Дискретная математика (1 семестр, 2025)

Лектор: Зухба Анастасия Викторовна
Автор конспекта: Гридчин Михаил

Смотрите также другие конспекты ВШПИ в репозитории

Сочетания, размещения, отображения.

Правило произведения
Если необходимо выбрать пару объектов $(a, b) : a \in A, b \in B$
Известно следующее: a можно выбрать из A n способами, а затем b выбрать из B ровно m способами, тогда пару (a, b) можно выбрать $n \cdot m$ способами.

Правило суммы
Пусть дано $A \cap B = \varnothing$ $|A| = n$, $|B| = m$
Количество способов выбрать элемент из A или B равно $n + m$.

Def. *Перестановка* (количество перестановок) — биекция конечного множества на себя.

Возьмем произвольное отображение $f : X \to Y$, $|X| = n$, $|Y| = m$
X - "нумерованные шарики", Y - "нумерованные ящики"

Взять n различных шариков разложить по n различных ящикам по одному в ящик, $n!$ - количество перестановок

Взять n различных шариков разложить по n различных ящикам, n^m - количество перестановок.

Def. *Сочетание* (количество сочетаний) из n по k - выбор k элементного подмножества и n элементного множества без учёта порядка (без возвращений).

Note. Без учёта прядка, значит: $1, 2, 3$ равно $3, 2, 1$.

Note. Возвращение: "вытащили шарик посмотрели и положили обратно". Пусть n объектов, будем выбирать по n' штук (иногда $n' = n$).

Обозначение. $C_n^k = \binom{n}{k}$.

Вывод формулы $C_n^k = \frac{n!}{k! \cdot (n-k)!}$. Выставим в ряд n шариков, будем брать k, а $n - k$ не будем брать,

Note. $C_n^k = C_n^{n-k}$

Def. *Размещение* - упорядоченный выбор k элементов из n (без возвращений), аккуратно достаём и кладём в рядочек.
$A_n^k = n \cdot (n-1) \dots (n-k+1) = \frac{n!}{(n-k)!}$

Пример. $n = \{1, 2, 3, 4\}$, выбор с возвращением набора $4, 1, 4, 2$.

Def. *Размещение с повторениями* — упорядоченный выбор k элементов из n с возвращениями.

Обозначение. $\overline{A_n^k}$ - размещение с повторениям.

Def. *Сочетание с повторениями* — выбор k элементного не упорядоченного набора из n элементного множества.

Пример. Пусть n видов конфет, ровно k конфет в детском подарке, нужно посчитать сколькими способами можно собрать такой подарочек. Возьмём 1-ого вида конфет k_1, 2-го - k_2, 3-го - k_3, …, n - k_n; $k_1 + k_2 + k_3 + \dots + k_n = k$ - представили k как разложение, $k_i \in \mathbb{N} \cup \{0\}$. Суммы закодируем неразличимыми шариками (белыми и чёрными), k - белых, $n-1$ - чёрных (перегородок)

*Ответ. $\overline{C_n^k} = C_{k+(n-1)}^k = C_{k+(n-1)}^{n-1}$

Обозначение. $\overline{C_k^k}$.

Пример. Пусть есть два вида шариков черные и белые, m - чёрных и t - белых. Сколькими способами их можно расставить в ряд. Выбираем из $m+t$ мест шарики.
Ответ. C_{m+t}^t

Пусть отображение $f : X \to Y$.

Определение. *Инъективное отображение* $x_1 \neq x_2 \implies f(x_1) \neq f(x_2)$.

Пример. В ящике (m ящиков) не более 1-го шарика (n шариков), где $n \leq m$. Возьмём первый из шариков и кладём в один из ящиков и так далее, получим
$m \cdot (m-1) \cdot (m-n+1) = \frac{m!}{(m-n)!} = [m]_n$

Def. *Сюръективное отображение* $\forall y \in Y \; \exists x \in X : f(x) = y$.

Пример. В терминах шариков и ящиков, значит, что нет пустых ящиков.

Если есть n - белых шариков, n - чёрных шариков и мы их как-то переставляем, предположим, что это $2n$ чисел из низ n - чётных и n - не чётных.

Def. *Неразличимые* — такие элементы множества, перестановка которых ни на что не влияет.

Инструменты:

1. Принцип Дирихле: n кроликов рассажены по m клетками и $m < n$, то хотя бы в одной клетке не менее двух кроликов ($\lceil \frac{n}{m} \rceil$ - округление вверх).

Теорема. Если утверждение зависит от $n \in \mathbb{N}$ и
2) верно для некоторого $n = k_0$ (база)
3) из истинности утверждения для $n = k$, следует истинность для $n = k + 1$ (шаг)
4) то утверждение верно для всех $n \geq k_0$, $n \in \mathbb{N}$

Пример. $1^2 + 2^2 + 3^2 + n^2 = \frac{n(n+1)(2n+1)}{6}$
Решение.

- База $n = 1$ $1^2 = \frac{1 \cdot (1+1)(2+1)}{6}$ - верно
- Шаг $n = k$ $1^2 + \ldots k^2 = \frac{k(k+1)(2k+1)}{6}$ $n = k + 1$ $1^2 + \ldots k^2 + (k+1)^2 = \frac{(k+1)(k+2)(2k+3)}{6}$
- $\frac{k(k+1)(2k+1)}{6} + (k+1)^2 = \frac{(k+1)(2k^2+k+6k+6)}{6} = \frac{(k+1)(2k^2)+4k+3k+k}{6} = \frac{(k+1)(k+2)(2k+3)}{6}$

Таблица-шпаргалка по основным видам отображений

р - различимо, нр - неразличимо

Положим, что $|X| = n, |Y| = m$.

X, Y	произвольно	инъективно $(m \geq n)$	сюръективно $(n \geq m)$	биективно $(n = m)$
X, Y - р	m^n	$\frac{m!}{(m-n)!}$	$m!S(n,m)$	$m!$
X - нр, Y - р	C^n_{n+m-1}	C^n_m	C^{m-1}_{n-1}	1
X - р, Y - нр	B_n	1	$S(n,m)$	1
X, Y - нр	$p(n)$	1	1	1

Формулы включения исключения. Биномиальные коэффициенты.

Пример. A — счётное множество, $2^A = \{s, s \subseteq A\}$ — множество подмножеств A, каждое s можно закодировать последовательностью из 0 и 1, каждой последовательности сопоставим бинарную дробь $s \Leftrightarrow 0110101\ldots \Leftrightarrow 0.0110\ldots \in [0,1]$, таким образом, каждому элементу s сопоставили число и каждому числу s.

Инструменты:

- принцип Дирихле

- математическая индукция
- формула включений-исключений

Формула включений-исключений

Пусть A и B конечные множества, формула включений-исключений:

$$|A \cup B| = |A| + |B| - |A \cap B| = (-1)^{1+1} \sum |A_i| + (-1)^{1+2} \sum_{i<j} |A_i \cap B_j|$$

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

Теорема

Для произвольных множеств A, B, C выполнено:

$$C \cap (A \cup B) = (C \cap A) \cup (C \cap B)$$

□
Рассмотрим элемент, который входит в это множество $(A \cup B) \cap C$, он одновременно входит в C и в одно из множеств A или B, может быть в оба. Без ограничения общности он входит в A и C, а значит он входит в $(A \cup C)$.
В обратную сторону. Рассмотрим какой-нибудь элемент из $(B \cap C)$,в такое случае он входит в C, а так же входит в $(A \cup B) \cap C$.
■

Теорема (формула включений-исключений)

Пусть $A_1, A_2, \ldots, A_N$ - конечные множества. Тогда:

$$|\bigcup_{i=1}^{N} A_i| = \sum_{i=1}^{N} |A_i| - \sum_{1 \le i < j \le N} |A_i \cap A_j| + \sum_{1 \le i < j < k \le N} |A_i \cap A_j \cap A_k| \ldots$$

То есть

$$\boxed{|\bigcup_{i=1}^{N} A_i| = \sum_{m=1}^{N} (-1)^{m+1} \sum_{1 \le i_1 < i_2 \ldots < i_m \le N} |\bigcap_{k=1}^{m} A_{i_k}|}$$

□
Докажем по индукции.
База индукции.

$$|A_1 \cup A_2| = (-1)^{1+1} \sum_{1 \le i_1 \le 2} |A_i| + (-1)^{2+1} \sum_{1 \le i < j \le 2} |A_i \cap A_j| = |A_1| + |A_2| - |A_1 \cap A_2|$$

Шаг. Пусть для $n \leq N$ формула выполняется. Рассмотрим два множества:

$$A_{N+1}, \quad B = \bigcup_{i=1}^{N} A_i$$

Очевидно, что поскольку A_{N+1} - это одно число, то $|A_{N+1}| = 1$.
Поскольку для двух множеств выполнено

$$|A_{N+1} \cup B| = |A_{N+1}| + |B| - |A_{N+1} \cap B| \quad (*)$$

По предположению индукции для B выполнено:

$$|B| = |\bigcup_{i=1}^{N} A_i| = \sum_{m=1}^{N} (-1)^{m+1} \sum_{1 \leq i_1 < \ldots < i_m \leq N} |\bigcap_{k=1}^{m} A_{i_k}|$$

Также из ранее доказанной теоремы пересечение с объединением - это объединение пересечений, то есть

$$A_{N+1} \cap B = A_{N+1} \cap (\bigcup_{i=1}^{N} A_i) = (A_{N+1} \cap A_1) \cup \ldots \cup (A_{N+1} \cap A_N) = \bigcup_{i=1}^{N} (A_i \cap A_{N+1})$$

Это объединение N множеств $C_i = A_i \cap A_{N+1}$. Применим к этому объединению формулу включений-исключений, которую мы уже считаем верной для N множеств по предположению индукции:

$$|B \cap A_{N+1}| = |\bigcup_{i=1}^{N} C_i| = \sum_{m=1}^{N} (-1)^{m+1} \sum_{1 \leq i_1 < \ldots < i_m \leq N} |\bigcap_{k=1}^{m} C_{i_k}|$$

Но $C_{i_k} = A_{i_k} \cap A_{n+1}$, поэтому:

$$\bigcap_{k=1}^{m} C_{i_k} = \bigcap_{k=1}^{m} (A_{i_k} \cap A_{N+1}) = (\bigcap_{k=1}^{m} A_{i_k}) \cap A_{N+1}$$

Таким образом:

$$|B \cap A_{N+1}| = \sum_{m=1}^{N} (-1)^{m+1} \sum_{1 \leq i_1 < \ldots < i_m \leq N} |(\bigcap_{k=1}^{m} A_{i_k}) \cap A_{N+1}|$$

Подставим всё в $(*)$:

$$|A_{N+1} \cup B| = |A_{N+1}| + |B| - |B \cap A_{N+1}|$$

$$= \underbrace{\sum_{m=1}^{N} (-1)^{m+1} \sum_{1 \leq i_1 < \ldots < i_m \leq N} |\bigcap_{k=1}^{m} A_{i_k}|}_{|B|} + |A_{N+1}| - \underbrace{\sum_{m=1}^{N} (-1)^{m+1} \sum_{1 \leq i_1 < \ldots < i_m \leq N} |(\bigcap_{k=1}^{m} A_{i_k}) \cap A_{n+1}|}_{|B \cap A_{N+1}|}$$

Перепишем последнее слагаемое:

$$-\sum_{m=1}^{N}(-1)^{m+\boxed{1}}(\dots)=\sum_{m=1}^{N}(-1)^{m+\boxed{2}}(\dots)=\sum_{m=1}^{N}(-1)^{(m+1)+1}(\dots)$$

То есть знак стал соответствовать члену порядка $m+1$.

Разобьём итоговую сумму на слагаемые:

Слагаемые без A_{N+1}:
Это просто $|B|$:

$$\sum_{m=1}^{N}(-1)^{m+1}\sum_{1\le i_1<\dots<i_m\le N}|\bigcap_{k=1}^{m}A_{i_k}|$$

Слагаемые, содержащие только A_{N+1}.
Заметим, что это только $|A_{N+1}|$, поскольку в остальных слагаемых помимо A_{N+1} в пересечении присутствует какое-то ещё множество.
Слагаемые, содержащие A_{N+1} и ещё m других множеств:
Они имеют вид:

$$|A_{i_1}\cap A_{i_2}\cap\dots\cap A_{i_m}\cap A_{N+1}|$$

И входят с коэффициентом $(-1)^{(m+1)+1}=(-1)^{m+2}$. Введём новую переменную: пусть $s=m+1$. Тогда такие слагаемые — это пересечения s множеств, одно из которых — A_{N+1}, а остальные $(s-1)$ выбраны среди первых N множеств.
Все такие слагаемые:

$$\sum_{s=2}^{N+1}(-1)^{s+1}\sum_{i_1<\dots<i_{s-1}}|\bigcap_{k=1}^{s-1}A_{i_k}\cap A_{N+1}|$$

Объединим всё это и получим требуемое.

$$|B\cup A|=\underbrace{\sum_{m=1}^{N}(-1)^{m+1}\sum_{\substack{\text{подмножества}\\ \text{из первых } N}}|\bigcap A_{i_k}|}_{\text{без } A_{N+1}}+\underbrace{|A_{N+1}|}_{\text{само } A_{N+1}}+\underbrace{\sum_{s=2}^{N+1}(-1)^{s+1}\sum_{i_1<\dots<i_{s-1}}|\bigcap_{k=1}^{s-1}A_{i_k}\cap A_{N+1}|}_{\text{включают } A_{N+1} \text{ и другие}}$$

Теперь заметим, что все возможные непустые подмножества из $N+1$ множеств можно разделить на два типа:

1. Те, что не содержат A_{N+1} - покрыты первой суммой
2. Те, что содержат A_{N+1} - покрыты второй и третьей суммой.
   Таким образом, вся сумма совпадает с

$$\sum_{m=1}^{N+1}(-1)^{m+1}\sum_{1\le i_1<\dots<i_m\le N+1}|\bigcap_{k=1}^{m}A_{i_k}|$$

Что и требовалось доказать.
■

Биномиальные и полиномиальные коэффициенты

Теорема (Бином Ньютона)

$$(x+y)^n = \sum_{k=0}^{n} C_n^k x^k y^{n-k}$$

Где $C_n^k = \frac{n!}{k!(n-k)!}$ — число сочетаний.

■ $(x+y)\cdot(x+y)\cdot\ldots\cdot(x+y)$ - ровно n раз. Давайте пока что когда мы пишем каждое из слагаемых мы не будем менять x и y местами, то есть xyx не будем записываться как x^2y. Тогда при честном перемножении мы будем получать всевозможные цепочки из x и y: $xxyxyy\ldots x$ - всего n штук, таких последовательностей 2^n - вариантов.

Зафиксируем некоторое k, нас интересуют только те у которых k сомножителей x. Наша задача узнать на каком из мест стоит x, из n мест выбрать x на которых x стоят. То есть C_n^k.

Может быть мы можем такими же рассуждениями получить для $(x+y+z)^n$ чего-нибудь. Давайте посмотрим слагаемые $x^{k_1}y^{k_2}z^{k_3}$, $k_1+k_2+k_3=n$. Каждое слагаемые имеет вид $xyzzyzxx\ldots$ - в каждой такой цепочке ровно n элементов. Для того чтобы найти те из них, которые $x^{k_1}y^{k_2}z^{k_3}$ мы сначала выберем k_1 место из всех n на которые поставим x, а потом из оставшихся выберем те на которые поставили y, на все остальные ставим z:
$C_n^{k_1}\cdot C_n^{k_2} = \frac{n!}{k_1!k_2!k_3!}$.

В общем виде. Если есть скобка с m переменными $(x_1+x_2+\ldots+x_m)^n$, хотим вычислить коэффициент при $x_1^{k_1}x_2^{k_2}\cdot\ldots\cdot x_m^{k_m}$, при этом $k_1+k_2+\cdots+k_m=n$. Мы каждый раз будем составлять последовательность из m элементов, на каждом из мест стоит один из видов $x:x_1x_3x_2x_5\ldots$. Нас нужно из n мест выбрать k_1 на котором стоит x_1, из оставшихся мест выбрать куда ставить x_2, потом из оставшихся x_3:
$C_n^{k_1}\cdot C_{n-k_1}^{k_2}\cdot C_{n-k_1-k_2}^{k_3}\cdot\ldots\cdot C_{n-k_1-k_2-\cdots-k_{m-1}}^{m} = \frac{n!}{k_1!k_2!\ldots k_m!}$. ■

Другое доказательство.
□ Каждому месту присвоим номер, давайте все их перемешаем и поставим в ряд, то есть $n!$ вариантов выстроим в ряд, просто перестановка чисел от 1 до n: $213547\ 15\ldots$. Первые k_1 счастливчиков, которые оказались в строю, на эти номера мы поставим x_1, следующих k_2 туда поставим x_2, на следующее x_3, ну и так далее. Таким образом по каждой перестановке мы последовательность определим, но тут срабатывает следующее: по перестановке последовательность определяется однозначно, зато каждой

последовательности такой, соответствует много перестановок: k_1 - все перемешать, k_2 перемешать, k_3 перемешать и так далее. То есть каждому слагаемому из $(x_1 + x_2 + \ldots + x_m)^n$ будет соответствовать $k_1!k_2! \ldots k_m!$ - перестановок. А нам нужно взаимно однозначное соответствие, тогда нужно $n!$ поделить на $k_1!k_2! \ldots k_m!$. ■

Пример. $(x_1 + x_2 + x_3)^4$
Если взять слагаемые $x_1x_2x_3x_2 \to 1234$. Давайте переставлять 1234 местами: 4132. $k_1 = 1$, $k_2 = 2$, $k_3 = 1$, первые k_1 будет x_1, эти 13 - x_2, следующие x_3. Для 1234 это будет 1243, а ещё 1423.

Общий вид биномиального коэффициента $C_n^k = \frac{n!}{k!(n-k)!}$.
Общий вид полиномиального коэффициента $\frac{n!}{k_1!k_2! \ldots k_m!}$

Пример. $(1 + x + y)^n$, $n \geq 5$, $x^2y^3 \cdot 1^{n-5}$ - коэффициент при разложении сколько будет? Это $\frac{n!}{2!3!(n-5)!}$.

Два приёма обращения с биномиальными коэффициентами.

1. производящие функции

> **Определение**
>
> Для последовательности $\{a_n\}$ мы можем записать формальный ряд $A(t) = \sum_{i=0}^{\infty} a_i t^i$. Представьте себе что нам как-то безумно повезло и мы знаем функцию $A(t)$ не только в виде формального ряда, а в виде чего-нибудь. Говорят что $A(t)$ - **производящая функция** последовательности $\{a_n\}$.

> **Определение**
>
> **Финитные последовательности** - это когда после какого-то номера всё остальное нули.

Пример. Последовательность $C_n^0C_n^1C_n^2 \ldots C_n^n, 0, 0, \ldots, 0$. Запишем производящую функцию $C_n^0x^0 + C_n^1x^1 + \ldots + C_n^nx^n + 0 + \ldots + 0 = (1 + x)^n$. Значит $(1 + x)^n$ - это производящая функция для вот этой последовательности.

Пример. $\sum_{n=1}^{n} C_n^k = 2^n$, подставим 1 в $(1 + x)^n$

Пример. $\sum_{k=0}^{n}(-1)^k C_n^k = 0$, подставим -1 в $(1 + x)^n$.

Пример. $\sum_{k=0}^{n} kC_n^k$.
$\left(\sum_{k=0}^{n} C_n^k x^k\right)' = \sum_{k=0}^{n} kC_n^k x^{k-1}$

$((1+x)^n)' = n(1+x)^{n-1}$, подставим $x = 1$ и получим $\sum_{k=0}^{n} kC_n^k = n \cdot 2^{n-1}$

Пример. Блуждание по сетке. Пусть есть робот который умеет делать шаг вверх и шаг в право, он ходит по линиям решётки. Решётка размера $m \times n$. Сколькими способами он может найти из точки A (левый нижний угол) в точку B (правый верхний угол).
$C_{m+n}^m = C_{m+n}^n = 1 \cdot C_{m+n-1}^m + 1 \cdot C_{m+n-1}^{m-1}$

Основа треугольника Паскаля $C_n^k = C_{n-1}^k + C_{n-1}^{k-1}$

Возьмём на решётки i- ую диагональ, причём $i < m$ и $i < n$. Через каждую такую точку проходит маршрут. Возьмём строку j, причём $j < m$ и $j < n$. Сколькими способами можем дойти из A в c, $m - j$ - по вертикали, $(n - (i - j))$ - по горизонтали. Сколькими способами можем дойти из c в B, j - по вертикали, $(i - j)$ - по горизонтали.

$$C_{m+n}^m = \sum_{j=0}^{i} C_{m+n-i}^{m-j} \cdot C_i^j$$

Вопрос. Почему $(i - j)$?

Рекуррентные соотношения. Числа Стирлинга.

$n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$ - факториал числа.

В прошлый раз обсуждали треугольник Паскаля:

1 1
1 2 1
1 3 3 1
. . . . . .

$C_n^k = C_{n-1}^{k-1} + C_{n-1}^k$ - отражает свойство треугольника Паскаля, $C_n^k = \frac{n!}{k!(n-k)!}$.

Числа Фибоначчи

Последовательность, чтобы получить следующий элемент последовательности нужно сложить два предыдущих:
$0, 1, 1, 2, 3, 5, \ldots$
$F_0, F_1, F_2, \ldots$
$F_{n+1} = F_n + F_{n-1}$, у неё порядок 2.

Если есть $\{x_i\}$ $i \in \mathbb{N}$, если $x_{i+k} = x_{n+k-1} \cdot u_1 + x_{n+k-2} \cdot u_2 + \cdots + x_n \cdot u_k$ $(*)$, $u_i \in \mathbb{R}$ - коэффициенты, $u_k \neq 0$. Такое уравнение называется линейное однородное рекуррентное уравнение порядка k.

Пример. $01011\ldots$, n элементов, два "0" не стоят подряд. Назовём последовательность N.

$N_n = N_{n-1} + N_{n-2}$, $N_{n-1} = 1$, $N_{n-2} = 10$. мы уверены что все последовательности и учли каждую один раз.

Характеристическое уравнение для линейного однородного рекуррентного уравнения порядка k.

Характеристический многочлен:

$\lambda^k = u_1\lambda^{k-1} + u_2\lambda^{k-2} + \cdots + u_k\lambda^0$

$X(\lambda) = x^k - u_1\lambda^{k-1} - u_2\lambda^{k-2} - \cdots - u_k$

Утверждение. Если у $X(\lambda)$ есть k различных действительных корней $\lambda_1, \lambda_2, \ldots, \lambda_k$, то любая последовательность $\{a_n\}$, удовлетворяющая $(*)$, может быть задана в виде $a_n = \alpha_1\lambda_1^n + \alpha_2\lambda_2^n + \cdots + \alpha_k\lambda_k^n$.

1. Если λ - корень характеристического многочлена, то последовательность $\{b_n\} \cdot b_n = \lambda^n$ удовлетворяет $(*)$.
2. $\{a_n\}$ и $\{b_n\}$ удовлетворяют $(*)$ $c, d \in \mathbb{R}$, то $\{c \cdot a_n + d \cdot b_n\}$ - удовлетворяет $(*)$.
3. Первые k элементов последовательности однозначно задают её всю, при условии что для неё выполняется $(*)$ и могут быть выбраны произвольным образом.
4. $\begin{matrix} 1, \lambda_1^1, \lambda_1^2, \ldots, \lambda_1^{k-1} \\ 1, \lambda_1^1, \lambda_1^2, \ldots, \lambda_1^{k-1} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ 1, \lambda_k^1, \lambda_k^2, \ldots, \lambda_k^{k-1} \end{matrix}$, они образуют линейно независимую систему и они образуют базис.

   $(a_1, a_2, \ldots, a_k)$ - этот вектор является линейное комбинацией векторов выше

   $\alpha_1 \cdot (1, \lambda_1^1, \lambda_1^2, \ldots, \lambda_1^{k-1})$

   $\alpha_2 \cdot (1, \lambda_1^1, \lambda_1^2, \ldots, \lambda_1^{k-1})$

   $\ldots\ldots\ldots\ldots\ldots\ldots\ldots$

   $\alpha_k \cdot (1, \lambda_k^1, \lambda_k^2, \ldots, \lambda_k^{k-1})$

Пример. Было $x_{n+2} = 3x_{n+1} + 4x_n$

$\lambda^2 = 3\lambda + 4$, λ - корень

$b_n = \lambda^n$

$\lambda^{n+2} = 3\lambda^{n+1} + 4\lambda^n$

Вернёмся к числам Фибоначчи.

$\lambda^2 = \lambda + 1$

$D = 5$, $\lambda_1 = \frac{1-\sqrt{5}}{2}$, $\lambda_2 = \frac{1+\sqrt{5}}{2}$

$F_n = \alpha\left(\frac{1-\sqrt{5}}{2}\right)^n + \beta\left(\frac{1+\sqrt{5}}{2}\right)^n$

$0 = F_0 = \alpha + \beta = 0$, $\beta = -\alpha$

$1 = F_1 = \alpha\left(\frac{1-\sqrt{5}}{2}\right) + \beta\left(\frac{1+\sqrt{5}}{2}\right) = 1$

$\alpha\left(\frac{1-\sqrt{5}-1-\sqrt{5}}{2}\right) = 1$

$\alpha = -\frac{1}{\sqrt{5}}$

$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)$

Здесь ситуация сложнее: $C_n^k = C_{n-1}^{k-1} + C_{n-1}^k$

Числа Стирлинга I рода

Мы ввели
$[x]_n = x(x-1)(x-2)\cdot\ldots\cdot(x-n+1) = \frac{x!}{(x-n)!} = s(n,0) + s(n,1)x + s(n,2)x^2 + \ldots + s(n,n)x^2$

$s(n,k)$ - коэффициент при x^k в $[x]_n$, числа Стирлинга I рода.
$s(n,n) = 1$
$s(n,k) = 0$, при $k > n$
$s(n,0) = 0$
$s(n,1) = (n-1)!\cdot(-1)^{n-1}$
$s(1,1) = 1$
$s(2,1) = s(1,0) - 1\cdot s(1,1) = -1$, $[x]_2 = x(x-1) = x^2 - x$

$[x]_{n+1} = [x]_n \cdot (x-n)$

$s(n+1,k) = (\ldots + s(n,k-1)x^{k-1} + s(n,k)x^k + \ldots)\cdot(x-n) = s(n,k-1) - n\cdot s(n,k)$

n\k	*0*	*1*	*2*	*3*	
1	***0***	***1***	***0***	***0***	***0***
2	***0***	***-1***	***1***	***0***	***0***
3	***0***			***1***	***0***
4	***0***				***1***

Где можно встретить числа Стирлинга?

Перестановка - биекция. Пусть $\{1,2,\ldots,n\}$. Тогда
$\pi = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \pi_1 & \pi_2 & \pi_3 & \ldots & \pi_n \end{pmatrix}$ - перестановка, $\pi(3) = \pi_3$

Пример. $\begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8 \\ 2\,7\,5\,4\,1\,3\,8\,6 \end{pmatrix} = (1\,2\,7\,8\,6\,3\,5\,1)\,(4)$
$\begin{pmatrix} 1\,2\,3\,4\,5 \\ 2\,1\,4\,3\,5 \end{pmatrix} = (1,2)\,(3,4)\,(5)$

$|s(n,k)| = c(n,k)$ - количество перестановок из n элементов с k циклами, $c(n,k)$ - не C_n^k.

Числа Стирлинга II рода

Возьмём $|X| = n$, X разбиваем на k непустых подмножеств. Разбиваем, значит,
$B_1 \cup B_2 \cup \cdots \cup B_n = X$, $B_i \cap B_j = \varnothing$, $i \neq j$, $B_i \neq \varnothing$

Note. $B_2 = \{2,3\}$, $B_3 = \{4\}$ и $B_2 = \{4\}$, $B_3 = \{1,3\}$.

Def. Числа Стирлинга II рода - неупорядоченное разбиение n элементного множества на k непустых подмножеств. Обозначение: $S(n,k)$.

$S(n,0) = 0,\ n \geq 1$
$S(0,0) = 1$
$S(n,1) = 1$

Пример. Найти: $S(n+1,k)$
Случай 1. $n+1$ - отдельное подмножество, тогда $S(n,k-1)$
Случай 2. $n+1$ - не отдельное подмножество, тогда $S(n,k) \cdot k$
Итого $S(n+1,k) = S(n,k-1) + S(n,k) \cdot k$.

Обозначение. $P(n,k)$ - разбиение числа на слагаемые.

Введение в теорию чисел. Функция Эйлера. Малая теорема Ферма.

Общие понятия о числах

1. Делимость (a делится на $b \iff a = bc$)
2. Деление с остатком ($a = bq + r, \quad q, r \in \mathbb{Z}, \quad 0 \leq r < |b|$). Например, $-5 = 2(-3) + 1$.
3. Простое число p - нет натуральных делителей кроме 1 и p. 1 - не простое число.
4. $\text{НОД}(a,b) = d, d \in \mathbb{N}$: 1) $a = da', b = db'$. 2) d - наибольший. 2') Любой общий делитель a и b является делителем d.
5. Числа a и b - взаимно просты, если $\text{НОД}(a,b) = 1$.
6. Если $\text{НОД}(a,b) = 1$ и $ac \mid b$. (ac делится на b), то $c \mid b$.
7. $НОК(a,b)$ - наименьшее $m \in \mathbb{N} : m \mid a, m \mid b$. $\text{НОК}(a,b) = \frac{ab}{\text{НОД}(a,b)}$
8. ***Теорема (основная теорема арифметики)***. Любое $m \in \mathbb{N}$ представимо единственным образов в виде произведения простых делителей.

$$m = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$$

Где p_i - простое, $k_i \in \mathbb{N}$.

Далее в этом блоке p - простые числа.

Утверждение. Количество простых чисел на $[1,n]$ обозначим, как $\pi(n)$. Тогда

$$\frac{\pi(n)}{n/\ln n} \to 1, n \to \infty$$

То есть $\pi(n) \sim \frac{1}{\ln n}$.

Def. $a \equiv b \pmod{m} \iff a - b \mid m$.

Свойства.

$$\begin{cases} a \equiv b \pmod{m} \\ c \equiv d \pmod{m} \end{cases} \implies \begin{cases} a + c \equiv b + d \pmod{m} \\ ac \equiv bd \pmod{m} \end{cases}$$

$$\begin{cases} ac \equiv bc \pmod{m} \\ \boxed{(c, m) = 1} \end{cases} \implies ac - bc \mid m \implies (a - b)c \mid m \implies a - b \mid m \implies \boxed{a \equiv b \pmod{m}}$$

Из алгоритма Евклида $(a, b) = (a - b, b) = \ldots = d = xa + yb$

Обратимость остатков. Рассмотрим уравнение

$$ax \equiv 1 \pmod{p} \iff \begin{cases} a \mid p \implies \varnothing \\ a \nmid p \implies (a, p) = 1 \implies \exists x, y \in \mathbb{Z} : ax + py = 1 \end{cases}$$

Рассмотрим последнее по модулю p:

$$ax \equiv 1 \pmod{p}$$

Другой способ решения: $a \nmid p \implies (a, p) = 1$. Рассмотрим различные ненулевые остатки от деления на p и всевозможные умножения a на $x < p$:

$$\begin{matrix} 1, & 2, & 3, & \ldots, & p - 1 \\ 1a, & 2a, & 3a, & \ldots, & a(p - 1) \end{matrix}$$

Докажем, что $\nexists i, j : ai \equiv aj \pmod{p}$. Действительно, тогда $a(i - j) \equiv 0 \pmod{p}$. Но $(a, p) = 1 \implies (i - j) \mid p$, но $i < p$ и $j < p$. Следовательно, $i = j$, что и требовалось. Следовательно, все остатки от деления ax на p - это какая-то перестановка чисел от 1 до p. То есть найдётся такое число $t \in \{1, 2, \ldots, p\} : ta \equiv 1 \pmod{p}$ - что и требовалось доказать.

Последний способ доказательства можно применить для лёгкого доказательства малой теоремы Ферма.

Теорема (малая теорема Ферма). $a^{p-1} \equiv 1 \pmod{p}$.

□ Поскольку $1a, 2a, \ldots, a(p - 1)$ дают все остатки от деления на p, то

$$1 \cdot 2 \cdot \ldots (p - 1) \equiv a \cdot 2a \cdot \ldots (p - 1)a \equiv a^{p-1} \cdot 1 \cdot 2 \ldots (p - 1) \pmod{p}$$

Но из свойства арифметики по модулю поскольку $(1 \cdot 2 \cdot \ldots (p - 1), p) = 1$, то $a^{p-1} \equiv 1 \pmod{p}$ ■

Теорема (теорема Вильсона).

$$(m - 1)! \equiv -1 \pmod{m} \iff \text{m - простое}$$

□

ШАГ1. Доказательство слева направо. Пусть m - составное. Это значит, что среди $(m - 1)!$

есть делители m. То есть $(m, (m-1)!) =: d \neq 1$. Перепишем формулировку теоремы в следующем виде:

$$(m-1)! + 1 = mk$$

Получаем, что $(m-1)! \mid d$, $mk \mid d$, но $1 \nmid d \implies$ противоречие.
ШАГ2. Доказательство справа налево. Пусть m - простое. Рассмотрим все ненулевые остатки от деления на m:

$$1, 2, 3, \ldots, (m-1) \quad (*)$$

Из обратимости остатков по простому модулю
$\forall a \in \{1, \ldots, m-1\} \exists x : a \cdot x \equiv 1 \pmod{m-1}$.
Начнём сопоставлять эти остатки. Числу $a = 1$ сопоставим $x = 1$, числу $a = 2$ сопоставим $x = x_2$, ..., числу $a = (m-1)$ сопоставим $x = (m-1)$. Несколько утверждений, связанные с сопоставлением:

1. x определён однозначно для любого a. Потому что если

$$ax \equiv ay \pmod{m} \implies x \equiv y \pmod{m} \implies x = y$$

2. Разным a соответствуют разные x. Аналогично если

$$a_1 x \equiv a_2 x \pmod{m} \implies a_1 \equiv a_2 \pmod{m} \implies a_1 = a_2$$

3. Если $t^2 \equiv 1 \pmod{m}$, то

$$(t-1)(t+1) \equiv 0 \pmod{m} \implies \begin{bmatrix} t \equiv 1 \pmod{m} \\ t \equiv m-1 \pmod{m} \end{bmatrix}$$

   Это значит, что кроме $a = 1$ и $a = (m-1)$ абсолютно все остальные остатки разбились на пары, причём взаимно однозначно. Это значит, что если мы возьмём произведение всех остатков, то каждый из остатков $\in \{2, 3, \ldots, (m-2)\}$ при умножении на свою пару даст 1. То есть

$$1 \cdot 2 \cdot 3 \cdot \ldots \cdot (m-2) \cdot (m-1) \equiv 1 \cdot (m-1) \equiv m - 1 \equiv -1 \pmod{m}$$

■

Def. *Функция Эйлера* $\varphi(n)$ - количество чисел ($\mathbb{N}$), меньших n и взаимно простых с ним.
Свойства.

- $\varphi(p) = p - 1$.
- $\varphi(p^2) = p^2 - p = p(p-1)$
- $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$
- Если $(m, n) = 1$, то $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$

□

ШАГ1. Рассмотрим сначала два простых p_1, p_2. Заметим, что среди чисел $1, 2, \dots p_1p_2$ нет чисел, которые делятся и на p_1, и на p_2 одновременно кроме p_1p_2.
То есть $\varphi(p_1p_2) = p_1p_2 - p_1 - p_2 + 1 = \varphi(p_1)\varphi(p_2)$.

ШАГ2. Докажем теперь в общем случае. Поскольку $(m, n) = 1$, то $\exists x, y \in \mathbb{Z} : mx + ny = 1$.
Тогда $\forall a \in \mathbb{Z}, \exists x_a, y_a \in \mathbb{Z} : mx_a + ny_a = a$.
Рассмотрим $mx + ny$ по-другому. Пусть $x \in \{0, \dots, n-1\}$, $y \in \{0, \dots, m-1\}$. Тогда выражение примет nm значений. Покажем, что это все возможные остатки от деления nm.
Пусть $mx_1 + ny_1 \equiv mx_2 + ny_2 \pmod{mn}$. Но тогда
$m(x_1 - x_2) + n(y_1 - y_2) \equiv 0 \pmod{mn} \implies (x_1 - x_2) \mid n, (y_1 - y_2) \mid m$. Но тогда
$x_1 = x_2, y_1 = y_2$
Значит, не может быть так, что разные пары чисел (x, y) дают одинаковый остаток на $mn \implies mx + ny$ - все возможные остатки от деления на mn.
Рассмотрим ряд чисел:

$$1, 2, 3, \dots, t, \dots, mn$$

Рассмотрим среди всех чисел от 1 до mn произвольное число t. Из только что доказанного

$$t \equiv mx + ny \pmod{mn}$$

То есть такие x, y существуют. Осталось понять, является ли t таким, что $(t, mn) = 1$.
От противного пусть

$$(t, mn) =: d \neq 1 \implies \begin{bmatrix}(t, m) \neq 1\\(t, n) \neq 1\end{bmatrix}$$

$(t, n) = 1 \iff (x, n) = 1$. ($(m, n) = 1 \implies x$ не имеет ни одного делителя с n).
$(t, m) = 1 \iff (y, m) = 1$.
Значит, чтобы $(t, mn) = 1$, требуется, чтобы $(x, n) = 1$ и $(y, m) = 1$. Таких чисел x ровно $\varphi(n)$, таких чисел y ровно $\varphi(m) \implies$ таких чисел t всего $\varphi(n) \cdot \varphi(m)$. ■

Теория чисел. Вычеты и невычеты. Расширенный алгоритм Евклида

Теорема Эйлера и алгоритм Евклида

Теорема (теорема Эйлера). Пусть дано n и число $a : (a, n) = 1$. Тогда $a^{\varphi(n)} \equiv 1 \pmod{n}$.
□
Выпишем все остатки от деления на n, взаимно простые с n:

$$r_1, r_2, \dots, r_{\varphi(n)}, \quad (r_i, n) = 1$$

Теперь умножим каждый из остатков на a:

$$a \cdot r_1, a \cdot r_2, \ldots, a \cdot r_{\varphi(n)} \pmod{n}$$

Каковы остатки от деления этих чисел на n? Они различные, т.к. если $\exists r_i, r_j : a \cdot r_i \equiv a \cdot r_j \pmod{n}$, то $a(r_i - r_j) \equiv 0 \pmod{n} \implies r_i = r_j$, т.к. $(a, n) = 1$.
Перемножим все остатки:

$$(a \cdot r_1)(a \cdot r_2) \ldots (a \cdot r_{\varphi(n)}) \equiv r_1 r_2 \ldots r_{\varphi(n)} \pmod{n}$$

Но $(r_i, n) = 1$, поделим обе части на произведение r_i (т.к. они взаимно просты с n) и получим:

$$\boxed{a^{\varphi(n)} \equiv 1 \pmod{n}}$$

■

Замечание. Если n - простое, то $\varphi(n) = n - 1$ и тождество превращается в $a^{n-1} \equiv 1 \pmod{n}$. Это и есть малая теорема Ферма.

Алгоритм Евклида. Тождество $(a, b) = (a - b, b)$ очевидно. Чтобы найти (a, b), воспользуемся следующим итеративным алгоритмом.

$$a_0 = a, \quad a_1 = b, \quad a_{i-1} = a_i q_i + a_{i+1}, \quad 0 \le a_{i+1} < |a_i|$$

Строим эту цепочку, пока $a_{i+1} \neq 0$. Утверждается, что $a_{t+1} = (a_0, a_1)$ - последний ненулевой остаток.
Пример: 6 и 4. $6 = 4 \cdot 1 + 2 \implies 2 = 6 - 4 \cdot 1 = x \cdot 6 + y \cdot 4$.

Расширенный алгоритм Евклида. $d = xa + yb$.
Стартуем с $x_t = -1, y_t = q_{t+1}$ и "раскручиваем": $x_i = y_i + 1, y_i = x_{i+1} - q_{i+1} y_i$. На каждом шаге (можно показать) $x_i a_i + y_i a_{i+1} = (a_0, a_1)$. В конце получаем $x_0 a_0 + y_0 a_1 = (a_0, a_1)$

Решение Диофантовых уравнений. $ax + by = c, \quad d = (a, b)$. Если $c \nmid d$, То решений нет. Иначе $c = kd, k \in \mathbb{Z}$. Решим уравнение $a\tilde{x} + b\tilde{y} = d$. Тогда нашли $\tilde{x}_0$ и $\tilde{y}_0$. Предположим, что у нас есть два решения:

$$\begin{matrix} a\tilde{x}_1 + b\tilde{y}_1 = d \\ a\tilde{x}_2 + b\tilde{y}_2 = d \end{matrix} (*) \implies a(\tilde{x}_1 - \tilde{x}_2) + b(\tilde{y}_1 - \tilde{y}_2) = 0$$

Заметим, что $a \mid d$ и $b(\tilde{y}_1 - \tilde{y}_2) \mid b$. Тогда $(\tilde{x}_1 - \tilde{x}_2) \mid \frac{b}{d}$. Тогда $\tilde{x}_1 - \tilde{x}_2 = \frac{b}{d} \cdot t$ и $\tilde{y}_1 - \tilde{y}_2 = \frac{a}{d} \cdot (-t), t \in \mathbb{Z}$. Тогда общее решение: $\tilde{x} = x_0 + \frac{b}{d} \cdot t, \quad \tilde{y} = y_0 - \frac{a}{d} \cdot t$. Чтобы получить из $(*)$ необходимое, умножим уравнение на $\frac{c}{d}$.

Квадратичные вычеты

Def. Число a называют *квадратичным вычетом* по модулю n, если
$\exists x \in \mathbb{Z} : x^2 \equiv a \pmod{n}$.
p - простое > 2.
Def. *Символ Лежандра*. $a \in \mathbb{Z}$.

$$\begin{aligned}
&(\tfrac{a}{p}) = 0, && \text{если } a \mid p \\
&(\tfrac{a}{p}) = 1, && \text{если } a \text{ - квадратичный вычет по } \pmod{p} \\
&(\tfrac{a}{p}) = -1, && \text{если } a \text{ - квадратичный невычет по } \pmod{p}
\end{aligned}$$

$x^2 \equiv (p-x)^2 \pmod{p}$. Рассмотрим все квадраты чисел:

$$1^2, 2^2, \dots, (\frac{p-1}{2})^2 \qquad \pmod{p}$$

Каждое из них - квадратичный вычет по определению. Они все различны.
□ Пусть $\exists x_i, x_j$:

$$x_i^2 \equiv x_j^2 \pmod{p}$$
$$\underset{\neq 0}{(x_i - x_j)} \cdot \underset{< p}{(x_i + x_j)} \equiv 0 \pmod{p}$$

Противоречие, значит $x_i = x_j$. ■

Следствие. Среди остатков от деления на p ровно $(\frac{p-1}{2})$ квадратичных вычетов (все числа имеют близнецов $x = (p-x)^2$, числа, большие p тождественно равны рассмотренным нами квадратам чисел по модулю p) и ровно $\frac{p-1}{2}$ квадратичных невычетов (ненулевых).

Теорема. $\boxed{(\frac{ab}{p}) = (\frac{a}{p}) \cdot (\frac{b}{p})}$ - символ Лежандра мультипликативен.
□
СЛУЧАЙ 0. Если $a \mid p$ или $b \mid p$, то $ab \mid p$ и символ Лежандра равен 0. Пусть $a \nmid p$ и $b \nmid p$.
СЛУЧАЙ 1. $a \equiv x^2, \quad b \equiv y^2$ - вычет, вычет. Возьмём произведение
$ab \equiv x^2 y^2 \pmod{p} \implies ab$ - квадратичный вычет. Тогда

$$\underset{=1}{(\tfrac{ab}{p})} = \underset{=1}{(\tfrac{1}{p})} \cdot \underset{=1}{(\tfrac{b}{p})}$$
$$1 = 1 \cdot 1$$

СЛУЧАЙ 2. Пусть a - квадратичный вычет, b -квадратичный невычет. То есть
$(\frac{a}{p}) = 1, \quad (\frac{b}{p}) = -1$. Рассмотрим произведение $a \cdot b$. Как минимум $(\frac{ab}{p}) \neq 0$.
Предположим, что $(\frac{ab}{p}) = 1$. Тогда

$$\exists x : a \equiv x^2 \pmod{p}, \quad (x, p) = 1$$
$$\exists y : ab \equiv y^2 \pmod{p} \quad (*)$$

По малой теореме Ферма $x \cdot x^{p-2} \equiv 1 \pmod{p}$. Обозначим $x_p^{-1} := x^{p-2} \in \mathbb{Z}$. Домножим $(*)$ на $(x_p^{-1})^2$.

$$(x_p^{-1})^2 ab \equiv (x_p^{-1})^2 x^2 b \equiv b \equiv y^2 \pmod{p}$$

Значит, b - квадратичный вычет - противоречие, значит, $(\frac{ab}{p}) = -1$. Тогда $-1 = 1 \cdot (-1)$

СЛУЧАЙ 3. Пусть a - квадратичный невычет и b - квадратичный невычет. Рассмотрим все ненулевые остатки от деления на p: $1, 2, \ldots, p-1$. Мы уже знаем, что среди них $\frac{p-1}{2}$ квадратичных вычетов и столько же квадратичных невычетов. Пусть V - множество всех вычетов, N - множество всех невычетов. $|V| = |N| = \frac{p-1}{2}$. Умножим все остатки на число $c : (p, c) = 1$:

$$\begin{matrix} 1, & 2, & \ldots, & p-1 \\ 1 \cdot c, & 2 \cdot c, & \ldots, & (p-1) \cdot c \end{matrix}$$

Мы много раз уже показывали, что все эти остатки разные. Предположим, что $c \in N$. Тогда по случаю 2 $\implies cV = N$. Мы получим все элементы из N (потому что во второй строке все числа различные). Но тогда и $cN = \{1, 2, \ldots, p-1\} \backslash N = V$. Это следует из того, что все числа разные, все невычеты мы уже получили, значит, мы можем получить толь то, что осталось, то есть только вычеты. То есть $(\frac{ab}{p}) = 1$, так как c - это невычет и N - это множество всех невычетов.
Получили доказательство мультипликативности символа Лежандра. ■

Теорема (критерий Эйлера).
a - квадратичный вычет по $\pmod{p} \iff a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.
a - квадратичный невычет по $\pmod{p} \iff a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.
□
ШАГ1. Доказываем слева направо первое утверждение. Пусть a - квадратичный вычет $\implies \exists x : a \equiv x^2 \pmod{p} \implies a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p}$.
ШАГ2. Покажем, что вторая строка - в точности первая. Действительно

$$a^{p-1} \equiv 1 \pmod{p} \implies (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 \pmod{p}$$

Значит, $a^{\frac{p-1}{2}} \in \{-1, 1\} \pmod{p}$.
ШАГ3. Доказательство в обратную сторону. Пусть a - квадратичный невычет. То есть $(\frac{a}{p}) = -1$. Тогда из мультипликативности $aV = N, \quad aN = V$. Обозначим

$$v := \prod_{v_i \in V} v_i$$

$$n := \prod_{n_i \in N} n_i$$

Заметим, что

$$av_1 \equiv n_1 \pmod{p}$$
$$av_2 \equiv n_2 \pmod{p}$$
$$\dots$$

Возьмём произведение всех уравнений:

$$a^{\frac{p-1}{2}} v \equiv n \pmod{p}$$

По теореме Вильсона $v \cdot n \equiv (p-1)! \equiv -1 \pmod{p}$. Умножим на n:

$$a^{\frac{p-1}{2}} vn \equiv n^2 \pmod{p} \iff a^{\frac{p-1}{2}} \equiv -n^2 \pmod{p}$$

Китайская теорема об остатках. Алгебраические структуры. Таблица Кэли

Китайская теорема об остатках

Теорема (Китайская теорема об остатках). Пусть $a_1, a_2, \dots, a_n$ - попарно взаимно простые числа, $r_1, r_2, \dots, r_n : 0 \le r_i < a_i$. Тогда

$$\exists N : \forall i \in \{1, 2, 3, \dots, n\} \implies N \equiv r_i \pmod{a_i}$$

Если N_1 и N_2 - решения системы сравнений, то $N_1 \equiv N_2 \pmod{a_1 \cdot a_2 \cdot \dots \cdot a_n}$.

□ Докажем по индукции по n.
База. $n = 1$. Очевидно, $\exists N_1 : N_1 \equiv r_1 \pmod{a_1}$ и
$\exists N_2 : N_2 \equiv r_1 \pmod{a_1} \implies N_1 \equiv N_2 \pmod{a_1}$.
Шаг. Пусть утверждение верно для $n \le k$. Рассмотрим $n = k + 1$. По предположению системы существует решение системы x:

$$\begin{cases} x \equiv r_1 \pmod{a_1} \\ x \equiv r_2 \pmod{a_2} \\ \dots \\ x \equiv r_k \pmod{a_k} \end{cases} \quad \exists N \text{ - решение системы}$$

Положим $d := a_1 \cdot a_2 \cdot \dots \cdot a_k$. По условию теоремы $(d, a_{k+1}) = 1$. Выпишем следующие числа:

$$N \quad N + d \quad N + 2d \quad \dots \quad N + (a_{k+1} - 1)d$$

Все эти числа дают разные остатки при делении на a. Действительно, положим, что это не так и существуют два числа $N + di$ и $N + dj$, которые дают одинаковый остаток при делении на a. Но тогда $(N + di) - (N + dj) \equiv 0 \pmod{a_{k+1}} \implies d(i - j) \equiv 0 \pmod{a_{k+1}}$. Но $(d, a_{k+1}) = 1 \implies i - j \equiv 0 \pmod{a_{k+1}} \implies i \equiv j \pmod{a_{k+1}} \implies i = j$. Так как $i, j < a_{k+1}$. Значит среди всех этих чисел представлены все остатки от деления на a_{k+1}, в том числе и

r_{k+1}
Пусть оно имеет вид $N + jd \equiv r_{k+1} \pmod{a_{k+1}}$. Теперь, если мы рассмотрим все остатки этого числа $N + jd$ на все остальные числа $a_1, a_2, \ldots, a_k$, то поскольку $d \mid a_i$, то $N + jd \equiv r_i \pmod{a_i}, \forall i \leq k$. То есть $N + jd$ всё ещё подходит. Мы доказали первую часть теоремы, так как смогли предъявить такое подходящее число $N' := N + jd$. Докажем теперь вторую часть теоремы. Рассмотрим два различных решения N_1, N_2, тогда из формулировки теоремы следует, что

$$\begin{cases} N_1 \equiv r_i \pmod{a_i} \\ N_2 \equiv r_i \pmod{a_1} \end{cases} \implies N_1 - N_2 \equiv 0 \pmod{a_i}$$

Получаем требуемое:

$$\begin{matrix} N_1 - N_2 \mid d \\ N_1 - N_2 \mid a_{k+1} \end{matrix} \implies N_1 - N_2 \mid d \cdot a_{k+1} \quad ((d, a_{k+1}) = 1)$$

■

Алгебраические структуры

Пусть дано множество M и операция $\times$, определённая на нём. Будем работать только с такими операциями, которые не выводят за пределы множества, то есть $\forall a, b : a \in M, b \in M \implies a \times b \in M$.

Def. Пусть задано множество M и операция $\circ$, заданная на нём. Если выполнена ассоциативность, т.е.

$$a \circ (b \circ c) = (a \circ b) \circ c$$

То эту структуру назовём *полугруппой*.
Пример: слова из алфавита $\{0, 1\}$ и операция конкатенации, определённая на этом множестве.

Def. Полугруппу, у которой существует единственный нейтральный элемент, то есть

$$\exists! e : a \circ e = e \circ a = a$$

Назовём *моноидом*.
Пример: слова из алфавита $\{0, 1\} \cup \{\epsilon\}$ (пустое слово) и операцией конкатенации слов, определённой на этом множестве.
Свойство: можно записать уравнение вида $a \circ x = b$, но не всегда можно решить.

Def. Моноид, для каждого элемента которого существует единственный обратный элемент, то есть

$$\forall x \exists! y : x \circ y = y \circ x = e$$

Назовём *группой*.

Про группы будем говорить всю следующую часть семестра.

Пример решения уравнения:

$$x \circ a = b$$
$$x \circ a \circ a^{-1} = b \circ a^{-1}$$
$$x \circ e = b \circ a^{-1}$$
$$\boxed{x = b \circ a^{-1}}$$

Пример: повороты пространства вокруг центра координат
Пример: пусть $m \in \mathbb{Z}$. $M := \{0, 1, \dots, m-1\}$ с операцией $+_m$ (сложение по модулю m) образует группу. Стандартное обозначение $(\mathbb{Z}_m, +)$.
Пример: пусть $p \in \mathbb{N}$, p - простое. Тогда $M := \{1, 2, \dots, p-1\}$ с операцией $\times_p$ (умножение по модулю p) образует группу. Стандартное обозначение $(\mathbb{Z}_p \backslash \{0\}, \times)$. Действительно, по малой теореме Ферма $a^{p-1} \equiv 1 \pmod{p} \iff a^{p-2} \equiv a^{-1} \pmod{p}$. Следовательно, для каждого элемента множества есть существует обратный элемент. (нейтральный элемент - 1)
Пример: рассмотрим M - множество перестановок (биекций) длины n. Обозначение перестановки:

$$\pi := \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ i_1 & i_2 & i_3 & \dots & i_n \end{pmatrix}, \quad \pi(j) = i_j$$

Определим операцию "композиция перестановок" на M ($\circ$) следующим образом:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ i_1 & i_2 & i_3 & \dots & i_n \end{pmatrix}, \quad \pi' = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ j_1 & j_2 & j_3 & \dots & j_n \end{pmatrix}$$
$$\pi \circ \pi' = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \pi(\pi'(1)) & \pi(\pi'(2)) & \pi(\pi'(3)) & \dots & \pi(\pi'(n)) \end{pmatrix}$$

Нейтральный элемент

$$e =: id := \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & 2 & 3 & \dots & n \end{pmatrix}$$

Обратный элемент

$$y = x^{-1} \iff y(x(i)) = i$$

Заметим, что поскольку функция $x(i)$ биективна, то она обратима, то есть
$\forall x \exists! y = x^{-1} \implies$ это группа.
Свойство: можно решить уравнение вида $a \circ x = b$.

Def. *Кольцо* $(M, +, \times)$ - это

1. коммутативная группа по сложению (то есть $+$ также коммутативен).

2. ассоциативна по $\times$
3. дистрибутивна $a \times (a + c) = a \times b + a \times c$.
   Пример: $(\mathbb{Z}_m, +, \times)$ - кольцо.
   Пример: $(\mathbb{Z}_2, \oplus, \wedge)$. Коммутативно по $\oplus$, нейтральный элемент - 0, обратный элемент - само число. Ассоциативна по $\wedge$. Также $(a \oplus b) \wedge c = a \wedge c \oplus b \wedge c \implies$ кольцо.
   Свойство: можно записать уравнение вида $a \times x + b = c$, но не всегда можно решить. Чтобы уравнение можно было решить, нужно определение поля.

Def. *Поле* $(M, +, \times)$ - это

1. коммутативная группа по $+$
2. $M \backslash \{0\}$ - коммутативная группа по $\times$
3. $a \times (b + c) = a \times b + a \times c$
   Пример: множества $\mathbb{Q}, \mathbb{R}, \mathbb{C}, (\mathbb{Z}_p, +, \times)$ - поля.

Конечные группы

Def. *Порядок группы* - количество элементов в ней.
Def. *Мультипликативная запись*:

$$(a \circ b) \circ c = a \circ (b \circ c)$$
$$\exists! e := 1$$
$$a \circ 1 = 1 \circ a = a$$
$$\forall x \exists! x^{-1}$$
$$x \circ x^{-1} = x^{-1} x = 1$$

Def. *Аддитивная запись*:

$$(a + b) + c = a + (b + c)$$
$$\exists! e := 0$$
$$a + 0 = 0 + a = a$$
$$\forall x \exists! (-x)$$
$$x + (-x) = (-x) + x = 0$$

Пример. Группы порядка k: $(\mathbb{Z}_k, +)$.

Def. *Таблица Кэли* - таблица для записи результатов применения операции ко всем парам элементов

Пример: таблица Кэли для группы порядка 2. В ней обязательно должен быть нейтральный элемент e и оставшийся элемент $a \neq e$. Заметим, что вариант может быть всего один, поскольку $ae = a, ea = a, ee = e$, остаётся только aa, значит, a - обратный элемент для $a \implies aa = e$

$\circ$	e	a
e	e	a
a	a	e

Значит, любые группы порядка 2 изоморфны (см. далее).

Пусть теперь $n = 3$. По аналогии заполним:

$\circ$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Гомоморфизм и изоморфизм. Циклические группы. Смежные классы

Аккуратнее про группы

Вспомним определение группы

Def. Множество M и операцию $\circ$ на нём ("$\circ$": $M \times M \to M$) называют *группой* G и пишут $G = (M, \circ)$, если:

0) "$\circ$" - алгебраическая операция, то есть $\forall a, b \in G(M) \implies a \circ b \in G$.

1. ассоциативность: $\forall a, b, c \in G \implies a \circ (b \circ c) = (a \circ b) \circ c$.
2. нейтральный элемент $\exists! e \in G : \forall a \in G \implies e \circ a = a \circ e = a$. Нетрудно показать, что нейтральный элемент единственный. Действительно,
   $e_1 \circ e_2 = e_1 = e_2 \circ e_1 = e_2 \implies e_1 = e_2$.
3. обратный элемент. $\forall a \in G \exists! b \in G : a \circ b = b \circ a = e$. Нетрудно показать, что обратный элемент может единственный. Действительно,

$$
\begin{aligned}
&a \circ b = a \circ c = e \quad \text{домножим на b слева} \\
&(b \circ a) \circ b = b = (b \circ a) \circ c = c \\
&b = c
\end{aligned}
$$

Свойство 1. $(a^n)^m = a^{nm}$ - по определению и по ассоциативности.
Свойство 2. $(a^{-1})^m \circ a^m = e$ по ассоциативности $\implies (a^{-1})^m = (a^m)^{-1} =: a^{-m}$.
Def. $a^0 := e$.
Def. *Порядок конечной группы* - количество элементов $:= |G|$.
Def. *Порядок элемента* $a \in G =: ord(a)$ - это такое наименьшее $m \in \mathbb{N} : a^m = e$.
Свойство 3. В конечных группах существуют порядки всех элементов (они конечны).
$\square$ Операция $(\circ)$ алгебраическая $\implies$ все степени элемента $a \in G$ также лежат в G.
Рассмотрим ряд:

$$a^1 \quad a^2 \quad a^3 \quad \dots \quad a^N, \quad N > |G|$$

Тогда $\exists i, j \in \{1, 2, 3, \ldots, N\} : a^i = a^j$ По принципу Дирихле. Тогда $a^{|i-j|} = e$. ■

Гомоморфизм и изоморфизм

Def. *Гомоморфизм групп* из группы G в группу G' - это такое отображение φ

$$\varphi : G \to G', \quad G = (M, \circ), \quad G' = (M', *)$$

Что $\boxed{\forall a, b \in G : \varphi(a \circ b) = \varphi(a) * \varphi(b)}$

Свойство гомоморфизма 1. $\varphi(a^{-1}) = (\varphi(a))^{-1}$, $\varphi(e) = e'$.
□

1. $\varphi(a \circ e) = \varphi(a) * \varphi(e) = \varphi(a) = \varphi(e \circ a) = \varphi(e) * \varphi(a) \implies \varphi(e \circ a) = \varphi(a \circ e) = \varphi(a)$.
2. $\varphi(a \circ a^{-1}) = \varphi(a^{-1} \circ a) = \varphi(e) = e' = \varphi(a) * \varphi(a^{-1}) = \varphi(a^{-1}) * \varphi(a)$. ■

Свойство гомоморфизма 2. $a^m = e \implies \varphi(a^m) = e'$ (из свойства гомоморфизма 1) $\varphi(a)^m = e'$ (по определению гомоморфизма) $\implies$ *порядок элемента $\varphi(a)$ является делителем порядка элемента a.*

Def. *Сюръективный гомоморфизм* из G на G' - гомоморфизм, такой, что

$$\forall b \in G' \exists a \in G : \varphi(a) = b \iff Im(\varphi) = \varphi(G) = G'$$

Def. *Изоморфизм* - гомоморфизм, являющийся биекцией. Обозначается: "$\cong$".

Свойство Изоморфизма. Изоморфизм - это гомоморфизм из G на G' и одновременно гомоморфизм из G' на G.

Таблицы Кэли.

Построим таблицу Кэли для множества на 4 элементах.

A:

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

B:

$\circ$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

В таблице A порядок каждого элемента кроме нейтрального равен 2.
В таблице B порядок каждого элемента равен 3.

Для таблицы A например можно взять множество пар по модулю 2 с поэлементным хором ($\oplus$) ($M = \{(0,0), (0,1), (1,0), (1,1)\}$). Нейтральный - $(0,0)$, обратный к $a \in M$ это сам a.
Для таблицы B подойдёт например $G(\mathbb{Z}_4, +)$.

Утверждение: группы, задающиеся таблицами Кэли для множества на 4 элементах неизоморфны.

□ По *второму свойству гомоморфизма* порядок элемента $\varphi(a)$ должен быть делителем порядка элемента a, $\forall a \in G'$. Но порядки элементов $\varphi(a)$ все кроме нейтрального равны 2, а у a порядки все кроме нейтрального равны 3. Как видим, 2 - не делитель 3. ■

Note. Группа порядка 5 всего одна.

Свойства групп

Свойство 4. Если $a^m = e$, то порядок a - делитель m, $m \in \mathbb{N}$.
□ Мы точно знаем, что $ord(a) \leq m$. Обозначим $n := ord(a)$. Разделим m на n с остатком:

$$m = nq + r \implies a^m = e = \underbrace{(a^n)^q}_{=e} \circ a^r = a^r$$

Но при этом $0 \leq r < n$ и при этом n - наименьшее натуральное число, при котором $a^n = e \implies r = 0$. ■

Def. Группа G называется *циклической*, если $\exists a \in G$ (порождающий элемент):

$$\forall b \in G \exists m \in \mathbb{Z} : a^m = b$$

Замечание. m в определении именно *целое*, не натуральное, что важно в следующем утверждении.
Утверждение. Группа $(\mathbb{Z}, +)$ - циклическая группа . Действительно, порождающий элемент - 1 или -1.
Следствие. Порождающий элемент не обязательно единственный.

Пример. Группа $(\mathbb{Z}_m, +)$ - циклическая группа. Порождающий элемент - 1.

Def. Если группа G циклическая и $|G| = m$, то её обозначают C_m.
Теорема. Все циклические группы из m элементов изоморфны между собой.
□ Пусть есть циклические группа C_m и C'_m, неизоморфные между собой:

$$\begin{array}{lccccc} C_m: & e & a & a^2 & \dots & a^{m-1} \\ C'_m: & e & b & b^2 & \dots & b^{m-1} \end{array}$$

Все элементы первой и второй групп различны, иначе бы порядки групп были меньше. То есть *порядок порождающего элемента совпадает с порядком группы*. Изоморфизм тривиальный. Сопоставим $\varphi(a^i) = b^i$. ■
Следствие. Всякая циклическая группа $C_m \cong (\mathbb{Z}_m, +)$.

Def. Будем говорить, что H - *подгруппа* группы $G(M, \circ)$ и записывать $H < G$, если

$$\begin{cases} H \subseteq G \\ H \text{ - группа относитаельно } (\circ) \end{cases}$$

Def (эквивалентное определение подгруппы). H - подгруппа G, если:

$$\begin{cases} H \subseteq G \\ \forall a, b \in H \implies a \circ b \in H \\ \forall a \in H \implies a^{-1} \in H \end{cases}$$

Теорема. Приведённые определения подгруппы эквивалентны.
□
Пусть выполнено первое. Тогда второе следует из аксиоматики группы напрямую.
Пусть выполнено второе. Тогда H замкнуто относительно групповой операции $(\circ)$, а также взятие обратного элемента также не выводит за пределы H из аксиоматики группы. Отдельно доказывается, что нейтральный элемент также лежит в H. Это следует из единственности e также из аксиоматики группы и из того, что $a \circ a^{-1} = e$.
■

Теорема (критерий подгруппы). H является подгруппой G тогда и только тогда, когда $\forall a, b \in H \implies a \circ b^{-1} \in H$ и $H \subseteq G$.
□ В одну сторону очевидно и в другую тоже очевидно.
Слева направо. Если $b \in H$, то и $b^{-1} \in H$, значит $a \circ b^{-1} \in H$.
Справа налево. Если $\forall a, b \in H$ верно, что $a \circ b^{-1} \in H$, тогда

1. возьмём $b = a$. Тогда $e \in H$.
2. возьмём $a = e$. Тогда $b^{-1} \in H$.
3. возьмём $b = b^{-1}$. Тогда $a \circ b^{-1^{-1}} = a \circ b \in H$. И получили первый пункт эквивалентного определения подгруппы ■

Теорема. Пусть дана произвольная группа G и элемент $a \in G : ord(a) = n, n \in \mathbb{N}$. Тогда

$$H := \{a^0, a^1, \dots, a^{n-1}\} < G$$

□ Заметим, что $H \subseteq G$. Тогда применим критерий подгруппы и получим требуемое. ■

Пример. Пример бесконечной группы, у которой есть конечные циклические подгруппы. Рассмотрим множество всех многочленов с коэффициентами по модулю m. Обозначается $\mathbb{Z}_m[x]$. Причём порядок каждого элемента - делитель m.

Def. Пусть $H < G$. Возьмём $g \in G$. Будем говорить, что gH - *левый смежный класс по подгруппе H с представителем g*, если

$$gH := \{g \circ h \mid h \in H\}$$

Утверждение. Смежные классы не пересекаются или совпадают.
□ Пусть $\exists z \in aH \cap bH \implies \exists h_1 \in H, h_2 \in H : z = a \circ h_1 = b \circ h_2 \implies a = b \circ h_2 \circ h_1^{-1}$, также

$$\implies \forall t \in aH \to t = a\tilde{h} = \underbrace{b \circ h_2 \circ h_1^{-1} \circ \tilde{h}}_{\in H} \implies t \in bH. \blacksquare$$

Нормальные подгруппы. Факторгруппы.

Теорема Лагранжа

На прошлой лекции было доказано, что левые (правые) смежные классы не пересекаются или совпадают.

Теорема (Лагранжа). Количество элементов в группе делится на количество элементов в подгруппе. Записывается:

$$\boxed{|G| = (G : H)|H|}$$

Где $(G : H)$ - индекс подгруппы H.

□
Докажем для левых смежных классов, для правых доказательство аналогично.

ШАГ 1. Докажем сначала, что количество элементов в $|gH| = |H|$. То есть, другими словами $\forall h_1, h_2 \in H, h_1 \neq h_2 \implies g \circ h_1 \neq g \circ h_2$. Действительно, если это не так и выполнено $g \circ h_1 = g \circ h_2$, то умножим обе части на $g^{-1} \in G$ слева. Получим:

$$g^{-1} \circ (g \circ h_1) = g^{-1} \circ (g \circ h_2)$$

$$e \circ h_1 = e \circ h_2$$

$$h_1 = h_2$$

Противоречие, значит, количество элементов в $|gH|$ действительно равно количеству элементов в $|H|$.

ШАГ 2. Докажем, что $\forall g \in G \implies g \in gH$. Действительно, поскольку H - подгруппа, то $e \in H$. Но тогда $g \circ e = g \in gH$.

ШАГ 3. Смежные классы не пересекаются или совпадают. Тогда группа G разбита на непересекающиеся подмножества $aH, bH, \ldots$, в каждом из которых ровно по $|H|$ элементов. Также каждый элемент G принадлежит какому-то смежному классу. Значит, количество элементов в G делится на количество элементов в H. Получили требуемое. А индекс подгруппы H - это количество различных смежных классов (левых)
■

Def. *Правый смежный класс по подгруппе H группы G с представителем $g \in G$*:

$$Hg := \{h \circ g \mid h \in H\}$$

Нормальные подгруппы

Def. Подгруппа $H < G$ называется *нормальной* (и обозначается $H \lhd G$), если $\forall g \in G \implies gH = Hg$.

Размышления. $gH = Hg \iff \{g \circ h \mid h \in H\} = \{h \circ g \mid h \in H\}$. Умножим на g^{-1} справа. Но тогда получим:

$$gHg^{-1} = H$$

Тогда можно ввести эквивалентное определение нормальной подгруппы.

Def (эквивалентное определение нормальной подгруппы).

$$H \lhd G \iff \forall g \in G, \forall h \in H \implies g \circ h \circ g^{-1} \in H$$

Теорема: Приведённые определения эквивалентны.
□
$1 \Rightarrow 2$: $H \lhd G \implies gH = Hg \implies \forall h_1 \in H \exists h_2 \in H : g \circ h_1 = h_2 \circ g \implies g \circ h_1 \circ g^{-1} = h_2 \in H$.
$1 \Leftarrow 2$: $\forall g \in G, \forall h \in H \implies g \circ h \circ g^{-1} \in H$. Тогда рассмотрим $gHg^{-1} = \{g \circ h \circ g^{-1} \mid h \in H\}$. Но это множество содержит столько же элементов, сколько и H. Почему меньше быть не может? Смотрите первый шаг доказательства теоремы Лагранжа. Тогда поскольку также все элементы $g \circ h \circ g^{-1} \in H \forall h \in H \forall g \in G$, то выполнено $gHg^{-1} = H$. Умножим на g справа, получим $gH = Hg$, это и требовалось показать.
■

Факторгруппы

"Нормальные подгруппы - это достаточно ценная вещь. С её помощью мы можем делать так называемые факторгруппы. Пусть есть множество каких-то объектов, которые вместе с операцией образуют группу. Элементов в ней может быть достаточно много, но иногда для наших прикладных целей столько элементов рассматривать не надо. Надо рассматривать какие-то более группы. Факторизация - это возможность объединять некоторые группы в подмножества и делать групповую операцию над укруплёнными подгруппами".

Def. Пусть $H \lhd G$. Рассмотрим смежные классы. Для определённости левые по H. Введём операцию $(aH) * (bH) := (a \circ b)H, a \in G, b \in G$. То есть это операция на множестве смежных классов, которая двум смежным классам сопоставляет третий.

Утверждение + Def. Множество смежных классов относительно данной операции образует группу (называемую *факторгруппой группы G по нормальной подгруппе H и обозначаемую G/H*).
□
ШАГ 1. Докажем ассоциативность $(*)$.

$$\forall a, b, c \in G \implies \begin{cases} ((aH) * (bH)) * (cH) = ((a \circ b)H) * (cH) = ((a \circ b) \circ c)H = (a \circ b \circ c)H \\ (aH) * ((bH) * (cH)) = (aH) * ((b \circ c)H) = (a \circ (b \circ c))H = (a \circ b \circ c)H \end{cases}$$

Получили требуемое.

ШАГ 2. Докажем существование нейтрального элемента. Докажем, что $eH = H$ - искомый нейтральный элемент. Действительно,

$$\forall a \in G \implies (aH) * (eH) = (a \circ e)H = (e \circ a)H = (eH) * (aH)$$

Теперь докажем единственность нейтрального элемента. Доказательство от противного. Пусть существуют nH и eH - нейтральные элементы относительно операции $(*)$. Заметим, что e - нейтральный элемент относительно операции $(\circ)$, а n - нет. Тогда:

$$(nH) * (eH) = (eH) = (nH)$$

Первое равенство из того, что nH - нейтральный, второе равенство из того, что eH - нейтральный. Получили, что $eH = nH$. Противоречие. Значит, нейтральный элемент единственный. Получили требуемое.

ШАГ 3. Докажем существование обратного элемента. Действительно,
$\forall a \in G \implies (aH) * (a^{-1}H) = (a^{-1}H) * (aH) = eH = H$.
Единственность доказывается аналогично шагу 2.

Значит, множество смежных классов относительно введённой операции $(*)$ образует группу.
■

Вопрос. Зачем нам нужна была нормальность подгруппы, если мы её нигде не использовали? Ответ: мы воспользовались нормальностью подгруппы H в тот момент, когда ввели операцию $(*)$. Оказывается, что её можно определить для нормальной подгруппы и нельзя для ненормальной. Действительно, корректности (независимости от представителя) должно быть выполнено:

$$\begin{cases} \forall a_1 \in aH \implies a_1H = aH \\ \forall b_1 \in bH \implies b_1H = bH \end{cases}$$

□
$(a_1H) * (b_1H) = (a_1 \circ b_1)H$. Покажем, что $(a_1 \circ b_1)H = (a \circ b)H$. Для этого нам достаточно найти хотя бы один общий элемент, чтобы они были равны (поскольку смежные классы не пересекаются или совпадают). Покажем, что $(a_1 \circ b_1) \in (a \circ b)H$. Действительно,

$$\begin{aligned} &a_1 \in aH \implies \exists h_a \in H : a_1 = a \circ h_a \\ &b_1 \in bH \implies \exists h_b \in H : b_1 = b \circ h_b \\ &a_1 \circ b_1 = a \circ \boxed{h_a \circ b} \circ h_b \end{aligned}$$

Но у нас нет коммутативности, чтобы поменять h_a и b местами, чтобы получить требуемое. В этот момент нам и приходит на помощь нормальность подгруппы. Мы знаем, что

$$bH = Hb \implies \forall h \in H \exists \tilde{h} \in H : h \circ b = b \circ \tilde{h}$$

Но тогда и для $\boxed{h_a \circ b}$ найдётся такой элемент $\tilde{h}_a : b \circ \tilde{h}_a = h_a \circ b$. Итого получаем:

$$a_1 \circ b_1 = a \circ b \circ \underbrace{\tilde{h}_a \circ h_b}_{=:\tilde{h} \in H} = a \circ b \circ \tilde{h}$$

Но так как $\tilde{h} \in H$, то и $(a_1 \circ b_1) \in (a \circ b)H$.
■

Вопрос. Сколько элементов в факторгруппе? Ответ: индекс H. Действительно, вся факторгруппа состоит из всех смежных классов, количество которых равно индексу H.

Гомоморфизм групп

Из прошлой лекции *гомоморфизм* - это такое отображение $\varphi : G(M, (\circ)) \to G'(M', (*))$, что $\forall a, b \in G \implies \varphi(a \circ b) = \varphi(a) * \varphi(b)$.
Уже доказанные свойства:

- $\varphi(e) = e'$
- $\varphi(a^{-1}) = (\varphi(a))^{-1}$. Следствие: $\varphi(a^m) = (\varphi(a))^m$
- порядок элемента $\varphi(a)$ является делителем порядка элемента a.

Def. *Образ гомоморфизма* - $\mathrm{Im}\varphi = \varphi(G) = \{\varphi(a) \mid a \in G\}$.
Теорема. Образ гомоморфизма - это подгруппа G'.
□
Из определения $Im\varphi \subseteq G'$. Применим *критерий подгруппы* для доказательства, что это подгруппа. Рассмотрим произвольные элементы $c, d \in Im\varphi$. По определению образа $\exists a, b \in G : \varphi(a) = c, \varphi(b) = d$. Рассмотрим $(c * d^{-1})$:

$$c * d^{-1} = \varphi(a) * \varphi(b^{-1}) = \varphi(a \circ b^{-1}) \in Im\varphi$$

Следовательно, $\mathrm{Im}\varphi < G'$ по критерию подгруппы.
■

Def. *Ядро гомоморфизма* - $\mathrm{Ker}\varphi = \{g \mid g \in G, \varphi(g) = e'\}$.
Теорема. Ядро гомоморфизма - это подгруппа G.
□
Из определения $\mathrm{Ker}\varphi \subseteq G$. Применим *критерий подгруппы* для доказательства, что это подгруппа. Возьмём произвольные $a, b \in \mathrm{Ker}\varphi$. Тогда:

$$\varphi(a \circ b^{-1}) = \varphi(a) * \varphi(b) = e' * (e')^{-1} = e' \implies a \circ b^{-1} \in Ker\varphi$$

Следовательно, $\mathrm{Ker}\varphi < G$ по критерию подгруппы.
■

Теорема. $Ker\varphi \lhd G$.
□

Рассмотрим произвольный элемент $g \in G$. Рассмотрим $g\mathrm{Ker}\varphi$. Поскольку $\mathrm{Ker}\varphi < G$, то $|g\mathrm{Ker}\varphi| = |(\mathrm{Ker}\varphi)g| = |\mathrm{Ker}\varphi|$. Рассмотрим произвольное $\boxed{t \in g\mathrm{Ker}\varphi}$. Для него $\exists h \in \mathrm{Ker}\varphi : t = g \circ h$. Рассмотрим $g \circ h \circ g^{-1}$. Для него выполнено $\varphi(g \circ h \circ g^{-1}) = \varphi(g) * \varphi(h) * \varphi(g^{-1})$. Заметим, что $\varphi(h) = e'$, так как $h \in \mathrm{Ker}\varphi$. Тогда $\varphi(g \circ h \circ g^{-1}) = e' \implies (g \circ h \circ g^{-1}) \in \mathrm{Ker}\varphi \implies \underbrace{g \circ h}_{=t} \in (\mathrm{Ker}\varphi)g \implies \boxed{t \in (\mathrm{Ker}\varphi)g}$. Но t и g были выбраны произвольно. Тогда по определению нормальной подгруппы $\mathrm{Ker}\varphi \lhd G$.
■

Факторгруппа по ядру гомоморфизма

Рассмотрим $G/\mathrm{Ker}\varphi$ (факторгруппа G по подгруппе $\mathrm{Ker}\varphi$).

Утверждение. Два элемента группы G содержатся в одном смежном классе по $\mathrm{Ker}\varphi \iff$ их образы совпадают. То есть $a, b \in g\mathrm{Ker}\varphi \iff \varphi(a) = \varphi(b)$. То есть между элементами $\mathrm{Im}\varphi$ и смежными классами биекция $\varphi(g) \iff g\mathrm{Ker}\varphi$.
□
$\Rightarrow$
Рассмотрим произвольные $a, b \in g\mathrm{Ker}\varphi \implies \exists h_a, h_b \in \mathrm{Ker}\varphi : a = g \circ h_a, b = g \circ h_b$. Рассмотрим $\varphi(a) = \varphi(g \circ h_a) = \varphi(g) * \underbrace{\varphi(h_a)}_{=e'} = \varphi(g)$. Аналогично, $\varphi(b) = \varphi(g)$. Тогда $\varphi(a) = \varphi(b)$.
$\Leftarrow$
Пусть $\varphi(a) = \varphi(b) \implies \varphi(a \circ b^{-1}) = \varphi(a) * (\varphi(b))^{-1} = e' \implies (a \circ b^{-1}) \in \mathrm{Ker}\varphi$. Тогда поскольку $a = (a \circ b^{-1}) \circ b \in (\mathrm{Ker}\varphi)b = b(\mathrm{Ker}\varphi)$. А также $a \in a\mathrm{Ker}\varphi$. А значит смежные классы совпадают, поскольку имеют общий элемент.
■

Теорема. $\mathrm{Im}\varphi \cong G/\mathrm{Ker}\varphi$ (гомоморфный образ группы изоморфен факторгруппе по ядру гомоморфизма).
□
В предыдущем утверждении мы доказали биекцию между $\mathrm{Im}\varphi$ и $G/\mathrm{Ker}\varphi (\times)$ $f : \varphi(g) \iff g\mathrm{Ker}\varphi$.

$$f(\varphi(g)) = g\mathrm{Ker}\varphi$$

$$f(\varphi(a) * \varphi(b)) = f(\varphi(a \circ b)) = (a \circ b)\mathrm{Ker}\varphi$$

$$f(\varphi(a)) \times f(\varphi(b)) = a\mathrm{Ker}\varphi \times b\mathrm{Ker}\varphi = (a \circ b)\mathrm{Ker}\varphi$$

Следовательно, $f(\varphi(a) * \varphi(b)) = f(\varphi(a)) \times f(\varphi(b))$. Значит, f - гомоморфизм. Но f - биекция. Следовательно, f - изоморфизм.
■

Теорема Кэли. Группа перестановок. Порядок элементов. Транспозиции.

Замечание. В этом блоке будем считать, что знак $(\circ)$ обозначает композицию и вычисляется *справа налево*, а произведение с опусканием знака или $(\cdot)$ обозначает групповую операцию.

Теорема Кэли

Теорема Кэли. Пусть G - конечная группа. $|G| =: n$. Тогда $\exists H < S_n : G \cong H$. То есть всякая конечная группа изоморфна некоторой подгруппе группы перестановок из n элементов. Другими словами $G \cong L_G < S_n$.
□
Так как G - конечная группа, пронумеруем все элементы этой группы, как $g_2, g_2, \dots g_n$. Рассмотрим левые сдвиги $L_a, a \in G$:

$$g_1 \to ag_1$$
$$g_2 \to ag_2$$
$$\dots$$
$$g_n \to ag_n$$

Поскольку все получившиеся элементы лежат в G, а также они все различны (иначе умножим на a^{-1} слева и получим равенство, см. предыдущие лекции), получаем, что L_a - это какая-то перестановка исходных элементов $g_1, g_2, \dots, g_n$ (взаимно однозначное соответствие). Рассмотрим L_a для всех $a \in G$. Заметим, что они образуют группу. Действительно, $L_e = e'$ (тождественная перестановка, $\forall g_i \in G \implies eg = g$). $L_a \circ L_{a^{-1}} = L_{a^{-1}} \circ L_a = L_e$. Действительно, $\forall g_i \in G \implies g_i = a^{-1}ag_i$. Также по определению $L_a \circ L_b = L_{ab} \implies L_a \circ (L_b \circ L_c) = (L_a \circ L_b) \circ L_c = L_{abc}$. Таким образом, доказали существование нейтрального элемента, обратного элемента и ассоциативность. Докажем теперь, что эта группа изоморфна группе G. Действительно, во первых мы доказали, что L_a - биекция $\forall a \in G$. А также мы показали, что $L_a \circ L_b = L_{ab} \implies$ по определению $G \cong L_G$. Поскольку $|L_G| = n$ и $L_G < S_n$, а также L_G - группа относительно той же групповой операции, что и S_n (композиция), то доказали альтернативную формулировку теоремы.
■

Группа перестановок

Def. *Перестановкой* назовём биекцию конечного множества на себя.

Def. *Перестановка в канонической записи* длины n обозначается следующим образом:

$$\pi := \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \pi(1) & \pi(2) & \pi(3) & \dots & \pi(n) \end{pmatrix}$$

Note. Перестановка - это также таблично заданная функция.

Def. *Произведение перестановок* длины n определим следующим образом:

$$\sigma \circ \pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}$$

$$\sigma \circ \pi := \begin{pmatrix} 1 & 2 & \dots & i & \dots & n \\ \sigma(\pi(1)) & \sigma(\pi(2)) & \dots & \sigma(\pi(i)) & \dots & \sigma(\pi(n)) \end{pmatrix}$$

Def. *Неканонической записью перестановки* длины n назовём такую перестановку, в которой аргументы могут быть перемешаны. При этом если $\pi(i) = i$, то этот столбец можно опустить.

Пример.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 4 & 3 & 1 \\ 1 & 4 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Def. *Обратной перестановкой* π^{-1} к перестановке π длины n назовём перестановку:

$$\pi^{-1} := \begin{pmatrix} \pi(1) & \pi(2) & \dots & \pi(n) \\ 1 & 2 & \dots & n \end{pmatrix}$$

Def. *Циклом* длины k перестановки длины n назовём последовательность элементов, где каждый элемент переходит в следующий, а последний - в первый и будем обозначать:

$$(i_1 \quad i_2 \quad \dots \quad i_k) = \begin{pmatrix} i_1 & i_2 & \dots & i_{k-1} & i_k \\ i_2 & i_3 & \dots & i_k & i_1 \end{pmatrix}$$

Note. Цикл - это биекция k-элементного множества на себя.

Note. Из предыдущего замечания следует, что цикл - это элемент группы перестановок.

Def. *Цикловой записью перестановки* длины n

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \pi(1) & \pi(2) & \pi(3) & \dots & \pi(n) \end{pmatrix}$$

Определяется представление перестановки в виде произведения непересекающихся циклов.

Пример. Рассмотрим перестановку

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$$

У неё есть следующие циклы:

$$1 \to 3 \to 5 \to 1$$
$$2 \to 4 \to 2$$

Значит

$$\pi = (1, 3, 5)(2, 4)$$

Утверждение. Любую перестановку можно разложить в непересекающиеся циклы.
Утверждение. Циклы перестановки коммутируют, то есть, если a и b - циклы, то $a \cdot b = b \cdot a$ и они задают одну и ту же перестановку. Доказательство по определению.
Утверждение. Любая перестановка раскладывается в произведение (композицию) **непересекающихся** циклов единственным образом с точностью до записи цикла и порядка циклов.

Утверждение. Порядок цикла длины k равен k, то есть $ord(i_1, i_2, \dots, i_k) = k$
□
Действительно, по определению цикла элемент i_1 переходит в элемент i_2 и так далее, то есть

$$i_1 \to i_2 \to \dots \to i_k \to i_1$$

Количество переходов равно k, а значит порядок каждого элемента равен k, значит и порядок всего цикла равен k. То есть $(i_1, i_2, \dots, i_k)^k = (i_1, i_2, \dots, i_k)$.
■

Def + теорема. Если перестановка записана в виде непересекающихся циклов длины $c_1, c_2, \dots, c_m$, то *порядком данной перестановки* равен $HOK(c_1, c_2, \dots, c_m)$.
□
Действительно, поскольку порядок перестановки должен делиться на порядок каждого цикла (чтобы элемент i перешёл сам в себя), а циклы не пересекаются, то $ord(\pi) = HOK(c_1, c_2, \dots, c_m)$.
■

Транспозиции

Def. *Транспозиция* - это цикл длины 2. То есть цикл (i_1, i_2).
Note. Транспозиция - это элемент группы перестановок
Note. Для транспозиции (a_i, a_j) обратная транспозиция - (a_i, a_j), то есть $(a_i, a_j)^2 = e = \mathrm{id}$.

Теорема. Любая перестановка представима в виде произведения транспозиций.
□
Нестрогое доказательство: из курса алгоритмов или из детского сада известно, что существуют сортировки сравнением. А значит, перестановка - это какое-то количество применённых операций $swap(a_i, a_j)$, что и задаёт транспозицию.

Строгое доказательство: Докажем сначала, что любой цикл можно разложить в произведение транспозиций. Действительно, рассмотрим цикл длины m:

$$(a_1 \quad a_2 \quad \dots \quad a_m)$$

Такой цикл можно представить в виде произведения транспозиций следующим образом:

$$(a_1 \quad a_2 \quad \dots \quad a_m) = (a_1 \quad a_m)\,(a_1 \quad a_{m-1}) \cdots (a_1 \quad a_3)\,(a_1 \quad a_2)$$

В данной записи умножение выполняется справа налево, как композиция функций. Действительно, элемент a_i, где $i \in \{2, 3, \dots, m-1\}$ сначала перейдёт в a_1, а на следующем шаге перейдёт в a_{i+1}, а далее к нему не будет выполнено никаких операций. Элемент a_1 перейдёт в a_2 на самом первом шаге, а далее к нему не будет выполнено никаких операций. Элемент a_m перейдёт в a_1 на последнем шаге. В результате получаем, что $\forall i \in \{1, 2, \dots, m\} : a_i \to a_{i+1 \pmod m}$. Значит, любой цикл представим в виде произведения транспозиций. Но любая перестановка представима в виде непересекающихся и коммутирующих циклов, а значит, что она представима и в виде произведения транспозиций.
■

Теорема. Пусть перестановка π задана произведением транспозиций:

$$\pi = t_1 t_2 \dots t_k$$

Тогда

$$\boxed{\pi^{-1} = t_k^{-1} t_{k-1}^{-1} \dots t_1^{-1} = t_k t_{k-1} \dots t_2 t_1}$$

□
Поскольку транспозиция - это элемент группы перестановок, то для транспозиций выполняется та же аксиоматика групп, что и для перестановок. Тогда если положим

$$\pi = t_1 t_2 \dots t_k$$

То для π^{-1} будет выполнено

$$\pi^{-1} = (t_1 t_2 \dots t_k)^{-1} = t_k^{-1} t_{k-1}^{-1} \dots t_1^{-1}$$

Докажем этот факт по индукции.

БАЗА. $k = 1$: $(t_1)^{-1} = t_1^{-1}$. Очевидно верно
ШАГ. Предположим, что предположение верно для k, докажем для $k+1$.
Пусть $\sigma = t_1 t_2 \dots t_k t_{k+1} = \sigma' t_{k+1}$, где $\sigma' = t_1 t_2 \dots t_k$. Тогда:

$$\sigma^{-1} = (\sigma' t_k)^{-1} = t_{k+1}^{-1} (\sigma')^{-1} = t_{k+1}^{-1} t_k^{-1} \dots t_1^{-1}$$

Получили требуемое.
Теперь, поскольку $t = t^{-1}$, получаем второе требуемое равенство.
■

Теорема. Для различных разложений перестановки в произведение транспозиций чётность количества транспозиций сохраняется.
□
Предположим противное, что для перестановки π существует разложение на чётное количество транспозиций и на нечётное количество транспозиций. Вспомним, что π^{-1} представляет обратное произведение транспозиций для π . Рассмотрим произведение $\pi \circ \pi^{-1}$, как произведение их транспозиций в одном и в другом случае.

$$\pi \circ \pi^{-1} = e = \underbrace{\sigma_1 \sigma_2 \dots \sigma_k}_{\text{нечётное количество}}$$

Докажем, что если e раскладывается в n транспозиций, то e раскладывается и в $n-2$ транспозиции. Рассмотрим в произведении такое $\sigma_p = (s,t)$, что элемент s правее ($\forall i > p$) не встречается. Рассмотрим σ_{p-1}. Есть несколько случаев.

1. $\sigma_{p-1} = (s,t)$, тогда $\sigma_{p-1}\sigma_p = e$.
2. $\sigma_{p-1} = (q,r)$, $\{q,r\} \cap \{s,t\} = \varnothing$. То есть они не пересекаются, следовательно, они коммутируют. Поменяем местами: $\sigma_{p-1}\sigma_p = \sigma_p\sigma_{p-1}$. То есть мы сместили выбранный s элемент левее
3. $\sigma_{p-1} = (s,r)$. Тогда $\sigma_{p-1}\sigma_p = \begin{pmatrix} s & r & t \\ t & s & r \end{pmatrix} = (s,t)(r,t)$. То есть мы опять сдвигаем s влево.
4. $\sigma_{p-1} = (t,r)$. Тогда $\sigma_{p-1}\sigma_p = \begin{pmatrix} s & t & r \\ r & s & t \end{pmatrix} = (s,r)(t,r)$. То есть мы опять сдвигаем s влево.

   Поймём, что произойдёт с s. Либо в какой-то момент подойдёт первый случай, и s сократится, либо получим, что s содержится в первой транспозиции, а правее не будет ни одной транспозиции, содержащей s (по построению). То есть

   $$e = (s,t')\underbrace{(\dots)\cdots(\dots)}_{\text{не содержат } s}$$

   Тогда s отображается в t'. Может ли быть такое, если $t' \neq s$? Нет, поскольку в итоге s должен перейти в s, чтобы перестановка была нейтральной. Значит, такого быть не может и в какой-то момент s сократится с какой-то ещё скобкой. То есть в какой-то момент выполнится критерий первого случая.
   Повторяя описанные выше действия, каждый раз сокращаются ровно 2 скобки, но поскольку изначально их было нечётное количество, то в конце концов останется одна скобка из двух разных элементов, а такого быть не может. Значит, наше предположение было неверным, и чётность количества транспозиций сохраняется.
   ■

Def. Чётность количества транспозиций в перестановке назовём *чётностью перестановки*.

Утверждение. В группе перестановок одинаковое количество чётных и нечётных перестановок. Доказательство почти тривиально (умножим на транспозицию (a_1, a_2))

Утверждение. Множество чётных перестановок образует подгруппу группы перестановок.

Утверждение. Подгруппа чётных перестановок является нормальной.

Введение в теорию графов.

Общие понятия

Def. *Графом* назовём совокупность из V - множество объектов (вершин) и E - множество пар объектов (рёбер)

Def. *Ребро* обозначается $e := (u, v) \in E$, где $u, v \in V$. Причём если $(u, v) = (v, u)$, то ребро будем называть неориентированным.

Def. Если $\forall u, v \in V$ считаем, что $(u, v) = (v, u)$, то есть порядок вершин в паре не имеет значения, то будем называть такой граф *неориентированным*. Если $(u, v) \neq (v, u)$, то такой граф будем называть *ориентированным* или *орграфом*.

По умолчанию, если не оговорено обратное, подразумеваются неориентированные графы.

Def. Ребро $(x, x) \in E$ будем называть *петлёй*.
Def. Рёбра $e_1 = (x, y), e_2 = (x, y), e_3 = (x, y), e_1, e_2, e_3 \in E$ в неориентированном графе будем называть кратными *рёбрами*.

Note. В ориентированном графе рёбра $e_1 = (x, y), e_2 = (y, x), e_1, e_2 \in E$ - всегда разные рёбра и потому кратными не считаются.

Def. Граф, в котором есть петли и кратные рёбра будем называть *псевдо мульти графом*.

По умолчанию, если не оговорено обратное, подразумеваются графы без петель и кратных рёбер.

Смежность и инцидентность

Def. *Матрицей смежности* назовём функцию $f : V \times V \to \{0, 1\}$. Если ребро (u, v) существует, то $f(u, v) := 1$, иначе $f(u, v) := 0$. Записывается матрица смежности, как таблица

$V \backslash V$	1	2	3	$\dots$	n
1	0	1	0	$\dots$	0
2	1	0	0	$\dots$	1
3	0	0	0	$\dots$	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	0
n	0	0	0	$\dots$	0

Note. Для неориентированных графов матрица симметричная относительно главной диагонали ($i = j$).

Def. Две вершины $u, v \in V$ называются *смежными*, если $(u, v) \in E$
Def. Два *ребра смежные*, если имеют общую вершину.

Def. Вершина v и ребро $(u, v) \in E$ называются *инцидентными*. Наряду с матрицей смежности используется также *матрица инцидентности*, функция $f : V \times E \to \{0, 1\}$, где пара если пара $(v, e), v \in V, e \in E$ инцидентная, то $f(v, e) = 1$, иначе $f(v, e) = 0$. Обозначим $|V| =: n$, $|E| =: m$, тогда матрица будет размера $n \times m$.

$V \backslash E$	e_1	e_2	e_3	$\dots$	e_m
v_1	1	1	0	$\dots$	0
v_2	1	0	0	$\dots$	1
v_3	0	1	1	$\dots$	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	0
v_n	0	0	1	$\dots$	1

Note. В каждом столбце ровно две единицы, а все остальные нули.

Маршруты, пути и простые пути

Def. *Маршрутом* в графе назовём список $(v_1, e_1, v_2, e_2, \dots, v_k, e_k, v_{k+1})$, где $v_i \in V$, $e_i = (v_i, v_{i+1}) \in E$.
Def. *Путём* (цепью) в графе назовём маршрут, в котором все рёбра различны.
Def. *Простым путём* в графе назовём путь, в котором все вершины различны, кроме, возможно, первой и последней.
Def. *Маршрут / путь / простой путь замкнут*, если $v_1 = v_{k+1}$
Def. Замкнутый путь - это *цикл*.
Def. Замкнутый простой путь - это *простой цикл*.

Утверждение 1. Если в графе существует цикл, то и существует простой цикл.
□
Поскольку существует цикл, то распишем его. $(v_1, e_1, v_2, e_2, \dots, v_{k+1} = v_1)$. Возьмём кратчайший фрагмент этой последовательности $(v_i, e_i, \dots, e_{j-1}, v_j = v_i)$, такой, что начальная и конечные вершины совпадают.

1. В этом кратчайшем фрагменте не менее трёх различных вершин (поскольку нет петель и кратных рёбер)
2. Все вершины кроме начала и конца различны
   Следовательно все рёбра различны, все вершины кроме начальной и конечной различны. Значит, этот фрагмент - простой цикл.
   ■

Утверждение 2. Если между двумя несовпадающими вершинами существует маршрут, то существует и простой путь между этими вершинами.
□
Запишем этот маршрут: $(u = v_1, e_1, v_2, e_2, \dots, e_j, v_{j+1} = v)$. На каждом шаге добавляем следующую вершину из маршрута в рассматриваемый фрагмент. Пусть стартуем из фрагмента $\varphi = (v_1, e_1, v_2)$. Если в φ появились повторяющиеся вершины, то удалим из

фрагмента всё, что между ними, и сам повтор. В любой момент времени список является маршрутом. В конце концов получим список, в котором все вершины уникальны.
■

Связность и компоненты связности

Def. Граф называется *связным*, если $\forall u, v \in V$ существует простой путь (маршрут, простой путь) из u в v.
Def. *Подграф* графа $G = (V, E)$ - это **граф** $G' = (V', E')$: $V' \subseteq V, E' \subseteq E$. Рёбра из E' инцидентны только вершинам из V'.
Def. Пусть граф G не является связным. Максимальные по включению связные подграфы называются *компонентами связности*.
Def. *Степень вершины* v в графе G - это количество рёбер, инцидентных v. Обозначается $\deg(v)$. Для ориентированных графов также различают *входящую степень* вершины и *исходящую степень* вершины. Обозначаются $\text{indeg}(v)$ и $\text{outdeg}(v)$ соответственно.

Def. В **ориентированном** графе G вершины u и v *сильно связаны*, если существует путь $u \to v$ и существует путь $v \to u$.

Def. *Полный граф* - это граф, такой, что $\forall u, v \in V \implies (u, v) \in E, (v, u) \in E$. Обозначается

$$\boxed{K_n \text{ - полный граф на } n \text{ вершинах}}$$

Def. *Двудольный граф* - это граф G, такой, что $V = L \cup R$, где $L \cap R = \varnothing$. При этом $\forall e(v_L, v_R) \in E \implies v_L \in L, v_R \in R$.

Def. *Полный двудольный граф* на долях размера n и m обозначается

$$\boxed{K_{n,m} \text{ - полный двудольный граф}}$$

Изоморфизм графов. Деревья.

Общие понятия

Утверждение

$$\sum_{v \in V} \deg v = 2|E|$$

□ Действительно, каждое ребро участвует в степени двух вершин. ■

Утверждение

В графе чётное количество вершин с нечётной степенью.

□ Действительно, из предыдущего утверждения сумма степеней всех вершин чётна, а значит, что эта сумма содержит чётное количество нечётных слагаемых. ■

Изоморфизм графов

Определение

Графы $G_1(V_1, E_1)$ и $G_2(V_2, E_2)$ называются **изоморфными**, если существует биекция $\varphi : V_1 \to V_2$, для которой выполняется $(v, u) \in E_1 \iff (\varphi(v), \varphi(u)) \in E_2$.

Деревья

Теорема (4 эквивалентных определения дерева)

Следующие определения эквивалентны.
Деревом называется:

1. Связный ациклический граф.
2. Между любыми двумя вершинами существует единственный простой путь.
3. Связный граф, такой, что $|V| = |E| + 1$.
4. Ациклический граф, такой, что $|V| = |E| + 1$.

□
$\boxed{1} \to \boxed{2}$. Докажем от противного, пусть простой путь не единственный. Докажем по индукции.
База. Самый длинный из этих простых путей имеет 2 ребра. $u \to t \to v$. Заметим, что второй маршрут - это либо $u \to v$, либо $u \to z \to v$. Тогда утверждение о существовании цикла тривиально.
Шаг. Пусть для всех $k \leq n$ если между вершинами два простых пути длины не более k, то есть цикл. Рассмотрим две вершины, между которыми два простых пути длины не более $n + 1$.
Два пути: $u \to \ldots \to v$, рассмотрим первую вершину после u в обоих путях. Назовём их t, z. Возможны два случая:

1. $t = z$. Тогда нужно применить предположение индукции к паре t, v.
2. $t \neq z$.
   - Все остальные вершины различны. Тогда два пути образуют цикл.

- Есть промежуточная вершина w, повторяющаяся в обоих путях. Следовательно, есть простой путь $u \to w$ - фрагмент первого пути, есть простой путь $u \to w$ - фрагмент второго пути. Эти фрагменты различны ($t \neq z$) и имеют длину не более n. Следовательно, по предположению индукции найдётся цикл.

Таким образом, если простой путь не единственный, то существует цикл. Получили требуемое.

$\boxed{2} \to \boxed{3}$. Поскольку существует единственный простой путь, то граф связный. Докажем утверждение по индукции.

Предположение. Пусть для всех графов с не более n вершинами требуемое выполнено.
База. Одно ребро - $1 + 1 = 2$
Шаг. Рассмотрим граф G, удовлетворяющий $\boxed{2}$ с $n + 1$ вершиной. Рассмотрим две вершины $u, v : (u, v) \in G$. Удалим ребро (u, v). Поскольку между u и v был единственный простой путь, то при удалении ребра (u, v) другого пути между u и v быть не может по $\boxed{2}$. Так что граф перестанет быть связным. Не может быть 3 и более компонент связности. Иначе будет отдельно существовать компонента связности, не содержащая ни u, ни v, а значит и при возвращении ребра (u, v) с ними не связанная, что противоречит связности исходного графа. Применим предположение индукции к каждой из двух получившихся компонент связности. В первой компоненте связности

$$|V_1| = |E_1| + 1$$

Во второй компоненте связности

$$|V_2| = |E_2| + 1$$

Тогда всего

$$|V_1| + |V_2| = |E_1| + |E_2| + 2$$

Но при этом по разделению

$$|E| = |E_1| + |E_2| + 1 \implies |V_1| + |V_2| = |V| = |E| + 1$$

Что и требовалось доказать.

$\boxed{3} \to \boxed{4}$. От противного, пусть в графе, для которого выполняется $\boxed{3}$ есть простой цикл. Рассмотрим этот цикл: $v_1 \to v_2 \to \ldots \to v_m \to v_1$. В этом цикле ровно m рёбер. Рассмотрим вершины, не входящие в цикл. Обозначим их $w_1, w_2, \ldots, w_k$, где $k + m = |V|$. Для каждой w_i рассмотрим кратчайший путь до цикла.
Утверждение. Первые рёбра этих путей попарно различны. От противного, пусть нашлись два кратчайших пути от w_i и от w_j, где первые рёбра совпадают:

$$w_i(w_iw_j)\underbrace{w_j(w_jt_1)t_1\dots v_i}_{l_1 \text{ рёбер}}$$

$$w_j(w_jw_i)\underbrace{w_i(w_iz_1)z_1\dots v_j}_{l_2 \text{ рёбер}}$$

Эти маршруты - кратчайшие простые пути. Предположим без ограничения общности, $l_1 \geq l_2$. Тогда с одной стороны от w_i к циклу кратчайший путь $l_1 + 1$, с другой стороны из пути от w_j можем выделить путь от w_i до цикла длины $l_2 < l_1 + 1$. Противоречие.

Количество рёбер m - из цикла, а также k попарно различных рёбер по одному от каждого кратчайшего пути. Итого $|E| = m + k = |V|$ рёбер. Противоречие, так как заявлено $|E| = |V| - 1$.

$\boxed{4} \to \boxed{1}$. Пусть выполнено $\boxed{4}$. Рассмотрим такой граф. Обозначим k - количество компонент связности. Рассмотрим каждую из компонент связности отдельно. Это связный ациклический граф, значит выполнен пункт $\boxed{1}$, значит, выполняется $\boxed{3}$, значит, $|V_i| = |E_i| + 1$. Сложим все эти равенства

$$\begin{gathered}|V_1| = |E_1| + 1\\ |V_2| = |E_2| + 1\\ \dots\\ |V_k| = |E_k| + 1\end{gathered}$$

Получим $|V| = |E_1| + \ldots + |E_k| + k$. Следовательно, $k = 1$. Что и требовалось доказать. ■

Определение

Изолированная вершина в графе — вершина степени 0.

Определение

Висячая вершина в дереве — вершина степени 1.

Код Прюфера. Остовные деревья. Теорема Кэли. Эйлеровы и гамильтоновы графы и пути.

Код Прюфера

Определение

Пусть дано конечное нумерованное дерево на n вершинах (то есть все вершины пронумерованы и имеют все номера от 1 до n). **Кодом Прюфера** называется последовательность из $n-2$ чисел (от 1 до n), сопоставленная данному дереву по следующему алгоритму:

1. Выбрать в дереве лист с наименьшим номером.
2. Добавить в последовательность номер вершины, с которой он соединён.
3. Удалить из рассмотрения лист вместе с ребром.
4. Повторять, пока не останется одно ребро.

Теорема (б/д)

Декодирование произвольного кода Прюфера существует и единственно. Алгоритм декодирования следующий:
выпишем все номера в список. Первым шагом берём наименьшую по номеру вершину из списка, не присутствующую в коде, соединяем с вершиной под первым номером в коде. Удаляем первый элемент из кода и рассмотренный элемент из списка. Повторяем до тех пор, пока код не опустеет. После этого соединяем два оставшихся элемента.

Теорема

Функция (алгоритм), которая сопоставляет дереву код Прюфера биективна.

□
Докажем биективность в несколько шагов.

Шаг 1. Покажем, что кодирование однозначное, то есть каждому дереву соответствует ровно один код Прюфера. Действительно, из алгоритма не возникает ситуации, когда приходится выбирать одну из нескольких вершин, поскольку все вершины имеют разные номера и выбираются по возрастанию номеров, если на очередном шаге существует несколько листов.

Каждому дереву соответствует ровно один код Прюфера, следовательно, это функция. Обозначим функцию, которая сопоставляет дереву код Прюфера как σ.

Шаг 2. Покажем, что σ сюръективна. Для этого опишем алгоритм, который последовательности $\{a_1, a_2, \ldots, a_{n-2}\}, a_i \in 1, 2, \ldots, n, \forall i \in \{1, \ldots, n-2\}$ сопоставляет исходное дерево. Алгоритм декодирования:

1. Выпишем в список все номера от 1 до n по одному разу.
2. Выберем наименьшую по номеру вершину из списка, не присутствующую в коде. Соединим её с вершиной под первым номером в коде.
3. Удалим первый элемент из кода Прюфера и рассмотренную вершину из списка.
4. Повторяем действия 2-3, пока код Прюфера не опустеет.
5. Соединим оставшиеся две вершины в списке ребром.

Почему мы получим исходное дерево после применения этого алгоритма декодирования? Предлагается доказать этот факт по индукции самостоятельно.

Таким образом, σ сюръективна, поскольку для каждого кода Прюфера мы умеем восстанавливать хотя бы одно дерево, из которого можно получить этот код.

Шаг 3. Докажем инъективность отображения σ из дерева в код по индукции.

> Заметим, что в коде Прюфера каждая вершина встретится ровно $\deg v - 1$ раз (мы записываем вершину ровно столько раз, пока она не станет листом, а это ровно $\deg v - 1$ раз).

Пусть есть два различных дерева $T_1 \neq T_2$. Будем рассматривать $\sigma(T_1)$ и $\sigma(T_2)$.

База. На трёх пронумерованных вершинах существует ровно три различных дерева: в каждом из них одна вершина имеет степень 2 (центр), а две другие — степени 1 (листья). Код Прюфера такого дерева состоит из одного элемента — номера центральной вершины. Поскольку $T_1 \neq T_2$, центры разные, значит, коды разные.

Шаг. Пусть для всех деревьев с количеством вершин не более N утверждение выполнено. То есть из $T_1 \neq T_2$ следует $\sigma(T_1) \neq \sigma(T_2)$. Рассмотрим дерево на $N+1$ вершине. Обозначим наименьший номер листа в T_1 как k_1, наименьший номер листа в T_2 как k_2. Возможны три случая:

1. $k_1 \neq k_2$. Без ограничения общности будем считать, что $k_1 < k_2$. А значит, что вершина с номером k_1 не является листом в T_2 (иначе бы она была выбрана в T_2, поскольку $k_1 < k_2$). Заметим, что $\sigma(T_1)$ не содержит k_1 (так как $\deg k_1 = 1$ в T_1), но код $\sigma(T_2)$ содержит k_1, так как степень вершины $k_1 \geq 2$ в T_2, а значит, она встретится в коде хотя бы один раз. Таким образом, коды различные.

2. $k_1 = k_2 = k$, но смежные с k вершины T_1 и T_2 различны. Тогда $\sigma(T_1) \neq \sigma(T_2)$, поскольку у них отличается первое число (коды Прюфера начинаются с разных чисел).
3. $k_1 = k_2 = k$, смежная вершина с k в T_1 и T_2 одинаковая. Тогда применим один шаг алгоритма. Рассмотрим коды $\sigma(T_1)$ и $\sigma(T_2)$ без первого элемента и T_1 и T_2 без вершины kПрименим предположение индукции и получим $\sigma(T_1) \neq \sigma(T_2)$. Замечание: теперь деревья T_1 и T_2 стали размера N, но числа на вершинах и в коде Прюфера достигают значения $N + 1$. Но поскольку в алгоритме нам важно, что между вершинами введён строгий порядок, то это не изменит доказательства.

Таким образом, σ инъективна.

σ инъективна и сюръективна, значит σ биективна.
■

Остовные деревья и теорема Кэли

> **Определение**
>
> **Остовное дерево** графа G — это подграф, включающий в себя все вершины G и являющийся деревом.

> **Теорема Кэли (о числе деревьев)**
>
> Количество деревьев на n различных (пронумерованных) вершинах равно n^{n-2}. (Количество остовных деревьев у полного графа на n вершинах равно n^{n-2})

□
Ранее мы доказали, что алгоритм, переводящий дерево в код Прюфера инъективен. Заметим, что мы попутно с этим доказали и теорему Кэли. Действительно, код Прюфера для дерева из n вершин содержит $n - 2$ числа. Каждое из чисел — одно из n номеров вершин дерева. Таким образом, всего возможно n^{n-2} различных кодов Прюфера, следовательно, и различных деревьев.
■

Эйлеровы графы и их свойства

> **Определение**
>
> Граф называется **эйлеровым**, если существует цикл, проходящий по каждому ребру ровно один раз. При этом граф (связный) / (без изолированных вершин) / (цикл

посещает все вершины, но необязательно один раз). Соответствующий цикл называют **эйлеровым циклом**.

По аналогии вводится понятие **эйлерова пути**.

Теорема

Следующие утверждения эквивалентны:

1. Граф эйлеров.
2. Все степени вершин чётные.
3. Рёбра графа можно разбить на непересекающиеся по рёбрам циклы.

□
$\boxed{1} \Rightarrow \boxed{2}$. Следует из чётности количества рёбер, входящих в путь и смежных с каждой отдельно рассматриваемой вершиной.
$\boxed{2} \Rightarrow \boxed{3}$. Стартуем из произвольной вершины, строим цикл пока он не замкнётся. Следующий шаг всегда можно сделать по чётности степеней. Удалить все рёбра цикла. Повторить.
$\boxed{3} \Rightarrow \boxed{1}$.
Доказательство по индукции по количеству непересекающихся циклов.
База. Если цикл один, то это и есть эйлеров цикл.
Шаг. Пусть для графов, распадающихся на не более n циклов, утверждение верно. Рассмотрим граф с $n+1$ циклом.
Рассмотрим (и запишем) $n+1$-ый цикл:

$$v_1 e_1 v_2 e_2 \dots e_{k-1} v_k$$

Удалим его из графа. Новый граф распадается на m компонент связности, для каждой из которых выполнено предположение индукции. Следовательно, для каждой компоненты связности есть эйлеров цикл (рёбра всех циклов разных связности попарно различны). Существует эйлеров цикл, в который входит вершина из $\{v_1, \dots, v_k\}$, поскольку исходный граф был связным. Возможны несколько случаев:

1. Компонент больше одной. Рассмотрим вершины u и w из разных компонент, связанных в исходном графе путём, следовательно, путь проходил через удалённые рёбра (то есть содержал одно или несколько рёбер из $\{e_1, \dots, e_{k-1}\}$). Значит, содержал и хотя бы одну из вершин $\{v_1, \dots, v_k\}$. Рассмотрим первое ребро, выходящее за пределы этой компоненты связности. Оно может соединяться только с вершиной v_i. Для каждой компоненты перечислим цикл, начиная с v_i. Получим цикл, проходящий по каждому ребру ровно один раз.

2. Компонента связности одна, и это эйлеров граф, содержащий все вершины исходного графа.

■

Гамильтоновы графы

> **Определение**
>
> Граф называют **гамильтоновым**, если существует цикл, проходящий по каждой вершине ровно один раз. Соответствующий цикл называют **гамильтоновым циклом**.

По аналогии вводится понятие **гамильтонова пути**.

Двудольные графы. Лемма Холла.

Def. *Двудольный граф* - это граф G, такой, что $V = L \cup R$, где $L \cap R = \varnothing$. При этом $\forall e(v_L, v_R) \in E \implies v_L \in L, v_R \in R$.

Def. Граф называется *k-раскрашиваемым*, если существует раскраска вершин в k цветов, такая что никакие 2 смежные вершины не имеют одного цвета. Такая раскраска называется *правильной*.

Утверждение. Любое дерево 2-раскрашиваемо.

Теорема. Следующие утверждения эквивалентны.

1. Граф двудольный
2. Граф 2-раскрашиваем
3. В графе нет циклов нечётной длины

□

Заметим, что $1 \iff 2$ тривиально, поскольку это одни и те же условия.
$1 \Rightarrow 3$. Пусть граф двудольный, то есть $V = L \cup R$. Рассмотрим произвольный цикл по вершинам.

$$v_{L_1}, v_{R_1}, v_{L_2}, v_{R_2}, \dots, v_{R_k}, v_{L_1}$$

Если последняя вершина в цикле из левой доли, то предпоследняя точно из правой доли, а значит, из чередования вершин из разных долей, количество рёбер в цикле чётно.

$3 \Rightarrow 2$. В графе G нет циклов нечётной длины. Возьмём от каждой компоненты связности остовное дерево и раскрасим его в два цвета. Покажем, что это правильная раскраска. Действительно, если бы существовало ребро из G, но из остовных деревьев,

соединяющее две вершины одного цвета (в одном и том же дереве!). Но тогда получим, что существует цикл нечётной длины проходящий, через эти две вершины. Противоречие, значит, раскраска правильная. Следовательно, граф 2-раскрашиваем.
■

Def. *Паросочетание* - это набор несмежных рёбер.

Def. *Вершинное покрытие* $S \subseteq V$ - это подмножество вершин графа $G(V, E)$ такое, что каждое ребро инцидентно по крайней мере одной вершине из S.

Def. Пусть $|L| \leq |R|$. Паросочетание называют *совершенным*, если каждая вершина из L инцидентна какому-то ребру из паросочетания.

Лемма Холла (о существовании совершенного паросочетания). В двудольном графе G ($|L| \leq |R|, |L| \geq 2$) существует совершенное паросочетание тогда и только тогда, когда $\forall X \subseteq L$ смежно не менее, чем с $|X|$ вершин из правой доли.
Вершину считаем смежными с множеством X, если она смежна по крайней мере с одной вершиной из X.

□
⇒
Если совершенное паросочетание существует, то $\forall X \subseteq L$ ровно $|X|$ вершин из доли R смежно с X по рёбрам паросочетания.
⇐
Пусть выполняется условие о количестве смежных. Если в графе построено паросочетание размера $k < |L|$, то есть паросочетание размера $k + 1$. Докажем это утверждение по индукции.
База. Изначально паросочетание пустое, а между L и R есть рёбра. Значит, есть по крайней мере одно ребро. Добавим его, получим паросочетание размера 1.
Шаг. Пусть построено паросочетание размера k. Поскольку $k < |L|$, то в левой доле есть вершина $x \in L$, не участвующая в паросочетании. Ориентируем рёбра из паросочетания из R в L, а остальные наоборот из L в R. Рассмотрим все вершины, достижимые из x (с учётом ориентации рёбер), обозначим это множество H. Обозначим H_L - множество вершин из H, лежащих в левой доле, H_R - множество вершин из H, лежащих в правой доле. Покажем, что в H есть вершина $y \in R$, не участвующая в паросочетании. Действительно, если бы все вершины из H_R участвовали в паросочетании, то по обратным рёбрам из паросочетания каждая вершина дополняет H вершиной своей пары в левой доле. Поэтому, если бы все H_R участвовали в паросочетании, то $|H_L| > |H_R|$, поскольку для каждой вершины из R есть ровно одна вершина из L, да ещё вершина x. Это противоречит условию леммы, поскольку множество H_L смежно только с H_R и при этом $|H_L| > |H_R|$. Следовательно, в H есть вершина $y \in R$, не участвующая в паросочетании. Рассмотрим путь $x \to y$. Заметим, что первое ребро будет строго не из паросочетания, второе строго из паросочетания, третье строго не из паросочетания и так далее. Заметим, что все эти вершины из пути смежны только с рёбрами паросочетания,

принадлежащим пути. Для x, y это выполнено, для остальных также тривиально. Исключим из паросочетания рёбра $(v_1, v_2), (v_3, v_4), \ldots, (v_{2k-1}, v_{2k})$ и добавим в него $(x, v_1), (v_2, v_3), \ldots, (v_{2k}, y)$. Заметим, что все вершины из пути по прежнему смежны только с рёбрами паросочетания, принадлежащим пути. И мы показали, что можем увеличить паросочетание на 1. Что и требовалось доказать.
■

Отношения порядка. Диаграмма Хассе. Ориентированные графы.

Отношение эквивалентности

Определение

Отношение эквивалентности $x \sim y$, $x \equiv y$ — это бинарный предикат $\sim: M \times M \to \{\text{True}, \text{False}\}$ (другими словами $(\sim)$ задаёт подмножество $S_\sim \subseteq M \times M$), удовлетворяющий следующим аксиомам:

1. $x \sim x$ — рефлексивность
2. $x \sim y \iff y \sim x$ — симметричность
3. $x \sim y, y \sim z \implies x \sim z$ — транзитивность

Отношения частичного порядка

Определение

Отношение частичного порядка — это бинарное отношение, которое удовлетворяет следующим аксиомам. Отношение частичного порядка бывает строгое $(\prec)$ и нестрогое $(\preccurlyeq)$.

Строгое	Нестрогое
1) $x \not\prec x$ — антирефлексивность	1) $x \preccurlyeq x$ — рефлексивность
2) $\forall x, y \Rightarrow ((x \prec y) \wedge (y \prec x)) = \text{False}$ — антисимметричность	2) $(x \preccurlyeq y) \wedge (y \preccurlyeq x) \implies x = y$ — антисимметричность
3) $x \prec y, y \prec z \implies x \prec z$ — транзитивность	3) $x \preccurlyeq y, y \preccurlyeq z \implies x \preccurlyeq z$ — транзитивность

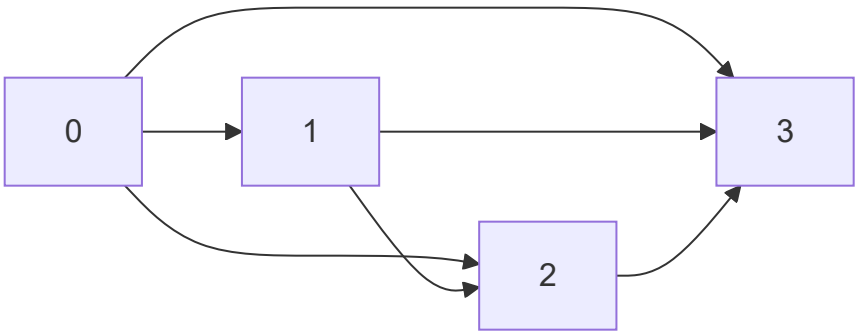
Note. Если $\forall x, y : (x \preccurlyeq y) \vee (y \preccurlyeq x)$, то такое отношение частичного порядка называют *линейным порядком*.

Ориентированный граф частичного порядка. Диаграмма Хассе.

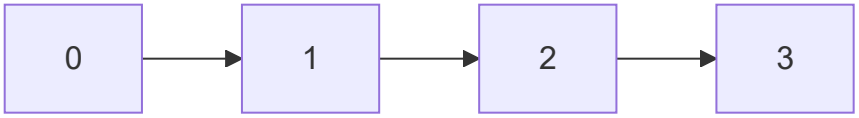
Определение

Ориентированный граф частичного порядка $G(V, E)$, $V \leftrightarrow M$
$(u, v) \in E \iff u \underset{(\preccurlyeq)}{\prec} v$

Пример. Граф частичного порядка для чисел $0, 1, 2, 3$ и порядку над ними из аксиом $\mathbb{N}$:



По транзитивности можно было бы оставить



Определение (отношение непосредственного следования)

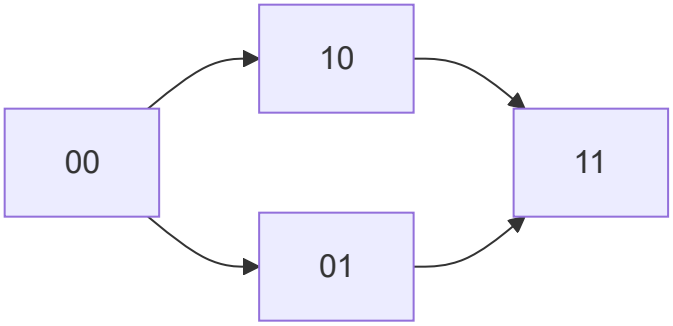
Пусть дано отношение частичного порядка ($\preccurlyeq$), $\preccurlyeq_n$. Будем говорить, что y **непосредственно следует** за x, если с одной стороны выполняется $x \preccurlyeq y$ и нет такого z, что $z \neq x, z \neq y$ и $x \preccurlyeq z, z \preccurlyeq y$.

Определение

Диаграмма Хассе — это (2 эквивалентных определения):

1. Граф отношения частичного порядка после транзитивной редукции
2. Граф отношения непосредственного следования

Пример (булев кубик порядка 2):



Note. Для нестрогого отношения частичного порядка также есть n петель.

Ориентированные графы

Определение

Между вершинами u и v орграфа G есть отношение **двухсторонней достижимости**, если существует путь (маршрут) $u \rightsquigarrow v$ и путь (маршрут) $v \rightsquigarrow u$.

Упражнение. Покажите, что отношение двусторонней достижимости — это отношение эквивалентности. Доказательство этого факта предлагается провести самостоятельно.

Определение

Классы эквивалентности относительно этого порядка называются **компонентами сильной связности**.

Определение

Ациклический ориентированный граф — это ориентированный граф, в котором нет замкнутых маршрутов положительной длины.

Теорема (эквивалентные определения ациклического орграфа)

Следующие условия эквивалентны (граф без петель):

1. Орграф G ациклический
2. Каждая компонента сильной связности имеет размер 1
3. Существует нумерация вершин такая, что $(u_i, u_j) \in E \Rightarrow i < j$

□
$\boxed{1} \Leftrightarrow \boxed{2}$ почти очевидно
$\boxed{3} \Rightarrow \boxed{1}$
Докажем от противного. Действительно, если бы существовал замкнутый маршрут, то мы бы получили маршрут

$$v_{i_1} \to v_{i_2} \to v_{i_3} \to \ldots \to v_{i_n} = v_{i_1}$$

И при этом

$$i_1 < i_2 < \ldots < i_n = i_1$$

Противоречит антисимметричности и антирефлексивности натуральных чисел
$\boxed{1} \Rightarrow \boxed{3}$
Докажем сначала, что если ориентированный граф ациклический, то в нём есть вершина с нулевой исходящей степенью.

Граф ациклический, значит все пути ограниченной длины. Рассмотрим путь наибольшей длины.

$$v_{i_1} \to v_{i_2} \to \ldots \to v_{i_k}$$

Все v_i различны из ацикличности. Если бы у v_{i_k} исходящая степень была бы не равна нулю, то мы бы могли добавить в этот путь ещё одно ребро и увеличить длину пути.

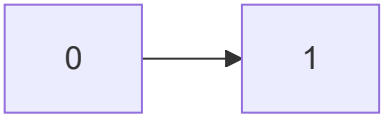
Докажем теперь требуемое по индукции по количеству вершин в графе G.
База. Если $n = 1$, то предположение выполнено.
Шаг. Пусть утверждение выполняется для всех $G(V, E) : |V| \leq n$. Рассмотрим ациклический орграф $G'(V', E') : |V'| = n + 1$. По только что доказанному утверждению в этом графе существует вершина с нулевой исходящей степенью. Сопоставим этой вершине номер $n + 1$ и удалим из рассмотрения. Для оставшегося графа существует требуемая нумерация числами от 1 до n. Что и требовалось доказать.
■

Note. Граф отношения частичного порядка ациклический, также существует нумерация вершин

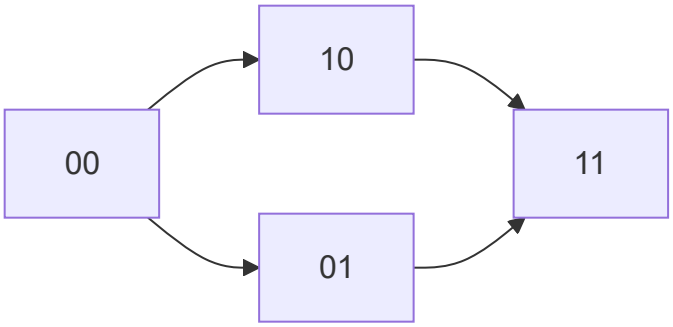
Note. Пусть дано отношение частичного порядка $(M, \prec)$. Рассмотрим граф частичного порядка. Он ациклический. Следовательно, существует нумерация вершин как в условии $\boxed{3}$. Дополним заданное отношение $(\prec)$ до линейного в соответствии с нумерацией и получим линейный порядок на исходном множестве.

Примеры графов частичного порядка

Булев кубик размера 1



Булев кубик размера 2



$a \leq b$ для всех $i \Rightarrow a_i \leq b_i$.

Булев кубик размера 3: