# Группы. Примеры числовых и нечисловых групп. Порядок элементов. Порядок группы. Циклическая группа. Порождающие элементы. Таблица Кэли

# 1 Группы

**Определение 1.1.** *Пусть есть множество $M$ и операция $\circ$, а также выполняется:*

*0. замкнутость относительно операции* $\forall a, b \in M \hookrightarrow (a \circ b) \in M$

*1. ассоциативность* $\forall a, b, c \in M \hookrightarrow a \circ (b \circ c) = (a \circ b) \circ c$

*2. существование нейтрального* $\exists!\ e : \forall a \in M \hookrightarrow a \circ e = e \circ a = a$

*3. существование обратного* $\forall a \in M\ \exists!\ a^{-1} \in M : a \circ a^{-1} = a^{-1} \circ a = e$

*Тогда будем говорить, что* $(M, \circ)$ *- группа.*

**Замечание 1.1.** *При выполнении замкнутости:*
*Выполнение первого пункта* $\Longleftrightarrow$ *полугруппа.*
*Выполнение первого и второго пунктов* $\Longleftrightarrow$ *моноид.*
*Выполнение трёх пунктов + коммутативность* $\forall a, b \in M \hookrightarrow a \circ b = b \circ a \Longleftrightarrow$ *абелева группа.*

**Замечание 1.2.** *Существует два варианта записи: мультипликативная и аддитивная. Их использовать одновременно НЕЛЬЗЯ*

| **Мультипликативная** | **Аддитивная** |
|---|---|
| $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ | $(a + b) + c = a + (b + c)$ |
| $\exists! e$ `(обознач."1"):` $a \cdot 1 = 1 \cdot a = a$ | $\exists! e$ `(обознач."0"):` $a + 0 = 0 + a = a$ |
| `Обр.:` $\exists! x^{-1} : x \cdot x^{-1} = x^{-1} \cdot x = 1$ | `Обр.:` $\exists! - x : x + (-x) = (-x) + x = 0$ |

# 2 Примеры числовых и нечисловых групп

## 2.1 Числовые группы

- $(\mathbb{Z}_m, +)$: нейтральный - 0, обратный - $(m - a)$
- $(\mathbb{Z}_p \backslash \{0\}, \times)$: нейтральный - 1, обратный - $a^{p-2}$

## 2.2 Нечисловые группы

- Группа перестановок (об этом в третьем билете темы)
- Группа симметрий правильного n-угольника (группа Диэдра): повороты и осевые симметрии, переводящие многоугольник в себя. Нейтральный - поворот на 0, обратный - поворот на $2\pi - \alpha$ или такая же симметрия

# 3 Порядки групп и элементов в группе

**Определение 3.1.** *Группу $G$ будем называть конечной, если* $|G| \in \mathbb{N}$.

**Определение 3.2.** *Порядок конечной группы - количество элементов* $|G|$.

**Определение 3.3.** *Порядок элемента* $a \in G$ *- наименьшее* $m \in \mathbb{N} : a^m = e$.

**Замечание 3.1.** *В конечной группе порядки элементов конечны. Порядок элемента не больше порядка группы.*

*Доказательство.* Возьмём какой-то $a \in G$. Рассмотрим его степени от 1 до $|G|+1$. По принципу Дирихле найдутся хотя бы две степени, значения которых совпадут, так как в группе всего $|G|$ элементов, а степень не выводит за пределы группы. Получаем ситуацию $a^i = a^j \implies a^{|i-j|} = e$. Тогда $ord(a) \mid |i-j|$, а $|i-j| \leqslant |G|$. □

**Лемма 3.1.** *Если $a^m = e$, то $ord(a) \mid m$.*

*Доказательство.* Пусть $m = ord(a) * q + r$, где $q \in \mathbb{Z},\ 0 \leqslant r < ord(a)$. Тогда $a^m = a^{ord(a)*q+r} = (a^{ord(a)})^q * a^r$. Но $a^m = e = e^q = (a^{ord(a)})^q$. Получаем $a^r = e$. Так как $ord(a)$ - наименьшая подходящая натуральная степень, а $r < ord(a)$, то $r = 0$. □

## 4 Циклическая группа. Порождающие элементы

**Определение 4.1.** *Группа $G$ называется циклической, если $\exists a \in G : \forall b \in G\ \exists m \in \mathbb{Z} : a^m = b$. При этом $a$ называется порождающим элементом.*

**Замечание 4.1.** *Группа не обязана быть конечной. Порождающий элемент a может быть не единственным. Например $(\mathbb{Z}, +)$ - элементов бесконечно, порождающим может быть как 1, так и -1.*

**Замечание 4.2.** *Конечные циклические группы ($|G| = m$) будем обозначать $C_m$.*

**Замечание 4.3.** *Порядок порождающего равен порядку группы $ord(a) = |G|$.*

## 5 Таблица Кэли

**Определение 5.1.** *Таблица Кэли (нет в программе, но может пригодиться) - это квадратная таблица, которая описывает операцию в конечной группе.*

**Замечание 5.1.** *В каждой строке и каждом столбце элементы не повторяются.*

*Доказательство.* Пусть в строке встретилось 2 одинаковых элемента. Тогда выполнено равенство $c \circ d = c \circ k$. Домножим на $c^{-1}$ слева и получим $d = k \implies$ это один и тот же столбец. □

Примеры таблиц Кэли:

| $\cdot$ | $e$ | $a$ |
|---|---|---|
| $e$ | $e$ | $a$ |
| $a$ | $a$ | $e$ |

| $\cdot$ | $e$ | $a$ | $b$ |
|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ |
| $a$ | $a$ | $b$ | $e$ |
| $b$ | $b$ | $e$ | $a$ |

| $\cdot$ | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $b$ | $c$ | $e$ |
| $b$ | $b$ | $c$ | $e$ | $a$ |
| $c$ | $c$ | $e$ | $a$ | $b$ |

| $\cdot$ | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $e$ | $c$ | $b$ |
| $b$ | $b$ | $c$ | $e$ | $a$ |
| $c$ | $c$ | $b$ | $a$ | $e$ |

## 6 На посмеяться после тяжёлого бота

Сидишь техаешь билет, хочешь вставить таблицу со сравнением мультипликативной и аддитивной записей, просишь помочь квен, а он такой:


Identity
Inferierse
Closevroperty
Associatiive
Example