Множество вещественных чисел

Опр: 1. Множество F с операциями $+$ и $\cdot$ называется полем, если выполняются следующие условия:

1. $(F,+)$ - абелева группа:
   (a) $\forall a,b,c \in F,\ a+(b+c)=(a+b)+c$ (ассоциативность);
   (b) $\exists\, 0\colon\ \forall a \in F,\ 0+a=a+0=a$ (существование нулевого элемента);
   (c) $\forall a \in F,\ \exists(-a)\colon a+(-a)=(-a)+a=0$ (существование обратного элемента);
   (d) $\forall a,b \in F,\ \ a+b=b+a$ (абелевость);
2. $(F\setminus\{0\},\cdot)$ - абелева группа:
   (a) $\forall a,b,c \in F,\ a\cdot(b\cdot c)=(a\cdot b)\cdot c$ (ассоциативность);
   (b) $\exists\, 1\neq 0\colon\ \forall a \in F,\ 1\cdot a=a\cdot 0=a$ (существование нулевого элемента);
   (c) $\forall a\neq 0 \in F,\ \exists a^{-1}\colon a\cdot a^{-1}=a^{-1}\cdot a=1$ (существование обратного элемента);
   (d) $\forall a,b \in F,\ a\cdot b=b\cdot a$ (абелевость);
3. $a\cdot(b+c)=a\cdot b+a\cdot c$ (дистрибутивность);

Примеры полей:

(1) $\mathbb{Q}$ - множество рациональных чисел (см. книгу Ландау для проверки свойств);

(2) $\mathbb{Z}_p$, p - простое;

Рассмотрим $\mathbb{Z}_p$: $m\sim n \Longleftrightarrow m-n \,\vdots\, p$ (одинаковые остатки при делении на p).
Классы эквивалентности: $0,1,2,\ldots,p-1$ - остатки при делении на p. Можно проверить, что $\mathbb{Z}_p$ (p - простое) - является полем.
В поле $\mathbb{Z}_p$ есть свойство $\underbrace{1+1+\ldots+1}_{\text{p}}=0$ в таком случае говорят, что задано поле характеристики p.

Если ноль никогда не получают, то говорят, что поле - характеристики 0.

$\mathbb{Z}_p \Rightarrow \underbrace{1+1+\ldots+1}_{\text{p}}=0$ - поле характеристики p.

$\mathbb{Q} \Rightarrow 1,\ 1+1,\ 1+1+1,\ \ldots$ - не будет 0, то есть это поле характеристики 0 (надо 0 раз сложить 1).

Опр: 2. Поле F называется упорядоченным, если на F задан линейный порядок (любые два элемента можно сравнивать), такой, что:

1) $\forall a,b,c \in F,\ a\le b \Leftrightarrow a+c\le b+c$;

2) $\forall a,b,c \in F,\ a\le b \wedge c\ge 0 \Rightarrow ac\le bc$;

Пример упорядоченного поля: $\mathbb{Q}$ - множество рациональных чисел.

Утв. 1. $1>0$

$\square$ Предположим противное $1<0 \Rightarrow$ вычитаем 1 справа и слева $\Rightarrow 0<-1 \Rightarrow$ умножим на $(-1) \Rightarrow$ по второму свойству $0<1$ - противоречие. $\blacksquare$

Тогда по свойству (1) получим, что $1+1>1>0$ и так далее. Поэтому упорядоченное поле всегда имеет характеристику поля 0.

Rm: 1. Элементы упорядоченного поля: $1, 1+1, \ldots, \underbrace{1+1+\ldots+1}_{\text{n}}, \ldots$ отождествляются с множеством натуральных чисел и обозначаются $\mathbb{N}$. (см. В.А. Зорич, 1-ый том для формального отождествления - индуктивные множества).

Rm: 2. Элементы вида $\dfrac{m}{n} = m \cdot n^{-1}$, где $m \in \mathbb{Z} = \mathbb{N} \cup \{-n \mid n \in \mathbb{N}\}$ и $n \in \mathbb{N}$ называем дробями, а их множество - множеством рациональных чисел $\mathbb{Q}$.

Опр: 3. Множество $\mathbb{R}$ называется множеством действительных или множеством вещественных чисел, если $\mathbb{R}$ - упорядоченное поле, на котором выполняется **аксиома полноты**:

Если $A \subset \mathbb{R}$, $A \neq \varnothing$, $B \subset \mathbb{R}$, $B \neq \varnothing$ и "$A \leq B$" (то есть $a \leq b$, $\forall a \in A$, $b \in B$), то $\exists c \in \mathbb{R}$, которое разделяет A и B, то есть $a \leq c \leq b$, $\forall a \in A$, $b \in B$.

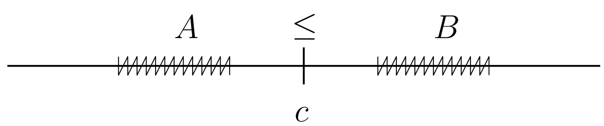

Рис. 1: Аксиома полноты

Смысл аксиомы полноты - дырок нет. Где есть дыры? Зачем аксиома полноты?

Утв. 2. В $\mathbb{Q}$ существуют дыры.

Например, между $A = \{\, x : x > 0 \wedge x^2 < 2 \,\}$ и $B = \{\, x : x > 0 \wedge x^2 > 2 \,\}$ нет элементов из $\mathbb{Q}$.

□ Проверим, что $A \leq B$: $x^2 < 2$, $y^2 > 2 \Rightarrow y^2 > x^2 \Rightarrow y^2 - x^2 > 0$, $(y-x)\underbrace{(y+x)}_{>0} > 0 \Rightarrow y - x > 0 \Rightarrow y > x$.

Пусть $\exists c$: $A \leq c \leq B \Rightarrow$ рассмотрим 3 варианта: (1) $c^2 > 2$, (2) $c^2 < 2$, (3) $c^2 = 2$. Покажем, что ни один из них - невозможен:
(3) $c^2 = 2$, представим c в виде $c = \dfrac{p}{q}$ - не сократима (так как рассматриваем множество рациональных чисел) т.е. НОД$(p, q) = 1 \Rightarrow p^2 = 2q^2 \Rightarrow p = 2k$, так как в квадрате только четные числа дают четные. Тогда $4k^2 = 2q^2 \Leftrightarrow 2k^2 = q^2 \Rightarrow q = 2m$, получили, что p и $q \,\vdots\, 2 \Rightarrow$ противоречие.

(2) $c^2 < 2$. Найдем $\varepsilon > 0$: $(c+\varepsilon)^2 < 2$

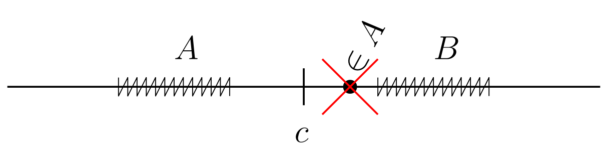

Рис. 2: Невозможность сценария (2)

$c^2 + 2c\varepsilon + \varepsilon^2 < 2 \Rightarrow 2c\varepsilon + \varepsilon^2 < \underbrace{2 - c^2}_{>0}$ тогда $\varepsilon(2c+\varepsilon) < 2 - c^2$. Пусть $0 < \varepsilon < 1$ - поскольку мы можем выбрать ε. Поэтому достаточно найти такое ε, что будет выполнено $\varepsilon(2c+\varepsilon) < \varepsilon(2c+1) < 2 - c^2$. Возьмем $\varepsilon = \dfrac{2 - c^2}{(2c+1)2017} \Rightarrow c + \varepsilon \in A$ и $c + \varepsilon > c$, а это противоречие с тем, что $A \leq c$.
(1) - упражнение - доказать, что и это невозможно.

$c^2 > 2$. Найдем $\varepsilon > 0$: $(c-\varepsilon)^2 > 2 \Rightarrow c^2 - 2c\varepsilon + \varepsilon^2 > 2 \Rightarrow 2c\varepsilon - \varepsilon^2 < \underbrace{c^2 - 2}_{>0}$ тогда $\varepsilon(2c - \varepsilon) < c^2 - 2$. Пусть $0 < \varepsilon < 1$ - поскольку мы можем выбрать ε. Поэтому достаточно найти такое ε, что будет выполнено $\varepsilon(2c-\varepsilon) < 2c\varepsilon < c^2 - 2$. Возьмем $\varepsilon = \dfrac{c^2-2}{(2c)2017} \Rightarrow c - \varepsilon \in B$ и $c - \varepsilon < c$, а это противоречие с тем, что $c \leq B$.
Следовательно нет рационального числа, которое бы разделяло эти два множества. ■

Утв. 3. В $\mathbb{R}$ существует $x > 0$: $x^2 = 2$, это $\sqrt{2}$.

□ Доказали в предыдущем утв. по аксиоме полноты есть c которое разделяет A и B. Доказали, что не может быть $c^2 > 2$ и $c^2 < 2$, а значит оно равно 2 ($c^2 = 2 \Rightarrow c = \sqrt{2}$). ■

Бесконечные десятичные дроби

Опр: 4. Бесконечные десятичные дроби - это набор последовательностей вида $a_0,a_1a_2\ldots a_n$, где $a_0 \in \mathbb{Z}$, $a_k \in \{0, 1, \ldots, 9\}$, $k \geq 1$.

Последовательности с $9999\ldots$ начиная с некоторого номера - запрещены. Почему запрещаем?
Пример: $10 \cdot 0{,}999\ldots = 9{,}999\ldots = 9 + 0{,}999\ldots \Leftrightarrow 10x = 9 + x$. Тогда получим, что $0{,}999\ldots = 1$.

Отношения порядка

$a_0,a_1a_2\ldots \leq b_0,b_1b_2\ldots$, когда $a_0, b_0 \geq 0$ (остальные случаи - как в школе). Либо $a_0 < b_0$, либо $a_0 = b_0$ и $a_1 < b_1$, либо $a_0 = b_0$, $a_1 = b_1$ и $a_2 < b_2$, либо ... - лексикографический порядок.

Сложение, умножение вводятся достаточно сложно - об этом можно прочитать в книжках Садовничего (Садовничий, Ильин).

Теорема 1. Справедливы следующие утверждения:

1. На множестве бесконечных десятичных дробей выполняется аксиома полноты;
2. Множество бесконечных десятичных дробей является моделью множества $\mathbb{R}$ (без доказательства);

□ Проведем доказательство в случае когда A и B состоят из неотрицательных чисел.
По условию: $A \neq \varnothing$, $B \neq \varnothing$ и $A \leq B$. Строим разделитель $c = c_0,c_1c_2\ldots$, где c_0 - минимальное b_0, которое встречается в B (т.к. неотрицательные числа).

Теперь смотрим только на дроби в B, которые начинаются с $c_0, \ldots$.
c_1 - это минимальное b_1, которое встречается в B в дробях вида $c_0,b_1\ldots$.
c_2 - это минимальное b_2, которое встречается в B в дробях вида $c_0,c_1b_2\ldots$.

Докажем, что построенная дробь $c = c_0,c_1c_2c_3\ldots$ разделяет A и B. Ясно, что $c \leq b$, $\forall b \in B$. Возьмем $b_0,b_1b_2\ldots$ и сравним с c. $c_0 \leq b_0$, $c_1 \leq b_1$, $c_2 \leq b_2$ и так далее - по построению. Поэтому $c \leq b$, $\forall b \in B$.

Возьмем $a_0,a_1\ldots a_n\ldots \in A$. Может ли случиться $a_0 > c_0$? - нет, так как тогда $a_0,a_1\ldots >$ дроби из B, начинающеся с $c_0, \ldots$. Пусть $a_0 = c_0$, может ли $a_1 > c_1$? - нет, так как тогда $a_0,a_1a_2 >$ дроби из B, начинающеся с $c_0,c_1\ldots$ и так далее.

Осталось проверить, что $c_0{,}c_1c_2\dots$ - допустимая запись, то есть нет $\dots 999\dots$ в конце. Пусть есть, но каждый раз брали наименьшую часть $\Rightarrow c_0{,}c_1c_2\dots c_n9999\dots$, но такой записи в B - нет, иначе в B в дроби начиная с некоторого момента будут идти только 9. ■

Аксиома полноты - тяжела для проверки на практике. Поэтому её обычно переформулируют.

Опр: 5. Если $c \geq a$, $\forall a \in A$, то c - называется верхней гранью A.

Опр: 6. Если у A есть хотя бы одна верхняя грань, то A называется ограниченным сверху множеством.

Опр: 7. Наименьшая из верхних граней множества A называется точной верхней гранью множества A и обозначается $\sup A$.

Опр: 8. Если $c \leq a$, $\forall a \in A$, то c - называется нижней гранью A.

Опр: 9. Если у A есть хотя бы одна нижняя грань, то A называется ограниченным снизу множеством.

Опр: 10. Наименьшая из нижних граней множества A называется точной нижней гранью множества A и обозначается $\inf A$.

Иллюстрация определений:

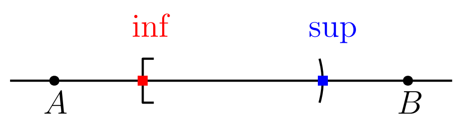

Рис. 3: Грани множеств: A - нижняя грань, B - верхняя грань

Теорема 2. Принцип полноты Вейрштрасса:
Если $A \neq \varnothing$ и ограничено сверху, то $\exists \sup A$. Если $A \neq \varnothing$ и ограничено снизу, то $\exists \inf A$.

□ Пусть $B = \{\text{верхние грани}\}$, $A \neq \varnothing$ - по условию, $B \neq \varnothing$ - так как A ограничено сверху $\Rightarrow A \leq B$. По аксиоме полноты существует разделитель c: $A \leq c \leq B$. $c \geq A \Rightarrow$ это верхняя грань. $c \leq B \Rightarrow$ это наименьшая верхняя грань $\Rightarrow c = \sup A$.

Пусть $B = \{\text{нижние грани}\}$, $A \neq \varnothing$ - по условию, $B \neq \varnothing$ - так как A ограничено снизу $\Rightarrow B \leq A$. По аксиоме полноты существует разделитель c: $B \leq c \leq A$. $c \leq A \Rightarrow$ это нижняя грань. $B \leq c \Rightarrow$ это наибольшая нижняя грань $\Rightarrow c = \inf A$. ■