# Множества.

1. **Множества. Мощность множества. Операции над множествами. Диаграммы Эйлера-Венна.**

**Множеством**- совокупность различимых объектов любой природы, называемых элементами данного множества.

Множество можно задать **перечислением** принадлежащих ему элементов, **указанием свойств**, которым элементы множества должны удовлетворять, или заданием **порождающей процедуры**.

**Конечное множество -** множество, содержащее конечное число элементов, в противном случае – **бесконечным**.

**Мощность** - число элементов конечного множества

**Пустые** - не содержащее ни одного элемента

**Операции над множествами**

К **основным операциям** над множествами относятся:

* объединение;
* пересечение;
* разность;
* дополнение.

***Объединение*** - множество элементов, каждый из которых принадлежит либо А, либо В.

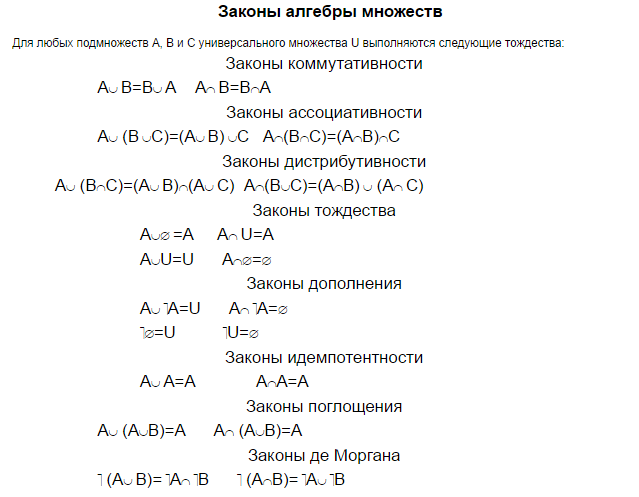
**Пересечение** - множество, состоящее из элементов, которые принадлежат и А и В

**Разность** (обозначается А\В) - множество всех тех и только тех элементов А, которые не содержатся в В.

**Дополнение**  (Ā или ¬А) - множество элементов, которые не принадлежат множеству А. 

1. **Алгебра подмножеств. Булеан.**

**Булеан** (степень множества, показательное множество, множество частей) — множество всех [подмножеств](https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D0%B4%D0%BC%D0%BD%D0%BE%D0%B6%D0%B5%D1%81%D1%82%D0%B2%D0%BE) данного множества A, обозначается \mathcal P(A) или 2^A (так как оно соответствует множеству отображений из A в 2 = \{ 0,1\}).

1. **Алгебры множеств: ассоциативности; коммутативности; тождества; идемпотентности; дистрибутивности; дополнения; де Моргана.**
2. **Декартово произведение множеств.**

**Декартовым произведением множеств *А* и *В*** называется множество пар, первая компонента которых принадлежит множеству *А*, вторая множеству *В.* Обозначают *АОписание: E:Для сайтаПрограммыЗеброид 4tempword_1.filesimage094.gifВ.*Таким образом  *АОписание: E:Для сайтаПрограммыЗеброид 4tempword_1.filesimage094.gifВ = {(x;y)* | *xОписание: E:Для сайтаПрограммыЗеброид 4tempword_1.filesimage002.gifA, yОписание: E:Для сайтаПрограммыЗеброид 4tempword_1.filesimage002.gifB}.*

**Декартовое умножение -** операция нахождения декартового произведения.

**Количество пар в декартовом произведении** *АОписание: E:Для сайтаПрограммыЗеброид 4tempword_1.filesimage094.gifВ* будет равно произведению числа элементов множеств.

**Кортеж** – упорядоченный набор из n элементов.

# Отображения и функции.

1. Соответствие между множествами. Свойства соответствий: область определения, область значений, сечения

**Соответствие между множествами** - любое подмножество их декартова произведения.Соответствия принято обозначать буквами *P, S, T, R* и др. Если  *xSy* – соответствие между элементами множеств *X* и *Y*, то, согласно определению, *SОписание: E:Для сайтаПрограммыЗеброид 4tempword_1.filesimage008.gifXОписание: E:Для сайтаПрограммыЗеброид 4tempword_1.filesimage094.gifY.*

**Область определения и множество значений соответствия -**  множество первых координат упорядоченных пар, принадлежащих соответствию S, называется областью определения, а множество вторых – областью значения. **Множествоопределения соответствия R** - Совокупность А всех элементов из Х, имеющих непустые образы.

**Множество значений соответствия R** - Множество B всех элементов из Y, имеющих непустой полный прообраз.

1. **Отображения. Образы и прообразы элементов.**

Отображение или функция - соответствие, при котором каждому элементу X соответствует единственный элемент Y.

 Если элементу *x* соответствует *y*, то *y* называется **образом элемента** *x*, а *x* - **прообразом элемента** *y*. Пишут: http://www.pm298.ru/Math/a01259.JPG или *y* = *f*(*x*). П**олным прообразом элемента** – один образ.

1. **Субъективное, инъективные и биективные отображения.**

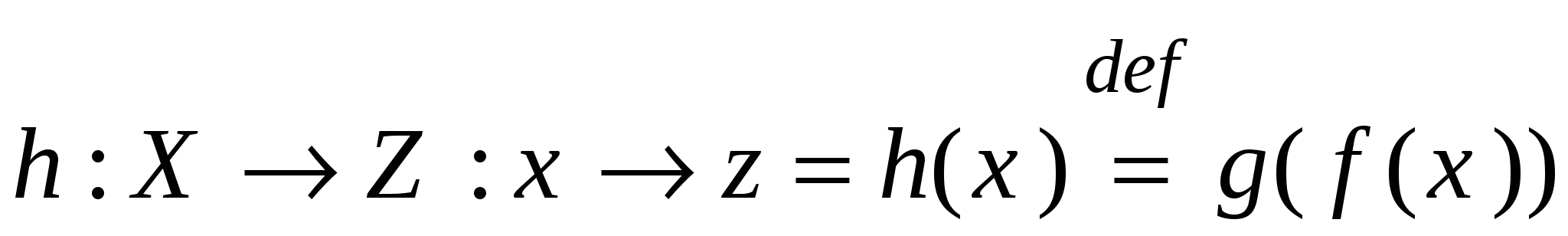
**Инъективным** – если элементы неравны, то неравны и функции от этих элементов.

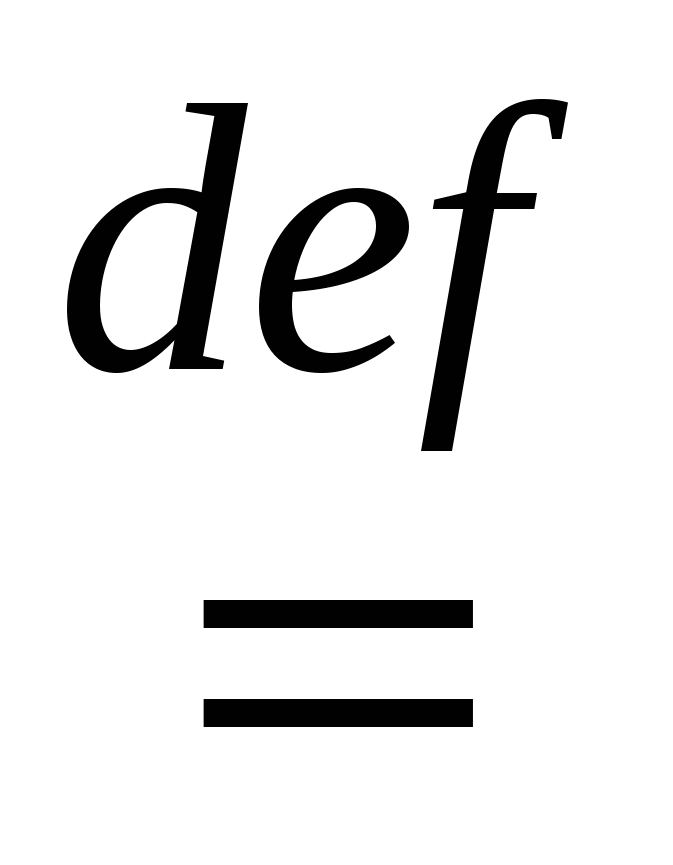
**Суръективным** - если множество значений *f*(X) совпадает с областью значений Y.

**Биективным** - если оно суръективно и инъективно одновременно.

1. **Композиция отображений. \*Транзитивное замыкание отображений**

Отображение



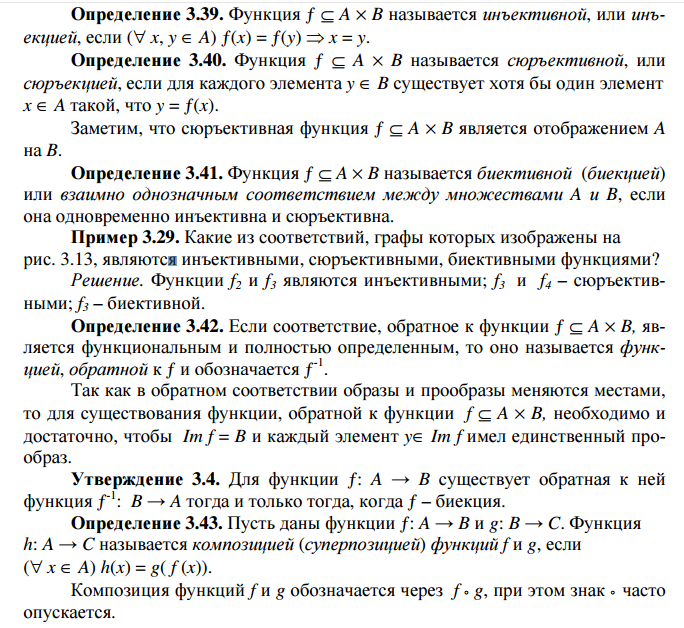
называется композицией (суперпозицией) отображений f и g или сложным отображением; знак «»читается как «равняется по определению».

**Транзитивное отношение** в математике - это такое отношение, при котором если один элемент соотносится с вторым, а второй с третьим, то и первый элемент соотносится с третьим.

**Транзитивным замыканием** -  пересечение всех транзитивных отношений, содержащих R как подмножество.

* Транзитивное замыкание рефлексивного отношения рефлексивно, так как транзитивное отношение содержит исходное отношение
* Транзитивное замыкание симметричного отношения симметрично.
* Транзитивное замыкание не сохраняет антисимметричность, например, для отношения \{(a, b), (b, c), (c, a)\} на множестве \{a, b, c\}
* Транзитивное замыкание транзитивного отношения — оно само.

1. **Функциональные отображения (функции). Суперпозиция функций.**



## Отношения.

1. **Отношение. Бинарные отношения. Инфиксная форма записи.**

**N-арным (n-местным) отношением** - любое подмножество прямого произведения A1 × A2 × …× An.

**Бинарное отношение** - всякое подмножество прямого произведения http://ok-t.ru/life-prog/baza2/588331855384.files/image014.gif на http://ok-t.ru/life-prog/baza2/588331855384.files/image016.gif

**Пример 1.8.2.** Пусть http://ok-t.ru/life-prog/baza2/588331855384.files/image723.gif

Положим http://ok-t.ru/life-prog/baza2/588331855384.files/image725.gif

http://ok-t.ru/life-prog/baza2/588331855384.files/image727.gif

Используют две формы записи принадлежности некоторой упорядоченной пары заданному бинарному отношению http://ok-t.ru/life-prog/baza2/588331855384.files/image729.gif инфиксную и префиксную. Инфиксная форма записи: http://ok-t.ru/life-prog/baza2/588331855384.files/image731.gif префиксная форма записи: http://ok-t.ru/life-prog/baza2/588331855384.files/image733.gif

Приведем еще несколько примеров бинарных отношений.

1. **Операции над бинарными отношениями.**

Так как отношения на http://ok-t.ru/life-prog/baza2/588341602791.files/image070.gif задаются подмножествами http://ok-t.ru/life-prog/baza2/588341602791.files/image371.gif , то для них определены все те же операции, что и для множеств, т.е. объединение, пересечение, дополнение, разность. Кроме того, над отношениями определены и некоторые другие операции.

**Обратное отношение** http://ok-t.ru/life-prog/baza2/588341602791.files/image373.gif .

Отношение http://ok-t.ru/life-prog/baza2/588341602791.files/image375.gif имеет место тогда и только тогда, когда имеет место http://ok-t.ru/life-prog/baza2/588341602791.files/image289.gif . Соответственно, http://ok-t.ru/life-prog/baza2/588341602791.files/image378.gif .

**Пример.** Если http://ok-t.ru/life-prog/baza2/588341602791.files/image193.gif – «быть моложе», то http://ok-t.ru/life-prog/baza2/588341602791.files/image373.gif – быть старше ; если http://ok-t.ru/life-prog/baza2/588341602791.files/image193.gif – «быть подчиненным, то http://ok-t.ru/life-prog/baza2/588341602791.files/image373.gif – быть начальником”.

**Пример**. Пусть http://ok-t.ru/life-prog/baza2/588341602791.files/image004.gif ={1,2,3,4,5}, http://ok-t.ru/life-prog/baza2/588341602791.files/image010.gif ={6,7,8,9}, http://ok-t.ru/life-prog/baza2/588341602791.files/image021.gif ={10,11,12,13}. Пусть http://ok-t.ru/life-prog/baza2/588341602791.files/image386.gif определены следующим образом: http://ok-t.ru/life-prog/baza2/588341602791.files/image193.gif ={(1,7), (4,6), (5,6), 2,8)}, http://ok-t.ru/life-prog/baza2/588341602791.files/image389.gif ={(6,10), (6,11), (7,10), (8,13)}. Определить отношения http://ok-t.ru/life-prog/baza2/588341602791.files/image391.gif .

Ответ: http://ok-t.ru/life-prog/baza2/588341602791.files/image373.gif ={(7,1), (6,4), (6,5), (8,2)}, http://ok-t.ru/life-prog/baza2/588341602791.files/image394.gif ={10,6), (11,6), (10,7), (13,13)}

**Составное отношение** (композиция) http://ok-t.ru/life-prog/baza2/588341602791.files/image396.gif .

Пусть заданы множества http://ok-t.ru/life-prog/baza2/588341602791.files/image398.gif и отношения http://ok-t.ru/life-prog/baza2/588341602791.files/image400.gif. Составное отношение действует из http://ok-t.ru/life-prog/baza2/588341602791.files/image203.gif в http://ok-t.ru/life-prog/baza2/588341602791.files/image205.gif посредством http://ok-t.ru/life-prog/baza2/588341602791.files/image404.gif , и из http://ok-t.ru/life-prog/baza2/588341602791.files/image205.gif в http://ok-t.ru/life-prog/baza2/588341602791.files/image407.gifпосредством http://ok-t.ru/life-prog/baza2/588341602791.files/image409.gif .

Составное отношение может быть определено и на одном множестве. В частности, если http://ok-t.ru/life-prog/baza2/588341602791.files/image411.gif , то составное отношение http://ok-t.ru/life-prog/baza2/588341602791.files/image413.gif .

**Пример**: если http://ok-t.ru/life-prog/baza2/588341602791.files/image193.gif – «быть сыном», то http://ok-t.ru/life-prog/baza2/588341602791.files/image415.gif – «быть внуком».

**Транзитивное замыкание** http://ok-t.ru/life-prog/baza2/588341602791.files/image417.gif .

Транзитивное замыкание http://ok-t.ru/life-prog/baza2/588341602791.files/image417.gif состоит из таких, и только таких пар элементов http://ok-t.ru/life-prog/baza2/588341602791.files/image356.gif из http://ok-t.ru/life-prog/baza2/588341602791.files/image070.gif , для которых в http://ok-t.ru/life-prog/baza2/588341602791.files/image070.gif существует цепочка из http://ok-t.ru/life-prog/baza2/588341602791.files/image422.gif элементов http://ok-t.ru/life-prog/baza2/588341602791.files/image070.gif , http://ok-t.ru/life-prog/baza2/588341602791.files/image424.gif , http://ok-t.ru/life-prog/baza2/588341602791.files/image426.gif , между соседними элементами которой выполняется http://ok-t.ru/life-prog/baza2/588341602791.files/image193.gif , т.е.

http://ok-t.ru/life-prog/baza2/588341602791.files/image429.gif .

Например, если http://ok-t.ru/life-prog/baza2/588341602791.files/image193.gif – отношение «быть сыном», то http://ok-t.ru/life-prog/baza2/588341602791.files/image417.gif – «быть прямым потомком». Если отношение http://ok-t.ru/life-prog/baza2/588341602791.files/image193.gif транзитивно то http://ok-t.ru/life-prog/baza2/588341602791.files/image432.gif .

**12.Свойства бинарных отношений: рефлексивность; антирефлексивность; симметричность; антисимметричность; транзитивность. Эквивалентность.**

**Основные типы бинарных отношений.**

Бинарное отношение R на множестве M называется ***рефлексивным***, если для любого a∈ M выполняется aRa .

Примеры: 1) отношения ≥ =≤ , , на множестве действительных чисел; 2) отношение «не быть начальником» на множестве сотрудников организации.

Бинарное отношение R на множестве M называется ***антирефлексивным***, если для любого a∈ M выполняется a-Ra .

Примеры: 1) отношения > <, на множестве действительных чисел; 2) отношение «быть начальником» на множестве сотрудников организации.

Бинарное отношение R на множестве M называется ***симметричным***, если для любых

a,b ∈ Mb,a ≠ b из aRb следует bRa .

Примеры: 1) отношения ≠ на множестве действительных чисел; 2) отношение «быть родственником» на множестве людей.

Бинарное отношение R на множестве M называется ***антисимметричным***, если для любых a,b ∈ M,a ≠b из aRb следует b-Ra.

Примеры: 1) отношения > ≥≤< , ,, на множестве действительных чисел; 2) отношение «быть сыном» на множестве людей.

Бинарное отношение R на множестве M называется ***транзитивным***, если для любых c,b,a ∈ M из aRb и bRc следует aRc .

Примеры: 1) отношения > ≥=≤< , ,,, на множестве действительных чисел; 2) отношение «быть начальником» на множестве сотрудников организации.

Бинарное отношение R на множестве M называется ***антитранзитивным***, если для любых c,b,a ∈M из aRb и bRc следует a-Rc.

Примеры: 1) отношение «несовпадение четности» на множестве целых чисел; 2) отношение «быть непосредственным начальником» на множестве сотрудников организации.

Бинарное отношение R на множестве M называется отношением ***эквивалентности***, если оно

• рефлексивно, • симметрично, • транзитивно.

Примеры: 1) отношение «иметь одинаковый остаток от деления на число k » на множестве целых чисел; 2) отношение «учиться в одной группе» на множестве учащихся.

Отношение эквивалентности R разбивает множество M на непересекающиеся подмножества так, что любые элементы одного подмножества находятся в отношении R, а любые элементы разных подмножеств не находятся в отношении R. Данные подмножества называются классами эквивалентности, а их количество – индексом разбиения.

* 1. **Отношение порядка: нестрого; строгого; полного; частичного порядка. Отношение предпорядка (доминирования). Замыкание отношений.**

Бинарное отношение R на множестве M называется отношением **нестрогого порядка**, если оно

• рефлексивно, • антисимметрично, • транзитивно.

Примеры: 1) отношение ≤ на множестве действительных чисел; 2) отношение «быть не старше» на множестве людей.

Бинарное отношение R на множестве M называется отношением **строгого порядка**, если оно

• антирефлексивно, • антисимметрично, • транзитивно.

Примеры: 1) отношение < на множестве действительных чисел; 2) отношение «быть начальником» на множестве сотрудников организации.

Элементы a,b∈M называются **сравнимыми по отношению порядка R**, если aRb или bRa . Множество M называется ***полностью упорядоченным множеством***, если любые два элемента в нем сравнимы по некоторому отношению порядка R.

Примеры: 1) множество действительных чисел по отношениям >≥=≤< ,,,, ; 2) отношение «быть не старше» на множестве людей.

Множество M называется частично упорядоченным множеством, если в нем есть хотя бы два элемента, несравнимые по некоторому отношению порядка R.

Примеры: 1) множество комплексных чисел отношениям > ≥≤< , ,, ; 2) отношение «быть начальником» на множестве сотрудников организации.

Отношения, в которых есть антисимметрия, но нет транзитивности, называют **предпорядком или отношением доминирования.**

**Транзитивным замыканием** (или просто **замыканием**) отношения ℜ называется бесконечное объединение Ri . Обозначим замыкание как R\* , т.е. R\* =R∪ R2 ∪...∪Rk .

Пример. Пусть на множестве целых чисел N задано отношение R={(x,y)|y=x+1}. Тогда замыканием R\* будет отношение {(x,y) | x < y}.

* 1. **\*Линейный порядок. Минимальный и максимальный элементы множества. Диаграмма Хассе.**

**Линейно упорядоченное множество** или **цепь** ― частично упорядоченное множество, в котором для любых двух элементов a и b имеет место a\leqslant b или b\leqslant a.

Важнейший частный случай линейно упорядоченных множеств ― вполне упорядоченные множества.

**Сечением** линейно упорядоченного множества P называется разбиение его на два подмножества A и B так, что A\cup B=P, A\cap B=\varnothing и для любых a\in A и b\in B, a\leqslant b Классы A и B называются соответственно нижним и верхним классами сечения.

Различаются следующие типы сечений:

* **скачок** ― в нижнем классе имеется наибольший элемент, а в верхнем ― наименьший;
* **дедекиндово сечение** ― в верхнем классе нет наименьшего элемента или в нижнем классе нет наибольшего, но не одновременно;
* **щель** ― в нижнем классе нет наибольшего элемента, а в верхнем ― наименьшего.

Линейно упорядоченное множество называется [**непрерывным**](https://ru.wikipedia.org/wiki/%D0%9D%D0%B5%D0%BF%D1%80%D0%B5%D1%80%D1%8B%D0%B2%D0%BD%D0%BE%D0%B5_%D0%BC%D0%BD%D0%BE%D0%B6%D0%B5%D1%81%D1%82%D0%B2%D0%BE), если все его сечения дедекиндовы.

**Частично упорядоченное множество** — математическое понятие, которое формализует интуитивные идеи упорядочения, расположения элементов в определённой последовательности. Неформально, множество частично упорядочено, если указано, какие элементы *следуют* за какими (какие элементы *больше* каких). В общем случае может оказаться так, что некоторые пары элементов не связаны отношением «*следует за*».

Из-за того, что в частично упорядоченном множестве могут быть пары несравнимых элементов, вводятся два различных определения: ***минимального элемента*** и *наименьшего элемента*.

Элемент a \in M называется *минимальным*, если не существует элемента b < a. Другими словами, a — минимальный элемент, если для любого элемента b \in Mлибо b>a, либо b=a, либо b и a несравнимы. Элемент a называется *наименьшим*, если для любого элемента b \in M имеет место неравенство b \geqslant a. Очевидно, всякий наименьший элемент является также минимальным, но обратное в общем случае неверно: минимальный элемент a может и не быть наименьшим, если существуют элементы b, не сравнимые с a.

Очевидно, что если в множестве существует наименьший элемент, то он единственен. А вот минимальных элементов может быть несколько. В качестве примера рассмотрим множество \mathbb{N}\setminus \{ 1 \} = \{ 2, 3, \ldots \} натуральных чисел без единицы, упорядоченное по отношению делимости \mid. Здесь минимальными элементами будут простые числа, а вот наименьшего элемента не существует.

**Аналогично вводятся понятия *максимального* и *наибольшего* элементов.**

**Диаграмма Хассе** — вид диаграмм, используемый для представления конечного частично упорядоченного множества в виде рисунка его транзитивного сокращения. Конкретно, для частично упорядоченного множества (S, \le) диаграмма представляет каждый элемент S как вершины на плоскости и отрезки или кривые, идущие *вверх* от элемента x к элементу y, если x \le y и не существует элемента z, для которого x \le z \le y. Эти кривые могут пересекаться, но не должны проходить через вершины, если только они не являются концами линии. Такая диаграмма с помеченными вершинами однозначно определяют частичный порядок.

## Комбинаторика.

* 1. **Размещения (с повторениями, без повторений). Убывающий факториал.**

**Теорема:** число **размещений** n различных элементов по k различным позициям есть (**без повторений**)

* A_{\,n}^{\,k}  = n(n - 1)(n - 2) \ldots (n - k + 1),

или, в терминах факториалов,

* A_n^k  = \frac{{n!}}{{(n - k)!}}.

*Примечание:* заметим, что в случае, когда число мест, по которым размещают предметы, совпадает с количеством самих предметов, т. е. когда k=n, рассматриваемая задача становится задачей о числе перестановок. В нашем случае при этом мы получаем в знаменателе дроби ноль факториал, и для того, что бы разные формулы, соответствующие одной и той же задаче, приводили к одинаковым результатам, полагают, что 0!=1.

***(С повторениями)***

Пусть даны nразличных видов предметов, которые можно разместить по k различным местам, причем выбирать предметы можно с повторениями (т.е. можно выбрать несколько предметов одного вида). Такие выборки называются размещениями с повторениями, а их количество вычисляется по формуле: \bar A_{\,n}^{\,k}  = n^k
.

***Убывающим факториалом*** порядка *n* числа *a* (обозначается (*a*)*n*) называется произведение:

43-1.gif (3007 bytes)

При *n* = 1: (*a*)*n = a*–0 = *a*;при*n* = 0: (*a*)*n =*1 (по определению).

1. **Перестановки (с повторениями, без повторений).**

**(Без повторений)**

**Перестановки в ряд:** *Перестановкой* из n элементов (или n-перестановкой) называется n-элементное упорядоченное множество, составленное из элементов n-элементного множества.

*Иначе*: Перестановкой из n элементов (или n-перестановкой) называется размещение из nэлементов по n без повторений.

Число перестановок из n элементов без *повторений* обозначается P_n  от французского слова*perturbation*.

**Теорема:** число способов расположить в ряд n различных объектов есть


P_n  = n(n - 1)(n - 2) \cdot  \ldots  \cdot 2 \cdot 1 = n!


**Замечание:** Рекуррентная формула: P_n  = nP_{n - 1}
.

**Перестановки симметричных объектов**

n различных предметов можно расположить по кругу (n - 1)! способами, а если их можно еще и переворачивать,то \frac{{(n - 1)!}}{2} различными способами.

**(С повторениями)**

Пусть даны n_1  элементов первого типа, n_2  — второго типа, n_k  — k-го типа, всего n элементов. Способы разместить их по n различным местам называются перестановками с повторениями. Их количество обозначается P_n (n_1 ,\,\,n_2 ,\,\, \ldots ,\,\,n_k
).

**Теорема:** число перестановок с повторениями есть

P_n (n_1 ,\,\,n_2 ,\,\, \ldots ,\,\,n_k ) = \frac{{n!}}{{n_1 !n_2
! \ldots n_k !}}.

## Сочетания с повторениями и без.

Пусть имеются предметы n различных видов предметов, и из них составляются наборы, содержащие k элементов. Такие выборки называются сочетаниями с повторением. Их число обозначается \bar C_n^{\,k} .

**Теорема:**число сочетаний с повторениями может быть вычислено по формулам:

\bar C_n^{\,k}  = C_{n + k - 1}^{\,k}  = C_{n + k - 1}^{\,n - 1}
.

Подсчитаем количество способов, которыми можно выбрать k из n различных предметов. Такие выборки называются сочетаниями, а их количество обозначается C_n^{\,k} .

При k < n, выбрать *k* предметов из n можно A_{\,n}^{\,k}  способами, переставляя их P_k  способами:

C_n^{\,k}  = \frac{{A_{\,n}^{\,k} }}{{P_k }} = \frac{{n!}}{{(n -
k)!\,\, \cdot k!}}.

Рекуррентная формула: C_m^n  = C_m^{n - 1} \frac{{m - n +
1}}{n}.

Свойства сочетаний: C_m^n  = C_m^{m - n} ;\;C_m^n  +
C_m^{n + 1}  = C_{m + 1}^{n + 1} .

1. **Бином Ньютона. Биномиальные коэффициенты.**

**Формула бинома Ньютона** для натуральных *n* имеет вид формула бинома Ньютона, где формула - **биномиальные коэффициенты**, представляющие из себя сочетания из *n* по *k*, *k=0,1,2,…,n*, а "!" – это знак факториала).

К примеру, известная формула сокращенного умножения "квадрат суммы" вида формула есть частный случай бинома Ньютона при *n=2*. Выражение, которое находится в правой части формулы бинома Ньютона, называют **разложением** выражения *(a+b)n*, а выражение формула называют ***(k+1)*-ым членом разложения**, *k=0,1,2,…,n*.

### Свойства биномиальных коэффициентов.

Для коэффициентов бинома Ньютона справедливы следующие свойства:

* коэффициенты, равноудаленные от начала и конца разложения, равны между собой формула, *p=0,1,2,…,n*;
* формула;
* сумма биномиальных коэффициентов равна числу *2*, возведенному в степень, равную показателю степени бинома Ньютона: формула;
* сумма биномиальных коэффициентов, стоящих на четных местах, равна сумме биномиальных коэффициентов, стоящих на нечетных местах.

Первые два свойства являются свойствами числа сочетаний.

1. **Формула Паскаля. Треугольник Паскаля.**

**Треугольник Паскаля** — бесконечная таблица биномиальных коэффициентов, имеющая треугольную форму. В этом треугольнике на вершине и по бокам стоят единицы. Каждое число равно сумме двух расположенных над ним чисел. Строки треугольника симметричны относительно вертикальной оси. Назван в честь Блеза Паскаля. Числа, составляющие треугольник Паскаля, возникают естественным образом в алгебре, комбинаторике, теории вероятностей, математическом анализе, теории чисел**.**

[Биномиальные коэффициенты](https://ru.wikipedia.org/wiki/%D0%91%D0%B8%D0%BD%D0%BE%D0%BC%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D0%BA%D0%BE%D1%8D%D1%84%D1%84%D0%B8%D1%86%D0%B8%D0%B5%D0%BD%D1%82) часто обозначаются \tbinom{n}{k} или \textstyle C_n^k и читаются как «число сочетаний из *n* элементов по *k*».

* Числа треугольника симметричны (равны) относительно вертикальной оси.
* В строке с номером *n*:
  + первое и последнее числа равны 1.
  + второе и предпоследнее числа равны *n*.
  + третье число равно [треугольному числу](https://ru.wikipedia.org/wiki/%D0%A2%D1%80%D0%B5%D1%83%D0%B3%D0%BE%D0%BB%D1%8C%D0%BD%D0%BE%D0%B5_%D1%87%D0%B8%D1%81%D0%BB%D0%BE) \textstyle T_{n-1}=\frac{n(n-1)}{2}, что также равно сумме номеров предшествующих строк.
  + четвёртое число является [тетраэдрическим](https://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D1%82%D1%80%D0%B0%D1%8D%D0%B4%D1%80%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B5_%D1%87%D0%B8%D1%81%D0%BB%D0%B0).
  + *m*-е число (при нумерации с 0) равно [биномиальному коэффициенту](https://ru.wikipedia.org/wiki/%D0%91%D0%B8%D0%BD%D0%BE%D0%BC%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D0%BA%D0%BE%D1%8D%D1%84%D1%84%D0%B8%D1%86%D0%B8%D0%B5%D0%BD%D1%82) \textstyle C_n^m = \binom{n}{m} = \frac{n!}{m!(n-m)!}.
* Сумма чисел восходящей диагонали, начинающейся с первого элемента (*n*-1)-й строки, есть *n*-е [число Фибоначчи](https://ru.wikipedia.org/wiki/%D0%A7%D0%B8%D1%81%D0%BB%D0%BE_%D0%A4%D0%B8%D0%B1%D0%BE%D0%BD%D0%B0%D1%87%D1%87%D0%B8):

{n-1\choose 0}+{n-2\choose 1}+{n-3\choose 2}+\ldots=F_n.

* Если вычесть из центрального числа в строке с чётным номером соседнее число из той же строки, то получится [число Каталана](https://ru.wikipedia.org/wiki/%D0%A7%D0%B8%D1%81%D0%BB%D0%BE_%D0%9A%D0%B0%D1%82%D0%B0%D0%BB%D0%B0%D0%BD%D0%B0).
* Сумма чисел *n*-й строки треугольника Паскаля равна 2^n.
* Все числа в *n*-й строке, кроме единиц, делятся на число *n*, если и только если *n* является [простым числом](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%81%D1%82%D0%BE%D0%B5_%D1%87%D0%B8%D1%81%D0%BB%D0%BE)[[4]](https://ru.wikipedia.org/wiki/%D0%A2%D1%80%D0%B5%D1%83%D0%B3%D0%BE%D0%BB%D1%8C%D0%BD%D0%B8%D0%BA_%D0%9F%D0%B0%D1%81%D0%BA%D0%B0%D0%BB%D1%8F#cite_note-mathworld-4) (следствие [теоремы Люка](https://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D0%BE%D1%80%D0%B5%D0%BC%D0%B0_%D0%9B%D1%8E%D0%BA%D0%B0)).
* Если в строке с нечётным номером сложить все числа с порядковыми номерами вида 3*n*, 3*n*+1, 3*n*+2, то первые две суммы будут равны, а третья на 1 меньше.
* Каждое число в треугольнике равно количеству способов добраться до него из вершины, перемещаясь либо вправо-вниз, либо влево-вниз.

## Графы.

1. **Графы: простой, мульти граф, псевдо граф.**

**Граф** — совокупность непустого [множества](https://ru.wikipedia.org/wiki/%D0%9C%D0%BD%D0%BE%D0%B6%D0%B5%D1%81%D1%82%D0%B2%D0%BE) вершин и наборов пар вершин (связей между вершинами).

Объекты представляются как вершины, или узлы графа, а связи — как дуги, или рёбра.

**Граф**, или **неориентированный граф** G — это [упорядоченная пара](https://ru.wikipedia.org/wiki/%D0%A3%D0%BF%D0%BE%D1%80%D1%8F%D0%B4%D0%BE%D1%87%D0%B5%D0%BD%D0%BD%D0%B0%D1%8F_%D0%BF%D0%B0%D1%80%D0%B0) G := (V, E), где V — это непустое [множество](https://ru.wikipedia.org/wiki/%D0%9C%D0%BD%D0%BE%D0%B6%D0%B5%D1%81%D1%82%D0%B2%D0%BE) **вершин** или **узлов**, а E — множество пар вершин, называемых **рёбрами**.

Вершины и рёбра графа называются также **элементами** графа, число вершин в графе |V| — **порядком**, число рёбер |E| — **размером** графа.

Вершины u и v называются  **концами** e=\{u,v\}. Ребро, в свою очередь, **соединяет** эти вершины. Две концевые вершины одного и того же ребра называются **соседними**.

Два ребра называются **смежными**, если они имеют общую концевую вершину.

Два ребра называются **кратными**, если множества их концевых вершин совпадают.

Ребро называется **петлёй**, если его концы совпадают, то есть e=\{v,v\}.

**Степенью** \deg V вершины V называют количество инцидентных ей рёбер (при этом петли считают дважды).

Вершина называется **изолированной**, если она не является концом ни для одного ребра; **висячей** (или **листом**), если она является концом ровно одного ребра.

**Простые графы** — графы, не имеющие петель и кратных рёбер.

**Мульти графы** — графы с *кратными* рёбрами, имеющими своими концами одну и ту же пару вершин.

**Псевдо графы** — это мульти графы, допускающие наличие петель.

1. **Маршруты, цепи, циклы. Связность.**

**Маршрутом** в графе - называют конечную последовательность вершин, в которой каждая вершина соединена со следующей в последовательности вершиной ребром. **Цепью** называется маршрут без повторяющихся рёбер. **Простой цепью** называется маршрут без повторяющихся вершин (откуда следует, что в простой цепи нет повторяющихся рёбер).

**Ориентированным маршрутом** (или **путём**) в орграфе называют конечную последовательность вершин и дуг, в которой каждый элемент инцидентен предыдущему и последующему.

**Циклом** называют цепь, в которой первая и последняя вершины совпадают. При этом **длиной** пути (или цикла) называют число составляющих его *рёбер*. Заметим, что если вершины u и v являются концами некоторого ребра, то согласно данному определению, последовательность (u,v,u) является циклом. Чтобы избежать таких «вырожденных» случаев, вводят следующие понятия.

Путь (или цикл) называют **простым**, если ребра в нём не повторяются; **элементарным**, если он простой и вершины в нём не повторяются.

Простейшие свойства путей и циклов:

* всякий путь, соединяющий две вершины, содержит элементарный путь, соединяющий те же две вершины;
* всякий простой *неэлементарный* путь содержит элементарный *цикл*;
* всякий *простой* цикл, проходящий через некоторую вершину (или ребро), содержит *элементарный* (под-)цикл, проходящий через ту же вершину (или ребро);
* петля — элементарный цикл.
* **Связным** называется граф, если для любых вершин u,v есть путь из u в v.
* **Сильно связным** или **ориентированно связным**, если он ориентированный, и из любой вершины в любую другую имеется ориентированный путь.

Бинарное отношение на множестве вершин графа, заданное как «существует путь из u в v», является отношением эквивалентности и, следовательно, разбивает это множество на классы эквивалентности, называемые **компонентами связности** графа. Если у графа ровно одна компонента связности, то граф связный. На компоненте связности можно ввести понятие **расстояния** между вершинами как минимальную длину пути, соединяющего эти вершины.

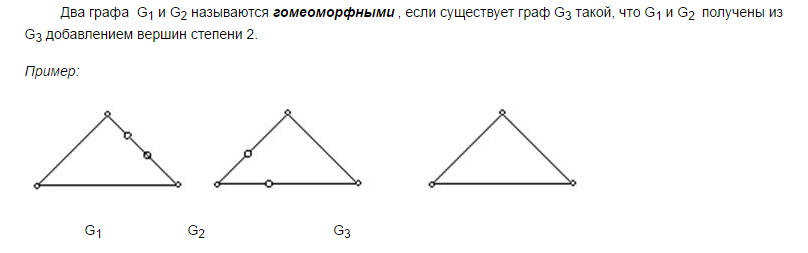
Всякий максимальный связный подграф графа G называется **связной компонентой** (или просто компонентой) графа G. Слово «максимальный» означает максимальный относительно включения, то есть не содержащийся в связном подграфе с большим числом элементов.

Ребро графа называется **мостом**, если его удаление увеличивает число компонент.

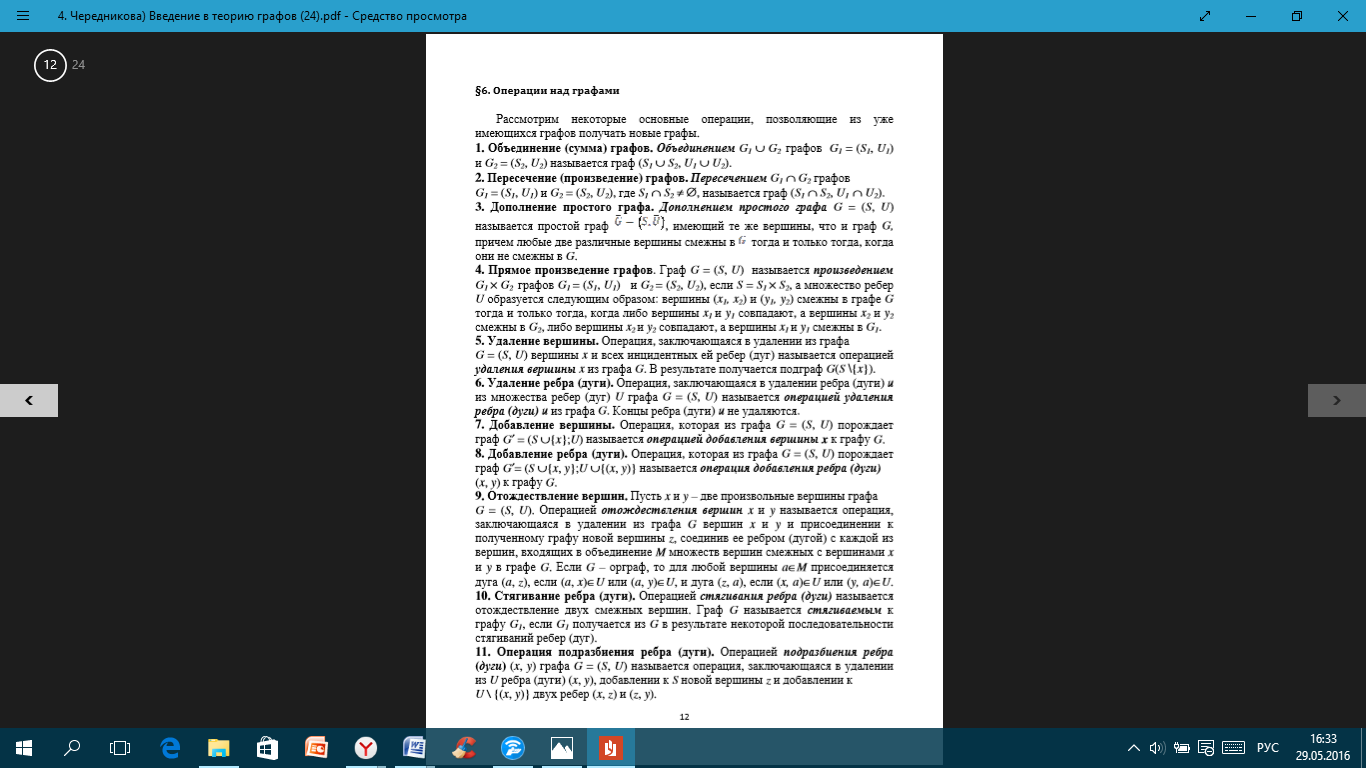
1. **Изоморфизм графов. Операции над графами. Гомеоморфизм графов.**

Графы G и H являются изоморфными, если путём перестановки строк и столбцов матрицы смежности графа G удается получить матрицу смежности графа H. Однако перебор всех возможных [перестановок](https://ru.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D0%B5%D1%81%D1%82%D0%B0%D0%BD%D0%BE%D0%B2%D0%BA%D0%B0) характеризуется вычислительной сложностью O(N!) (при условии, что сравнение матриц смежности производится за время, не зависящее от N, что обычно несправедливо и дополнительно увеличивает приведенную оценку), что существенно ограничивает применение подобного подхода на практике. Существуют методы ограниченного перебора возможных пар предположительно-изоморфных вершин (аналог [метода ветвей и границ](https://ru.wikipedia.org/wiki/%D0%9C%D0%B5%D1%82%D0%BE%D0%B4_%D0%B2%D0%B5%D1%82%D0%B2%D0%B5%D0%B9_%D0%B8_%D0%B3%D1%80%D0%B0%D0%BD%D0%B8%D1%86)), однако они незначительно улучшают приведенную выше асимптотику.

В [теории графов](https://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D0%BE%D1%80%D0%B8%D1%8F_%D0%B3%D1%80%D0%B0%D1%84%D0%BE%D0%B2) **изоморфизмом графов** G=\left \langle V_G, E_G \right \rangle и H=\left \langle V_H, E_H \right \rangle называется [биекция](https://ru.wikipedia.org/wiki/%D0%91%D0%B8%D0%B5%D0%BA%D1%86%D0%B8%D1%8F) между множествами вершин графов f \colon\ V_G \rightarrow V_H такая, что любые две вершины u и v графа G смежны тогда и только тогда, когда вершины f(u) и f(v) смежны в графе H. Здесь графы понимаются неориентированными и не имеющими весов вершин и ребер. В случае, если понятие изоморфизма применяется к ориентированным или взвешенным графам, накладываются дополнительные ограничения на сохранение ориентации дуг и значений весов. Если изоморфизм графов установлен, они называются изоморфными и обозначаются как G\simeq H**.**



**Операции над графами.**

.

1. **Представления графов. Матрицы смежности, инцидентности, весов графа. Список ребер графа.**

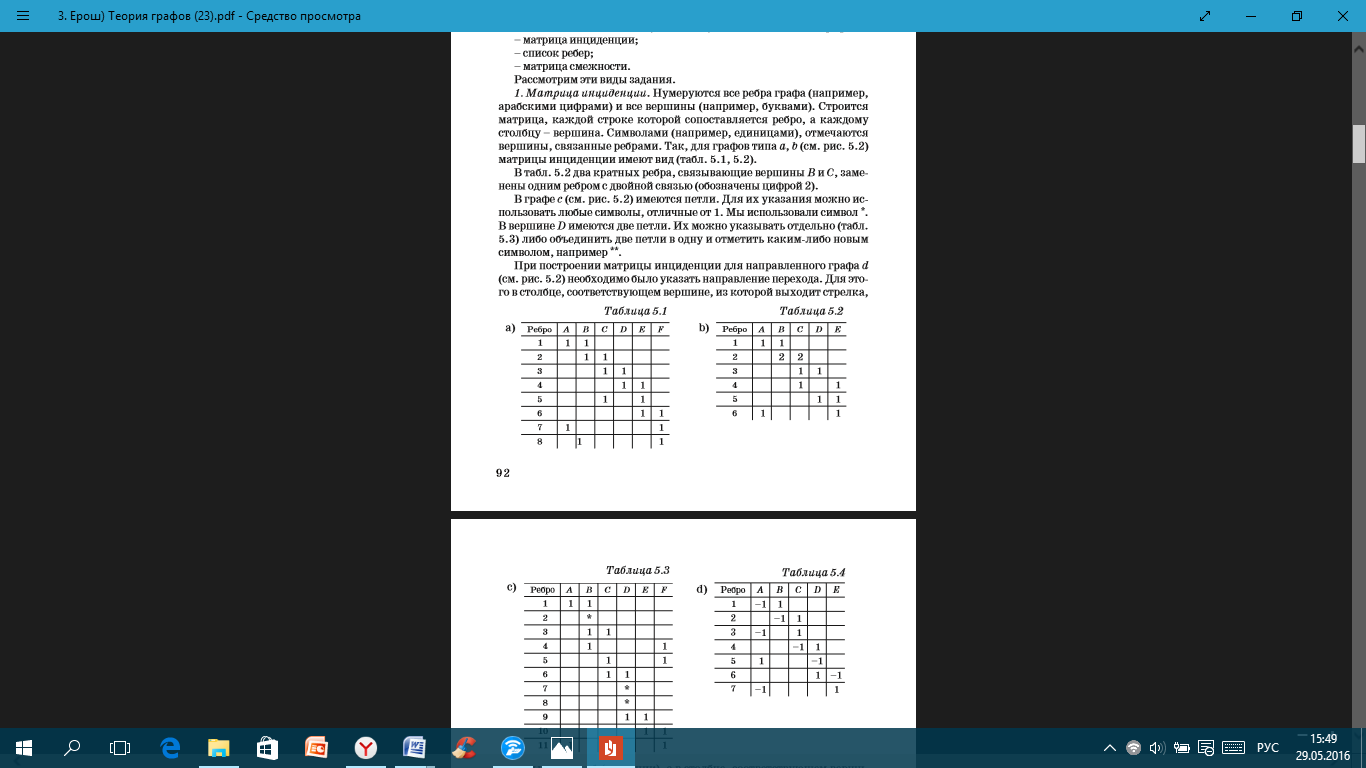
Для того чтобы использовать задания в виде графов при решении разнообразных оптимизационных задач, применяют различные эквивалентные способы задания. Основным требованием является взаимная однозначность графического изображения и выбранного способа задания. Чаще всего используются следующие виды задания графа:

– матрица инцидентности;

– список ребер;

– матрица смежности.

1. **Матрица инциденции.**

Нумеруются все ребра графа (например, арабскими цифрами) и все вершины (например, буквами). Строится матрица, каждой строке которой сопоставляется ребро, а каждому столбцу – вершина. Символами (например, единицами), отмечаются вершины, связанные ребрами. Далее заполняется таблица. Пример: 

1. **Список рёбер.**

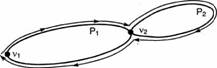
Этот список является сокращением матрицы ин циденции. Число строк, как и ранее, равно числу ребер графа, а стол‑ бцов только два. В первом указываются вершины, из которых вы‑ ходят ребра, а во втором – в которые входят.

1. **Матрица смежности.**

Каждой строке и каждому столбцу соответствует вершина графа. На пересечении строки и столбца ставятся символы, на‑ пример 1, если эти вершины связаны одним ребром, 2 – если двумя и т. д. Очевидно, что для ненаправленных графов без петель матрица смежности симметрична относительно главной диагонали. Если исключить избыточную информацию (главную диагональ и верхнюю правую половину матрицы), то получим треугольную таблицу. Матрицы смежности для направленного графа не являются симметричными относительно главной диагонали, и поэтому они не сжимаются до треугольных таблиц.

1. **Эйлеровы графы. Гамильтоновы цепи и циклы. Гамильтоновы графы.**

**Эйлеровым путем** в графе называется путь, содержащий все ребра графа.   
**Эйлеровым циклом** в графе называется цикл, содержащий все ребра графа  
Граф, обладающий эйлеровым циклом, называется **эйлеровым графом**.

**Теорема 2. (Теорема Эйлера) Связный граф является эйлеровым тогда и только тогда, когда степень каждой его вершины четная.**  
**Доказательство. Необходимость.**Пусть G— эйлеров граф. Эйлеров цикл этого графа, проходя через каждую его вершину, входит в нее по одному ребру, а выходит по другому. Это означает, что каждое прохождение вершины по циклу вносит слагаемое 2 в ее степень. По­скольку цикл содержит все ребра графа, то степени всех вершин будут четными.   
**Достаточность.**Предположим, что степени всех вершин связ­ного графа Gчетные. Начнем цепь G1 из произвольной вершины v1, и будем продлевать ее, выбирая каждый раз новое ребро. Так как степени вершин четные, то, попав в некоторую вершину, мы всегда будем иметь в распоряжении еще не пройденное ребро. Таким образом, построение це­пи Р1обязательно закончится в вершине v1, и Р1будет циклом. Если Р1содержит все ребра графа G, то построен эйлеров цикл. В противном слу­чае, удалив из Gребра Р1, получим граф G2. Так как степени всех вер­шин графов Gи Р1 были четными, то и G2будет обладать этим свойст­вом. В силу связности Gграфы Р1 и G2должны иметь хотя бы одну об­щую вершину v2. Теперь, начиная из v2, построим в G цикл Р2подобно тому, как построили Р1.  
Объединим циклы Р1 иР2следующим образом: пройдем часть Р1 от вершины v1 до вершины v2, затем пройдем цикл Р2,затем — оставшуюся часть Р1 от v2 до v1 (см. рис. 28).  


Если объединенный цикл не эйлеров, то, проделав аналогичные построения, получим еще больший цикл. Поскольку степени вершин во всех графах, составленных из ребер, не попавших в строящийся цикл, четные, и число ребер в этих графах убывает, то процесс закончится построением эйлерова цикла. Теорема доказана.

Рассмотрим построенный граф G. В этом графе вершины 2 и 4 имеют нечетную степень, следовательно, граф G не является эйлеровым. Это означает, что желаемую прогулку по мостикам совершить нельзя.

**Гамильтоновы цепи и циклы, графы.**

Простая **цепь** (цикл) в псевдографе G называется **гамильтоновой** (гамильтоновым), если она (он) проходит через каждую вершину псевдографа G.

Псевдограф, у которого есть гамильтонов цикл, называется **гамильтоновым графом**.

Очевидно, вопросы существования гамильтоновых цепей и циклов в псевдографах сводятся к аналогичным вопросам для простых графов. Следует отметить, что до сих пор неизвестны необходимые и достаточные условия существования в произвольном простом графе гамильтонова цикла или гамильтоновой цепи. Однако имеется класс графов, в которых заведомо существуют гамильтоновы цепи и циклы – это полные графы. Таким образом, полнота графа является простейшим достаточным условием существования гамильтоновых цепей и циклов в простом графе.

Очевидным простейшим *необходимым условием* существования гамильтоновых цепей и циклов в простом графе является его связность. Более тонким необходимым условием существования гамильтоновых цепей и циклов в простом графе является отсутствие в нем точек сочленения, то есть вершин, удаление которых увеличивает число компонент связности.

1. **Ациклический граф. Лес. Деревья. Свойства деревьев. Корневые деревья. Высота ордерева.**

Любой связный неориентированный граф, не содержащий циклов, называется (неориентированным) **деревом**.

Любой неориентированный граф без циклов называется **лесом** или **ациклическим графом.**

**Лес** — упорядоченное множество упорядоченных деревьев.

.Таким образом, компонентами связности любого леса являются деревья.

Пусть G = (S,U) и . Тогда следующие условия эквивалентны:

1) G – дерево;

2) G – связный граф и m = n − 1;

3) G – ациклический граф и m = n − 1;

4) любые две различные вершины графа соединяет единственная простая цепь;

5) G – ациклический граф, такой, что если какую-либо пару его несмежных вершин соединить ребром, то полученный граф будет содержать ровно один цикл.

**Ориентированным деревом (ордеревом**) называется ориентированный граф G = (S,U), удовлетворяющий следующим двум условиям:

1. Существует единственная вершина xi ∈ S, называемая корнем, не имеющая предшествующих вершин
2. Любой вершине xj, отличной от xi, в орграфе G непосредственно предшествует ровно одна вершина.

**Ветвью ордерева** называется путь из корня в лист.

**Высотой** ордерева называется длина его наибольшей ветви.

**Дерево** — это [связный](https://ru.wikipedia.org/wiki/%D0%A1%D0%B2%D1%8F%D0%B7%D0%BD%D1%8B%D0%B9_%D0%B3%D1%80%D0%B0%D1%84) [ациклический граф](https://ru.wikipedia.org/wiki/%D0%90%D1%86%D0%B8%D0%BA%D0%BB%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9_%D0%B3%D1%80%D0%B0%D1%84).[[1]](https://ru.wikipedia.org/wiki/%D0%94%D0%B5%D1%80%D0%B5%D0%B2%D0%BE_(%D1%82%D0%B5%D0%BE%D1%80%D0%B8%D1%8F_%D0%B3%D1%80%D0%B0%D1%84%D0%BE%D0%B2)#cite_note-1) Связность означает наличие путей между любой парой вершин, ацикличность — отсутствие циклов и то, что между парами вершин имеется только по одному пути.

1. **Цикломатическое число графа.**

**Цикломатическое число графа** — минимальное число рёбер, которые надо удалить, чтобы граф стал ациклическим. Для связного графа существует соотношение: p_1(G) = p_0(G) + |E(G)| - |V(G)|, где p_1(G) — цикломатическое число, p_0 — число *компонент связности* графа, |E(G)| — число *рёбер*, а |V(G)| — число *вершин*.

***В графе число n определяет число независимых циклов в нем.***

Доказательство следует из того, что если в граф **G**добавить ребро **(a,b)**, то возможны два случая.

если в **G**вершины **a** и**b**связаны цепью, то в расширенном графе **G’**добавится еще один цикл, т.е. будет **m’=m+1, p’=p, n ’=n +1**;

если в **G**вершины **a** и**b**цепьюне связаны, то в расширенном графе **G’** уменьшится на единицу число компонент связности, т.е. **m’=m+1, p’=p-1, n ’=n .**

Для любого графа можно проделать такую процедуру. Удалим из него все ребра и затем будем вводить их по одному. Для графа без ребер утверждение теоремы верно (число циклов и число ребер равно 0, число вершин равно числу компонент связности). Каждое новое ребро будет приводить к описанным выше двум случаям, то есть будет выполняться утверждение теоремы.

1. **Остовное дерево графа. Задача о минимальном остове. Алгоритм Краскала.**

**Остовное дерево** — ациклический связный подграф данного связного неориентированного графа, в который входят все его вершины. Проще говоря, остовное дерево состоит из некоторого подмножества рёбер графа, таких, что из любой вершины графа можно попасть в любую другую вершину, двигаясь по этим рёбрам, и в нём нет циклов, то есть из любой вершины нельзя попасть в саму себя, не пройдя какое-то ребро дважды.

**Задача о минимальном остове.**

Эта задача возникает при проектировании линий электропередачи, трубопроводов, дорог и т.д., когда требуется заданные центры соединить некоторой системой каналов (связей) таким образом, чтобы любые два центра были связаны непосредственно или через другие каналы, и чтобы общая длина (стоимость) каналов связей была минимальной.

Определение. Граф называется *взвешенным,*если его ребрам или дугам приписаны некоторые числа (веса).

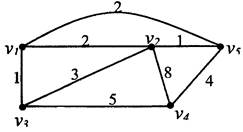
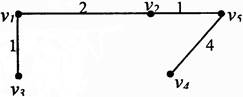
Определение. Остовным деревом или *остовом*графа называется связный подграф без циклов, содержащий все вершины исходного графа. Подграф содержит часть или все ребра исходного графа.

Задача о минимальном остове формулируется следующим образом: *во взвешенном связном графе найти остов минимального веса, то есть остов, суммарный вес ребер которого является минимальным.*

Рассмотрим **алгоритм Краскала** построения минимального остова графа. Остов строится постепенно, на каждом шаге добавляется одно ребро. В алгоритме используются два правила.

1) Первое ребро остова - ребро минимального веса в исходном графе.

2) Если в остов уже добавлено *i*(*i<n-1*)ребер, то следующее ребро *еi*+1, есть ребро минимального веса среди ребер, которые еще не включены в остов и не составляют циклов с уже добавленными ребрами.

Найти минимальный остов в графе

Построение остова начнем с ребра (*v*1,*v*j), так как оно имеет минимальный вес (можно было начать и с ребра *(v2,v5)).*Порядок присоединения ребер к остову:

http://ok-t.ru/studopediaru/baza15/381962504907.files/image008.gif

Вес остова: W=1+2+1+4=8.

Заметьте, что ребра (*v*2,*v*3), (*v*1,*v*5)не были включены в остов, хотя имели вес меньший, чем ребро (*v4,v*5)*,*так как они образовывали циклы с уже включенными ребрами.

1. **Представление свободных деревьев кодом Прюфера.**

Код Прюфера — это способ однозначного кодирования n-вершинного помеченного дерева упорядоченной последовательностью из n-2 номеров его вершин. Из теоремы Кэли следует, что каждой такой последовательности можно сопоставить некоторое дерево, и наоборот, то есть между ними существует взаимооднозначное соответствие.

В ходе составления кода Прюфера из дерева поочерёдно удаляются вершины, пока их не останется только две. Без ограничения общности предполагается, что вершины помечены целыми числами. Первым элементом кода Прюфера будет номер вершины, смежной с минимальным по номеру листом. После добавления в код Прюфера первого элемента, лист с минимальным номером удаляется из дерева. Далее снова нужно найти лист с минимальным номером и вписать в код Прюфера номер вершины, смежной с ним, после чего удалить этот лист из дерева, и так далее, пока в дереве не останется только две вершины. На этом построение кода Прюфера заканчивается, так как в него уже были добавлены n-2 номера вершины.

**Восстановление дерева по коду Прюфера**

По построению очевидно, что количество вхождений некоторого числа k в код Прюфера ровно на единицу меньше степени соответствующей вершины. Сразу посчитаем и запишем степень каждой вершины. После этого мы можем узнать номера всех листьев и вычислить номер минимального из них. Из построения, следует, что этот лист связан ребром с первой вершиной из кода Прюфера. Таким образом, первое ребро графа найдено.

После нахождения первого ребра следует уменьшить на единицу степени двух его вершин. После нахождения новых рёбер будем делать также, чтобы степени в массиве соответствовали степеням разности исходного графа уже с найденным. Разность двух этих графов будет соответствовать состоянию, в котором находился граф после составления некоторой части кода. Следовательно, к хранящимся степеням можно заново применить тот же ход --- найти лист с минимальным номером, и определить, что он соединён ребром со следующим элементом кода. Далее опять уменьшить степень каждой из соединённых вершин, и повторить ту же процедуру, и так далее...

Когда представленный алгоритм пройдёт все элементы кода Прюфера, в массиве степеней останутся единицы в двух местах и нули во всех остальных. Следовательно, нужно соединить ребром две вершины с оставшимися единичными степенями, получив последнее n-1-ое ребро.

Как для составления кода Прюфера по графу, так и для обратного преобразования, существуют алгоритмы, работающие за линейное от количества вершин время, то есть с асимптотической сложностью O(n).

1. **Полный двудольный граф.**

**Двудо́льный граф** или **бигра́ф** — граф, множество вершин которого можно разбить на две части таким образом, что каждое ребро графа соединяет какую-то вершину из одной части с какой-то вершиной другой части, то есть не существует ребра, соединяющего две вершины из одной и той же части.

**Полный двудольный граф** (*биклика*) — специальный вид двудольного графа, у которого любая вершина первой доли соединена со всеми вершинами второй доли вершин.

1. **Плоские и планарные графы. Формула Эйлера.**

**Плоский граф**- граф, изображённый на плоскости так, что его вершины — это точки плоскости, а рёбра — непересекающиеся кривые на ней. Области, на которые граф разбивает плоскость, называются его гранями. Неограниченная часть плоскости — тоже грань, так называемая внешняя грань.

**Плана́рный граф** — граф, который может быть изображён на плоскости без пересечения ребер. Иначе говоря, граф планарен, если он изоморфен некоторому плоскому графу**.**

### Формула Эйлера

Для связного плоского графа справедливо следующее соотношение между количеством вершин |V(G)|, рёбер |E(G)| и граней |F(G)| (включая внешнюю грань):

\ |V(G)|-|E(G)|+|F(G)| = 2.

Оно было найдено [Эйлером](https://ru.wikipedia.org/wiki/%D0%AD%D0%B9%D0%BB%D0%B5%D1%80,_%D0%9B%D0%B5%D0%BE%D0%BD%D0%B0%D1%80%D0%B4) в 1736 г.[[1]](https://ru.wikipedia.org/wiki/%D0%9F%D0%BB%D0%B0%D0%BD%D0%B0%D1%80%D0%BD%D1%8B%D0%B9_%D0%B3%D1%80%D0%B0%D1%84#cite_note-Harary_126-1) при изучении свойств выпуклых [многогранников](https://ru.wikipedia.org/wiki/%D0%9C%D0%BD%D0%BE%D0%B3%D0%BE%D0%B3%D1%80%D0%B0%D0%BD%D0%BD%D0%B8%D0%BA). Это соотношение справедливо и для других поверхностей с точностью до коэффициента, называемого [эйлеровой характеристикой](https://ru.wikipedia.org/wiki/%D0%AD%D0%B9%D0%BB%D0%B5%D1%80%D0%BE%D0%B2%D0%B0_%D1%85%D0%B0%D1%80%D0%B0%D0%BA%D1%82%D0%B5%D1%80%D0%B8%D1%81%D1%82%D0%B8%D0%BA%D0%B0" \o "Эйлерова характеристика). Это [инвариант](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D0%B2%D0%B0%D1%80%D0%B8%D0%B0%D0%BD%D1%82_(%D0%BC%D0%B0%D1%82%D0%B5%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0)) поверхности, для плоскости или сферы он равен двум, а, например, для поверхности [тора](https://ru.wikipedia.org/wiki/%D0%A2%D0%BE%D1%80_(%D0%BF%D0%BE%D0%B2%D0%B5%D1%80%D1%85%D0%BD%D0%BE%D1%81%D1%82%D1%8C)) — нулю.

Формула имеет множество полезных следствий. Во-первых, все плоские укладки одного графа имеют одинаковое количество граней. Во-вторых, если **каждая грань ограничена не менее чем тремя рёбрами** (при условии, что в графе больше двух рёбер), а **каждое ребро разделяет две грани**, то

3|F(G)| \le 2|E(G)|,

следовательно,

|E(G)| \le 3|V(G)|-6,

то есть, при большем числе рёбер такой граф заведомо непланарен. Обратное утверждение не верно: в качестве контрпримера можно взять [граф Петерсена](https://ru.wikipedia.org/wiki/%D0%93%D1%80%D0%B0%D1%84_%D0%9F%D0%B5%D1%82%D0%B5%D1%80%D1%81%D0%B5%D0%BD%D0%B0). Отсюда следует, что в планарном графе всегда можно найти вершину степени не более 5.

Общая формула также легко обобщается на случай несвязного графа:

|V(G)|-|E(G)|+|F(G)|=1+|C(G)|,

где |C(G)| — количество компонент связности в графе.

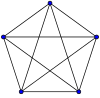
1. **Непланарность графов K5 и K3,3. Теорема Понтрягина-Куратовского.**

**Условия непланарности:**

**достаточное условие** — если граф содержит полный [двудольный подграф](https://ru.wikipedia.org/wiki/%D0%94%D0%B2%D1%83%D0%B4%D0%BE%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D0%B3%D1%80%D0%B0%D1%84) K3,3 или [полный подграф](https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D0%BB%D0%BD%D1%8B%D0%B9_%D0%B3%D1%80%D0%B0%D1%84) K5, то он является непланарным;

**необходимое условие** — если граф непланарный, то он должен содержать больше 4 вершин, степень которых больше 3, или больше 5 вершин степени больше 2.

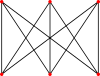
### Полный граф с пятью вершинами

[](https://commons.wikimedia.org/wiki/File:Complete_graph_K5.svg?uselang=ru)K5, полный граф с 5 вершинами

**Лемма.** [Полный граф](https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D0%BB%D0%BD%D1%8B%D0%B9_%D0%B3%D1%80%D0%B0%D1%84) с пятью вершинами (К5) нельзя уложить на плоскость.

**Доказательство.** Для него не выполняется E \leqslant 3V - 6.

«Домики и колодцы»

[](https://commons.wikimedia.org/wiki/File:Complete_bipartite_graph_K3,3.svg?uselang=ru)Граф «домики и колодцы» (K3,3)

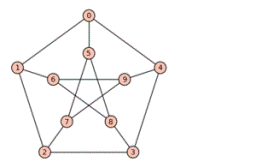
**Задача о трёх колодцах**. Есть три дома и три колодца. Можно ли так проложить дорожки между домами и колодцами, чтобы от каждого дома к каждому колодцу вела дорожка, и никакие две дорожки не пересекались бы. Мосты строить нельзя.

**Лемма.** Полный [двудольный граф](https://ru.wikipedia.org/wiki/%D0%94%D0%B2%D1%83%D0%B4%D0%BE%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D0%B3%D1%80%D0%B0%D1%84) с тремя вершинами в каждой из долей (К3,3) нельзя уложить на плоскость.

**Доказательство.** По формуле Эйлера граф имеет 5 граней.

С другой стороны: любая грань (включая внешнюю) содержит не менее 4 рёбер. Поскольку каждое ребро включается в ровно две грани, получается соотношение 4F \leqslant 2E, *F* — количество граней, *E* — количество рёбер. Подставляем в это неравенство *F* = 5 и *E* = 9 и видим, что оно не выполняется.

**Теорема Понтрягина — Куратовского**

[](https://commons.wikimedia.org/wiki/File:Kuratowski.gif?uselang=ru)В общем случае найти K5 или K3,3 довольно сложно. [Граф Петерсена](https://ru.wikipedia.org/wiki/%D0%93%D1%80%D0%B0%D1%84_%D0%9F%D0%B5%D1%82%D0%B5%D1%80%D1%81%D0%B5%D0%BD%D0%B0) несложно стянуть в K5, но в нём есть и K3,3.

Очевидно утверждение: если граф *G* содержит подграф, [гомеоморфный](https://ru.wikipedia.org/w/index.php?title=%D0%93%D0%BE%D0%BC%D0%B5%D0%BE%D0%BC%D0%BE%D1%80%D1%84%D0%B8%D0%B7%D0%BC_%D0%B3%D1%80%D0%B0%D1%84%D0%BE%D0%B2&action=edit&redlink=1) K5 или K3,3, то его невозможно разложить на плоскости. Оказывается, верно и обратное.

|  |
| --- |
| Граф планарен *тогда и только тогда, когда* он не содержит подграфов, [гомеоморфных](https://ru.wikipedia.org/w/index.php?title=%D0%93%D0%BE%D0%BC%D0%B5%D0%BE%D0%BC%D0%BE%D1%80%D1%84%D0%B8%D0%B7%D0%BC_%D0%B3%D1%80%D0%B0%D1%84%D0%BE%D0%B2&action=edit&redlink=1) полному графу из пяти вершин (K5) или графу «домики и колодцы» (K3,3). |

Теорему также можно сформулировать в следующем варианте (иногда его называют «теорема Вагнера»).

|  |
| --- |
| Граф планарен *тогда и только тогда, когда* не содержит подграфов, [стягивающихся](https://ru.wikipedia.org/wiki/%D0%A1%D1%82%D1%8F%D0%B3%D0%B8%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D1%80%D0%B5%D0%B1%D1%80%D0%B0) в K5или K3,3. |

1. **Хроматические графы. Теорема о раскраске планарных графов в пять цветов. Гипотеза четырех красок. Теорема Хивуда.**

**K-хроматический граф** — граф, хроматическое число которого равно *K*. То есть вершины графа можно раскрасить *K* цветами так, что у любого ребра концы будут разного цвета, но так раскрасить *K* − 1 цветами — уже нельзя.

**K-раскрашиваемый граф** — граф, хроматическое число которого не превосходит *K*. То есть его вершины можно раскрасить *K* разными цветами так, что у любого ребра концы будут разного цвета.

**Хроматическое число графа G** — минимальное число цветов, в которые можно раскрасить вершины графа G так, чтобы концы любого ребра имели разные цвета. Обозначается χ(*G*).

## 1. Определение

Хроматическое число графа — минимальное число *k*, такое что множество *V* вершин графа можно разбить на *k* непересекающихся классов C_1, C_2, \ldots, C_k:

V=\bigcup_i^{} C_i;\ C_i\cap C_j=\varnothing,

таких, что вершины в каждом классе независимы, то есть любое ребро графа не соединяет вершины одного и того же класса.

**Хроматический класс графа G** — минимальное число цветов, в которые можно раскрасить ребра графа G так, чтобы смежные ребра имели разные цвета. Обозначается χ'(*G*). Проблема реберной раскраски произвольного плоского кубического графа без мостов тремя цветами эквивалентна знаменитой Проблеме четырех красок. Реберная раскраска определяет 1-факторизацию графа.

**Раскраской графа** называется такое приписывание цветов его вершинам, что никакие две смежные вершины не получают одинакового цвета. В k-раскраске графа используется k цветов.

***Гипотеза четырех красок*: всякий планарный граф можно раскрасить в четыре цвета.**

Единодушно признается, что гипотеза справедлива, но маловероятно, что она будет доказана в общем случае. Если доказательство будет найдено, то улучшить результат (т.е. уменьшить количество цветов) окажется невозможным: например, для планарного графа *K*4 меньше чем четырьмя цветами обойтись нельзя.

Чтобы убедиться в этом, предположим, что гипотеза четырех красок справедлива, и возьмем произвольную плоскую карту G. Пусть G\*— граф, являющийся основой карты, геометрически двойственной к карте G. Так как две области карты G смежны тогда и только тогда, когда соответствующие им вершины графа G\* смежны, то карта G 4-раскрашиваема, поскольку граф G\* 4-раскрашиваем.

Обратно, предположим, что каждая плоская карта 4-раскрашиваема. Пусть Н — любой планарный граф, а Н\*— граф, двойственный к графу Н и нарисованный так, что каждая его область содержит точно одну вершину графа Н. Связный плоский псевдограф Н\* можно перевести в плоский граф Н', добавляя две новые вершины на каждую петлю графа Н\* и одну новую вершину на каждое ребро из множества кратных ребер. Теперь 4-раскрашиваемость графа Н' означает 4-раскрашиваемость графа Н. Таким образом, эквивалентность обеих формулировок доказана.

Если будет доказана гипотеза четырех красок, то результат будет неулучшаем, поскольку легко привести примеры планарных 4-хроматических графов. Таковы графы К4 и W6, изображенные на рис. В каждом из этих графов не менее четырех треугольников, что является в силу теоремы Грюнбаума необходимым условием 4-хроматичности.

**Теорема (о пяти красках, Теорема Хивуда)**: Всякий связный планарный граф G можно правильно раскрасить не более чем 5-ю красками.

Доказательство: Индукцией по числу p вершин графа.  
Базис: Для графа с числом вершин p= k ≤ 5 Теорема очевидна, ибо всякие 5 вершин раскрашиваемы 5-ю различными красками.

Предположение индукции: Допустим, что любой связный планарный граф с числом вершин k < p 5-раскрашиваем. Шаг индукции: Покажем, что любой связный граф планарный граф с p вершинами 5-раскрашиваем. Т.к. граф G связен и планарен, то он имеет вершину v степени S ≤ 5. Удалим из G вершину V вместе с инцидентными ей ребрами. Полученный планарный граф G’=G-v имеет число вершин k < p и потому по предположении индукции все компоненты связности графа G’ можно раскрасить не более чем 5-ю цветами. Возможны следующие случаи: 1) степень вершины v не более 4. Пусть для определенности deg(v)=4. Смежные с v вершины v1, v2,…,v4 получат в G’ не более 4-х красок. Вершину v можно раскрасить любой из оставшейся красок.

2) Deg(v) = 5. Если смежные с v вершины v1, v2,…,v5 имеют в совокупности r ≤ 4 красок, то вершину v можно раскрасить в оставшийся цвет. Пусть теперь вершины v1, v2,…,v5окрашены в 5 цветов C1, C2,…,C5 соответственно. Натянем на вершины v1, v2,…,v5 из G подграф H, соединив v1, v2,…,v5 в H ребрами так, как они соединены в G. Подграф H – планарный ⇒ H не содержит K5, значит в H среди вершин v1, v2,…,v5 существуют две несмежные вершины, ибо если все вершины v1, v2,…,v5 смежны, то граф H содержит K5, чего нет. Пусть для определенности вершины v1,v2 не смежны. Склеим v1, v2 с вершиной v. Полученный связный граф по предположению индукции 5-раскрашиваем. При этом 4 вершины v, v3, v5 получат: r ≤ 4 краски.

Расклеим назад v1, v2, v. Вершины v1, v2 оставим их прежний цвет (как у v). Тогда вершины v1, v2,…,v5 [v1, v2 – одинаково раскрашены] имеют r ≤ 4 цвета. Вершину v перекрасим в один из оставшихся цветов. Шаг индукции установлен. Теорема доказана.

## Булева алгебра.

1. **Булевы функции. Интерпретация булевых функций. Замена переменных и суперпозиция. Существенные и фиктивные (несущественные)переменные.**

Пусть http://ok-t.ru/studopediaru/baza4/670615101478.files/image018.gif исходный алфавит переменных.

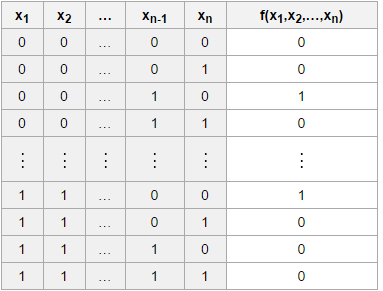
**Функцией алгебры логики** http://ok-t.ru/studopediaru/baza4/670615101478.files/image020.gif **от переменных** http://ok-t.ru/studopediaru/baza4/670615101478.files/image022.gif называется функция, принимающая значения 1, 0 и аргументы которой также принимают значения 1, 0.

Обычно функции алгебры логики называют булевыми функциями. Название «булевы функции» возникло в связи с использованием функций рассматриваемого типа в алгебре логики, начало которой было положено трудами ирландского ученого 19 века Дж. Буля. Областью определения булевой функции от n переменных служит совокупность всевозможных   
n-мерных упорядоченных наборов http://ok-t.ru/studopediaru/baza4/670615101478.files/image024.gif , где http://ok-t.ru/studopediaru/baza4/670615101478.files/image026.gif .

Следует отметить, что любой такой набор можно рассматривать как представление некоторого целого неотрицательного числа в двоичной системе счисления. Например, набору (0,1,0,1) соответствует число http://ok-t.ru/studopediaru/baza4/670615101478.files/image028.gif , а набору (1,1,1) – число http://ok-t.ru/studopediaru/baza4/670615101478.files/image030.gif .

Все наборы размерности n нумеруются целыми числами от 0,2n-1. Отсюда нетрудно заметить, что число таких наборов равно 2n.

Всякая булева функция от n переменных может быть задана с помощью таблицы истинности:



В алгебре логики особое значение имеют следующие булевы функции, которые называют элементарными булевыми функциями:

1) http://ok-t.ru/studopediaru/baza4/670615101478.files/image039.gif – константа 0;

2) http://ok-t.ru/studopediaru/baza4/670615101478.files/image041.gif – константа 1;

3) http://ok-t.ru/studopediaru/baza4/670615101478.files/image043.gif – тождественная функция;

4) http://ok-t.ru/studopediaru/baza4/670615101478.files/image045.gif – отрицание х;

5) http://ok-t.ru/studopediaru/baza4/670615101478.files/image047.gif – конъюнкция *x* и y;

6) http://ok-t.ru/studopediaru/baza4/670615101478.files/image049.gif – дизъюнкция х и у;

7) http://ok-t.ru/studopediaru/baza4/670615101478.files/image051.gif – импликация х и у;

8) http://ok-t.ru/studopediaru/baza4/670615101478.files/image053.gif – эквивалентность х и у;

9) http://ok-t.ru/studopediaru/baza4/670615101478.files/image055.gif – сложение х и у по mod2;

10) http://ok-t.ru/studopediaru/baza4/670615101478.files/image057.gif – функция Шеффера;

11) http://ok-t.ru/studopediaru/baza4/670615101478.files/image059.gif – стрелка Пирса.

Переменная *x*i в функции http://ok-t.ru/studopediaru/baza4/670615101478.files/image071.gif называется **фиктивной**, если http://ok-t.ru/studopediaru/baza4/670615101478.files/image073.gif = http://ok-t.ru/studopediaru/baza4/670615101478.files/image075.gif при любых значениях остальных переменных.

В этом случае функция http://ok-t.ru/studopediaru/baza4/670615101478.files/image020.gif , по существу, зависит от *(n-1)*– переменной, т.е. представляет собой функцию http://ok-t.ru/studopediaru/baza4/670615101478.files/image078.gif от *(n-1)* переменной. Говорят, что функция *g* получается из функции *f*удалением фиктивной переменной, а функция *f* получается из *g* введением фиктивной переменной, причем эти функции являются равными.

Благодаря введению фиктивных переменных любую булеву функцию от http://ok-t.ru/studopediaru/baza4/670615101478.files/image037.gif переменных можно считать функцией от любого большего числа переменных. Поэтому любую конечную совокупность булевых функций можно считать зависящими от одного и того же числа переменных. установить взаимно-однозначное соответствие между булевыми переменными и пропозициональными переменными,

* установить связь между булевыми функциями и логическими связками,
* оставить расстановку скобок без изменений.

|  |
| --- |
| **Суперпозиция (сложная функция)** — это функция, полученная из некоторого множества функций путем подстановки одной функции в другую или отождествления переменных. |

* Множество всех возможных не эквивалентных друг другу суперпозиций данного множества функций образует [замыкание](http://neerc.ifmo.ru/wiki/index.php?title=%D0%9F%D1%80%D0%B5%D0%B4%D1%81%D1%82%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5_%D1%84%D1%83%D0%BD%D0%BA%D1%86%D0%B8%D0%B8_%D1%84%D0%BE%D1%80%D0%BC%D1%83%D0%BB%D0%BE%D0%B9,_%D0%BF%D0%BE%D0%BB%D0%BD%D1%8B%D0%B5_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B_%D1%84%D1%83%D0%BD%D0%BA%D1%86%D0%B8%D0%B9) данного множества функций.

Рассмотрим две [булевы функции](http://neerc.ifmo.ru/wiki/index.php?title=%D0%9E%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5_%D0%B1%D1%83%D0%BB%D0%B5%D0%B2%D0%BE%D0%B9_%D1%84%D1%83%D0%BD%D0%BA%D1%86%D0%B8%D0%B8): функцию f от n аргументов f(x_{1}, x_{2}, ..., x_{n}) и функцию g от m аргументов g(y_{1}, y_{2}, ..., y_{m}).

Тогда мы можем получить новую функцию из имеющихся двумя способами:

1. Подстановкой одной функции в качестве некоторого аргумента для другой;
2. Отождествлением аргументов функций.

Пусть задана некоторая  БФ**f(x1, x2, …,xk, …,xn).**Переменная **xk**этой функции называется существенной, если найдётся набор ДВОИЧНЫХ значений   < **a1, a2, …,ak -1, ak +1,  …, an**  >  такой, что: **f(a1, a2, …,ak -1, 0, ak +1,  …, an**  **)** <>  **f(a1, a2, …,ak -1, 1, ak +1,  …, an**  **).**

1. **Формулы. Эквивалентность булевых формул. Основные эквивалентности. Реализация функций формулами.**

Как мы видели, геометрическое и табличное представления булевых функций подходят лишь для функций с небольшим числом аргументов. Формулы позволяют удобно представлять многие функции от большего числа аргументов и оперировать различными представлениями одной и той же функции.

Булева формула Φ называется тождественно истинной, если она истинна при любых значениях входящих в нее переменных, т.е. функция fΦ тождественно равна 1.

Две логические формулы называются **равносильными**, если при любых значениях входящих в них логических переменных эти формулы принимают одинаковые значения.

### Эквивалентность булевых формул

Булевы формулы Φ и Ψ называются **эквивалентными**, если соответствующие им функции fΦ и fΨ равны.

Обозначение: Φ equivΨ. Эквивалентные формулы называют также тождественно равными, а выражения вида Φ equivΨ **логическими тождествами**.

### Основные эквивалентности (тождества)

Таким образом, эквивалентные формулы являются различными заданиями одной и той же булевой функции. Ниже мы приводим ряд пар эквивалентных формул (тождеств), отражающих существенные свойства логических операций и важные соотношения между различными операциями. Они часто позволяют находить для булевых функций по одним задающим их формулам более простые формулы. Большинство из приводимых тождеств имеют собственные имена. Часто их называют законами логики.

Пусть ˆ - это одна из функций and, or, +. Для этих трех функций выполнены следующие две эквивалентности (законы ассоциативности и коммутативности).

1. Ассоциативность:

|  |  |
| --- | --- |
| ((X_1 \circ X_2) \circ X_3) \equiv (X_1 \circ(X_2 \circ X_3)) | (1) |

1. Коммутативность:

|  |  |
| --- | --- |
| (X_1 \circ X_2)  \equiv (X_2 \circ X_1 ) | (2) |

1. Дистрибутивные законы:

|  |  |
| --- | --- |
| \begin{array}{l}        ((X_1 \vee X_2) \wedge X_3) \equiv ((X_1 \wedge X_3)\vee (X_2 \wedge X_3))\\        ((X_1 \wedge X_2) \vee X_3) \equiv ((X_1 \vee X_3)\wedge (X_2 \vee X_3))\\        ((X_1 + X_2) \wedge X_3) \equiv ((X_1 \wedge X_3)+ (X_2 \wedge X_3))\end{array} | (3) |

1. Двойное отрицание:

|  |  |
| --- | --- |
| \neg (\neg X) \equiv X | (4) |

1. Законы де Моргана (внесение отрицания внутрь скобок):

|  |  |
| --- | --- |
| \begin{array}{c}        \neg (X_1 \vee X_2) \equiv (\neg X_1 \wedge \neg X_2)\\        \neg (X_1 \wedge X_2) \equiv (\neg X_1 \vee \neg X_2)        \end{array} | (5) |

1. Законы упрощения:

|  |  |
| --- | --- |
| \begin{array}{c}        (X \wedge X) \equiv X  \hspace{20mm}  (X \vee X) \equiv X \\        (X \wedge \neg X) \equiv 0  \hspace{20mm}  (X \vee \neg X) \equiv 1 \\        (X \wedge 0) \equiv 0  \hspace{20mm}  (X \vee 0) \equiv X \\        (X \wedge 1) \equiv X  \hspace{20mm}  (X \vee 1) \equiv 1        \end{array} | (6) |

Некоторые законы упрощения имеют собственные названия: эквивалентности в первой строке называются законами идемпотентности, (X \wedge \neg X) \equiv 0- это закон противоречия, (X \vee \neg X) \equiv 1- это закон исключенного третьего. Эквивалентности в двух последних строках иногда называют законами 0 и 1.

Следующие две эквивалентности позволяют выразить импликацию и сложение по модулю 2 через дизъюнкцию, конъюнкцию и отрицание.

|  |  |
| --- | --- |
| (X_1 \rightarrow X_2) \equiv (\neg X_1 \vee X_2) | (7) |
| (X_1 + X_2) \equiv (( X_1 \wedge \neg X_2)\vee (\neg X_1\wedge X_2)) | | | (8) |
|  |  |  |  |

Из определения эквивалентности формул непосредственно следует **Принцип замены эквивалентных подформул:**

пусть формула alphaявляется подформулой формулы Φ, формула alpha' эквивалентна alphaи формула Φ' получена из Φ посредством замены некоторого вхождения alphaна alpha'. Тогда Φ' эквивалентна Φ, т.е. Φ' equivΦ.

Применяя этот принцип и используя основные тождества, можно находить для заданной формулы другие эквивалентные ей формулы. Часто это может приводить к существенному упрощению исходной формулы. Например, если в формуле ((X and0)or Y) заменим на основании тождеств (6) подформулу (X and0) на 0, то получим эквивалентную формулу (0 orY). По закону коммутативности(2) эта формула эквивалентна формуле (Y or0), которая, в свою очередь, по одному из тождеств группы (6) эквивалентна формуле Y. Эту цепочку эквивалентных преобразований можно записать также следующим образом:

((X \wedge 0)\vee Y) \underset{(6)}{\equiv}(0 \vee Y)\underset{(2)}{\equiv}(Y \vee 0)\underset{(6)}{\equiv} Y

В этой цепочке вспомогательные номера под знаками эквивалентности указывают, с помощью какой группы основных тождеств эта эквивалентность получается.

Выведем еще несколько важных логических тождеств, позволяющих проводить упрощения сложных формул. Их называют законами поглощения.

|  |  |
| --- | --- |
| X \vee (X \wedge \Phi){\equiv}X |  |

Действительно,

        X \vee (X \wedge \Phi) \underset{(6)}{\equiv} (X \wedge 1) \vee(X \wedge \Phi)        \underset{(3)}{\equiv} X \wedge (1 \vee \Phi) \underset{(2,6)}{\equiv} X \wedge 1 \underset{(6)}{\equiv}X      

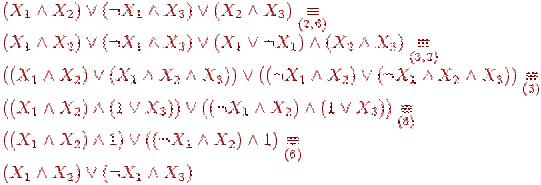
|  |  |
| --- | --- |
| (X \wedge \Phi) \vee (\neg X \wedge \Phi) {\equiv} \Phi |  |

Действительно,

        (X \wedge \Phi) \vee (\neg X \wedge \Phi) \underset{(3)}{\equiv}        (X \vee \neg X) \wedge \Phi \underset{(6)}{\equiv} 1 \wedge \Phi        \underset{(6)}{\equiv} \Phi

|  |  |
| --- | --- |
| (X_1 \wedge  X_2) \vee (\neg X_1 \wedge X_3) \vee ( X_2        \wedge  X_3) {\equiv} (X_1 \wedge X_2) \vee (\neg X_1 \wedge X_3) |  |

Действительно,



1. **Алгебра булевых функций (алгебра Буля). Функциональная полнота булевых функций.**

**Булевой алгеброй**[[1]](https://ru.wikipedia.org/wiki/%D0%91%D1%83%D0%BB%D0%B5%D0%B2%D0%B0_%D0%B0%D0%BB%D0%B3%D0%B5%D0%B1%D1%80%D0%B0#cite_note-1)[[2]](https://ru.wikipedia.org/wiki/%D0%91%D1%83%D0%BB%D0%B5%D0%B2%D0%B0_%D0%B0%D0%BB%D0%B3%D0%B5%D0%B1%D1%80%D0%B0#cite_note-2)[[3]](https://ru.wikipedia.org/wiki/%D0%91%D1%83%D0%BB%D0%B5%D0%B2%D0%B0_%D0%B0%D0%BB%D0%B3%D0%B5%D0%B1%D1%80%D0%B0#cite_note-3) называется непустое [множество](https://ru.wikipedia.org/wiki/%D0%9C%D0%BD%D0%BE%D0%B6%D0%B5%D1%81%D1%82%D0%B2%D0%BE) *A* с двумя [бинарными операциями](https://ru.wikipedia.org/wiki/%D0%91%D0%B8%D0%BD%D0%B0%D1%80%D0%BD%D0%B0%D1%8F_%D0%BE%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D1%8F) \land (аналог [конъюнкции](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BD%D1%8A%D1%8E%D0%BD%D0%BA%D1%86%D0%B8%D1%8F)), \lor (аналог [дизъюнкции](https://ru.wikipedia.org/wiki/%D0%94%D0%B8%D0%B7%D1%8A%D1%8E%D0%BD%D0%BA%D1%86%D0%B8%D1%8F)), [унарной операцией](https://ru.wikipedia.org/wiki/%D0%A3%D0%BD%D0%B0%D1%80%D0%BD%D0%B0%D1%8F_%D0%BE%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D1%8F) \lnot(аналог [отрицания](https://ru.wikipedia.org/wiki/%D0%9E%D1%82%D1%80%D0%B8%D1%86%D0%B0%D0%BD%D0%B8%D0%B5)) и двумя выделенными элементами: 0 (или Ложь) и 1 (или Истина) такими, что для всех *a*, *b* и *c* из множества *A* верны следующие [аксиомы](https://ru.wikipedia.org/wiki/%D0%90%D0%BA%D1%81%D0%B8%D0%BE%D0%BC%D0%B0):

|  |  |  |
| --- | --- | --- |
| a \lor (b \lor c) = (a \lor b) \lor c | a \land (b \land c) = (a \land b) \land c | [ассоциативность](https://ru.wikipedia.org/wiki/%D0%90%D1%81%D1%81%D0%BE%D1%86%D0%B8%D0%B0%D1%82%D0%B8%D0%B2%D0%BD%D0%BE%D1%81%D1%82%D1%8C_(%D0%BC%D0%B0%D1%82%D0%B5%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0)) |
| a \lor b = b \lor a | a \land b = b \land a | [коммутативность](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BC%D1%83%D1%82%D0%B0%D1%82%D0%B8%D0%B2%D0%BD%D0%BE%D1%81%D1%82%D1%8C) |
| a \lor (a \land b) = a | a \land (a \lor b) = a | законы поглощения |
| a \lor (b \land c) = (a \lor b) \land (a \lor c) | a \land (b \lor c) = (a \land b) \lor (a \land c) | [дистрибутивность](https://ru.wikipedia.org/wiki/%D0%94%D0%B8%D1%81%D1%82%D1%80%D0%B8%D0%B1%D1%83%D1%82%D0%B8%D0%B2%D0%BD%D0%BE%D1%81%D1%82%D1%8C) |
| a \lor \lnot a = 1 | a \land \lnot a = 0 | дополнительность |

**Функциональная полнота** множества [логических операций](https://ru.wikipedia.org/wiki/%D0%9B%D0%BE%D0%B3%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D0%BE%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D1%8F) или [булевых функций](https://ru.wikipedia.org/wiki/%D0%91%D1%83%D0%BB%D0%B5%D0%B2%D0%B0_%D1%84%D1%83%D0%BD%D0%BA%D1%86%D0%B8%D1%8F) — это возможность выразить все возможные значения таблиц истинности с помощью формул из элементов этого множества. [Математическая логика](https://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D1%82%D0%B5%D0%BC%D0%B0%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D0%BB%D0%BE%D0%B3%D0%B8%D0%BA%D0%B0) обычно использует такой набор операций: [конъюнкция](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BD%D1%8A%D1%8E%D0%BD%D0%BA%D1%86%D0%B8%D1%8F) (\land), [дизъюнкция](https://ru.wikipedia.org/wiki/%D0%94%D0%B8%D0%B7%D1%8A%D1%8E%D0%BD%D0%BA%D1%86%D0%B8%D1%8F) (\lor), [отрицание](https://ru.wikipedia.org/wiki/%D0%9E%D1%82%D1%80%D0%B8%D1%86%D0%B0%D0%BD%D0%B8%D0%B5) (\neg), [импликация](https://ru.wikipedia.org/wiki/%D0%98%D0%BC%D0%BF%D0%BB%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F) (\to) и [эквиваленция](https://ru.wikipedia.org/wiki/%D0%AD%D0%BA%D0%B2%D0%B8%D0%B2%D0%B0%D0%BB%D0%B5%D0%BD%D1%86%D0%B8%D1%8F" \o "Эквиваленция) (\leftrightarrow).

Критерий Поста описывает необходимые и достаточные условия функциональной полноты множеств булевых функций. Был сформулирован американским математиком [Эмилем Постом](https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D1%81%D1%82,_%D0%AD%D0%BC%D0%B8%D0%BB%D1%8C_%D0%9B%D0%B5%D0%BE%D0%BD) в [1941 году](https://ru.wikipedia.org/wiki/1941_%D0%B3%D0%BE%D0%B4).

**Критерий:**

Множество булевых функций является функционально полным [тогда и только тогда](https://ru.wikipedia.org/wiki/%D0%A2%D0%BE%D0%B3%D0%B4%D0%B0_%D0%B8_%D1%82%D0%BE%D0%BB%D1%8C%D0%BA%D0%BE_%D1%82%D0%BE%D0%B3%D0%B4%D0%B0), когда оно не содержится полностью ни в одном из [предполных классов](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%B5%D0%B4%D0%BF%D0%BE%D0%BB%D0%BD%D1%8B%D0%B5_%D0%BA%D0%BB%D0%B0%D1%81%D1%81%D1%8B" \o "Предполные классы).

1. **Нормальные формы булевых функций: ДНФ, КНФ. СДНФ и СКНФ. Приведение с СДНФ.**

**Канонические формы логических формул**

Всякая логическая формула определяет некоторую булевую функцию. С другой стороны, для всякой булевой функции можно записать бесконечно много формул, ее представляющих. Одна из основных задач алгебры логики — нахождение **канонически**х форм (т. е. формул, построенных по определенному правилу, канону), а также наиболее простых формул, представляющих булевы функции.

Если логическая функция выражена через дизъюнкцию, конъюнкцию и отрицание переменных, то такая форма представления называется **нормальной**. Среди нормальных форм выделяют такие, в которых функции записываются единственным образом. Их называют **совершенными**.

Особую роль в алгебре логики играют классы дизъюнктивных и конъюнктивных совершенных нормальных форм. В их основе лежат понятия элементарной дизъюнкции и элементарной конъюнкции.

Формулу называют **элементарной конъюнкцией**, если она является конъюнкцией одной или нескольких переменных, взятых с отрицанием или без отрицания. Одну переменную или ее отрицание считают **одночленной элементарной конъюнкцией**.

Формула называется **элементарной дизъюнкцией**, если она является дизъюнкцией (быть может, одночленной) переменных и отрицаний переменных.

**ДНФ И СДНФ**

Формула называется **дизъюнктивной нормальной формой**(ДНФ), если она является дизъюнкцией неповторяющихся элементарных конъюнкций. ДНФ записываются в виде: **А1 v А2 v ... v Аn** , где каждое **Аn**— элементарная конъюнкция.

Формула **А**от **k**переменных называется **совершенной дизъюнктивной нормальной формой** (СДНФ), если:   
1.А является ДНФ, в которой каждая элементарная конъюнкция есть конъюнкция **k** переменных **х1, х2, …, xk**, причем на i-м месте этой конъюнкции стоит либо переменная **хi**либо ее отрицание;   
2. Все элементарные конъюнкции в такой ДНФ попарно различны.

**Например:**А = х1 & НЕ х2 v х1 & х2

Совершенная дизъюнктивная нормальная форма представляет собой формулу, построенную по строго определенным правилам с точностью до порядка следования элементарных конъюнкций (дизъюнктивных членов) в ней.

Она является примером однозначного представления булевой функции в виде формульной (алгебраической) записи.

**Теорема о СДНФ**  
Пусть **f(x1 х2, …, хn)** – булева функция от **n** переменных, не равная тождественно нулю. Тогда существует совершенная дизъюнктивная нормальная форма, выражающая функцию f.

**Алгоритм построения СДНФ по таблице истинности:**

1.В таблице истинности отмечаем наборы переменных, на которых значение функции f = 1.   
2.Записываем для каждого отмеченного набора конъюнкцию всех переменных следующим образом: если значение некоторой переменной в этом наборе равно 1, то в конъюнкцию включаем саму переменную, в противном случае – ее отрицание.   
3.Все полученные конъюнкции связываем операциями дизъюнкции.

**КНФ И СКНФ**  
 Формула называется **конъюнктивной нормальной формой** (КНФ), если она является конъюнкцией неповторяющихся элементарных дизъюнкций. КНФ записываются в виде: **А1 & А2 & ... & Аn** , где каждое **Аn**– элементарная дизъюнкция.

Формула **А** от **k** переменных называется **совершенной конъюнктивной нормальной формой** (СКНФ), если:   
1. А является КНФ, в которой каждая элементарная дизъюнкция есть дизъюнкция **k** переменных **x1, х2, …, хk,** причем на i-м месте этой дизъюнкции стоит либо переменная xi, либо ее отрицание;   
2. Все элементарные дизъюнкции в такой КНФ попарно различны.

**Например:**А = (х1 v НЕ х2) & (х1 v х2)

**Теорема о СКНФ**

Пусть**f(x1 х2, …, хn)** – булева функция от **n** переменных, не равная тождественно нулю. Тогда существует совершенная конъюнктивная нормальная форма, выражающая функцию f.

**Алгоритм построения СКНФ по таблице истинности:**

1.В таблице истинности отмечаем наборы переменных, на которых значение функции f = 0.

2.Записываем для каждого отмеченного набора дизъюнкцию всех переменных следующим образом: если значение некоторой переменной в этом наборе равно 0, то в дизъюнкцию включаем саму переменную, в противном случае – ее отрицание.

3.Все полученные дизъюнкции связываем операциями конъюнкции.

*Из алгоритмов построения СДНФ и СКНФ следует, что если на большей части наборов значений переменных функция равна 0, то для получения ее формулы проще построить СДНФ, в противном случае – СКНФ.*

# Алгебраические структуры.

1. **Алгебраические операции (*n*-арная). Ранг операции.**

Пусть А – непустое множество.

Отображение множества Аn в А называется n**-арной (n-местной) алгебраической операцией** на множестве А, а число n (n ≥ 1) – рангом операции. Выделение (фиксация) некоторого элемента множества А называется нульарной (нульместной) операцией на множестве А, число 0 – рангом нульарной операции. Определение 4.3. Частичная функция из множества Аn в А называется частичной n-арной алгебраической операцией на множестве А.

Пусть http://www.vevivi.ru/best/images/servus/85/26/5622685.png. Отображение http://www.vevivi.ru/best/images/servus/86/26/5622686.png назы­вается http://www.vevivi.ru/best/images/servus/87/26/5622687.png- местной операцией на множестве http://www.vevivi.ru/best/images/servus/76/26/5622676.png. Число http://www.vevivi.ru/best/images/servus/87/26/5622687.png- **ранг опера­ции.**

1. **Бинарные алгебраические операции (БАО): нейтральный и симметричный элементы. Аддитивная и мультипликативная форма записи БАО.**

Отображение множества А×А в А называется **бинарной алгебраической операцией** на множестве А. Примерами бинарных алгебраических операций являются обычное сложение и умножение на множестве целых чисел, объединение и пересечение на булеане непустого множества.

Нейтральные элементы

Пусть \*– бинарная алгебраическая операция на непустом множестве А.

Элемент е \* А называется **нейтральным** относительно операции ∗, если (∀a ∈ А) a \* e = e \* a = a.

**Теорема**. Если нейтральный элемент относительно операции ∗ существует, то он единственен. Доказательство. Пусть e и e′ – нейтральные элементы относительно операции \*. Тогда e = e \* e′ = e′, то есть e = e′.

Симметричные элементы

Пусть ∗ есть бинарная алгебраическая операция на непустом множестве А и элемент е ∈ А – нейтральный элемент относительно ∗.

Элемент а ′ ∈ А называется **симметричным** к элементу а ∈ А относительно операции ∗, если а ∗ a' = a ′∗ a = е. В этом случае элемент а называется симметризуемым, а элементы а и а ′ – **взаимно симметричными**.

**Аддитивная и мультипликативная форма записи бинарной алгебраической операции**

Для обозначения бинарной алгебраической операции ∗ наиболее часто используются аддитивная и мультипликативная формы записи. При **аддитивной** форме записи операцию ∗ называют сложением, а ее результат a ∗ b – суммой а и b. При этом вместо a ∗ b пишут а + b. Нейтральный элемент относительно сложения называют нулевым элементом (или нулем) и обозначают символом 0. Элемент, симметричный к элементу а, называют противоположным к элементу а и обозначают через –а.

При **мультипликативной** форме записи операцию ∗ называют умножением, а ее результат а ∗ b – произведением а и b. При этом вместо а ∗ b пишут a ⋅ b. Нейтральный элемент относительно умножения называют единичным элементом (или единицей) и обозначают символом 1. Элемент, симметричный к элементу а, называют обратным к элементу а и обозначают через а-1.

1. **Алгебраическая структура (универсальная алгебра, алгебра). Основа (носитель, основное, несущее множество) алгебры. Тип и сигнатура алгебры.**

**Алгебраической структурой** (универсальной алгеброй или просто алгеброй) называется упорядоченная пара А АА А = < A, Σ >, где A – непустое множество и Σ – множество алгебраических операций на A. Таким образом, алгебра представляет собой непустое множество A вместе с заданной на нем совокупностью операций Σ = {f1, …, fm, …}, где fi: i nA → A и ni – ранг операции fi.

Множество A называется основным (несущим) множеством или **основой (носителем) алгебры**.

Упорядоченная последовательность рангов (n1,…, nm) называется **типом алгебры**;

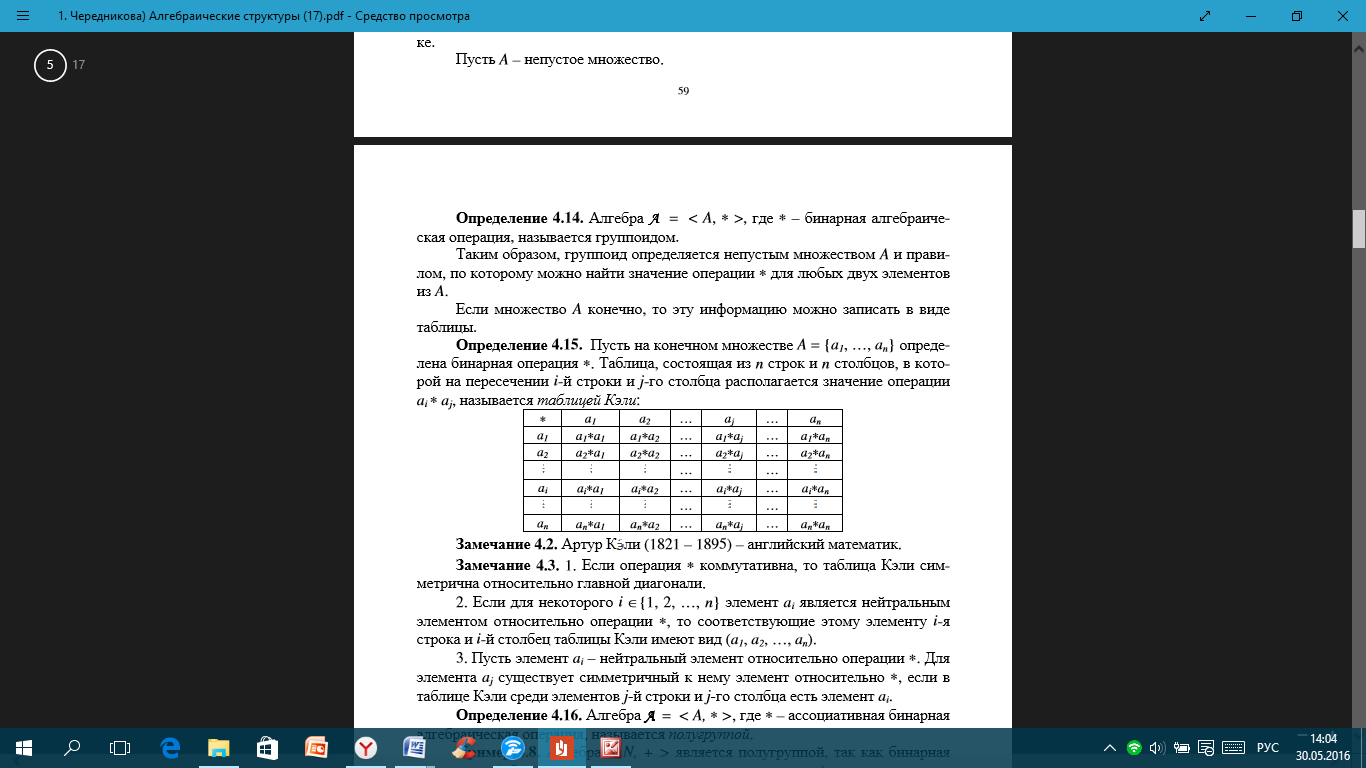
Множество операций Σ ΣΣ Σ называется **сигнатурой алгебры**. Если < A, Σ > – алгебра, то также говорят, что множество A есть алгебра относительно операций Σ.

Наиболее частым является случай, когда сигнатура конечна. Если Σ = {f1, …, fm}, то вместо записи А АА А = < A, {f1, …, fm }> обычно употребляется запись А АА А = < A, f1, …, fm >.

1. **Алгебры с одной бинарной операцией: группоид. Таблица Кэли.**

АА А = < A, ∗ >, где ∗ – бинарная алгебраическая операция, называется **группоидом.** Таким образом, группоид определяется непустым множеством A и правилом, по которому можно найти значение операции ∗ для любых двух элементов из A. Если множество A конечно, то эту информацию можно записать в виде таблицы.

Пусть на конечном множестве A = {a1, …, an} определена бинарная операция ∗. Таблица, состоящая из n строк и n столбцов, в которой на пересечении i-й строки и j-го столбца располагается значение операции ai ∗ aj, называется **таблицей Кэли**:



1. Если операция ∗ коммутативна, то таблица Кэли симметрична относительно главной диагонали. 2. Если для некоторого i ∈{1, 2, …, n} элемент ai является нейтральным элементом относительно операции ∗, то соответствующие этому элементу i-я строка и i-й столбец таблицы Кэли имеют вид (a1, a2, …, an). 3. Пусть элемент ai – нейтральный элемент относительно операции ∗. Для элемента aj существует симметричный к нему элемент относительно ∗, если в таблице Кэли среди элементов j-й строки и j-го столбца есть элемент ai.

1. **Полугруппа. Моноид. Группа. Конечная группа. Порядок группы.**

Алгебра А АА А = < A, ∗ >, где ∗ – ассоциативная бинарная алгебраическая операция, называется **полугруппой**.

Алгебра А АА А = < A, ∗ >, в которой ∗ является ассоциативной бинарной алгебраической операцией и существует нейтральный элемент e относительно ∗, называется **моноидом**. Другими словами, моноидом является полугруппа с нейтральным элементом

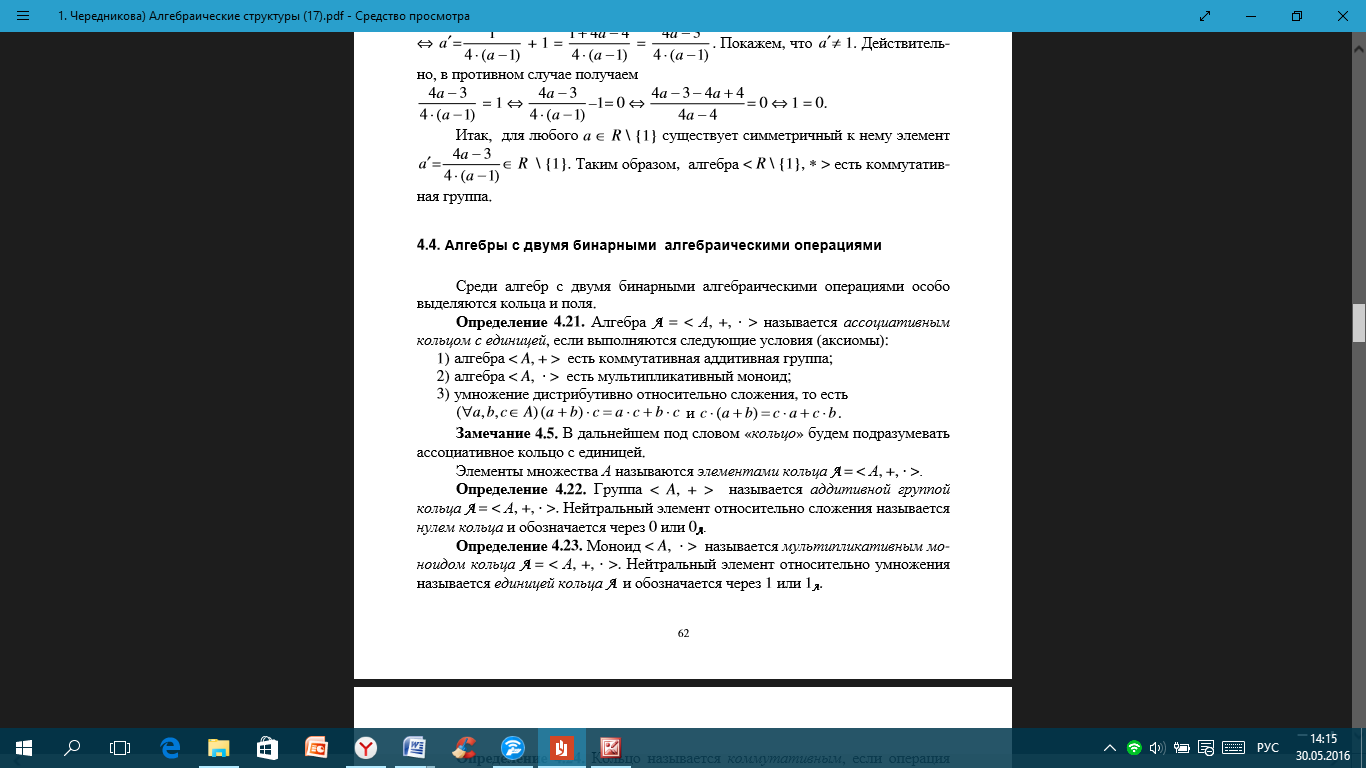
Алгебра А АА А = < А, > называется **группой,** если выполняются условия (аксиомы): 1) ∗ – ассоциативная бинарная операция; 2) существует нейтральный элемент относительно ∗; 3) для каждого элемента a ∈ А существует симметричный к нему элемент a ′ ∈ А относительно операции ∗. Таким образом, **группа – это моноид, в котором каждый элемент симметризуем.**

Полугруппа, моноид или группа называется **коммутативной (коммутативным) или абелевой (абелевым),** если бинарная алгебраическая операция коммутативна.

Если носитель группы имеет конечную мощность, то группа называется **конечной**, а мощность ее носителя – **порядком группы**. В противном случае группа называется бесконечной.

1. **Алгебры с двумя алгебраическими операциями: кольцо, поле.**

Среди алгебр с двумя бинарными алгебраическими операциями особо выделяются кольца и поля.

Алгебра А АА А = < А, +, · > **называется ассоциативным кольцом с единицей**, если выполняются следующие условия (аксиомы): 1) алгебра < A, + > есть коммутативная аддитивная группа; 2) алгебра < A, · > есть мультипликативный моноид; 3) умножение дистрибутивно относительно сложения, то есть 

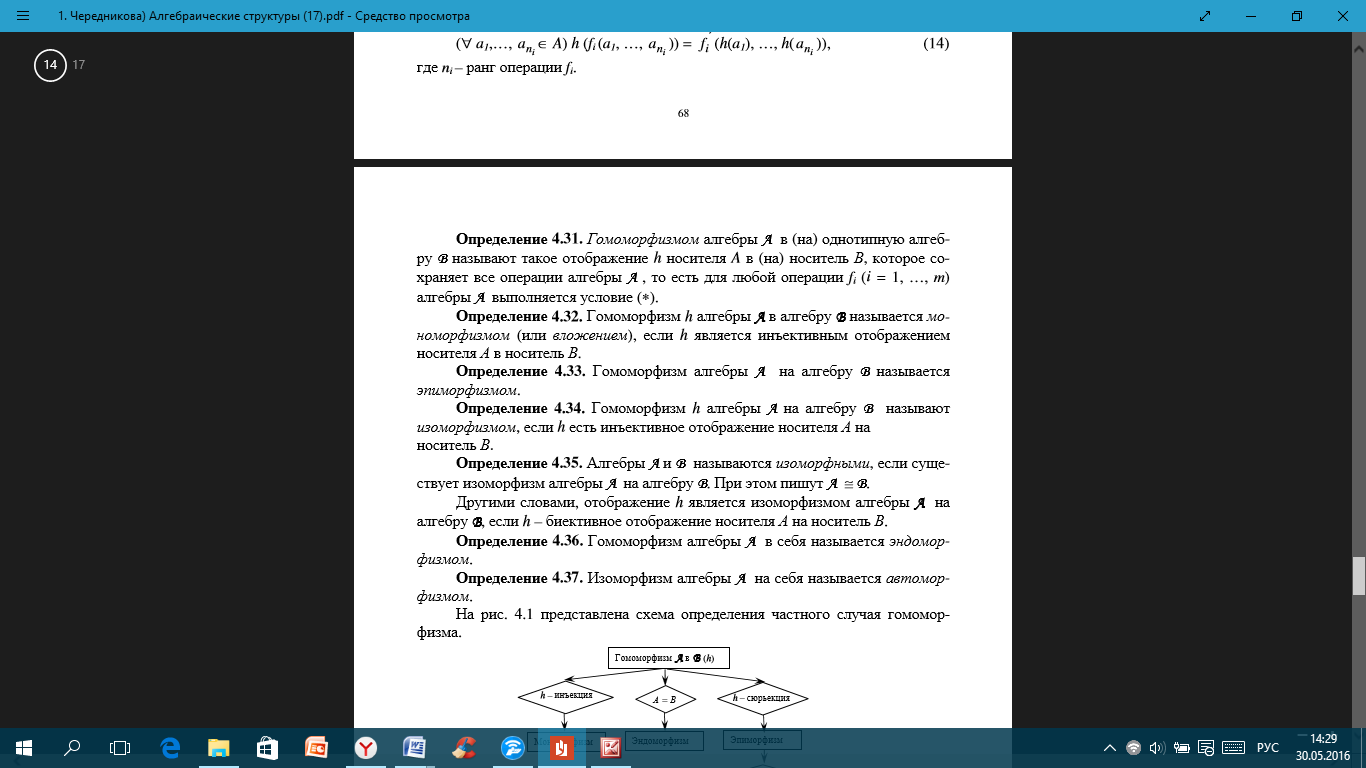
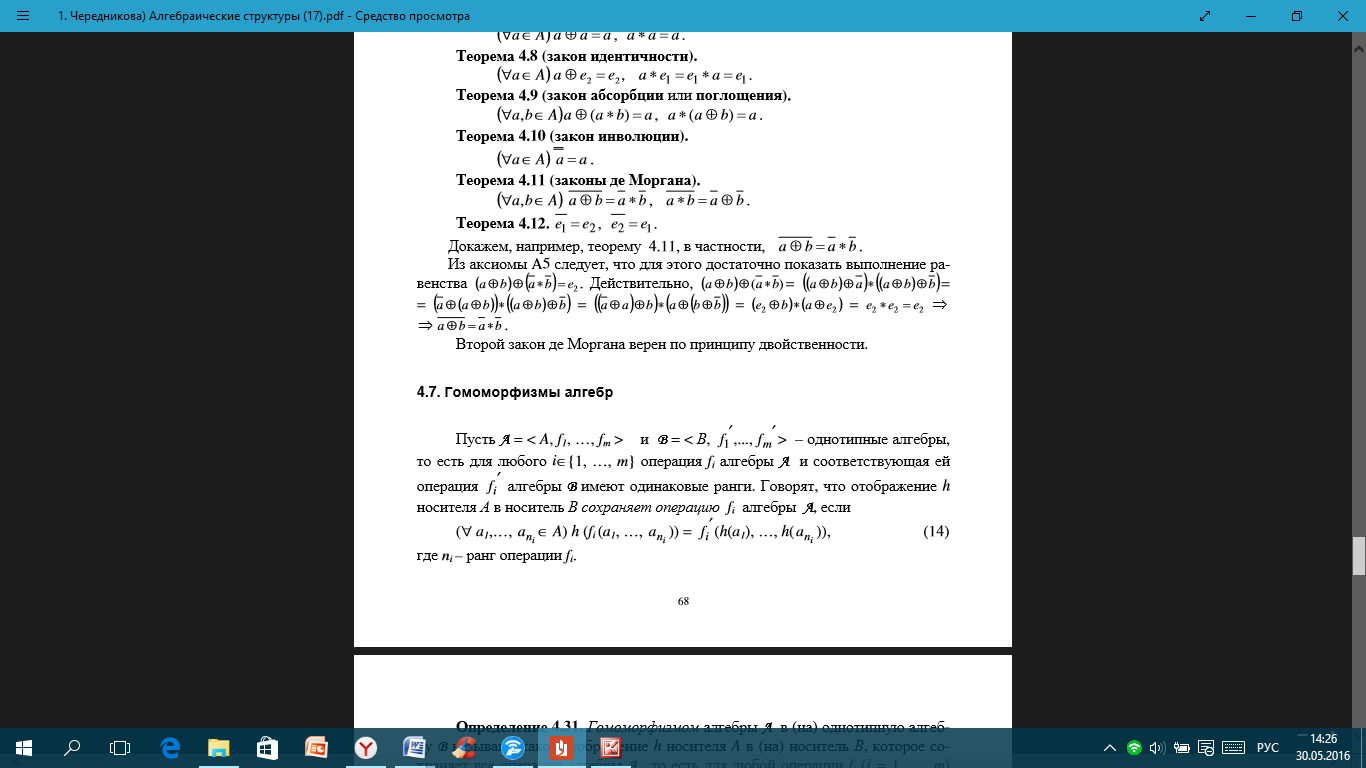
Элементы множества А называются элементами кольца А АА А = < А, +, · >.

**Полем** называется коммутативное кольцо, в котором нуль кольца отличен от единицы кольца и для каждого ненулевого элемента существует обратный к нему относительно операции умножения.

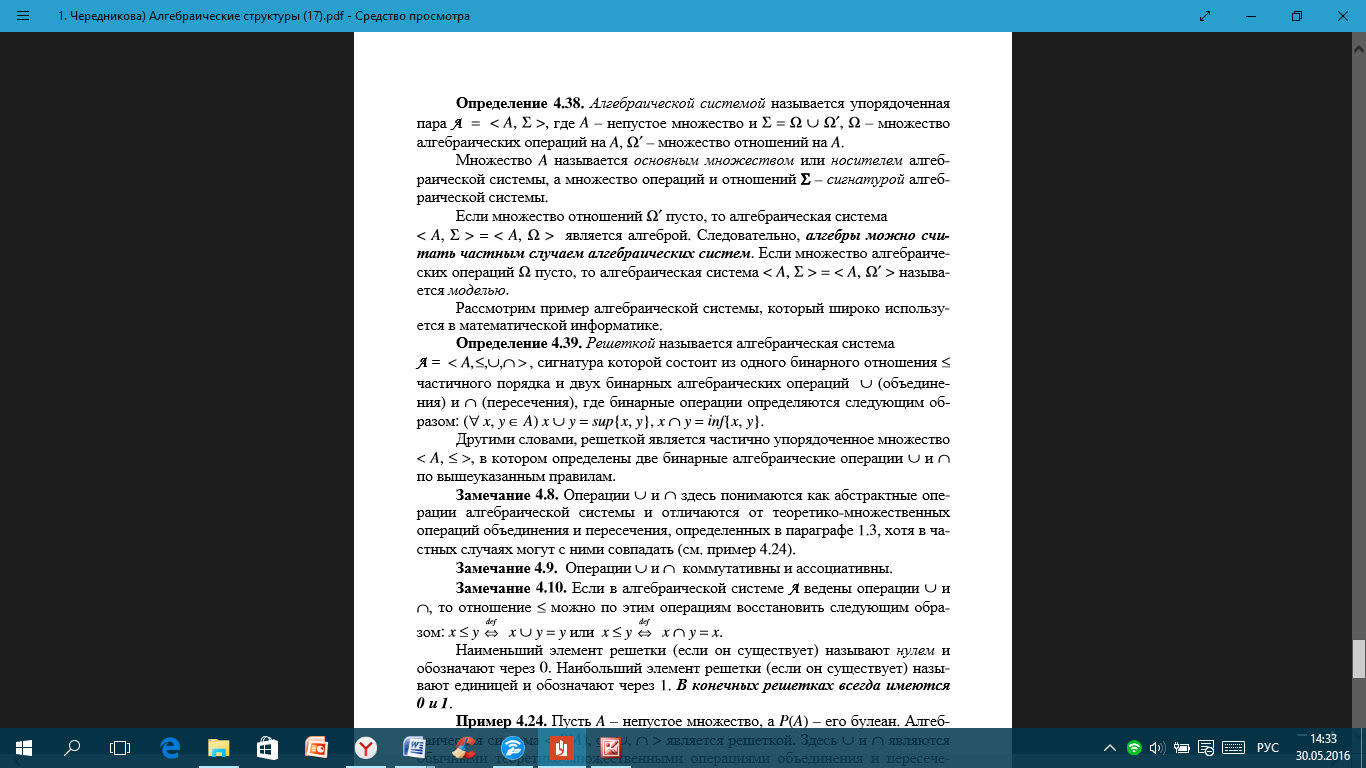
Кольцо целых чисел < Z, +, · > полем не является, так как ни один ненулевой элемент, кроме 1, не обладает обратным к нему.

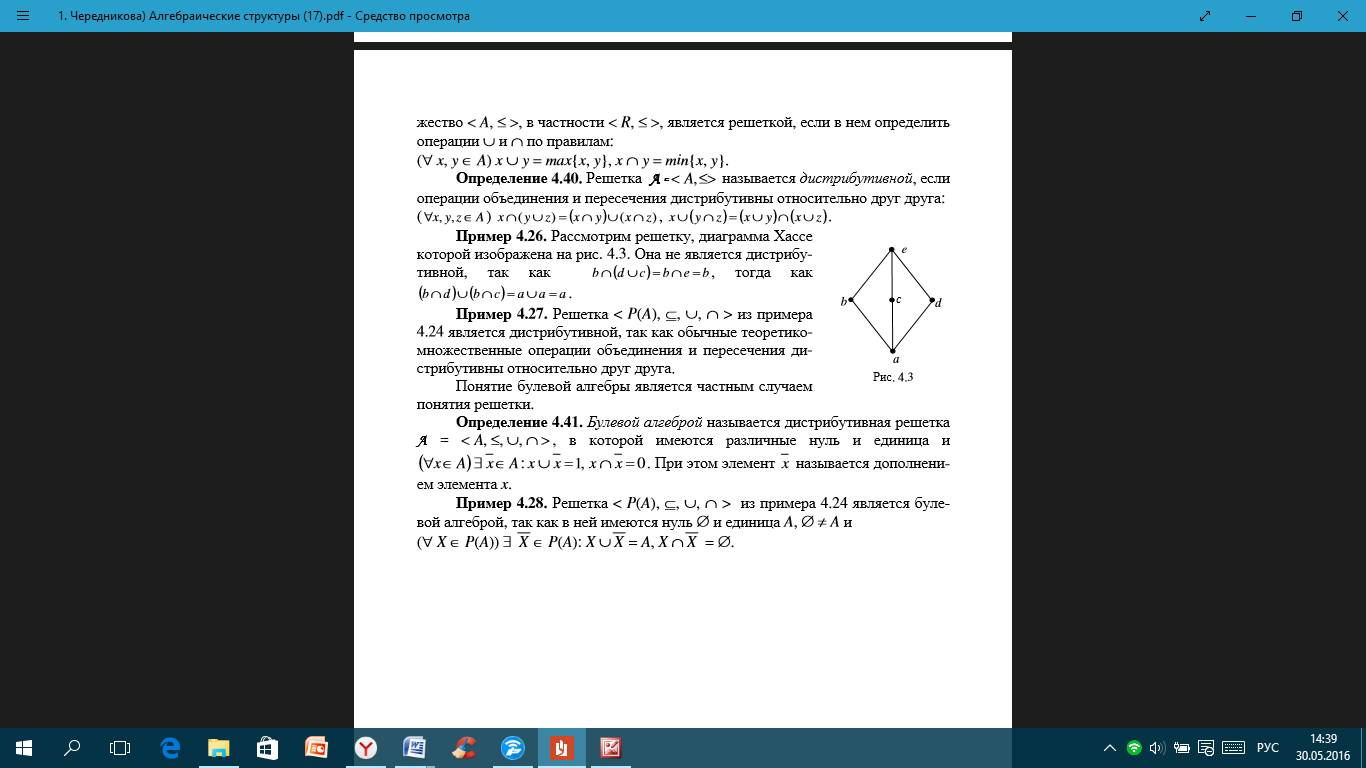
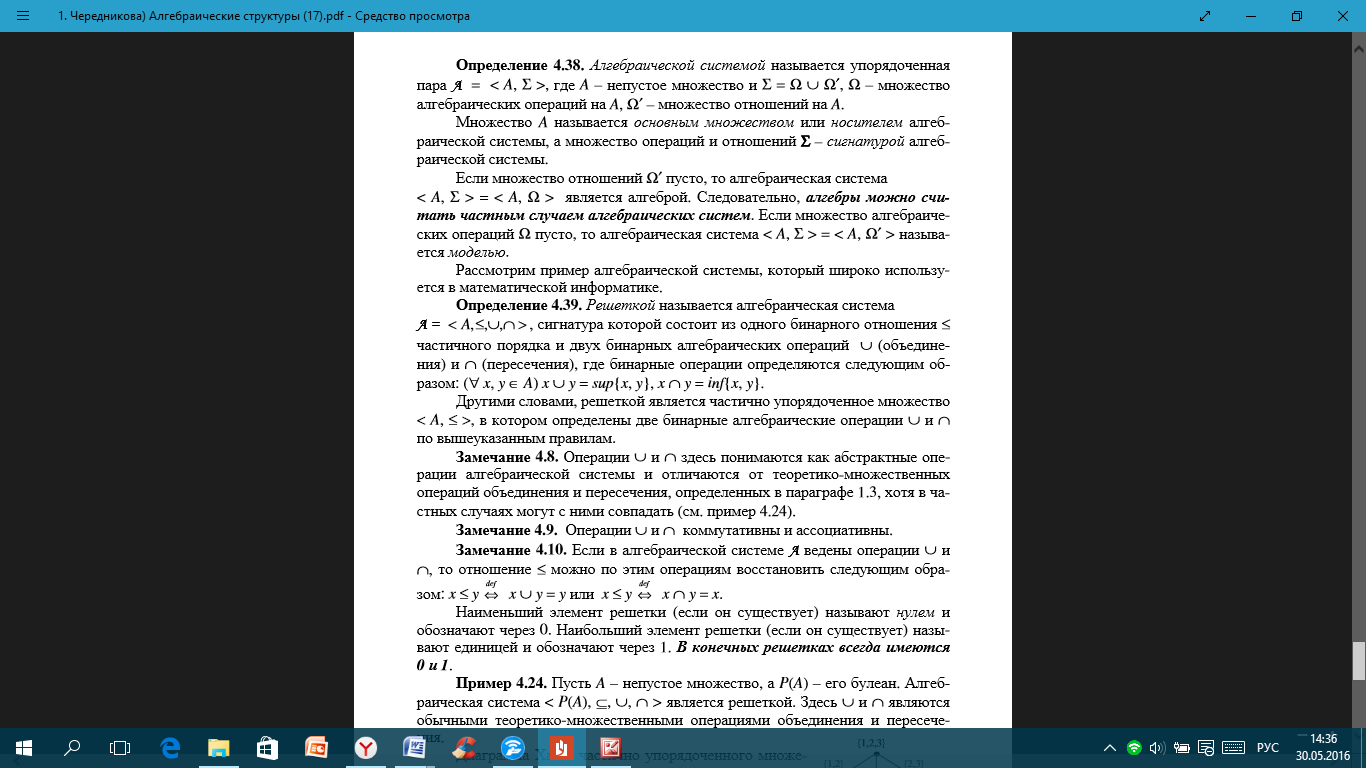
Множества Q, R и С образуют **бесконечные поля** относительно обычных операций сложения и умножения, которые соответственно называются полем рациональных чисел, полем действительных чисел и полем комплексных чисел.

1. **\*Гомоморфизмы алгебр. Мономорфизм (вложение).Изоморфизм. Изоморфные алгебры. Эндоморфизм. Автоморфизм.**

.

1. **\*Алгебраические системы. Модель.**



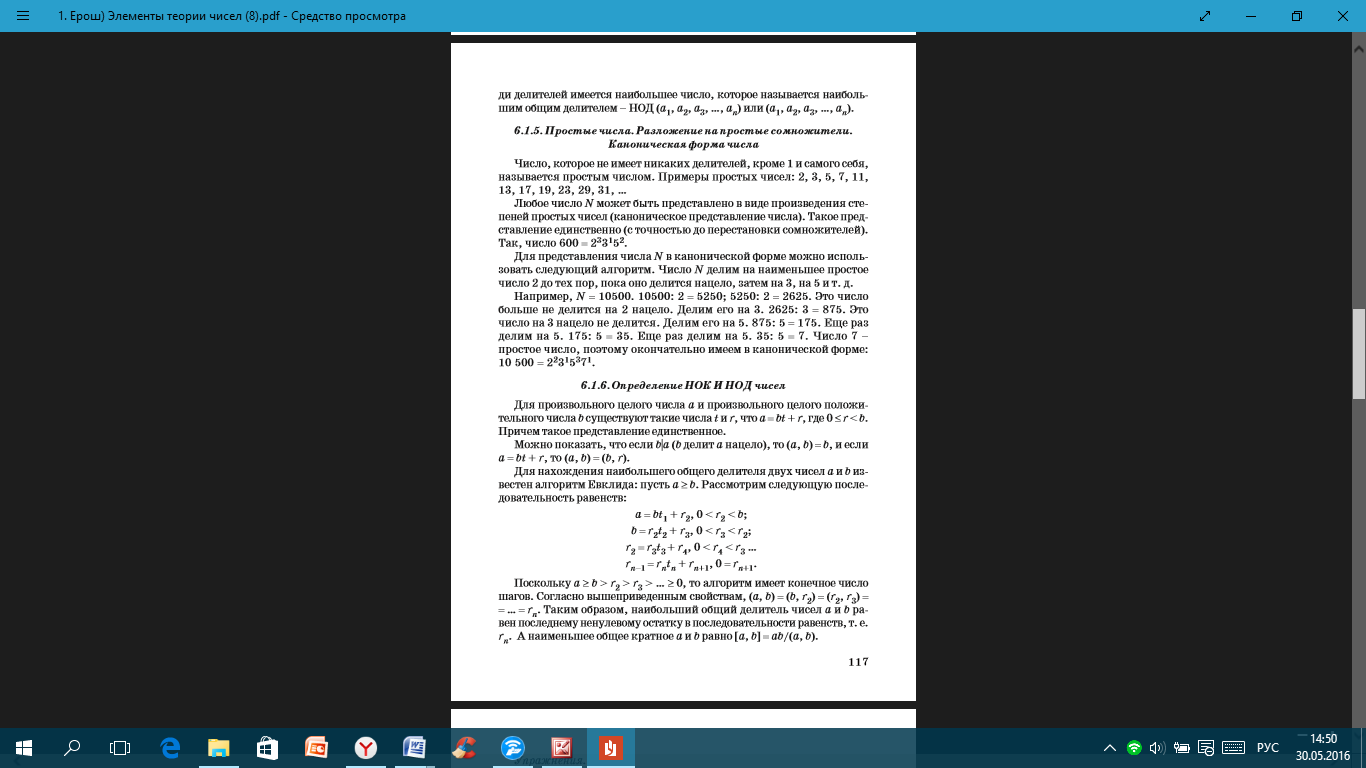
1. **\*Решетка. Нуль и единица решетки. Дистрибутивная решетка.**

# Элементы теории чисел.

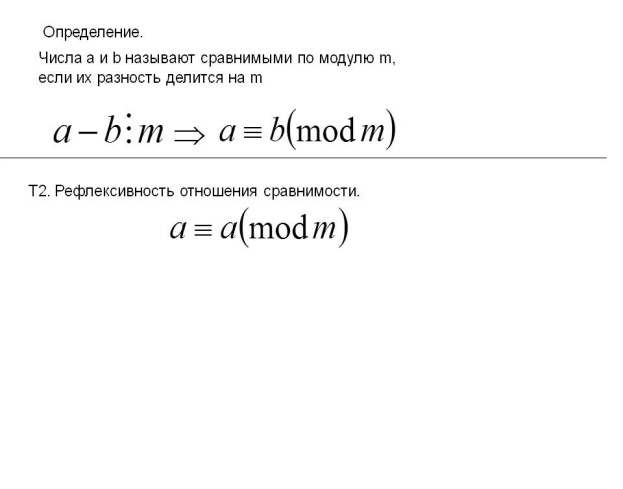
1. **НОК, НОД. Алгоритм Евклида нахождения НОД.**

Пусть имеется n целых чисел: a1, a2, a3, …, an. **Общим кратным** этих чисел называется целое число, которое делится нацело на каждое из этих чисел. Наименьшее из этих общих кратных называется наименьшим общим кратным чисел a1, a2, a3, …, an и обозначается **НОК** (a1, a2, a3, …, an) или [a1, a2, a3, …, an].

Пусть имеется n целых чисел a1, a2, a3, …, an. Общим делителем этих чисел называется число, которое нацело делит каждое их этих чисел. Среди делителей имеется наибольшее число, которое называется наибольшим общим делителем – **НОД** (a1, a2, a3, …, an) или (a1, a2, a3, …, an).



1. **Сравнимость чисел по модулю. Классы вычетов.**

**** Множество всех чисел, сравнимых с a по модулю m, называется **классом вычетов a по модулю m**, и обычно обозначается [a]_m или \bar a_m. Таким образом, сравнение a\equiv b\pmod{m} равносильно равенству классов вычетов [a]_m=[b]_m[[10]](https://ru.wikipedia.org/wiki/%D0%A1%D1%80%D0%B0%D0%B2%D0%BD%D0%B5%D0%BD%D0%B8%D0%B5_%D0%BF%D0%BE_%D0%BC%D0%BE%D0%B4%D1%83%D0%BB%D1%8E#cite_note-10).

Любое число класса называется *вычетом* по модулю m. Пусть для определенности r―[остаток от деления](https://ru.wikipedia.org/wiki/%D0%94%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5_%D1%81_%D0%BE%D1%81%D1%82%D0%B0%D1%82%D0%BA%D0%BE%D0%BC) любого из представителей выбранного класса на m, тогда любое число q из этого класса можно представить в виде q = mt + r, где t —[целое](https://ru.wikipedia.org/wiki/%D0%A6%D0%B5%D0%BB%D0%BE%D0%B5_%D1%87%D0%B8%D1%81%D0%BB%D0%BE). Вычет равный [остатку](https://ru.wikipedia.org/wiki/%D0%94%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5_%D1%81_%D0%BE%D1%81%D1%82%D0%B0%D1%82%D0%BA%D0%BE%D0%BC) r называется *наименьшим неотрицательным вычетом*, а вычет \rho, самый малый по абсолютной величине, называется *абсолютно наименьшим вычетом*.При r < \frac {m}{2}\ \rho=r, в противном случае \rho = r - m. Если m-[чётное](https://ru.wikipedia.org/wiki/%D0%A7%D1%91%D1%82%D0%BD%D1%8B%D0%B5_%D0%B8_%D0%BD%D0%B5%D1%87%D1%91%D1%82%D0%BD%D1%8B%D0%B5_%D1%87%D0%B8%D1%81%D0%BB%D0%B0" \o "Чётные и нечётные числа)и r = \frac{m}{2}, то \rho = -\frac{m}{2}. Поскольку сравнимость по модулю m является [отношением эквивалентности](https://ru.wikipedia.org/wiki/%D0%9E%D1%82%D0%BD%D0%BE%D1%88%D0%B5%D0%BD%D0%B8%D0%B5_%D1%8D%D0%BA%D0%B2%D0%B8%D0%B2%D0%B0%D0%BB%D0%B5%D0%BD%D1%82%D0%BD%D0%BE%D1%81%D1%82%D0%B8) на множестве целых чисел \mathbb{Z}, то классы вычетов по модулю m представляют собой [классы эквивалентности](https://ru.wikipedia.org/wiki/%D0%9E%D1%82%D0%BD%D0%BE%D1%88%D0%B5%D0%BD%D0%B8%D0%B5_%D1%8D%D0%BA%D0%B2%D0%B8%D0%B2%D0%B0%D0%BB%D0%B5%D0%BD%D1%82%D0%BD%D0%BE%D1%81%D1%82%D0%B8); их количество равно m.

Множество всех классов вычетов по модулю m обозначается \mathbb{Z}_m или \mathbb{Z}/m\mathbb{Z}[[12]](https://ru.wikipedia.org/wiki/%D0%A1%D1%80%D0%B0%D0%B2%D0%BD%D0%B5%D0%BD%D0%B8%D0%B5_%D0%BF%D0%BE_%D0%BC%D0%BE%D0%B4%D1%83%D0%BB%D1%8E#cite_note-12) или \mathbb{Z}/(m)[[13]](https://ru.wikipedia.org/wiki/%D0%A1%D1%80%D0%B0%D0%B2%D0%BD%D0%B5%D0%BD%D0%B8%D0%B5_%D0%BF%D0%BE_%D0%BC%D0%BE%D0%B4%D1%83%D0%BB%D1%8E#cite_note-13).

Операции сложения и умножения на \mathbb{Z} [индуцируют](https://ru.wikipedia.org/w/index.php?title=%D0%98%D0%BD%D0%B4%D1%83%D1%86%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%BD%D0%B0%D1%8F_%D0%BE%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D1%8F&action=edit&redlink=1) соответствующие операции на множестве \mathbb{Z}_m:[a]_m+[b]_m=[a+b]_m

[a]_m\cdot [b]_m=[a\cdot b]_m

Относительно этих операций множество \mathbb{Z}_m является конечным [кольцом](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BB%D1%8C%D1%86%D0%BE_(%D0%B0%D0%BB%D0%B3%D0%B5%D0%B1%D1%80%D0%B0)), а для [простого](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%81%D1%82%D0%BE%D0%B5_%D1%87%D0%B8%D1%81%D0%BB%D0%BE) m — конечным полем.

1. **Теорема Ферма.**

Теорема утверждает, что:

|  |
| --- |
| Для любого [натурального числа](https://ru.wikipedia.org/wiki/%D0%9D%D0%B0%D1%82%D1%83%D1%80%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D0%B5_%D1%87%D0%B8%D1%81%D0%BB%D0%BE) n>2 уравнение  a^n+b^n=c^n\,\!  не имеет решений в целых ненулевых числах a, b, c. |

Встречается более узкий вариант формулировки, утверждающий, что это уравнение не имеет *натуральных* решений. Однако очевидно, что если существует решение для целых чисел, то существует и решение в натуральных числах. В самом деле, пусть a, b, c — целые числа, дающие решение уравнения Ферма. Если n чётно, то |a|, |b|, |c| тоже будут решением, а если нечётно, то перенесём все степени отрицательных значений в другую часть уравнения, изменив знак. Например, если бы существовало решение уравнения a^3 + b^3 = c^3 и при этом a отрицательно, а прочие положительны, то b^3 = c^3 + (|-a|)^3, и получаем натуральные решения c, |a|, b. Поэтому обе формулировки эквивалентны.

Обобщениями утверждения теоремы Ферма являются опровергнутая [гипотеза Эйлера](https://ru.wikipedia.org/wiki/%D0%93%D0%B8%D0%BF%D0%BE%D1%82%D0%B5%D0%B7%D0%B0_%D0%AD%D0%B9%D0%BB%D0%B5%D1%80%D0%B0) и открытая [гипотеза Ландера — Паркина — Селфриджа](https://ru.wikipedia.org/wiki/%D0%93%D0%B8%D0%BF%D0%BE%D1%82%D0%B5%D0%B7%D0%B0_%D0%9B%D0%B0%D0%BD%D0%B4%D0%B5%D1%80%D0%B0_%E2%80%94_%D0%9F%D0%B0%D1%80%D0%BA%D0%B8%D0%BD%D0%B0_%E2%80%94_%D0%A1%D0%B5%D0%BB%D1%84%D1%80%D0%B8%D0%B4%D0%B6%D0%B0).

1. **Функция Эйлера. Теорема Эйлера.**

**Фу́нкция Э́йлера** \varphi(n) — [мультипликативная](https://ru.wikipedia.org/wiki/%D0%9C%D1%83%D0%BB%D1%8C%D1%82%D0%B8%D0%BF%D0%BB%D0%B8%D0%BA%D0%B0%D1%82%D0%B8%D0%B2%D0%BD%D0%B0%D1%8F_%D1%84%D1%83%D0%BD%D0%BA%D1%86%D0%B8%D1%8F) [арифметическая функция](https://ru.wikipedia.org/wiki/%D0%90%D1%80%D0%B8%D1%84%D0%BC%D0%B5%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D1%84%D1%83%D0%BD%D0%BA%D1%86%D0%B8%D1%8F), равная количеству [натуральных чисел](https://ru.wikipedia.org/wiki/%D0%9D%D0%B0%D1%82%D1%83%D1%80%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D0%B5_%D1%87%D0%B8%D1%81%D0%BB%D0%BE), меньших n и [взаимно простых](https://ru.wikipedia.org/wiki/%D0%92%D0%B7%D0%B0%D0%B8%D0%BC%D0%BD%D0%BE_%D0%BF%D1%80%D0%BE%D1%81%D1%82%D1%8B%D0%B5_%D1%87%D0%B8%D1%81%D0%BB%D0%B0) с ним. При этом полагают по определению, что число 1 взаимно просто со всеми натуральными числами, и \varphi(1)=1.

Например, для числа 24 существует 8 меньших него и взаимно простых с ним чисел (1, 5, 7, 11, 13, 17, 19, 23), поэтому \varphi(24)=8.

### Общие сведения

Функция Эйлера \varphi(n) показывает, сколько натуральных чисел из отрезка [1,\;n-1] имеют c n только один общий делитель — единицу. Функция Эйлера определена на множестве [натуральных чисел](https://ru.wikipedia.org/wiki/%D0%9D%D0%B0%D1%82%D1%83%D1%80%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D0%B5_%D1%87%D0%B8%D1%81%D0%BB%D0%BE), и значения её лежат в множестве натуральных чисел.

Как следует из определения, чтобы вычислить \varphi(n), нужно перебрать все числа от 1 до n-1 и для каждого проверить, имеет ли оно общие делители с n, а затем подсчитать, сколько чисел оказались взаимно простыми с n. Эта процедура для больших чисел n весьма трудоемка, поэтому для вычисления \varphi(n) используют другие методы, которые основываются на специфических свойствах функции Эйлера.

**Теоре́ма Э́йлера** в [теории чисел](https://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D0%BE%D1%80%D0%B8%D1%8F_%D1%87%D0%B8%D1%81%D0%B5%D0%BB) гласит:

### Если a и m [взаимно просты](https://ru.wikipedia.org/wiki/%D0%92%D0%B7%D0%B0%D0%B8%D0%BC%D0%BD%D0%BE_%D0%BF%D1%80%D0%BE%D1%81%D1%82%D1%8B%D0%B5_%D1%87%D0%B8%D1%81%D0%BB%D0%B0), то a^{\varphi(m)} \equiv 1 \pmod m, где \varphi(m) — [функция Эйлера](https://ru.wikipedia.org/wiki/%D0%A4%D1%83%D0%BD%D0%BA%D1%86%D0%B8%D1%8F_%D0%AD%D0%B9%D0%BB%D0%B5%D1%80%D0%B0).

### С помощью теории чисел доказательство.

Пусть x_1, \dots, x_{\varphi(m)} — все различные натуральные числа, меньшие m и взаимно простые с ним.

Рассмотрим все возможные произведения x_i a для всех i от 1 до \varphi(m).

Поскольку a взаимно просто с m и x_i взаимно просто с m, то и x_i a также взаимно просто с m, то есть x_i a \equiv x_j\pmod m для некоторого j.

Отметим, что все остатки x_i a при делении на m различны. Действительно, пусть это не так, то существуют такие i_1 \neq i_2, что

x_{i_1} a \equiv x_{i_2} a\pmod m

или

(x_{i_1} - x_{i_2}) a \equiv 0\pmod m.

Так как a взаимно просто с m, то последнее равенство равносильно тому, что

x_{i_1} - x_{i_2} \equiv 0\pmod m или x_{i_1} \equiv x_{i_2}\pmod m.

Это противоречит тому, что числа x_1, \dots, x_{\varphi(m)} попарно различны по модулю m.

Перемножим все сравнения вида x_i a \equiv x_j\pmod m. Получим:

x_1 \cdots x_{\varphi(m)} a^{\varphi(m)} \equiv x_1 \cdots x_{\varphi(m)}\pmod m

или

x_1 \cdots x_{\varphi(m)} (a^{\varphi(m)}-1) \equiv 0\pmod m.

Так как число x_1 \cdots x_{\varphi(m)} взаимно просто с m, то последнее сравнение равносильно тому, что

a^{\varphi(m)}-1 \equiv 0\pmod m

или

a^{\varphi(m)} \equiv 1\pmod m. [■](https://ru.wikipedia.org/wiki/Q.E.D.)

# Алгебра многочленов.

1. **Конечные поля Галуа. Порядок конечного поля.**

**Конечным полем** называется конечный набор элементов, на котором определены операции сложения, умножения, вычитания и деления (кроме деления на 0), удовлетворяющие [аксиомам поля](https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D0%BB%D0%B5_(%D0%B0%D0%BB%D0%B3%D0%B5%D0%B1%D1%80%D0%B0))[[7]](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BD%D0%B5%D1%87%D0%BD%D0%BE%D0%B5_%D0%BF%D0%BE%D0%BB%D0%B5#cite_note-autogenerated2-7).

 Число элементов в поле называется его **поря́дком**.

1. **Неприводимые многочлены. Алгоритм Евклида для многочленов.**

**Неприводимый многочлен** — [многочлен](https://ru.wikipedia.org/wiki/%D0%9C%D0%BD%D0%BE%D0%B3%D0%BE%D1%87%D0%BB%D0%B5%D0%BD), неразложимый на нетривиальные (неконстантные) многочлены. Неприводимые многочлены являются [неприводимыми элементами](https://ru.wikipedia.org/wiki/%D0%9D%D0%B5%D0%BF%D1%80%D0%B8%D0%B2%D0%BE%D0%B4%D0%B8%D0%BC%D1%8B%D0%B9_%D1%8D%D0%BB%D0%B5%D0%BC%D0%B5%D0%BD%D1%82) [кольца многочленов](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BB%D1%8C%D1%86%D0%BE_%D0%BC%D0%BD%D0%BE%D0%B3%D0%BE%D1%87%D0%BB%D0%B5%D0%BD%D0%BE%D0%B2).

[Многочлен](https://ru.wikipedia.org/wiki/%D0%9C%D0%BD%D0%BE%D0%B3%D0%BE%D1%87%D0%BB%D0%B5%D0%BD) p(x_1,x_2,..,x_n) от n переменных над [полем](https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D0%BB%D0%B5_(%D0%B0%D0%BB%D0%B3%D0%B5%D0%B1%D1%80%D0%B0)) k называется **неприводимым** над k, если он является простым элементом [кольца](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BB%D1%8C%D1%86%D0%BE_(%D0%B0%D0%BB%D0%B3%D0%B5%D0%B1%D1%80%D0%B0)) k[x_1,x_2,..,x_n], то есть не является константой и не представим в виде произведения p=qr, где q и r ― многочлены с коэффициентами из k, отличные от констант.

Многочлен называется **абсолютно неприводимым**, если он неприводим над алгебраическим замыканием поля коэффициентов. Абсолютно неприводимые многочлены одной переменной ― это многочлены 1-й степени и только они. В случае нескольких переменных существуют абсолютно неприводимые многочлены сколь угодно высокой степени — например, любой многочлен вида

p(x_1,x_2,..,x_{n-1})+x_n абсолютно неприводим.

Корни неприводимого многочлена называются [сопряжёнными](https://ru.wikipedia.org/wiki/%D0%A1%D0%BE%D0%BF%D1%80%D1%8F%D0%B6%D1%91%D0%BD%D0%BD%D1%8B%D0%B9_%D0%BA%D0%BE%D1%80%D0%B5%D0%BD%D1%8C).

**Алгоритм Евклида для многочленов.**Алгоритм Евклида позволяет найти наибольший общий делитель двух многочленов, т.е. многочлен наибольшей степени, на который делятся без остатка оба данных многочлена.   
Алгоритм основан на том факте, что для любых двух многочленов от одного переменного, *f*(*x*) и *g*(*x*), существуют такие многочлены *q*(*x*) и *r*(*x*), называемые соответственно частное и остаток, что

*f*(*x*) = *g*(*x*)∙*q*(*x*) + *r*(*x*),   (\*)

при этом степень остатка меньше степени делителя, многочлена *g*(*x*), и, кроме того, по данным многочленам *f*(*x*) и *g*(*x*) частное и остаток находятся однозначно. Если в равенстве (\*) остаток *r*(*x*) равен нулевому многочлену (нулю), то говорят, что многочлен  *f*(*x*) делится на *g*(*x*) без остатка.  
Алгоритм состоит из последовательного деления с остатком сначала первого данного многочлена, *f*(*x*), на второй, *g*(*x*):

*f*(*x*) = *g*(*x*)∙*q*1(*x*) + *r*1(*x*),  (1)

затем, если *r*1(*x*) ≠ 0, – второго данного многочлена, *g*(*x*), на первый остаток – на многочлен *r*1(*x*):

*g*(*x*) = *r*1(*x*)∙*q*2(*x*) + *r*2(*x*),   (2)

далее, если  *r*2(*x*) ≠ 0, – первого остатка, *r*1(*x*), на второй остаток,  *r*2(*x*):

*r*1(*x*) = *r*2(*x*)∙*q*3(*x*) + *r*3(*x*),  (3)

затем, если *r*3(*x*) ≠ 0, – второго остатка на третий:

*r*2(*x*) = *r*3(*x*)∙*q*4(*x*) + *r*4(*x*),   (4)

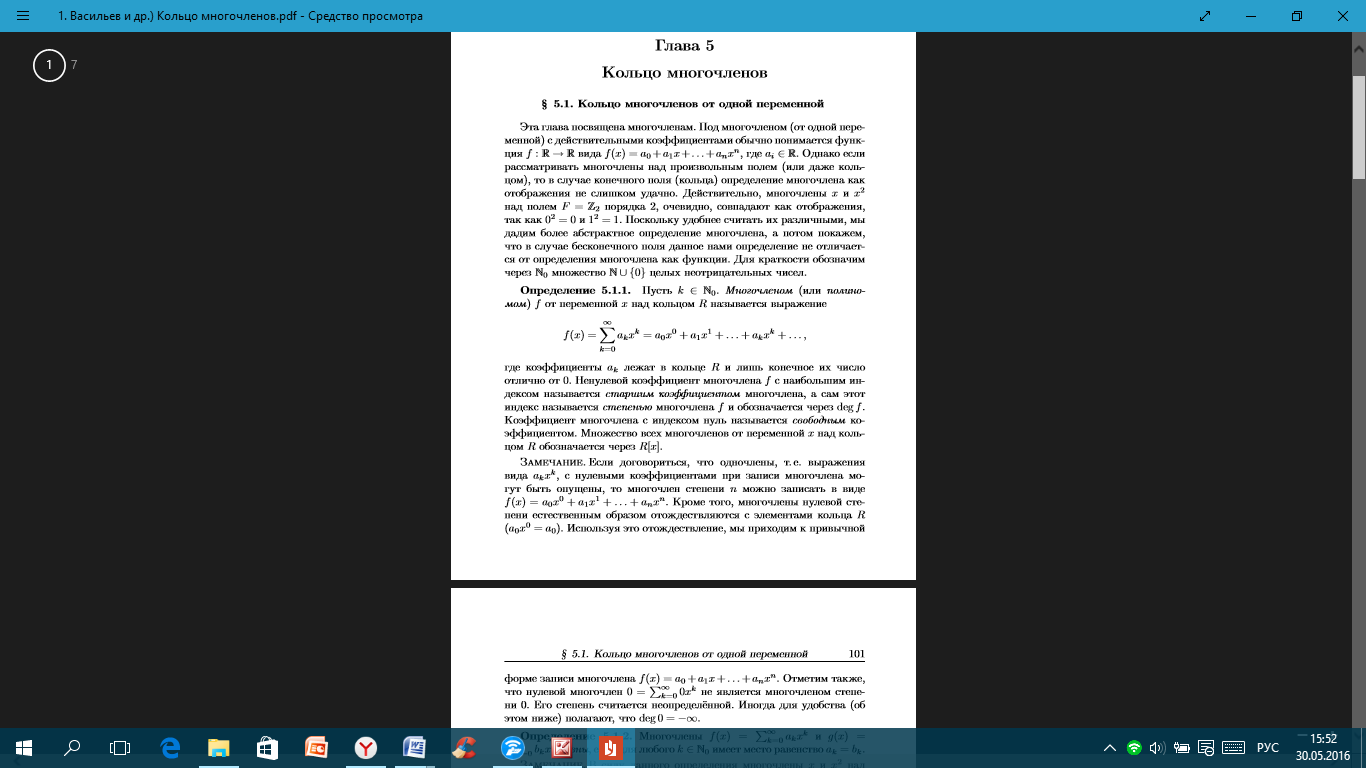
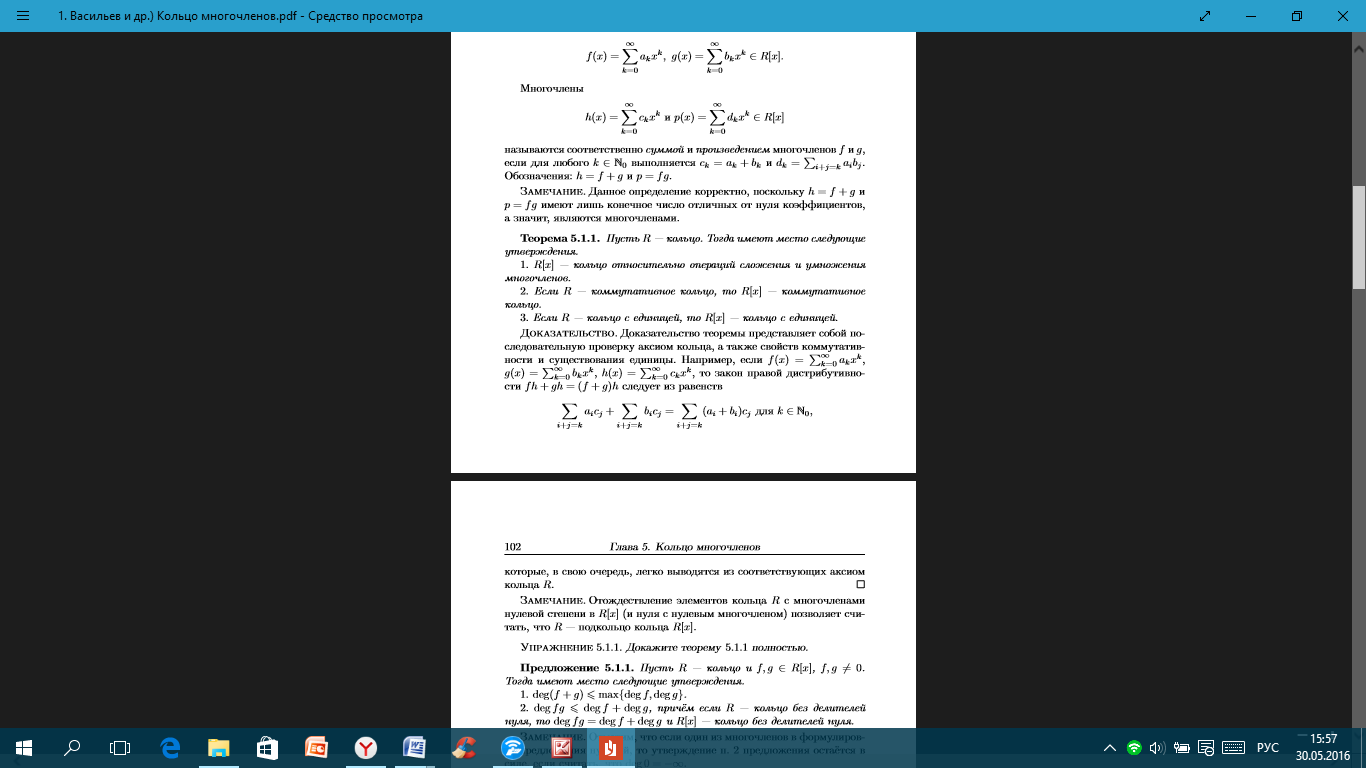
и т.д. Поскольку на каждом этапе степень очередного остатка уменьшается, процесс не может продолжаться бесконечно, так что на некотором этапе мы обязательно придем к ситуации, когда очередной, *n* + 1-й остаток *rn*+ 1 равен нулю:

|  |  |
| --- | --- |
| *rn*–2(*x*) = *rn*–1(*x*)∙*qn*(*x*) + *rn*(*x*), | (*n*) |
| *rn–1*(*x*) = *rn*(*x*)∙*qn*+1(*x*) + *rn*+1(*x*), | (*n*+1) |
| *rn+1*(*x*) = 0. | (*n*+2) |

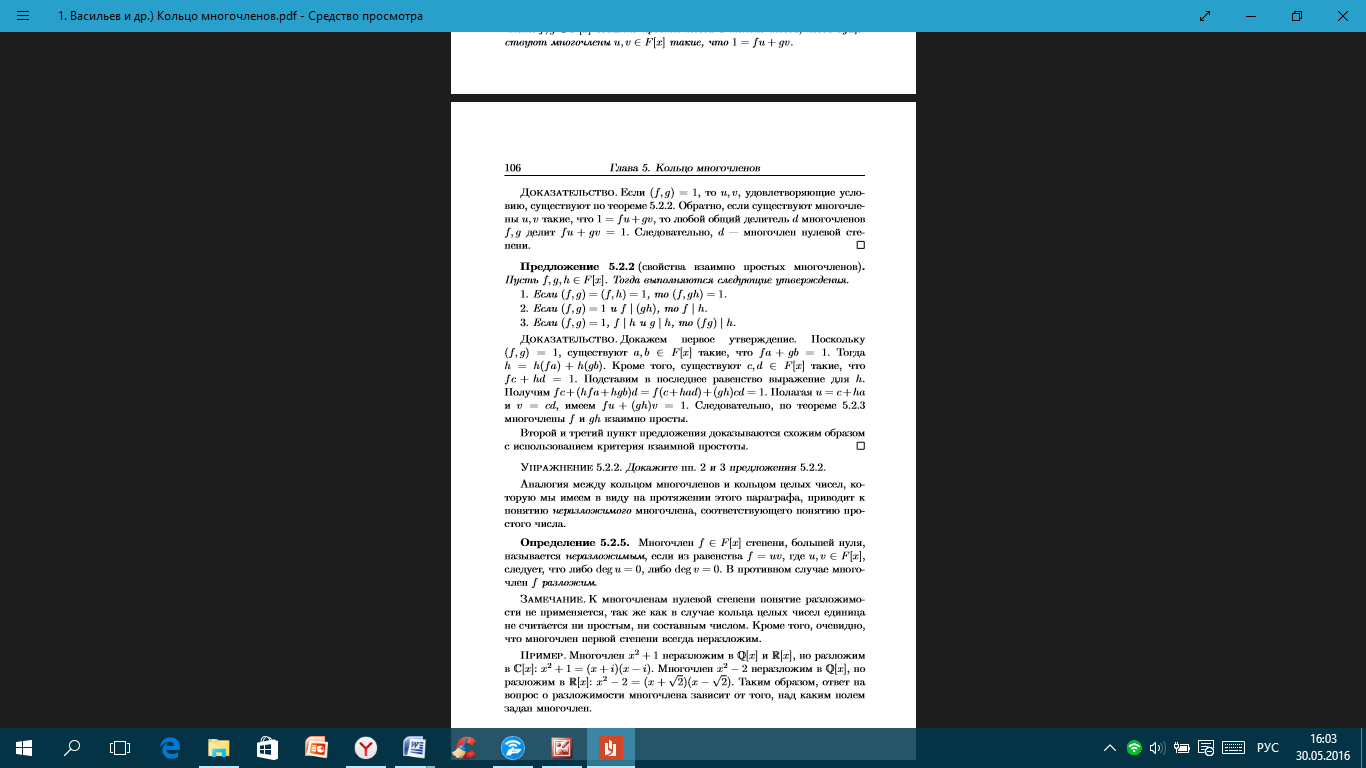
Тогда последний не равный нулю остаток *rn* и будет наибольшим общим делителем исходной пары многочленов  *f*(*x*) и *g*(*x*).  
Действительно, если в силу равенства (*n* + 2)  подставить 0 вместо  *rn*+ 1(*x*) в равенство (*n* + 1), затем – полученное равенство *rn*– 1(*x*) = *rn*(*x*)∙*qn*+ 1(*x*) вместо *rn – 1*(*x*) – в равенство (*n*), получится, что   *rn*– 2(*x*) = *rn*(*x*)∙*qn*+ 1(*x*) *qn*(*x*) + *rn*(*x*), т.е.  *rn*– 2(*x*) = *rn*(*x*)( *qn*+ 1(*x*) *qn*(*x*) + 1), и т.д. В равенстве (2) после подстановки получим, что *g*(*x*) = *rn*(*x*)∙*Q*(*x*), и, наконец, из равенства (1) – что  *f*(*x*) = *rn*(*x*)∙*S*(*x*), где *Q*и *S*– некоторые многочлены. Таким образом, *rn*(*x*) – общий делитель двух исходных многочленов, а то, что он наибольший (т.е. наибольшей возможной степени), следует из процедуры алгоритма.  
Если наибольший общий делитель двух многочленов не содержит переменную (т.е. является числом), исходные многочлены  *f*(*x*) и *g*(*x*) называются *взаимно-простыми*.

1. **Кольцо многочленов.**

**Кольцо многочленов** — это [кольцо](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BB%D1%8C%D1%86%D0%BE_(%D0%BC%D0%B0%D1%82%D0%B5%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0)), образованное многочленами от одной или нескольких переменных с коэффициентами из другого кольца.

** **

1. **Неразложимые многочлены.**

****