определение матрицы над произвольным множеством K . Если же на множестве K определены какие-либо операции, то на множестве матриц могут быть определены те или иные полезные операции. Например, если на множестве K определена бинарная операция $\circ$, то для пары матриц одинакового размера можно определить операцию, которую мы будем обозначать тем же символом, по правилу

$$\begin{pmatrix} a_{11} & \dots & a_{1j} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{i1} & \dots & a_{ij} & \dots & a_{in} \\ \dots & \dots & \dots & \dots & \dots \\ a_{m1} & \dots & a_{mj} & \dots & a_{mn} \end{pmatrix} \circ \begin{pmatrix} b_{11} & \dots & b_{1j} & \dots & b_{1n} \\ \dots & \dots & \dots & \dots & \dots \\ b_{i1} & \dots & b_{ij} & \dots & b_{in} \\ \dots & \dots & \dots & \dots & \dots \\ b_{m1} & \dots & b_{mj} & \dots & b_{mn} \end{pmatrix} =$$

$$\begin{pmatrix} a_{11} \circ b_{11} & \dots & a_{1j} \circ b_{1j} & \dots & a_{1n} \circ b_{1n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{i1} \circ b_{i1} & \dots & a_{ij} \circ b_{ij} & \dots & a_{in} \circ b_{in} \\ \dots & \dots & \dots & \dots & \dots \\ a_{m1} \circ b_{m1} & \dots & a_{mj} \circ b_{mj} & \dots & a_{mn} \circ b_{mn} \end{pmatrix}.$$

Такое определение операции над матрицами называют *покомпонентным*.

Пусть операция $\circ$ коммутативна (ассоциативна). Проверьте, что на множестве матриц при покомпонентном определении операции соответствующая операция также будет коммутативной (ассоциативной). Верно ли, что если в множестве K есть элемент, нейтральный относительно операции $\circ$, то и множество матриц над M при покомпонентном определении операции также будет нейтральный элемент?

В основном нас будет интересовать ситуация, когда множество K является кольцом. Сложение матриц над кольцом K определим покомпонентно. Но, конечно же, хочется определить ещё и операцию умножения. Чтобы не погружать вас сразу в матричные глубины, мы пока ограничимся квадратными матрицами одного размера. Это, в частности, означает, что количество элементов в любой строке одной матрицы совпадает с количеством элементов в любом столбце второй матрицы. И сначала мы определим, что значит строку элементов кольца K умножить на столбец элементов того же кольца.

Пусть есть строка $(a_1, a_2, \dots, a_n)$ и столбец $\begin{pmatrix} b_1 \\ b_2 \\ \dots \\ b_n \end{pmatrix}$, составленные из

элементов кольца K . Их *произведением* (именно строки на столбец!) называют элемент кольца K , равный $a_1 b_1 + a_2 b_2 + \dots + a_n b_n$.

Пусть теперь у вас есть две квадратные матрицы над кольцом K одного размера n . Тогда их произведением называется квадратная матрица того же размера, у которой на ij -м месте (т.е. на пересечении i -й строки и j -го столбца) стоит произведение i -й строки первой матрицы на j -го столбца второй матрицы.

Например, если рассматривается множество квадратных матриц размера 2×2 , то определение операций сложение и умножения будут выглядеть так:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix};$$

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}.$$

Хотя умножение матриц выглядит причудливо, через некоторое время вы убедитесь, что оно весьма практично.



Понять естественность указанного способа умножения строки на столбец легко, если рассмотреть следующий житейский пример.

Вы пришли в продуктовый магазин и набрали в свою корзину покупки: полкило сливочного масла, два пакета молока, триста грамм конфет «Птичье молоко» и булочку с маком. Запишем эти числовые сведения в строку:

(0,5; 2; 0,3; 1).

На кассе, куда вы подошли оплатить покупку, есть прайс-лист:

Сливочное масло, 1 кг – 650 р.

Молоко, 1 пакет – 46 р.

Конфеты «Птичье молоко» – 340 р.

Булочка с маком, 1 шт. – 17 р.

Видите, цены записаны в столбец:

$$\begin{pmatrix} 650 \\ 46 \\ 340 \\ 17 \end{pmatrix}.$$

Компьютер кассового аппарата умножает строку ваших покупок на столбец цен и сообщает, сколько вы должны заплатить за покупку.

Выполнив задание 6, вы докажете, что множество матриц размера 2×2 над произвольным кольцом само является кольцом. Его обозначают $M_2(K)$. На самом деле кольцом относительно операций сложения и умножения будет и множество квадратных матриц произвольного размера. Но об этом позже, за рамками этого вводного курса.



Конечно, определить таким же образом операции над матрицами можно не только для колец, но и полуколец. Особый интерес представляет случай квадратных матриц над полукольцом положительных чисел с операциями $\min$ и $+$. В настоящее время эта алгебраическая структура используется для анализа и построения алгоритмов оптимального планирования.

Вернёмся к обсуждению свойств колец. Они для вас привычны, и вам, скорее всего, даже в голову не приходило, что хорошо было бы их доказать.

Возможно, многие из вас считают, что свойство, обратное свойству 0, тоже верно.



Как вы думаете, верно ли следующее утверждение: если произведение двух элементов кольца равно 0, то хотя бы один из множителей равен 0?

Давайте внимательно посмотрим на кольцо функций из $\mathbf{R}$ в $\mathbf{R}$ относительно операций сложения и умножения. Какая функция является нулём в этом кольце? Ясно, что это функция, тождественно равная 0 – только она, будучи прибавленной к любой функции её не меняет. Рассмотрим две функции: $f(x) = x + |x|$ и $g(x) = x - |x|$ (здесь $|x|$ обозначает абсолютную величину числа x). Каждая из этих функций не является 0 кольца функций. Однако $f(x)g(x) = x^2 - |x|^2 = 0$ для любого элемента x из $\mathbf{R}$. Так что уже в школе вы знали такое кольцо, в котором произведение двух ненулевых элементов равно 0.

Определение 5.12. Ненулевые элементы a и b кольца K называются *делителями нуля*, если $ab = 0$.

Указанные нами функции $f(x)$ и $g(x)$ являются делителями нуля в кольце функций из $\mathbf{R}$ в $\mathbf{R}$.



Проверьте, что элементы 2 и 3 являются делителями нуля в кольце $\mathbf{Z}_6$.

Определение 5.13. Коммутативное ассоциативное кольцо без делителей нуля называются *областью целостности*.

Кольцо целых чисел является областью целостности. Сам термин «область целостности» возник потому, что такие кольца по своим свойствам очень похожи на кольцо целых чисел.

Пусть K – произвольное ассоциативное кольцо с 1. Через K^* обозначают множество всех обратимых (т.е. таких, для которых есть обратный элемент относительно операции умножения) элементов. Ясно, что $1 \in K^*$.



Какой элемент обратен 1? А $0 \in K^*$?

Теорема 5.8. В ассоциативном кольце с 1 множество обратимых элементов является группой относительно операции умножения.

Доказательство. В силу теоремы 5.3 (найдите её формулировку!) произведение обратимых элементов – снова обратимый элемент. Значит, множество обратимых элементов замкнуто относительно операции умножения, и ввиду ассоциативности кольца является полугруппой. У неё есть нейтральный элемент – это 1 кольца. Снова, по теореме 5.3, обратный элемент к каждому элементу этой полугруппы также обратим и, следовательно, принадлежит этой полугруппе. Тем самым эта полугруппа является группой. $\square$

Определение 5.14. Коммутативное ассоциативное кольцо с 1, каждый ненулевой элемент которого обратим, называется *полем*.

Кольцо рациональных чисел и кольцо действительных чисел являются полями.

Теорема 5.9. Любое поле является областью целостности.

Доказательство. Предположим, что в некотором поле есть ненулевые элементы a и b , для которых $ab=0$. По определению поля, элемент a обратим. Тогда $b = 1 \cdot b = (a^{-1}a)b = a^{-1}(ab) = a^{-1} \cdot 0 = 0$, что противоречит с $b \neq 0$. $\square$

Кольцо целых чисел: делимость и взаимная простота целых чисел

С кольцом целых чисел вы знакомы с 6-го класса. Только тогда вы не называли его кольцом. И было это давно. Поэтому напомним основные понятия и свойства кольца целых чисел.

Определение 5.15. Разделить целое число a на целое число $b \neq 0$ с остатком – это значит найти такие целые числа q и r , для которых $a = bq + r$, причём $0 \leq r < |b|$. Число q называют *частным* при делении числа a на b , а число r – *остатком*.



Разделите с остатком число -10 на 4 , а число -12 на -5 .

Определение 5.16. Говорят, что целое число a *делится на целое число b* , или, по-другому, что число a *кратно числу b* , если существует такое целое число c , для которого $a = bc$. В этом случае число b называют *делителем* числа a .

Следующее утверждение очевидно: если целое число $b \neq 0$, то целое число a кратно числу b тогда и только тогда остаток при делении числа a на число b равен 0 .

Тот факт, что число b является делителем числа a , записывают так: $b \mid a$. В свою очередь, если a делится на b , пишут $a : b$.



Докажите, что если числа a_1 и a_2 делятся на число b , то для любых целых чисел u_1 и u_2 число $u_1a_1 + u_2a_2$ тоже делится на b . Сформулируйте обратное утверждение. Будет ли оно верным?

Ясно, что 0 делится на любое целое число.



Есть ли число, которое делится на 0 ? Если да, приведите пример хотя бы одного из них; если нет, объясните почему.

Определение 5.17. *Общим делителем* целых чисел a и b называют целое число d , которое делит оба эти числа. *Общим кратным* целых чисел a и b называют целое неотрицательное число c , которое делится и на a , и на b .



Какое число будет общим кратным для чисел 0 и 5?

Для любого ненулевого целого числа a его делитель не больше, чем $|a|$. Поэтому у такого числа лишь конечное число делителей. Число 0 и здесь отличилось – у него делителем является любое целое число. Поэтому определение наибольшего общего делителя двух целых чисел может показаться несколько необычным.

Определение 5.18. *Наибольшим общим делителем* целых чисел a и b называют наибольший элемент относительно обычного порядка $\leq$ в множестве всех неотрицательных общих делителей чисел a и b , не превосходящих ни $|a|$, ни $|b|$. *Наименьшим общим кратным* целых чисел a и b называют наименьший элемент относительно обычного порядка $\leq$ в множестве всех неотрицательных общих кратных чисел a и b .



Найдите наибольший общий делитель и наименьшее общее кратное
а) чисел -4 и 6 ; б) чисел 100 и 0 ; в) чисел -1024 и -1024 ; г) чисел 0 и 0 .

Заметим, что для любого целого числа a наибольший общий делитель этого числа и числа 0 равен $|a|$, а их наименьшее общее кратное равно 0 .



Объясните высказанное утверждение относительно наибольшего общего делителя и наименьшего общего кратного, когда хотя бы одно из чисел равно 0 .

Существование и единственность наибольшего общего делителя d двух целых чисел a и b следует из того, что $0 \leq d \leq \max \{|a|, |b|\}$. Существование и единственность наименьшего общего кратного m двух целых чисел a и b следует из того, что $d \geq \min \{|a|, |b|\}$.

Если задуматься, то становится ясно, что на кольце целых чисел определены ещё две бинарные операции: вычисление наибольшего общего делителя двух целых чисел – эту операцию будем обозначать НОД – и вычисление наименьшего общего кратного двух целых чисел – эту операцию будем обозначать НОК.

В школе вас учили искать наибольший общий делитель и наименьшее общее кратное, используя разложение чисел на простые множители. Однако, сама задача нахождения простых множителей настолько трудоёмка, что на этом

основаны современные криптографические системы: зашифрованная информация утратит своё значение раньше, чем удастся её расшифровать. Но ещё в IV веке до н.э. древнегреческим ученым Аристотелем был опубликован алгоритм вычисления наибольшего общего делителя двух натуральных чисел, который носит название алгоритма Евклида. Вот неформальное, но вполне строгое описание этого алгоритма для целых чисел.

Пусть a и b – ненулевые целые числа (если одно число 0, то мы с этим разобрались раньше).

Если $a \mid b$ или $b \mid a$, то $\text{НОД}(a, b) = \min \{|a|, |b|\}$.

Если $a \nmid b$ или $b \nmid a$, то разделим a на b с остатком: $a = bq_1 + r_1$.

Если $r_1 \mid b$, то процесс закончен, иначе разделим b на r_1 с остатком: $b = r_1q_2 + r_2$.

Если $r_2 \mid r_1$, то процесс закончен, иначе разделим r_1 на r_2 с остатком: $r_1 = r_2q_3 + r_3$.

...

Многоточие означает, что мы продолжаем этот процесс, пока один из получающихся остатков не разделится на следующий уже без остатка. Оказывается, если процесс в какой-то момент закончится, то последний ненулевой остаток и будет равен $\text{НОД}(a, b)$.

Теорема 5.10. Для любых ненулевых чисел a и b процесс в алгоритме Евклида заканчивается за конечное число шагов и последний ненулевой остаток равен $\text{НОД}(a, b)$.

Доказательство. По определению остатка, получаем последовательность $|b| > r_1 > r_2 > \dots > r_k > \dots$. При этом все $r_k \geq 0$. Однако между 0 и $|b|$ не более чем $|b| - 1$ натуральных чисел, значит, не позже чем через $|b|$ шагов процесс закончится, т.е. $r_{n+1} = 0$ для некоторого n , а $r_n \neq 0$.

Выпишем всю историю получения остатков:

$$a = bq_1 + r_1;$$

$$b = r_1q_2 + r_2;$$

$$r_1 = r_2q_3 + r_3;$$

$$r_2 = r_3q_4 + r_4;$$

...

$$r_{n-3} = r_{n-2}q_{n-1} + r_{n-1};$$

$$r_{n-2} = r_{n-1}q_n + r_n;$$

$$r_{n-1} = r_nq_{n+1}.$$

Последнее равенство означает, что $r_n \mid r_{n-1}$. Поднимаясь на строчку выше, мы видим, что r_n делит правую часть равенства, а значит, $r_n \mid r_{n-2}$. Еще поднимаемся на одну строку и получаем, что $r_n \mid r_{n-3}$. И так далее, доходим до второй строки сверху и получаем, что $r_n \mid b$. Наконец, рассматривая первую строку, получаем, что $r_n \mid a$. Тем самым r_n – положительный общий делитель чисел a и b .

Чтобы показать, что он наибольший общий делитель, перепишем историю получения остатков в следующем виде:

$$r_1 = a - bq_1;$$

$$r_2 = b - r_1q_2;$$

$$r_3 = r_1 - r_2q_3;$$

...

$$r_{n-2} = r_{n-4} - r_{n-3}q_{n-2};$$

$$r_{n-1} = r_{n-3} - r_{n-2}q_{n-1};$$

$$r_n = r_{n-2} - r_{n-1}q_n.$$

Если теперь c – некоторый положительный общий делитель чисел a и b , то первая строка в этих записях показывает, что $c \mid r_1$. Тогда вторая строка показывает, что $c \mid r_2$. Глядя на третью строку, делаем вывод, что $c \mid r_3$. И т.д. Добравшись до последней строки, делаем вывод, что $c \mid r_n$. В силу положительности c и r_n , получаем, что $c \leq r_n$, т.е. r_n – наибольший общий делитель чисел a и b . $\square$

Следствие 5.11. Для любых целых чисел a и b существуют такие целые числа u и v , что $au + bv = \text{НОД}(a, b)$.

Доказательство. Последнее равенство в «переписанной истории» показывает, как r_n выражается через r_{n-1} и r_{n-2} с некоторыми целыми коэффициентами: $r_n = r_{n-2} - r_{n-1}q_n$. Подставим в это равенство выражение из предыдущей строки:

$$r_n = r_{n-2} - (r_{n-3} - r_{n-2}q_{n-1})q_n = r_{n-2}(1 + q_{n-1}q_n) - r_{n-3}q_n.$$

Теперь r_n выражено с целыми коэффициентами $1 + q_{n-1}q_n$ и $-q_n$ через r_{n-2} и r_{n-3} . Подставим в полученное равенство выражение для r_{n-2} :

$$\begin{aligned} r_n &= r_{n-2}(1 + q_{n-1}q_n) - r_{n-3}q_n = (r_{n-4} - r_{n-3}q_{n-2})(1 + q_{n-1}q_n) - r_{n-3}q_n = \\ &= r_{n-4}(1 + q_{n-1}q_n) - r_{n-3}(q_{n-2}(1 + q_{n-1}q_n) + q_n). \end{aligned}$$

Теперь r_n выражено с целыми коэффициентами через r_{n-3} и r_{n-4} . Продолжая этот процесс, мы придём к выражению r_n через a и b с некоторыми целыми коэффициентами, которые и обозначим как u и v . $\square$

Определение 5.19. Целые числа a и b называются взаимно простыми, если $\text{НОД}(a, b) = 1$.

Теорема 5.12. (Критерий взаимной простоты) Целые числа a и b взаимно просты тогда и только тогда, когда существуют целые числа u и v такие, что $au + bv = 1$.

Доказательство. Если a и b взаимно просты, то существование целых чисел u и v , для которых $au + bv = 1$, следует из определения и следствия 5.11. Обратно, если $au + bv = 1$ и d – некоторый положительный общий делитель чисел a и b , то d является положительным делителем числа 1, а у числа 1 нет положительных делителей, отличных от него самого. Значит, $d = 1$. $\square$

Кольца вычетов по модулю n

Некоторое время назад вы обнаружили, что в кольце $\mathbb{Z}_6$ элементы 2 и 3 являются делителями нуля. А какие элементы обратимы в этом кольце?



Укажите все обратимые элементы в кольце $\mathbb{Z}_6$.

Давайте найдём ответ на данный вопрос в общем случае.

Теорема 5.13. Элемент a из $\mathbb{Z}_n$ обратим тогда и только тогда, число a взаимно просто с n .

Доказательство. Пусть элемент a из $\mathbb{Z}_n$ обратим. Тогда существует такой элемент u из $\mathbb{Z}_n$, для которого au даёт остаток 1 при делении на n . Иными словами, $au = nq + 1$. Значит, $au - nq = 1$. По критерию взаимной простоты (теорема 5.12) числа a и n взаимно просты.

Обратно. Пусть a и n взаимно просты. По критерию взаимной простоты существуют такие целые числа u и v , для которых $au + nv = 1$. Разделим u на n с остатком: $u = nq + r$. Заметим, что $r \in \mathbb{Z}_n$. В то же время,

$$au + nv = a(nq + r) + nv = ar + n(v + aq).$$

Поэтому $ar = n(-v - aq) + 1$, т.е. $(-v - aq)$ – частное при делении на n , а 1 – остаток. Это означает, что r – элемент, обратный к a в $\mathbb{Z}_n$. $\square$

Чтобы кольцо $\mathbb{Z}_n$ оказалось полем, надо, чтобы каждый его ненулевой элемент был обратим. По теореме 5.13 это значит, что любое натуральное число, меньшее n , должно быть взаимно просто с n . Такое возможно в том и только том случае, когда n – простое число. Тем самым, имеем

Следствие 5.14. Кольцо $\mathbb{Z}_n$ является полем тогда и только тогда, когда n – простое число.

Поле Z_2 является самым маленьким по числу элементов полем: в нём всего два элемента – 0 и 1. Тем не менее, именно оно играет особо важную роль в компьютерных делах – ведь в компьютере вся информация кодируется этими двумя символами, и многие алгоритмы построены на том, что это элементы поля.

Следующее по числу элементов поле – это Z_3 . Его элементы – 0, 1 и 2. Элемент 2 противоположен элементу 1, поэтому можно вместо 2 писать -1 , т.е. считать, что $Z_3 = \{0, 1, -1\}$. Это очень удобно для выполнения действий над элементами этого поля.



Элементы поля Z_3 используются в качестве цифр в так называемой уравновешенной троичной системе счисления. Она намного экономнее двоичной системы при записи чисел, и в ней легко реализуются арифметические операции над числами (особенно операция вычитания). В МГУ даже был построен компьютер, процессор которого работал в уравновешенной троичной системе счисления. Он получил название «Сетунь» по имени речки, протекающей недалеко от МГУ. К сожалению, электронная база, позволяющая легко реализовать три различных состояния, пока не создана, поэтому развития данная линия вычислительной техники не получила. Но те, кому интересен этот феномен, могут без больших усилий найти о нём информацию.

Задания для самостоятельной работы

1. Объясните, почему для любой операции её нейтральный элемент всегда обладает симметричным.

2.^T Укажите все элементы, которые в множестве целых чисел обладают обратными относительно операции умножения.

3.^T В группе S_5 вычислите

а) произведение $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}$; б) степень $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}^3$; в) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix}^{-1}$.

4.^T В группе S_4 решите уравнения

а) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} X = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$; б) $X \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$.

5. Докажите, что в любой группе для любого элемента a из этой группы квадратное уравнение $x \circ x = a \circ x$ имеет и при том единственное решение.

6. Проверьте, что множество квадратных матриц размера 2×2 с элементами из произвольного кольца K является

- а) коммутативной группой относительно сложения;
- б) кольцом относительно операций умножения и сложения.

7. Пусть K – произвольное кольцо с 1. Проверьте, что матрица $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ является нейтральным элементом относительно умножения.

8. Пусть K – ассоциативное кольцо. Проверьте, что кольцо $M_2(K)$ тоже ассоциативно.

9.^T В кольце $M_2(\mathbf{R})$ вычислите

$$\text{а) } \begin{pmatrix} -1 & 2 \\ 3 & 1 \end{pmatrix} \begin{pmatrix} 2 & -5 \\ 4 & 1 \end{pmatrix}; \quad \text{б) } \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}^3; \quad \text{в) } \begin{pmatrix} 3 & 1 \\ -1 & 1 \end{pmatrix}^{-1}.$$

10. Является ли кольцо $M_2(\mathbf{R})$ полем? Ответ «да» надо обосновать, ответ «нет» аргументировать приведением примера ненулевой необратимой матрицы.

11. Верно ли утверждение: если сумма двух целых чисел a_1 и a_2 делится на b , то и каждое из чисел a_1 и a_2 делится на b ?

12.^T Укажите все обратимые элементы а) кольца $\mathbf{Z}_{12}$; б) кольца $\mathbf{Z}_{18}$.

13.^T На известном вам языке программирования запрограммируйте алгоритм Евклида.

14.^T На известном вам языке программирования запрограммируйте алгоритм нахождения для заданных целых чисел a и b таких целых чисел u и v , чтобы $au + bv = \text{НОД}(a, b)$ и значение $|u| + |v|$ было бы наименьшим.

15.^T На известном вам языке программирования запрограммируйте алгоритм нахождения всех обратимых элементов в кольце $\mathbf{Z}_n$.

Лекция 6. Метод математической индукции

Есть удивительный и очень важный способ доказательства математических утверждений, в которых в том или ином виде фигурируют натуральные числа. Он получил название метода математической индукции. Не вдаваясь в подробности происхождения этого названия, поясним суть этого метода.

Базовая версия метода математической индукции

Представьте себе, что на числовой оси в каждой точке, изображающей натуральное число, помещена лампочка. При этом лампочки соединены так, что если зажигается лампочка в точке n , тут же зажигается лампочка в точке $n + 1$. Что произойдёт, если зажечь лампочку в точке 1? Каждому ясно, что зажгутся все лампочки на числовой оси.

Пусть у нас имеется некоторое утверждение, в котором фигурирует натуральное число n . Выражаясь языком лекции 1 – мы располагаем некоторым предикатом $P(n)$. Будем считать, что лампочка в точке n зажигается тогда и только тогда, когда $P(n) = 1$. Фраза «если зажигается лампочка в точке n , тут же зажигается лампочка в точке $n + 1$ » попросту означает, что импликация $P(n) \Rightarrow P(n + 1)$ истинна для любого натурального числа n . Если это так и, кроме того, $P(1) = 1$, то все лампочки зажглись и, значит, утверждение $P(n)$ истинно для любого натурального n .

Сформулируем то, что мы обсудили, следующим образом.

Принцип математической индукции. Пусть $P(n)$ – предикат от натурального аргумента n , для которого выполнены условия:

- 1) высказывание $P(1)$ истинно;
- 2) из истинности высказывания $P(n)$ следует истинность высказывания $P(n + 1)$.

Тогда высказывание $P(n)$ истинно для любого натурального числа n .

Тем самым доказательство с использованием принципа математической индукции всегда состоит из двух частей:

- 1) проверки истинности $P(1)$ (так называемая, *база индукции*);
- 2) доказательства истинности импликации $P(n) \Rightarrow P(n + 1)$ (называемого *шагом индукции* или, по-другому, *индуктивным переходом*).

Пример 1. Доказать, что $1 + 3 + \dots + (2n - 1) = n^2$.

Доказательство. Обозначим через a_n левую часть доказываемого равенства, а через b_n – его правую часть. Тогда $P(n)$ – это утверждение $a_n = b_n$.

База индукции. Проверяем, что $P(1)$ истинно:

$$a_1 = 1;$$

$$b_1 = 1.$$

Значит, $a_1 = b_1$.

Шаг индукции. Считаем, что $P(n)$ истинно, т. е. $a_n = b_n$. Тогда

$$\begin{aligned} a_{n+1} &= 1 + 3 + \dots + (2n-1) + (2n+1) = a_n + (2n+1) = b_n + (2n+1) = \\ &= n^2 + (2n+1) = (n+1)^2 = b_{n+1}, \end{aligned}$$

т. е. $P(n+1)$ тоже истинно.

Согласно принципу математической индукции утверждение $P(n)$ истинно для любого натурального числа n . □

Конечно, при доказательстве методом математической индукции совсем необязательно вводить обозначения a_n , b_n , $P(n)$, но надо всегда отчётливо понимать, какое именно утверждение, зависящее от n , предполагается доказать и как связаны компоненты этого утверждения при переходе от n к $n+1$.

Модификация шага индукции

В рассмотренном нами «лампочном устройстве» изменим условие того, когда зажигается следующая лампочка: пусть лампочка в точке $n+1$ зажигается в том и только том случае, если зажжены все предыдущие лампочки. Ясно, что и в такой конструкции, как только зажжется лампочка в точке 1, гореть будут все лампочки.

Принцип математической индукции (с МШ). Пусть $P(n)$ – предикат от натурального аргумента n , для которого выполнены условия:

- 1) высказывание $P(1)$ истинно;
- 2) из истинности высказывания $P(k)$ для всех $k \leq n$ следует истинность высказывания $P(n+1)$.

Тогда высказывание $P(n)$ истинно для любого натурального числа n .

Пример 2. Доказать, что любое натуральное число можно представить в виде

$$3^{u_0} \cdot 2^{v_0} + 3^{u_1} \cdot 2^{v_1} + \dots + 3^{u_s} \cdot 2^{v_s},$$

где $u_0 > u_1 > \dots > u_s \geq 0$ и $0 \leq v_0 < v_1 < \dots < v_s$ – целые числа. (Возможно, что в сумме присутствует только одно слагаемое, $s = 0$.)

Доказательство. База индукции. $n = 1 = 3^0 \cdot 2^0$, т. е. $u_0 = v_0 = 0$.

Шаг индукции. Предположим, что для всех $k \leq n$ утверждение истинно. Рассмотрим число $n + 1$. Возможны два случая: число $n + 1$ чётно и число $n + 1$ нечётно. Рассмотрим их отдельно.

Пусть $n + 1$ чётно, т. е. $n + 1 = 2m$ для некоторого натурального m . По предположению индукции число m представимо в указанном виде. Тогда ясно, что и $2m$ тоже представимо в требуемом виде: достаточно просто каждый показатель степени числа 2 в таком представлении увеличить на 1.

Пусть $n + 1$ нечётно. Выберем целое неотрицательное число u_0 таким, чтобы $3^{u_0} \leq n + 1 < 3^{u_0+1}$. Число $(n + 1) - 3^{u_0}$ чётно и меньше, чем $3^{u_0+1} - 3^{u_0} = 2 \cdot 3^{u_0}$. По предположению индукции число $((n + 1) - 3^{u_0}) / 2$ представимо в виде $3^{u_1} \cdot 2^{v_1} + \dots + 3^{u_s} \cdot 2^{v_s}$, для некоторых $u_1 > \dots > u_s \geq 0$ и $0 \leq v_1 < \dots < v_s$. Значит, $n + 1 = 3^{u_0} \cdot 2^0 + 3^{u_1} \cdot 2^{v_1+1} + \dots + 3^{u_s} \cdot 2^{v_s+1}$, причём $u_0 > u_1$ в силу соотношений $3^{u_1} \cdot 2^{v_1+1} + \dots + 3^{u_s} \cdot 2^{v_s+1} = (n + 1) - 3^{u_0} < 2 \cdot 3^{u_0}$.

Шаг индукции доказан. Следовательно, доказано утверждение. $\square$

Модификация базы индукции

Часто требуется доказать утверждение для всех натуральных n , начиная с некоторого числа. Можно представить себе, что первая горящая лампочка оказалась не в точке 1, а в некоторой точке $m > 1$.

Принцип математической индукции (с МБ). Пусть $P(n)$ – предикат от натурального аргумента n , для которого выполнены условия:

- 1) высказывание $P(m)$ истинно;
- 2) из истинности высказывания $P(n)$ для $n \geq m$ следует истинность высказывания $P(n + 1)$.

Тогда высказывание $P(n)$ истинно для любого натурального числа n , большего или равного m .

Пример 3. Доказать, что при всех натуральных $n \geq 5$ выполняется $2^n > n^2$.

Доказательство. База индукции. При $n = 5$ имеем $2^5 = 32 > 25 = 5^2$.

Шаг индукции. Пусть утверждение доказано для n , т. е. считаем выполненным неравенство $2^n > n^2$. Тогда $2^{n+1} = 2 \cdot 2^n > 2n^2 > n^2 + 2n + 1$, поскольку неравенство $n^2 > 2n + 1$, равносильное неравенству $(n - 1)^2 - 2 > 0$, при $n \geq 5$ очевидно.

Разумеется, можно применять метод математической индукции с одновременно модифицированными вариантами и базы, и шага индукции.

Математическая индукция с большим шагом

Предположим, что в нашей лампочной гирлянде лампочку в каждой точке n удалось связать не со следующей лампочкой, а лампочкой в точке $n + k$ (нас интересует $k > 1$). Чтобы обеспечить горение лампочек во всех точках начиная с некоторого m , придется «вручную» зажечь лампочки в точках $m, m + 1, \dots, m + k - 1$.

Принцип математической индукции (с БШ). Пусть $P(n)$ – предикат от натурального аргумента n , для которого выполнены условия:

- 1) высказывания $P(m), P(m + 1), \dots P(m + k - 1)$ истинны;
- 2) из истинности высказывания $P(n)$ для $n \geq m$ следует истинность высказывания $P(n + k)$.

Тогда высказывание $P(n)$ истинно для любого натурального числа n , большего или равного m .

Пример 4. В некоторой стране есть денежные купюры номиналом 3 и 5 тугриков. Доказать, что любую сумму, не меньшую 8 тугриков, можно уплатить этими купюрами.

Доказательство. База индукции: $8 = 3 + 5$; $9 = 3 + 3 + 3$; $10 = 5 + 5$.

Шаг индукции. Если сумму в n тугриков можно заплатить этими купюрами, то и сумму $n + 3$ тоже можно уплатить.

По-другому эту разновидность метода называют *индукцией с множественной базой*.

Метод обратной математической индукции

Ещё раз модифицируем наше «лампочное устройство». Пусть в нём лампочки соединены так, что при горящей лампочке в точке n обязательно горит лампочка в точке $n - 1$. Если нам с помощью какого-то приёма удалось зажечь лампочку в какой-то далёкой точке m , то автоматически зажгутся и все предыдущие лампочки.

Принцип обратной математической индукции. Пусть $P(n)$ – предикат от натурального аргумента n , для которого выполнены условия:

- 1) высказывание $P(m)$ истинно;
- 2) из истинности высказывания $P(n)$ для $n \leq m$ следует истинность высказывания $P(n - 1)$.

Тогда высказывание $P(n)$ истинно для любого натурального числа n , меньшего или равного m .

В качестве примера мы рассмотрим доказательство важного неравенства, которое называют неравенством между средним арифметическим и средним геометрическим. Напомним, что *средним арифметическим* чисел $x_1, x_2, \dots, x_n$ называют число $\frac{x_1+x_2+\dots+x_n}{n}$, а *средним геометрическим* тех же чисел называют число $\sqrt[n]{x_1 x_2 \dots x_n}$.

Теорема 6.1. Для любых неотрицательных чисел $x_1, x_2, \dots, x_n$ среднее арифметическое этих чисел не меньше их среднего геометрического.

Доказательство. Заметим, что, если хотя бы одно из чисел равно 0, то требуемое неравенство очевидно выполняется. Поэтому будем считать, что все числа положительные.

Сначала по индукции докажем это неравенство для $n = 2^m$.

База индукции: $m = 1$. Неравенство для этого m имеет вид $\frac{x_1+x_2}{2} \geq \sqrt{x_1 x_2}$. Оно, скорее всего, знакомо вам ещё со школы.



Докажите это неравенство.

Шаг индукции. Пусть утверждение доказано для m ; докажем его для $m + 1$.

$$\begin{aligned} \frac{x_1+x_2+\dots+x_{2^{m+1}}}{2^{m+1}} &= \frac{\frac{x_1+x_2+\dots+x_{2^m}}{2^m} + \frac{x_{2^m+1}+x_{2^m+2}+\dots+x_{2^{m+1}}}{2^m}}{2} \geq \\ &\geq \frac{2^m \sqrt{x_1 x_2 \dots x_{2^m}} + 2^m \sqrt{x_{2^m+1} x_{2^m+2} \dots x_{2^{m+1}}}}{2} \geq \\ &\geq \sqrt{2^m \sqrt{x_1 x_2 \dots x_{2^m}} \cdot 2^m \sqrt{x_{2^m+1} x_{2^m+2} \dots x_{2^{m+1}}}} = 2^{m+1} \sqrt{x_1 x_2 \dots x_{2^{m+1}}}. \end{aligned}$$



Укажите, в каком месте этой цепочки равенств и неравенств мы воспользовались предположением индукции, в каком – утверждением базы индукции, а в каком – свойством корней.

Приступим теперь к доказательству общего утверждения.

Шаг (обратной) индукции. Предположим, что теорема верна для некоторого n ; покажем, что тогда она верна для $n - 1$.

Рассмотрим произвольные положительные числа $x_1, x_2, \dots, x_{n-1}$. Положим $x_n = \frac{x_1+x_2+\dots+x_{n-1}}{n-1}$. Ясно, что $x_n > 0$.

По предположению индукции $\frac{x_1+x_2+\dots+x_n}{n} \geq \sqrt[n]{x_1 x_2 \dots x_n}$. Значит,

$$\frac{x_1+x_2+\dots+x_{n-1} + \frac{x_1+x_2+\dots+x_{n-1}}{n-1}}{n} \geq \sqrt[n]{x_1 x_2 \dots x_{n-1} \frac{x_1+x_2+\dots+x_{n-1}}{n-1}}.$$

Преобразуем левую часть неравенства:

$$\frac{x_1 + x_2 + \dots + x_{n-1} + \frac{x_1 + x_2 + \dots + x_{n-1}}{n-1}}{n} = (x_1 + x_2 + \dots + x_{n-1}) \frac{1 + \frac{1}{n-1}}{n} = \frac{x_1 + x_2 + \dots + x_{n-1}}{n-1}.$$

Получаем $\frac{x_1 + x_2 + \dots + x_{n-1}}{n-1} \geq \sqrt[n]{x_1 x_2 \dots x_{n-1} \frac{x_1 + x_2 + \dots + x_{n-1}}{n-1}}$. Поскольку обе части неравенства положительны, их можно возвести в n -ю степень, сохраняя знак неравенства: $\left(\frac{x_1 + x_2 + \dots + x_{n-1}}{n-1}\right)^n \geq x_1 x_2 \dots x_{n-1} \frac{x_1 + x_2 + \dots + x_{n-1}}{n-1}$. Сокращая обе части неравенства на положительное число $\frac{x_1 + x_2 + \dots + x_{n-1}}{n-1}$, получаем $\left(\frac{x_1 + x_2 + \dots + x_{n-1}}{n-1}\right)^{n-1} \geq x_1 x_2 \dots x_{n-1}$. Извлечём из обеих частей неравенства корень степени $n-1$. Имеем $\frac{x_1 + x_2 + \dots + x_{n-1}}{n-1} \geq \sqrt[n-1]{x_1 x_2 \dots x_{n-1}}$. А это и требовалось получить.

Поскольку для любого натурального числа n найдется натуральное число m , для которого $n \leq 2^m$, неравенство доказано для всех натуральных n .

Задания для самостоятельной работы

1. Докажите равенства:

а) $\sum_{k=1}^n k^2 = \frac{n(n+1)(2n+1)}{6};$

б) $\sum_{k=1}^n (-1)^{k+1} k = \frac{1 + (-1)^{n+1}(2n+1)}{4};$

в) $\sum_{k=1}^{2n} \frac{(-1)^{k+1}}{k} = \sum_{k=n+1}^{2n} \frac{1}{k}.$

2. Докажите *неравенство Бернулли*:

$$(1+x)^n \geq 1 + nx$$

для натуральных n и $x \geq -1$.

3. Докажите неравенства $\sqrt{n} \leq \sum_{k=1}^n \frac{1}{\sqrt{k}} < 2\sqrt{n}$, где n – любое натуральное число.

4. Докажите справедливость неравенства $\sqrt{6 + \sqrt{6 + \dots + \sqrt{6}}} \leq 3$ при произвольном количестве корней в записи левой части.

5. Докажите, что $\frac{1}{2} \cdot \frac{3}{4} \cdot \frac{5}{6} \cdot \dots \cdot \frac{2n-1}{2n} < \frac{1}{\sqrt{n+1}}$ при любом натуральном n .

6. Докажите, что $10^n + 18n - 1$ делится на 27 при любых натуральных n .

7. Плоскость разрезана на части n прямыми, причём $n \geq 3$, нет ни одной пары параллельных прямых и не все прямые проходят через одну точку. Докажите, что хотя бы одна из частей – треугольник.

8. Докажите, что для любого натурального n найдется n -значное число, составленное только из цифр 1 и 2 и делящееся на 2^n .

9. Объясните, где ошибка в доказательстве следующего утверждения.

Утверждение. Все лошади одного цвета.

Доказательство.

Если есть только одна лошадь, то она своей масти, так что база индукции верна. Для индуктивного перехода предположим, что есть n лошадей (с номерами от 1 до n). По индуктивному предположению лошади с номерами от 1 до $n - 1$ одинаковой масти. Аналогично лошади с номерами от 2 до n также имеют одинаковую масть. Но лошади с номерами от 2 до $n - 1$ не могут менять свою масть в зависимости от того как они сгруппированы – это лошади, а не хамелеоны. Поэтому все n лошадей должны быть одинаковой масти.

10. Докажите, что любое натуральное число можно представить в виде суммы нескольких различных членов последовательности Фибоначчи. (Последовательность Фибоначчи a_n определяется условиями $a_1 = 1$, $a_2 = 2$, $a_n = a_{n-1} + a_{n-2}$ при $n \geq 3$.)

Лекция 7. Комбинаторика

В этой лекции мы возвращаемся к истокам курса – теории множеств. Только посмотрим теперь на них немного с другой стороны – количественной: нас будет интересовать вопрос, сколько элементов содержит множество, если оно получено из других конечных множеств применением каких-либо операций над ними. По-другому можно сказать, что мы будем интересоваться количеством комбинаций, составленных из элементов конечных множеств. Отсюда и название этого интереснейшего раздела математики – *комбинаторика*.

Создавая алгоритм, разработчик обязан оценить и объём памяти, который потребуется, и число операций, которое предстоит выполнить компьютеру для обработки данных. Эти оценки опираются на те комбинаторные схемы, о которых рассказывается в этой лекции и с которыми вы будете знакомиться в будущем. А сейчас самое первое и самое необходимое.

Формула включения и исключения. Правило суммы

Пусть даны конечные множества A и B . Как узнать количество элементов в объединении этих множеств, если известны количества элементов в каждом из них? Каждому ясно, что этой информации недостаточно: ответ зависит от того, сколько элементов содержится одновременно в A и в B . Ведь если мы выпишем все элементы из A и все элементы из B , то их общие элементы окажутся выписанными дважды. Значит, из суммы количество элементов в множествах A и B надо вычесть количество элементов в их пересечении. Количество элементов в множестве M обозначают $|M|$. Следовательно, справедлива следующая формула:

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Эту формулу называют *формулой включения и исключения* для двух множеств. Она проиллюстрирована на рис. 7.1, где A – некоторое множество прямоугольников, а B – некоторое множество ромбов.

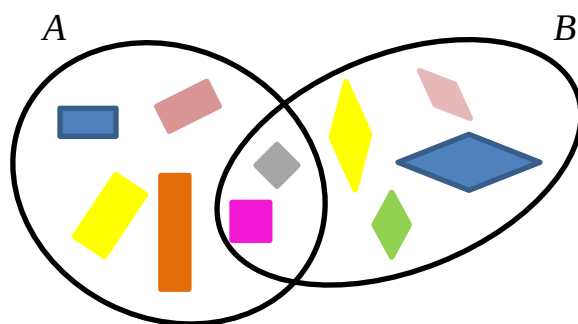


Рис. 7.1.

Частный случай этой формулы – когда $A \cap B = \emptyset$. В этом случае $|A \cup B| = |A| + |B|$. И вообще, если дано разбиение конечного множества M на подмножества $A_1, A_2, \dots, A_n$, то $|M| = \sum_{i=1}^n |A_i|$. Эта формула называется *правилом суммы*.



Формулу включения и исключения можно распространить и на большее число множеств. Например, для трёх множеств A, B и C эта формула будет иметь следующий вид:

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

Попытайтесь доказать эту формулу.

Правило произведения

Пусть нам снова даны конечные множества A и B и $|A| = n$. Пусть каждый элемент из множества A соединён ровно с k элементами из множества B , не обязательно одними и теми же. Сколько пар получается при таком соединении? Ответ легко получить, если представить ситуацию двудольным орграфом (см. рис. 7.2, где $k = 3$):

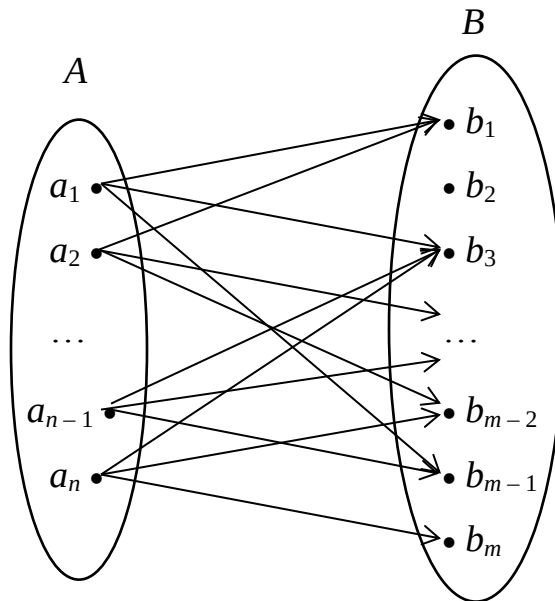


Рис. 7.1.

Ясно, что количество парных комбинаций ровно столько, сколько рёбер в этом графе, т.е. kn . Получаем следующее комбинаторное правило.

Если каждый элемент n -элементного множества комбинируется ровно с k элементами другого (или того же самого) множества, то количество парных комбинаций равно произведению k на n .

Это правило называют *правилом произведения*.

С помощью этого правила легко доказать следующую теорему.

Теорема 7.1. Пусть A и B – конечные множества. Тогда $|A \times B| = |A| |B|$.

Доказательство. По определению декартова произведения, каждый элемент множества A комбинируется с каждым элементом множества B . По правилу произведения таких комбинаций $|A| |B|$. В то же время все такие комбинации и образуют множество $A \times B$. $\square$

В задании 3 для самостоятельного решения вам предложено обобщить эту теорему на произвольное число конечных множеств:

$$|M_1 \times M_2 \times \dots \times M_k| = |M_1| |M_2| \dots |M_k|.$$

Напомним, что $M \times M \times \dots \times M$, где множитель M записан k раз, обозначают M^k .

Следствие 7.2. Пусть M – конечное множество. Тогда $|M^k| = |M|^k$.

Покажем применение этой формулы на примере следующей задачи.

Пример 1. Сколько существует трёхзначных чисел, записанных только нечётными цифрами?

Решение. Каждое трёхзначное число естественно представлять себе как кортеж длины 3, составленный из цифр (с запретом иметь на первом месте цифру 0). В нашей задаче множество цифр $M = \{1, 3, 5, 7, 9\}$. Любая из них может стоять на любом месте, так что множество кортежей длины 3 с элементами из этого множества содержит 5^3 элементов, а значит, и нужных трехзначных чисел 125.

Размещения и перестановки

Изменим немного условие задачи, рассмотренной в примере 1.

Пример 2. Имеется пять карточек, на каждой из которых написана ровно одна нечётная цифра и каждая цифра написана ровно на одной карточке. Сколько трёхзначных чисел можно составить, используя эти карточки?

Чем отличается эта задача от задачи примера 1? Конечно, тем, что теперь в трёхзначном числе никакая цифра не может встречаться дважды. Давайте рассуждать по шагам. Однозначное число можно получить, взяв любую из 5 карточек, т.е. их у нас 5. Двухзначное число мы получим, если к выбранной на первом шаге карточке добавим ещё одну из оставшихся четырёх. Правило произведения говорит нам, что так мы можем получить $5 \cdot 4 = 20$ чисел. Теперь осталось к каждой паре карточек справа приложить ещё одну карточку из трёх оставшихся. Комбинаций из трёх карточек у нас может получиться $20 \cdot 3 = 60$. Значит, и трёхзначных чисел можно составить 60. Как видите, их более, чем в 2

раза меньше, чем просто трёхзначных чисел, записанных с помощью пяти нечетных цифр.

Рассмотренную в примере 2 ситуацию можно понимать так: имеется 3 расположенных в ряд места, и на них требуется разместить три элемента из 5-элементного множества. Поэтому в общем случае говорят, что это задача о размещении элементов n -элементного множества по k местам. Выведем для количества размещений общую формулу.

Пусть M – конечное множество, $|M| = n$, а k – натуральное число, не превосходящее n .

Определение 7.1. Размещением k элементов множества M называется расположение произвольных k элементов из M в некотором порядке.

Поскольку в множестве каждый элемент имеется в единственном экземпляре, в любом размещении нет повторяющихся элементов. Нас будет интересовать, сколько существует k -элементных размещений у n -элементного множества. Количество таких размещений обозначают A_n^k , читают: « A из n по k ». Для подсчёта числа размещений из n элементов по k нам потребуется формула $n(n - 1)(n - 2) \dots (n - k + 1)$. Такое произведение называют *факториальной степенью* числа n и обозначают $n^{(k)}$. При этом договариваются, что $n^{(1)} = n$. Для $n^{(n)}$ применяют другое обозначение: $n!$ (читают «эн факториал» и без крика). Удобно считать, что $0! = 1$, хотя по определению такое произведение возникнуть не может (позже появятся дополнительные аргументы в пользу такой договорённости).



Объясните равенства $n^{(k)} = \frac{n!}{(n-k)!}$ и $n^{(k+1)} = n^{(k)}(n-k)$.

Теорема 7.3. $A_n^k = n^{(k)}$.

Доказательство проведем индукцией по k .

База индукции. $k = 1$. Ясно, что размещений из одного элемента ровно n – ведь это просто возможность выбора одного элемента из n . Так что $A_n^1 = n = n^{(1)}$.

Шаг индукции. Пусть M – множество из n элементов, а M_k – множество всех размещений по k элементов из множества M . По предположению индукции $|M_k| = n^{(k)}$. Рассмотрим множество M_{k+1} . Каждый его элемент получен из некоторого размещения $a_1 a_2 \dots a_k$ приписыванием ещё одного элемента, не фигурирующего в этой записи. Поэтому способов приписать к данному размещению ещё один элемент ровно $n - k$. Следовательно, каждое размещение из M_{k+1} получается как комбинация каждого элемента из M_k с $n - k$ элементами из множества M . По

правилу произведения $|M_{k+1}| = |M_k| (n - k) = n^{(k)} (n - k) = n^{(k+1)}$. Шаг индукции доказан, а, следовательно, и теорема доказана.

Определение 7.2. Размещение n элементов n -элементного множества называют перестановкой.

Название совершенно естественно, поскольку любые два таких размещения различаются только порядком записанных в них элементов, т. е. одно размещение получается из другого некоторой перестановкой его элементов.

Количество перестановок, образованных элементами n -элементного множества обозначают P_n . Из теоремы 7.3 получаем

Следствие 7.4. $P_n = n!$

Сочетания. Количество равномоощных подмножеств

Командир отделения сержант Иванов должен назначить в дозор трёх солдат своего отделения. В его отделении 9 подчинённых. Сколькими способами он может назначить дозор?

Как бы он ни придумал, кого отправить в дозор, объявлять их фамилии он будет в некотором порядке, т. е. как некоторое размещение трёх элементов из 9. Вариантов размещений имеется A_9^3 . Обозначим тех, кого он назвал А, Б, В – именно в таком порядке. Но ясно, что, если бы он назвал Б, А, В или В, А, Б, то состав дозора от этого никак бы не изменился. Перестановок элементов А, Б и В шесть, значит, реально различных вариантов в 6 раз меньше, т. е. количество вариантов назначить дозор из трёх человек у него $A_9^3 / 6$.



Во взводе три отделения, поэтому через два дня на третий сержанту Иванову придется назначать дозор. Хватит ли ему вариантов назначения дозоров, чтобы в течение года ни один вариант не повторялся?

В общем виде задача звучит так. Имеется n -элементное множество. Из него надо выбрать k -элементное подмножество. Сколькими способами это можно сделать?

Подмножество из k элементов называют k -сочетанием. Количество k -сочетаний из n -элементного множества обозначают C_n^k . Иными словами, C_n^k – это количество k -элементных подмножеств в n -элементном множестве. Отметим ещё, что $C_n^0 = 1$, поскольку это означает, что мы выбираем пустое подмножество, а это можно сделать только одним способом – вообще не брать элементы. Из примера с сержантом Ивановым напрашивается формула $C_n^k = \frac{A_n^k}{k!}$

Теорема 7.5. $C_n^k = \frac{n!}{(n-k)!k!}$.

Доказательство. При $k = 0$ формула справедлива в силу нашей договорённости, что $0! = 1$. Пусть теперь $k > 0$ и M – множество из n элементов, а M_k – множество всех размещений по k элементов из множества M . Пусть $a_1 a_2 \dots a_k$ – некоторое размещение k элементов из M . Поставим ему в соответствие подмножество $\{a_1, a_2, \dots, a_k\}$. Ясно, что это некоторое всюду определённое, однозначное и сюръективное отображение f множества M_k на множество всех подмножеств множества M , состоящих из k элементов. Обозначим это множество подмножеств через $\mathcal{B}_k(M)$. Тогда $|\mathcal{B}_k(M)| = C_n^k$. Все размещения, состоящие из одного и того же набора элементов, очевидно, образуют один класс ядерной эквивалентности отображения f . По теореме 4.7 количество классов совпадает с $|\mathcal{B}_k(M)|$. В свою очередь в каждом классе содержится одинаковое количество элементов, а именно P_k . Следовательно, $A_n^k = |\mathcal{B}_k(M)| P_k$, откуда легко получается нужная формула.



Укажите значение C_n^n .

Числа сочетаний обладают многими важными свойствами, здесь и сейчас мы рассмотрим два из них.

- 1) $C_n^k = C_n^{n-k}$;
- 2) $C_n^k = C_{n-1}^k + C_{n-1}^{k-1}$.

Первое из этих равенств объясняется совсем просто. Каждый раз, выбрав подмножество, содержащее k элементов, вы одновременно получаете подмножество, состоящее из $n - k$ элементов. Тем самым у вас между множествами $\mathcal{B}_k(M)$ и $\mathcal{B}_{n-k}(M)$ имеется взаимно-однозначное соответствие, а это означает, что они содержат одно и то же число элементов.

Для обоснования второго равенства в множестве M зафиксируем какой-нибудь элемент a . Тогда все k -элементные подмножества распределятся по двум непересекающимся классам: в один класс попадут те, которые не содержат a , а в другой – те, которые его содержат. Первые, очевидно, являются k -элементными подмножествами множества $M \setminus \{a\}$, т.е. образуют множество $\mathcal{B}_k(M \setminus \{a\})$. Их количество C_{n-1}^k . Вторые подмножества получены из $(k - 1)$ -элементных подмножеств множества $M \setminus \{a\}$ добавлением в каждое из них элемента a . Значит, таких подмножеств $|\mathcal{B}_{k-1}(M \setminus \{a\})| = C_{n-1}^{k-1}$. По правилу суммы

$$C_n^k = |\mathcal{B}_k(M)| = |\mathcal{B}_k(M \setminus \{a\})| + |\mathcal{B}_{k-1}(M \setminus \{a\})| = C_{n-1}^k + C_{n-1}^{k-1}.$$

Бином Ньютона. Биномиальные коэффициенты

Рассмотрим выражение $(a + b)^n$. В школе вы для $n = 2$ и $n = 3$ раскрывали скобки и после приведения подобных членов получали формулы

$$(a + b)^2 = a^2 + 2ab + b^2 \text{ и } (a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3.$$

Наша цель – научиться записывать $(a + b)^n$ в развёрнутом виде, т.е. без скобок, для любого натурального числа n . Докажем методом математической индукции следующую формулу:

$$(a + b)^n = \sum_{i=0}^n C_n^i a^{n-i} b^i.$$

База индукции: $n = 1$. Формула $a + b = C_1^0 a + C_1^1 b$ очевидна, потому что $C_1^0 = C_1^1 = 1$.

Шаг индукции. Пусть формула доказана для $n = k - 1$. Проверим равенство для $n = k$.

$$\begin{aligned} (a + b)^k &= (a + b)^{k-1}(a + b) = \left(\sum_{i=0}^{k-1} C_{k-1}^i a^{k-1-i} b^i\right)(a + b) = \\ &= \sum_{i=0}^{k-1} C_{k-1}^i a^{k-i} b^i + \sum_{i=0}^{k-1} C_{k-1}^i a^{k-1-i} b^{i+1} = \\ &= \sum_{i=0}^{k-1} C_{k-1}^i a^{k-i} b^i + \sum_{i=1}^k C_{k-1}^{i-1} a^{k-i} b^i + b^k = \\ &= C_k^0 a^k + \sum_{i=1}^k (C_{k-1}^i + C_{k-1}^{i-1}) a^{k-i} b^i + C_k^k b^k = \sum_{i=0}^k C_k^i a^{k-i} b^i. \end{aligned}$$

Здесь мы воспользовались тем, что $C_{k-1}^0 = C_k^0 = C_k^k = 1$, и свойством $C_k^i = C_{k-1}^i + C_{k-1}^{i-1}$.

Тем самым, формула верна для любого натурального n .

Полученная формула называется *формулой бинома Ньютона*. Термин «бином» (в переводе на русский – двучлен) звучит здесь потому, что в степень возводится сумма двух чисел. Числа C_n^i , как мы видим, выступают в роли коэффициентов при одночленах $a^{n-i} b^i$. Поэтому по-другому их называют *биномиальными коэффициентами*. В литературе вы также можете встретиться с другим обозначением этих чисел: $\binom{n}{k}$

Продолжим свойств биномиальных коэффициентов.

$$3) \sum_{i=0}^n C_n^i = 2^n.$$

С одной стороны, это равенство легко получить из формулы бинома Ньютона, если положить $a = b = 1$. С другой стороны, сумма всех биномиальных коэффициентов – это количество всех подмножеств n -элементного множества. А как было показано на предыдущей лекции, общее число всех подмножеств n -элементного множества равно 2^n .

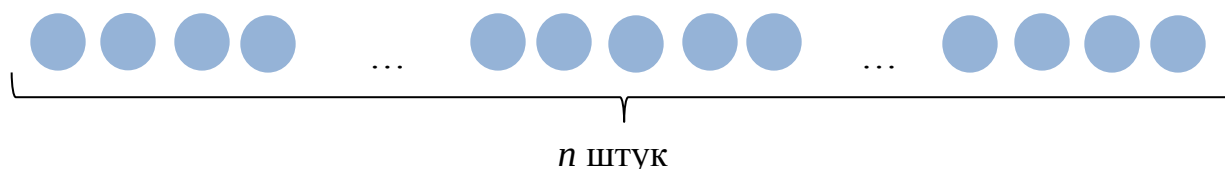
$$4) \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} C_n^{2i} = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} C_n^{2i+1} = 2^{n-1}.$$

Это свойство озвучивают обычно так: «Сумма биномиальных коэффициентов с чётными верхними индексами равна сумме биномиальных коэффициентов с нечётными верхними индексами и равна 2^{n-1} ». Оно получается, если в формуле бинома Ньютона положить $a = 1$, а $b = -1$ и затем воспользоваться свойством 3).

Сочетания с повторениями.

Рассмотрим следующую задачу. Имеется n одинаковых предметов и k ящиков. Сколько существует вариантов разложить все предметы в эти ящики (некоторые из ящиков могут остаться пустыми)?

Представим, что все наши предметы – это выложенные в один ряд шары.



Все шары одинаковы, поэтому можно представить себе, что мы берем несколько первых шаров и намерены положить их в первый ящик. Чтобы зафиксировать наше решение, поставим после последнего из выбранных шаров перегородку. Например, если мы решили в первый ящик положить три шара, то фиксация этого решения выглядит так:



Если же мы решили в первый ящик ничего не класть, то ситуация будет выглядеть так:



Затем мы установим вторую перегородку, обозначив то множество шаров, которое отправится во второй ящик. Затем третью, и т.д. Если будет решено какой-то ящик оставить пустым, то в соответствующем месте появятся две перегородки без шаров между ними:



А может быть и три идущие подряд перегородки, если два подряд ящика остаются пустыми. И т.д.

Как только будет установлена $k - 1$ перегородка, все шары окажутся распределённым по k ящикам.

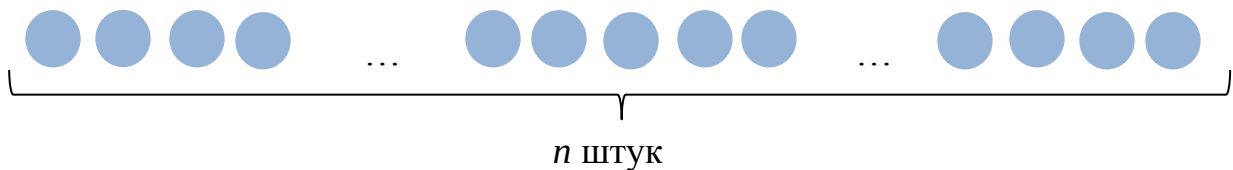
У нас получился ряд из $n + k - 1$ предметов. В нём $k - 1$ мест занимают перегородки. Значит, как только мы укажем $k - 1$ мест из $n + k - 1$ возможных мест, мы получим распределение шаров по ящикам. А это можно сделать C_{n+k-1}^{k-1} способами. Или по-другому C_{n+k-1}^n .

Применённый нами приём решения задачи получил название *метода шаров и перегородок*.

Применим этот метод для решения ещё одной задачи.

Имеется n одинаковых предметов и k ящиков. Сколько существует вариантов разложить все предметы в эти ящики так, чтобы ни один ящик не оказался пустым?

Снова представим, что все наши предметы – это выложенные в один ряд шары.



Чтобы распределить эти шары по n ящикам нам снова надо поставить $k - 1$ перегородок. Только теперь запрещается ставить в один промежуток между шарами больше одной перегородки, а также ставить их перед всем рядом шаров и после него. Тем самым, у нас $n - 1$ мест, в которые можно поместить $k - 1$ перегородок. Значит, количество вариантов равно C_{n-1}^{k-1} .

А теперь ещё одна (вкусная) задача.

Вася хочет угостить 7 знакомых девушек пирожными: каждую – одним. В кондитерской, куда он зашёл за пирожными, есть 4 вида пирожных: наполеоны, эклеры, бисквиты и песочные. Вася задумался, какой набор ему купить (не исключая, что все пирожные в наборе будут одинаковыми). На обдумывание одного варианта он тратит полминуты. Сколько времени Вася будет пребывать в задумчивости?

Давайте рассуждать. Приготовим 4 коробочки, чтобы в каждую складывать пирожные одного вида. На одной напишем «наполеоны», на другой – «эклеры», на третьей – «бисквиты», на четвертой – «песочные». Теперь ясно, что надо взять семь шаров и распределить их по этим четырём коробкам. Сколько шаров в коробочку попало, столько таких пирожных Вася и купит. Значит, число вариантов равно $C_{7+4-1}^{4-1} = C_{10}^3 = 120$. На выбор варианта Вася потратит 1 час.

В общем случае ситуацию можно описать так. Имеются предметы n различных видов; предметы одного вида друг от друга неотличимы. Сколько

имеется вариантов составить комплект из k предметов? Каждый такой комплект называется *сочетанием с повторениями*. Число сочетаний с повторениями обозначается как $\overline{C}_n^k$, и это число равно, как мы видели, C_{n+k-1}^{k-1} .

Задания для самостоятельной работы

1. Докажите правило суммы для n конечных множеств, воспользовавшись методом математической индукции.

2. Пусть $M_1, M_2, \dots, M_n$ – конечные множества. Докажите, что $|M_1 \times M_2 \times \dots \times M_n| = |M_1| |M_2| \dots |M_n|$.

3. Чему равно $n^{(k)} (n-k)^{(m-k)}$ при условии $k < m < n$?

4. Верно ли, что при любом натуральном n число $\frac{n^{(k)} n^{(n-k)}}{n!}$ целое для любого $k \leq n$?

5. Объясните, почему число C_p^k при простом p и $0 < k < p$ делится на p .

6.^Т В языке племени Тили-Вили 5 гласных букв и 10 согласных. В словах этого языка никогда не стоят рядом две гласные или две согласные. Какое наибольшее число семибуквенных слов может быть в этом языке?

7.^Т В высшей лиге первенства России по футболу участвуют 16 команд. Сколько имеется вариантов распределения первых трех мест среди этих команд, если предположить, что на старте первенства все они имеют одинаковые шансы?

8.^Т На полоске бумаги написано число 1234567890. Полоску разрезают на 4 части так, что каждый разрез проходит между цифрами. Сколькими способами это можно сделать?

9.^Т В $\triangle ABC$ на стороне AC отмечено 19 точек. Каждую из них соединили отрезком с вершиной B . Сколько треугольников можно увидеть на таком чертеже?

10.^Т На плоскости начерчено 100 прямых «общего положения», т.е. никакие три не пересекаются в одной точке и никакие две не параллельны.

а) Сколько точек пересечения имеют эти прямые?

б) Сколько треугольников образовано пересечением этих прямых?

Содержание

Лекция 1. Множества и логика	5
Понятие множества. Способы задания множества	5
Подмножества	8
Элементы математической логики	9
Операции над множествами	16
Декартово произведение множеств	18
Ещё раз о математической логике. Предикаты	19
Задания для самостоятельной работы	25
Лекция 2. Графы	27
Понятие графа. Простейшие свойства графов	27
Маршруты в графе и связность	29
Обыкновенные графы и деревья	32
Двудольные графы	35
Ориентированные графы	37
Представление графа матрицей смежности	39
Задания для самостоятельной работы	40
Лекция 3. Бинарные и другие отношения	42
Определение отношения	42
Операции над отношениями	44

Из недавнего прошлого в довольно скорое будущее: несколько слов о базах данных	45
Частный случай: бинарные отношения. Свойства бинарных отношений	46
Бинарные отношения на множестве и их свойства	49
Отношения эквивалентности	53
Отношения порядка	56
Взаимосвязь между отношениями и предикатами	60
Задания для самостоятельной работы	60
 Лекция 4. Отображения	 63
Определение отображения	63
Свойства отображений	64
Операции над отображениями	66
Взаимно-однозначные отображения. Равномощные множества	68
Особенности функциональных отображений	72
Задания для самостоятельной работы	75
 Лекция 5. Операции на множестве	 77
Определение операции на множестве	77
Бинарные операции и их свойства	78
Полугруппы и группы	81
Кольца и поля	85
Кольцо целых чисел: делимость и взаимная простота целых чисел	92
Кольца вычетов по модулю n	96

Задания для самостоятельной работы	97
Лекция 6. Метод математической индукции	99
Базовая версия метода математической индукции	99
Модификация шага индукции	100
Модификация базы индукции	101
Математическая индукция с большим шагом	102
Метод обратной математической индукции	102
Задания для самостоятельной работы	104
Лекция 7. Комбинаторика	106
Формула включения и исключения. Правило суммы	106
Правило произведения	107
Размещения и перестановки	108
Сочетания. Количество равномощных подмножеств	110
Бином Ньютона. Биномиальные коэффициенты	112
Сочетания с повторениями.	113
Задания для самостоятельной работы	115
Содержание	116