НАТУРАЛЬНЫЕ ЧИСЛА

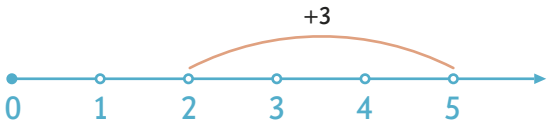
Изучение математики начинается со счета предметов.
Так возникает множество **натуральных** чисел:

$\mathbb{N} = \{1, 2, 3, \dots\}$

координатный луч

Натуральные числа могут быть изображены на координатном луче точками, причем расстояние между каждыми соседними равно единичному отрезку.

Операция сложения "+" на множестве натуральных чисел соответствует сдвигу вдоль координатного луча вправо.



$2 + 3 = 5$

Операция "+" не выводит за пределы $\mathbb{N}$
($\mathbb{N}$ замкнуто относительно сложения).

ПРОБЛЕМЫ В $\mathbb{N}$:

1. Операция вычитания "-", как сдвиг вдоль координатного луча влево, не всегда возможна;

2. Реальная ситуация → Математическая модель

Днем температура воздуха повысилась на 5° и стала равной 3°. Какой температура была ночью?

Уравнение $x + 5 = 3$

НЕРАЗРЕШИМО В $\mathbb{N}$

ЦЕЛЫЕ ЧИСЛА

Множество **целых** чисел $\mathbb{Z} = \{0, \pm1, \pm2, \pm3, \dots\}$ получается добавлением к $\mathbb{N}$ отрицательных чисел и 0.

$x = -2 \in \mathbb{Z}$ есть решение уравнения $x + 5 = 3$.
$-2 = 3 - 5$.

Целые числа могут быть изображены на координатной прямой:

координатная прямая

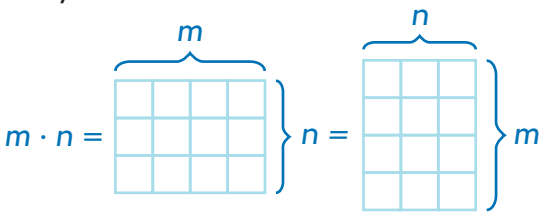
- сложение (сдвиг вправо) и вычитание (сдвиг влево) не выводят за пределы $\mathbb{Z}$;
- 0 — нейтральный элемент по сложению:

$\forall\, m \in \mathbb{Z}$ 1) $m + 0 = 0 + m = m$;
2) $-m + m = m + (-m) = 0$.

Операция умножения "·" вводится через сложение:

$$m \cdot n = \underbrace{m + m + \dots + m}_{n \text{ раз}} = \underbrace{n + n + \dots + n}_{m \text{ раз}}$$

Для натуральных чисел результат умножения есть площадь прямоугольника:



- Множество $\mathbb{Z}$ замкнуто относительно умножения:
  $\forall\, m, n \in \mathbb{Z} \quad m \cdot n \in \mathbb{Z}$
- 1 — нейтральный элемент по умножению:
  $\forall\, m \in \mathbb{Z} \quad m \cdot 1 = 1 \cdot m = m.$

ПРОБЛЕМА:

1 ▶ Реальная ситуация ➡ Математическая модель

Как разделить 3 яблока поровну между 5 ребятами?

Уравнение $x \cdot 5 = 3$

НЕРАЗРЕШИМО В $\mathbb{Z}$

РАЦИОНАЛЬНЫЕ ЧИСЛА

Множество **рациональных** чисел $\mathbb{Q} = \{m/n$, где $n \in \mathbb{N}, m \in \mathbb{Z}\}$ помимо целых содержит все дроби.

$$x \cdot 5 = 3 \;\Rightarrow\; x = \frac{3}{5} \in \mathbb{Q}$$

Чтобы построить дробь 3/5 на координатной прямой, нужно разделить единичный отрезок на 5 равных частей и отложить от начала координат 3 такие части.

- Рациональные числа можно складывать, вычитать и умножать;
- Рациональные числа можно делить на отличное от 0 число;
- На числовой прямой множество $\mathbb{Q}$ всюду плотно (в любом сколь угодно малом интервале содержится бесконечно много дробей).

ПРОБЛЕМА:

1 ▶ Реальная ситуация ➡ Математическая модель

Как отмерить на координатной прямой отрезок, длина которого равна диагонали квадрата со стороной 1?

Уравнение $x^2 = 2$

НЕРАЗРЕШИМО В $\mathbb{Q}$

ВЕЩЕСТВЕННЫЕ ЧИСЛА

Множество **вещественных (действительных)** чисел $\mathbb{R}$ содержит все точки координатной прямой.

$\mathbb{R}$ получается добавлением к $\mathbb{Q}$ **иррациональных** чисел, таких как $\sqrt{2}$, $\sqrt{3}$ и т. д.

$$x^2 = 2 \;\Rightarrow\; x = \sqrt{2} \in \mathbb{R}$$

ПРОБЛЕМА:

Уравнение $x^2 + 1 = 0$ НЕРАЗРЕШИМО В $\mathbb{R}$

3 ГРУППЫ, КОЛЬЦА, ПОЛЯ

ОПРЕДЕЛЕНИЕ

Группа — это множество, на котором задана операция *, обладающая следующими свойствами:

1. $a*(b*c) = (a*b)*c$ (закон ассоциативности);
2. существование единицы: $a*1 = 1*a = a$;
3. существование обратного: $a^{-1}*a = a*a^{-1} = 1$.

Если $a*b = b*a$ (закон коммутативности), то группа называется коммутативной (**абелевой**).

ПРИМЕРЫ:

Множество	Операция
$\mathbb{Z}/m\mathbb{Z}$ (остатки по модулю m)	$+$ (абелева)
$\mathbb{Z}$	$+$ (абелева)
$\mathbb{Q}\backslash\{0\}$ (без нуля)	$\cdot$ (абелева)
движения прямой	$\circ$
движения окружности	$\circ$
движения плоскости	$\circ$
S_n (перестановки)	$\circ$

ОПРЕДЕЛЕНИЕ

Кольцо* — это абелева группа по сложению с операцией умножения такая, что

1. $a \cdot (b + c) = a \cdot b + a \cdot c$ (закон дистрибутивности);
2. $a \cdot b = b \cdot a$
3. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
4. $a \cdot 1 = a$.

ПРИМЕРЫ: $\mathbb{Z}$, $\mathbb{Z}/m\mathbb{Z}$, $\mathbb{Q}\backslash\{0\}$.

ОПРЕДЕЛЕНИЕ

Поле — это кольцо,в котором
$\forall\, a \neq 0\ \exists\, a^{-1}$ (обратный элемент): $a \cdot a^{-1} = 1$.

Таким образом, поле является абелевой группой по сложению, а без нуля — абелевой группой по умножению.

ПРИМЕРЫ: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}/p\mathbb{Z}$, где p — простой модуль.
$\mathbb{Z}$ полем не является.

ПРИМЕЧАНИЕ* мы будем рассматривать только коммутативные ассоциативные кольца с единицей, хотя существуют и другие.