1. Числовые системы: $\mathbb{R}$, $\mathbb{C}$, $\mathbf{H}$

Аксиоматическое описание вещественных чисел таково: прямая или, что то же — *система вещественных чисел* (иногда говорят — *действительных чисел*), это *полное, линейно упорядоченное поле.* Его обозначают $\mathbb{R}$.

"Поле" и "порядок" — алгебраические понятия, "полнота" — понятие топологическое.

1.1. Аксиоматика $\mathbb{R}$.

Определение 1.1. Множество $\mathcal{A}$ называется *полем*, если в нём определены две алгебраические операции — *сложение* $(+)$ и *умножение* (которое обозначают символом $(\cdot)$ (точкой), но обычно его опускают). Операция $+$ сопоставляет паре элементов x и y такой (единственный) элемент z, что $x + y = z$. Этот элемент называется *суммой* x и y. Операция умножения любой паре элементов x и y сопоставляет такой (единственный) элемент ζ, что $xy = \zeta$. Этот элемент называется *произведением* x и y. Сами элементы x и y называются в первом случае слагаемыми, во втором — сомножителями. В $\mathcal{A}$ есть два особых элемента — 0 (нуль) и 1 (единица) $(0 \neq 1)$. При этом выполняются следующие аксиомы:

$A.1$. От перемены мест слагаемых сумма не меняется и от перемены мест сомножителей произведение не меняется (или $x + y = y + x$ и $xy = yx\ \forall x, y$). Это — переместительный (по-другому говорят — коммутативный) закон сложения и умножения.

$A.2$. Если к сумме двух элементов прибавить третье, получится тот же результат, как если к первому слагаемому прибавить сумму второго и третьего слагаемых (или $(x + y) + z = x + (y + z)\ \forall x, y, z$). Аналогичное свойство ($(xy)z = x(yz)\ \forall x, y, z$) имеет место и для умножения. Это — сочетательный (ассоциативный) закон сложения и умножения. Остальные аксиомы мы формулируем только на символьном языке.

$A.3$. $\forall x, y, z\ \ ((x+y)z = xz+yz)$ — распределительный (дистрибутивный) закон.

$A.4$. $\forall x\ (x + 0 = x\ \wedge x \cdot 1 = x)$ — свойства нуля и единицы.

$A.5$. $\forall a, b\ (\exists\ x : a + x = b)$ — существование разности.

$A.6$. $\forall a \neq 0, b\ (\exists\ x : ax = b)$ — существование частного.

Пример 1.1. Простейший пример поля доставляет множество $\{0, 1\}$ такое, что $0 + 0 = 1 + 1 = 0,\ 0 + 1 = 1 + 0 = 1,\ 0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0,\ 1 \cdot 1 = 1.$

Вернёмся к числам из $\mathbb{R}$. Существующее согласно аксиоме $A.5$ единственное решение $x \in \mathbb{R}$ уравнения $a + x = b$ называется *разностью* чисел b и a и обозначается $b - a$. Разность чисел 0 и a называется числом, *противоположным* числу a и обозначается $-a$. Единственное решение уравнения $ax = b$, существующее (при $a \neq 0$) в силу аксиомы $A.6$, называется *частным* чисел b и a и обозначается $\frac{b}{a}$ (или b/a).

Числа 1, 2=1+1, 3=1+1+1,... называются натуральными, они образуют *натуральный ряд*, обозначаемый $\mathbb{N}$. А если к $\mathbb{N}$ добавить 0 и все числа, противоположные натуральным, мы получим множество всех *целых* чисел, обозначаемое $\mathbb{Z}$.

Если $a \neq 0$, то число $\frac{1}{a}$ называется *обратным* к a, оно обозначается еще и a^{-1}. Отношение $\frac{p}{q}, p \in \mathbb{Z}, q \in \mathbb{N}$ называется *рациональным числом* или *дробью.* Множество рациональных чисел обозначают $\mathbb{Q}$.

Аксиомы порядка.

Определение 1.2. Множество $\mathcal{B}$, между элементами которого определено отношение $\leq$ ("не превосходит") , удовлетворяющее аксиомам

$A.7.\forall x\ (x \leq x)$.

$A.8.(x \leq y)$ и $(y \leq x) \Rightarrow (x = y)$.

$A.9.(x \leq y)$ и $(y \leq z) \Rightarrow (x \leq z)$.

$A.10.\forall x, y\ (x \leq y) \vee (y \leq x)$.

$A.7 - A.9$ называется *частично упорядоченным*, а если удовлетворяются все аксиомы $A.7 - A.10$, то множество называется *линейно упорядоченным.*

Отношение $\leq$ называется еще *отношением неравенства.* Соотношения $x \leq y$ и $y \geq x$ равносильны; если $x \leq y$ и при этом $x \neq y$, то пишем $x < y$ (аналогично, если $y \geq x$ и $x \neq y$, то пишем $x > y$).

Пример 1.2. Множество $\{a, b, c\}$ с отношением неравенства $a \leq a$, $b \leq b$, $c \leq c$, $a \leq b$ и $a \leq c$ (b и c несравнимы) — частично упорядочено, а если $a \leq b \leq c$, то оно линейно упорядочено.

Аксиома $A.11$ связывает алгебраическую и порядковую структуры $\mathbb{R}$.

$A.11.\forall x > 0, \quad y > 0 \Rightarrow (x + y > 0) \ \wedge \ (xy > 0)$.

$A.13$. (Аксиома Архимеда). *Для любых положительных чисел a и b найдется натуральное число n такое, что $na > b$.*

Аксиомы полноты.

$A.13$. (Аксиома Дедекинда). *Пусть множество $\mathbb{R}$ (или $\mathbb{Q}$) разбито на два непустых подмножества A и B так, что для любого элемента $a \in A$ и любого элемента $b \in B$ выполнено неравенство $a \leq b$ (т. е. B лежит "справа" от A). Тогда найдется число $c \in \mathbb{R}$ такое, что $a \leq c$ $\forall a \in A$ и $c \leq b$ $\forall b \in B$.* Описанное разбиение $\mathbb{R}$ ($\mathbb{Q}$) и называется *дедекиндовым сечением.*

Сам Дедекинд строил теорию действительных чисел, исходя из сечений рациональных чисел, постулируя, что при каждом описанном разбиении $\mathbb{Q}$ возможно одно из трех: либо в A есть максимальный элемент, либо в B есть минимальный элемент (тогда по определению это — рациональные числа), либо ни в первом классе нет максимального числа, ни во втором — минимального. В этом случае будем говорить, что сечение определяет новый объект — *иррациональное число.*

Таким образом, $\sqrt{2}$ — это (с дедекиндовой точки зрения) сечение всех дробей $a = p/q > 0$ и $a \leq 0$, для которых $p^2/q^2 < 2$ и тех дробей $b = m/n, b > 0$, для которых $m^2/n^2 > 2$. Для корректности теории (на этом пути) необходимо было бы ввести еще одну аксиому — аксиому Архимеда, которая понадобится и нам, но чуть позже.

Мы пойдем несколько иным путём и в качестве дедекиндовой аксиомы полноты примем аксиому относительно разбиения всего $\mathbb{R}$.

Полнота — одно из важнейших математических понятий. Во множестве вещественных чисел она вводилась многими разными способами (и разными людьми), причем каждый из них оставил свой значительный след в математике. Приведем некоторые утверждения равносильные аксиоме Дедекинда и дающие каждое свой ключ к построению теории вещественного числа.

Определение 1.3. Множество $A \subset \mathbb{R}$ называется *ограниченным сверху*, если существует такое число $b \in \mathbb{R}$, что для любого числа a из A выполнено неравенство: $a \leq b\ \forall a \in A$; число α называется *верхней гранью* (иногда говорят *точной верхней гранью*) множества A, если для любого $a \in A$ выполнено неравенство $a \leq \alpha$ и для любого $\varepsilon > 0$ найдется $a(\varepsilon) \in A$ такое, что $a(\varepsilon) > \alpha - \epsilon$.

Аналогично определяется, что такое *множество ограниченное снизу* и что такое *нижняя грань*.

Пример 1.3. Множество $\mathbb{N}$ ограничено снизу, но неограничено сверху, множество $\mathbb{Z}$ неограничено ни снизу, ни сверху,

Множество $\{1, 1.1, 1.11, 1.111, \ldots\}$ ограничено и сверху и снизу, его нижняя грань — $\{1\}$, а верхняя — $\{\frac{10}{9}\}$.

$A.13a$). (Аксиома Вейерштрасса) *Всякое непустое ограниченное сверху (снизу) множество (в $\mathbb{R}$) имеет верхнюю (нижнюю) грань.*

Определение 1.4. Множество $\{x \in \mathbb{R} \mid a \leq x \leq b\}(\{x \in \mathbb{R} \mid a < x < b\})$ называется *отрезком* (*интервалом*) и обозначается $[a, b]$ ($]a, b[$ или(a, b)). Число $b - a$ называется *длиной* отрезка (интервала) $[a, b]((a, b))$; если $a \leq a' < b' \leq b$, то говорят, что отрезок $[a', b']$ *вложен в* $[a, b]$ Если задана система $\{[a_n, b_n]\}_{n \in N}$ вложенных отрезков, то говорят, что их длины стремятся к нулю, если для любого $\varepsilon > 0$ найдётся такое N, что длины всех отрезков $[a_n, b_n]$ при $n > N$ меньше ε.

Пример 1.4. Отрезок $[0, 1]$ далее обозначается I. Длина его равна единице.

$A.13b$. (Аксиома Кантора). *Любая последовательность отрезков вложенных друг в друга (лежащих в $\mathbb{R}$), длины которых стремятся к нулю, имеет единственную общую точку.*

Определение 1.5. Точка $\widehat{a}$ называется *предельной для множества* A, если для любого числа $\varepsilon > 0$ найдется число $a' = a'(\varepsilon) \neq a$ такое, что $|a' - \widehat{a}| < \varepsilon$.

Пример 1.5. У множества $\{\frac{1}{3}, \frac{2}{3}, \frac{1}{4}, \frac{3}{4} \ldots, \frac{1}{n}, 1 - \frac{1}{n}\}, n \geq 3$ две предельные точки $\{0\}$ и $\{1\}$.

$A.13c$). (Аксиома Больцано-Вейерштрасса). *Любое бесконечное ограниченное (сверху и снизу) подмножество* $\mathbb{R}$ *имеет предельную точку.*

Определение 1.6. Совокупность вещественных чисел $\{x_1, x_2, \ldots, x_n, \ldots\}$ (или $\{x_n\}_{n\in\mathbb{N}}$) называется *числовой последовательностью.*

Говорят, что числовая последовательность $\{x_1, x_2, \ldots, x_n, \ldots\}$ является *сходящейся*, если найдется такое число a, что для любого $\varepsilon > 0$ существует номер $N \in \mathbb{N}$ (зависящий от ε), при котором $|x_n - a| < \varepsilon$, если $n > N$ (или на символическом языке $\exists a \in \mathbb{R} :\ \forall\varepsilon > 0\ \exists N \in \mathbb{N} : (\forall n > N\ (|x_n - a| < \varepsilon))$.

Число a называется в этом случае *пределом* последовательности $\{x_n\}_{n\in\mathbb{N}}$. При этом пишут $a = \lim_{n\to\infty} x_n$.

Числовая последовательность $\{x_1, x_2, \ldots, x_n, \ldots\}$ называется *фундаментальной*, если $\forall\ \varepsilon > 0\ \exists\ N \in \mathbb{N} : (\forall m, n > N(|x_n - x_m| < \varepsilon))$.

Пример 1.6. Последовательности $\{\frac{1}{n}\}_{n\in\mathbb{N}}$ и $(1+\frac{1}{n})^n$, $n \in \mathbb{N}$ фундаментальны. Предел первой $\{0\}$. Нам предстоит доказать, что второй предел существует. Его обозначают буквой e.

Легко понять, что сходящаяся последовательность фундаментальна. В $\mathbb{R}$ (и вообще в полных пространствах, о которых речь впереди) верно и обратное.

$A.13d$). (Аксиома Коши) *Фундаментальная последовательность чисел из* $\mathbb{R}$ *является сходящейся.*

Теорема. *Введённая аксиоматика* $A.1 - A.13$ *непротиворечива. Она описывает единственный объект (с точностью до изоморфизма), обозначаемый* $\mathbb{R}$.

Изоморфизм — это алгебраическое понятие, возможность установить взаимно однозначное соответствие между двумя алгебраическими объектами, где каждому элементу одного объекта ставится ровно один объект другого, при котором все алгебраические свойства сохраняются.

Эта теорема не будет доказываться со всею подробностью: мы будем апеллировать к наглядности (полагая, что каждый человек как-то представляет себе множество чисел и умеет производить действия с дробями) и наметим путь как говорят "наивного" доказательства.

Для такого "наивного" доказательства сформулированной теоремы надо вывести из системы аксиом множество утверждений типа: нуль и единица определяются аксиоматикой однозначно и т. п. А затем доказать, например, такое утверждение:

Упражнение 1.1. $0 < 1$.

А дальше можно мысленно вообразить себе прямую, изобразить на ней нуль и "справа" единицу, при сложении единиц нуля не получается (это извлекается из аксиом), значит "отложится" натуральный ряд 1, 2, 3, ...; затем -1, -2, ... , т. е. "отложатся" целые числа, затем дроби и, наконец, с помощью идеи сечения, заткнутся все дыры. Так воссоздаётся в сознании образ вещественной прямой $\mathbb{R}$. Теперь вообразим, что имеется другой объект $\mathbb{R}'$ с теми же аксиомами. У него имеются нуль и единица. Обозначим их $0'$ и $1'$. Поставим их в соответствие с нулём и единицей на нашей модели. Сопоставим $1' + 1'$ элемент 2 первоначальной модели, обозначим $1' + 1'$ через $2'$, и будем это продолжать, так что в $\mathbb{R}'$ "вложится" натуральный ряд, затем дроби, а затем сечения в $\mathbb{R}'$ приведут к тому, что установится взаимно однозначное соответствие $\mathbb{R}'$ с нашей числовой прямой $\mathbb{R}$. Это и означает единственность описанного аксиомами объекта.

Более детальное построение действительного числа см., например, в учебнике В. А. Зорича.

Итак:

Действительное число — это:

— сечение во множестве рациональных чисел;

— верхняя грань возрастающей (или нижняя грань убывающей) последовательности конечных десятичных дробей;

— общий элемент последовательности вложенных друг в друга отрезков с рациональными концами;

— предельные точки бесконечных ограниченных множеств рациональных чисел;

— пределы фундаментальных последовательностей рациональных чисел.

Но чаще всего будем представлять себе вещественное число, как бесконечную десятичную дробь, оканчивающуюся не одними лишь девятками, у которой каждая конечная дробь даёт приближение числа с недостатком.

При всём этом требуется идентифицировать одинаковые числа. В вейерштрассовском, например, случае две возрастающие конечные последовательности десятичных дробей $\{x_n\}_{n\in\mathbb{N}}$ и $\{x'_n\}_{n\in\mathbb{N}}$ определяют одно число тогда и только тогда, когда $x_n - x'_n \to 0$, при $n \to \infty$. Аналогично производится идентификация и в остальных случаях (продумайте это).

Нам нужно осмыслить еще и такой результат:

Теорема 1.1 (о равносильности свойств полноты). *Свойства полноты, выраженные в аксиомах Дедекинда, Вейерштрасса, Кантора, Больцано – Вейерштрасса и Коши равносильны.*

Доказательство. Введем два обозначения: если $A \cup B$ — дедекиндово разбиение $\mathbb{R}$, то дедекиндово сечение, порожденное этими множествами (т. е. само число, определяемое этим разбиением), обозначим $A|B$; верхнюю грань множества A обозначим $\sup A$.

1. Исходим из того, что аксиома Дедекинда выполняется. Пусть $\mathcal{A}$ —- непустое ограниченное сверху множество в $\mathbb{R}$. Обозначим через B совокупность тех $b \in \mathbb{R}$, для которых $a \le b\ \forall a \in \mathcal{A}$ и A — дополнение к B ($A = \mathbb{R} \setminus B$.) Тогда $B \neq \emptyset$ (см. определение 1. 3), A непусто, ибо $\mathcal{A} \subset A$. Пусть $c = A|B$ — дедекиндово сечение. Из определения дедекиндова сечения следует, что $a \le c\ \forall a \in A$ и значит, $a \le c\ \forall a \in \mathcal{A}$. Допущение, что при некотором $\varepsilon > 0$ в интервале $(a - \varepsilon, a)$ нет чисел из $\mathcal{A}$ противоречиво:

тогда $a - \varepsilon \in B$. Значит, $c = \sup \mathcal{A}$, т. е. *из аксиомы Дедекинда следует аксиома Вейерштрасса.*

2. Пусть $\{\Delta_n = [a_n, b_n]\}_{n\in\mathbb{N}}$ — последовательность вложенных друг в друга отрезков, длины которых стремятся к нулю. Тогда $\{a_n\}_{n\in\mathbb{N}}$— возрастающая ограниченная сверху, а $\{b_n\}_{n\in\mathbb{N}}$ — убывающая ограниченная снизу последовательности. По аксиоме Вейерштрасса они имеют вехнюю и нижнюю грани. Обозначим их c и c' соответственно. Из определений следует, что $c \leq c'$. Допущение, что $c < c'$ противоречит тому, что длины отрезков Δ_n стремятся к нулю. Доказано, что *из аксиомы Вейерштрасса следует аксиома Кантора.*

3. *Из аксиомы Кантора следует аксиома Больцано – Вейерштрасса.*

Не ограничивая себя в общности, считаем, что бесконечное ограниченное множество A лежит на отрезке $\Delta_1 = [0, 1]$. Разделим его пополам. Пересечение A с одной из половин отрезка Δ_1 — бесконечное ограниченное множество. Обозначим эту половину отрезка $\Delta_2 = [a_2, b_2]$. Далее поступаем аналогично. Получаем последовательность вложенных друг в друга отрезков $\{\Delta_n\}_{n\in\mathbb{N}}$, стремящихся (в силу аксиомы Архимеда) по длине к нулю. Применяем аксиому Кантора. Общая точка всех отрезков — искомая.

Метод доказательства этого фрагмента называется *методом деления пополам.*

4. *Из аксиомы Больцано – Вейерштрасса следует аксиома Коши.*

Фундаментальная последовательность ограничена и сверху и снизу (докажите это самостоятельно). В силу аксиомы Больцано – Вейерштрасса существует предельная точка. Она и является пределом.

6. *Из аксиом Коши и Архимеда следует аксиома Дедекинда.*

Не ограничив себя в общности, можно считать, что имеется $A \cup B$ — дедекиндово разбиение $\mathbb{R}$, и не нет числа, которое является сечением $A|B$. Тогда для любого n обозначим через x_n такое число вида k/n, что $x_n \in A$ а $x_n + 1/n \in B$.(Из аксиомы Архимеда такое x_n существует). Последовательность $\{x_n\}_{n\in\mathbb{N}}$ — фундаментальна. Ее предел, существующий по аксиоме Коши, является сечением $A|B$. Противоречие. $\square$

В дальнейшем нам придётся не раз использовать некоторые свойства натуральных чисел и самого натурального ряда. Вот важнейшие его свойства.

1 (Принцип математической индукции). *Если подмножество A натурального ряда $\mathbb{N}$ таково, что $1 \in A$ и вместе с числом $a \in A$ в A содержится число $a + 1$, то $A = \mathbb{N}$.*

Замечание. Методом математической индукции доказывается следующая формула *бинома Ньютона:*

$$(a + b)^n = \sum_{k=0}^{n} C_n^k a^k b^{n-k}, \quad \text{где} \quad C_n^k = \frac{n(n-1)\cdots(n-k+1)}{k!}.$$

(Другое и более распространённое сейчас обозначение для C_n^k — это $\binom{n}{k}$.)

Натуральное число p называют *простым*, если не существует двух натуральных чисел m и n, больших единицы и при этом таких, что $p = mn$ $(2, 3, 5, 7 \ldots$ — простые числа).

2 (Основная теорема арифметики). *Натуральное число однозначно (с точностью до порядка сомножителей) разлагается в произведение простых сомножителей.*

Замечания. Будем считать, что мы построили $\mathbb{R}$. Это весьма замечательный объект. Он может служить примером большого числа важнейших математических понятий. $\mathbb{R}$ — это абелева группа, кольцо, поле, векторное пространство (это — алгебраические понятия); частично упорядоченное и линейно упорядоченное множества (это понятия, характеризующие порядковые структуры); однородное пространство (это — геометрическое понятие); топологическое пространство, метрическое пространство (это понятия общей топологии); пространство с мерой, нормированное пространство (все эти понятия либо уже появились, либо потом появятся у нас) и ещё многое другое.

Концепция построения всей математики на базе теории множеств в своём зародыше восходит к Кантору. Эта концепция была воспринята и поддержана Гильбертом, а сама попытка выстроить всю математику, базируясь на этой концепции, была предпринята Н. Бурбаки (коллективному автору французских, в основном, математиков; о нём можно прочитать в статье А. Б. Сосинский "Умер ли Никола Бурбаки" Математическое просвещение, МЦНМО, вып. 2, 1998). Сущность этой концепции кратко выразил А. Н. Колмогоров в следующих словах: "Специальные разделы математики занимаются структурами, принадлежащими к тем или иным типам структур. Каждый род структур определяется соответствующей системой аксиом, выраженной на языке теории множеств."

Теория множеств (мы поговорим о ней позже и будем касаться её лишь мимоходом) является фундаментом (по Кантору – Гильберту – Бурбаки) математического здания. На первом этаже этого здания размещаются простейшие структуры. Там есть "начальная комната алгебры", где изучаются объекты с одной операцией (как, например, абелевы группы), с двумя операциями (как кольца и поля), есть помещение для порядковых структур, для общей топологии (где изучают свойства полноты, компактности, метризуемости и т. п.). Там же имеется комната для пространств с мерой (о ней поговорим, когда коснёмся интегрального исчисления). На следующем этаже структуры соединяются. Там и расположена та теория действительного числа, которую мы здесь изучали — в этой теории соединяются алгебра, порядок и топология.

Докажем две знаменитые теоремы.

Теорема 1.2. *(Пифагор (?)). Нет дроби, которая в квадрате равна двум.*

Доказательство. Приведём всем известное рассуждение, расположив его в набор "надписанных" импликаций (логических ходов, которые будем обозначать символами $\Rightarrow$ ("*из ... следует*"), над которыми будем надписывать *ссылки* либо на аксиомы, либо на известные или уже доказанные утверждения).

Доказательство нашей теоремы проводится "от противного". Допустим, что существуют такие целые m и n, что $\frac{m}{n} = \sqrt{2}$ ($\overset{\text{арифм}_1}{\Rightarrow}$ m и n можно предположить взаимно простыми, т. е. не содержащими общих простых множителей) и тогда:

$$\frac{m^2}{n^2} = 2 \overset{\text{акс}_1}{\Rightarrow} m^2 = 2n^2 \overset{\text{арифм}_2}{\Rightarrow} m = 2k (k \in \mathbb{Z}) \overset{\text{акс}_2}{\Rightarrow} 4k^2 =$$

$$2n^2 \overset{\text{акс}_3}{\Rightarrow} 2k^2 = n^2 \overset{\text{арифм}_2}{\Rightarrow} n = 2l (l \in \mathbb{Z}).$$

Последнее противоречит взаимной простоте m и n. □

Символ □ означает конец доказательства. Наши символы акс$_i$ означают, что с помощью аксиом, с которыми мы оперировали, можно производить те операции, которые здесь проделаны; арифм$_1$ означает следствие из основной теоремы арифметики [1], арифм$_2$ — это утверждение, что квадрат нечётного числа нечётен.

Отрезок $[0,1]$ прямой $\mathbb{R}$ называют *континуумом.* Будем иногда обозначать его I.

Теорема 1.3. *(Кантор). Континуум нельзя пересчитать.*

Читатель мог слышать иную формулировку этого утверждения: *мощность континуума больше мощности счётного множества* — в одном из дальнейших разделов эти термины будут разъяснены, но для нас сейчас важен *метод* доказательства — знаменитый (канторовский) *диагональный процесс. Доказательство* снова будем вести от противного.

Пусть континуум пересчитываем и последовательность $\{a^j\}_{j\in\mathbb{N}}$, $a^j \in I$ его исчерпывает. Пусть $0.a_1^j, a_2^j, \ldots$ бесконечная десятичная дробь, не оканчивающаяся одними девятками, которая (по Вейерштрассу) представляет число a^j. Положим $\bar{a}_j^j$ равным единице, если $a_j^j \neq 1$ и равным двум, если $a_j^j = 1$. Тогда $0.\bar{a}_1^1, \bar{a}_2^2, \ldots, \bar{a}_j^j \ldots$ это число из континуума, не совпадающее ни с одним из чисел a^j. Противоречие. Теорема доказана.

1.2. Построение поля $\mathbb{C}$ комплексных чисел.

Расширим числовое поле вещественных чисел и построим поле комплексных чисел $\mathbb{C}$. Эта процедура стандартна для алгебры: поле $\mathbb{R}$ расширяется введением корня уравнения $x^2 + 1 = 0$.Среди вещественных чисел нет такого числа, которое было бы корнем этого уравнения. При отсутствии такого объекта будем считать (формальным) корнем этого уравнения символ i. Назовем его *мнимой единицей.* А дальше поступим так, как поступают алгебраисты, которые строят "расширение полей". А именно, будем рассматривать всевозможные полиномы вида $a_0 + a_1 i + a_2 i^2 + \cdots + a_n i^n$, $a_i \in \mathbb{R}$. Но ведь мы условились, что $i^2 = -1$, откуда можно привести подобные члены, и мы получим сумму вида $z = x + iy$, где x и y - вещественны (при этом $z = x + iy = 0 \Leftrightarrow x = y = 0$). Такие символы можно складывать , вычитать, перемножать и делить. Если $z_1 = x_1 + iy_1, z_2 = x_2 + iy_2$, то

$$z_1 \pm z_2 := (x_1 + x_2) \pm i(y_1 + y_2),\ z_1 z_2 := (x_1 x_2 - y_1 y_2) + i(x_1 y_2 + x_2 y_1),$$

а если $z_2 \neq 0$, то

$$(z_1 : z_2) := \frac{(x_1 x_2 + y_1 y_2) + i(x_2 y_1 - x_1 y_2)}{x_2^2 + y_2^2}.$$

[1] На самом деле используется лишь разложимость на простые множители, единственность не нужна.

Проверяется, что совокупность комплексных чисел, обозначаемая $\mathbb{C}$, будет обладать свойствами коммутативности, ассоциативности, дистрибутивности, т. е. $\mathbb{C}$ — это поле.

Но можно, следуя старой традиции, исходящей ещё от Гаусса, избрать геометрический метод построения поля $\mathbb{C}$. Комплексные числа можно изображать на декартовой плоскости с ортогональным единичным базисом $e_1 = (1, 0)$, $e_2 = (0, 1)$. Если первый вектор обозначить как 1, а второй — буквой i, то тогда число $z = xe_1 + ye_2$ запишется, как $x + iy$. Число $x - iy$ называют *сопряжённым* числу $z = x + iy$ и обозначают $\bar{z}$. Величину $r = |z| = \sqrt{z\bar{z}} = \sqrt{x^2 + y^2}$ $(z = x + iy)$ называют *модулем* комплексного числа z (термины "модуль комплексного числа" и "сопряжённые комплексные числа" ввёл Коши). Угол φ (а на самом деле совокупность углов, отличающихся на $2\pi n,\ n \in \mathbb{Z}$), образованный вектором (x, y) с осью Ox называют *аргументом* z. Таким образом, $z = r(cos\varphi + i\sin\varphi)$.

Числа складываются, как векторы, а умножаются, перемножая модули и складывая аргументы: если $z_k = r(\cos\varphi_k + i\sin\varphi_k)$, $k = 1, 2$, то $z_1z_2 = r_1r_2(\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2))$. Отсюда следует *формула Муавра*: если $z = r(\cos\varphi + i\sin\varphi)$, то $z^n = r^n(\cos n\varphi + i\sin n\varphi)$.

1.3. Построение тела H кватернионов.

После построения вещественных и комплексных чисел могло создаться впечатление, что числа можно построить и в трёхмерном пространстве и в пространствах бо́льшего числа измерений. Но это оказалось не так. Выяснилось, что числа, сходные [2] с комплексными, существуют только в четырёхмерном пространстве. Они были открыты замечательным ирландским учёным Гамильтоном, который на базе этих чисел создал векторное исчисление, играющее фундаментальную роль в физике и технике. Познакомимся вкратце с кватернионами и векторным исчислением.

Если для определения комплексных чисел потребовалась одна мнимая единица, то для кватернионов нужны три единицы. Обозначим их так, как это принято со времён Гамильтона— жирными буквами $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$ (ведь они не только числа, но и (совместно с обычной единицей) базисные четырёхмерные векторы). Они называются *мнимыми кватернионами.* Так что кватернион — это число $q = a + b_1\mathbf{i} + b_2\mathbf{j} + b_3\mathbf{k}$. Оно разбивается на вещественную часть (число a, которое будем, как и в комплексном случае обозначать $\mathrm{Re}q$ и мнимая часть $\mathrm{Im}q = b_1\mathbf{i}+b_2\mathbf{j}+b_3\mathbf{k}$, определяемая вектором $\mathbf{b} = (b_1, b_2, b_3)$.

Нам надлежит определить сложение и умножение кватернионов. Сложение кватернионов покоординатное, как и в случае комплексных чисел. Оно коммутативно и ассоциативно.

А для того, чтобы определить умножение, надо построить таблицу умножения базисных чисел 1,$\mathbf{i}$, $\mathbf{j}, \mathbf{k}$.

Правила составления этой таблицы просты.

[2] и то не до конца — нет коммутативности, а поле без коммутативности называют *телом*

1) Единица, умноженная (справа или слева) на любой мнимый кватернион, как и положено единице, оставляет его без изменения.

2) Квадраты мнимых кватернионов равны -1.

3) Умножение мнимых кватернионов не коммутативно, а “антикоммутативно”: при перемене мест сомножителей число умножается на -1.

4) Умножение мнимых кватернионов друг на друга подчинено циклическому правилу: $\mathbf{i}\cdot\mathbf{j}=\mathbf{k}$, $\mathbf{j}\cdot\mathbf{k}=\mathbf{i}$, $\mathbf{k}\cdot\mathbf{i}=\mathbf{j}$.

Вот теперь мы готовы выписать всю таблицу умножения 4×4.

$$1\cdot 1=1,\quad \mathbf{i}\cdot 1=\mathbf{i},\quad \mathbf{j}\cdot 1=\mathbf{j},\quad \mathbf{k}\cdot 1=\mathbf{k},$$

$$1\cdot\mathbf{i}=\mathbf{i},\quad \mathbf{i}\cdot\mathbf{i}=-1,\quad \mathbf{j}\cdot\mathbf{i}=-\mathbf{k},\quad \mathbf{k}\cdot\mathbf{i}=\mathbf{j},$$

$$1\cdot\mathbf{j}=\mathbf{j},\quad \mathbf{i}\cdot\mathbf{j}=\mathbf{k},\quad \mathbf{j}\cdot\mathbf{j}=-1,\quad \mathbf{k}\cdot\mathbf{j}=-\mathbf{i},$$

$$1\cdot\mathbf{k}=\mathbf{k},\quad \mathbf{i}\cdot\mathbf{k}=-\mathbf{j},\quad \mathbf{j}\cdot\mathbf{k}=\mathbf{i},\quad \mathbf{k}\cdot\mathbf{k}=-1.$$

Умножение кватернионов. Скалярное, векторное и смешаное произведения.

Пусть даны два кватерниона $q=a_1+b_1\mathbf{i}+b_2\mathbf{j}+b_3\mathbf{k}$ и $q'=a_1'+b_1'\mathbf{i}+b_2'\mathbf{j}+b_3'\mathbf{k}$. Перемножим их, следуя дистрибутивному закону. Напишем отдельные выражения для вещественных и мнимых частей:
$\mathrm{Re}qq'=a_1a_1'-b_1b_1'-c_1c_1'-d_1d_1'=a_1a_1'-\mathbf{b}\cdot\mathbf{b}'$,
т. е. вещественная часть произведения равна разности произведения вещественных частей сомножителей минус скалярное произведение векторов, из которых образована мнимая часть сомножителей.
Убедитесь, что для мнимой части имеет место следующее выражение:
$\mathrm{Im}qq'=a_1\mathrm{Im}q'+a_1'\mathrm{Im}q+[\mathrm{Im}q,\mathrm{Im}q']$,
где через $[\mathbf{b},\mathbf{b}']$ обозначается векторное произведение векторов $\mathbf{b}$ и $\mathbf{b}'$, т. е. вектор

$$\mathbf{i}\begin{vmatrix} b_2 & b_3\\ b_2' & b_3'\end{vmatrix}-\mathbf{j}\begin{vmatrix} b_1 & b_3\\ b_1' & b_3'\end{vmatrix}+\mathbf{k}\begin{vmatrix} b_1 & b_2\\ b_1' & b_2'\end{vmatrix}.$$

Более подробно о кватернионах (в частности, об их геометрической интерпретации см. в брошюре В. И. Арнольда Геометрия комплексных чисел, кватернионов и спинов. М. Изд. МЦНМО, 2002.

1.4. Приложение: знаменитые числа

Число π.

π — трансцендентное число, равное 3.141592653589793285..., отношение длины окружности к диаметру (обозначение стало общепринятым после работы Эйлера 1736 г., а впервые оно появилось у У. Джонса (1706 г.)).

Число π, пожалуй, наиболее часто встречается в различных математических формулах среди всех других чисел. Оно имеет множество различных определений и представлений. Вот некоторые из них:

— отношение площади круга к квадрату его радиуса;

— отношение площади поверхности сферы к квадрату её диаметра;

— отношение трёх четвертей объёма шара к кубу его радиуса;

(Объёмы шаров и сфер в бо́льших размерностях также содержат число π). Вот ряды, представляющие π:

$$\pi = 4(1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + ...)$$

(ряд Лейбница-Грегори);

$$\pi = \left(6(1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + ...)\right)^{1/2}$$

(Эйлер). (Значения ζ-функции Римана $\zeta(x) = \sum_{k\geq 0} \frac{1}{k^x}$ при $x = 2s,\ s \in \mathbb{N}$ содержат π в степени $2s$).

π — число трансцендентное (Линдеманн (1982)).

Число e.

e — трансцендентное число, равное 2.71828182845904523 54..., предел последовательности $x_n = (1 + \frac{1}{n})^n$ при n стремящемся к бесконечности.

Обозначение этому числу дал Эйлер. Число e является основанием натуральных логарифмов. Иногда (не вполне обоснованно) это число называют неперовым (в честь Непера — одного из изобретателей логарифмов; Непер пользовался следующим приближением числа e: $x_{10000000} = (1 + \frac{1}{1000000})^{1000000} = 2.718281693...$).

Число e имеет такое геометрическое определение: это такое число, что площадь криволинейной трапеции, ограниченной осью OX, графиком функции $y = \frac{1}{x}$ и двумя вертикальными прямыми, проведёнными в единице и этом числе, равна единице.

Огромная роль числа e в математике объясняется тем, что функция $f(x) = e^x$ инвариантна относительно дифференцирования: $f'(x) = f(x)$. В силу этого имеет место следующее представление:

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \frac{1}{4!} + \dots .$$

Трансцендентность e была доказана Ш. Эрмитом.

Корень из двух.

$\sqrt{2}$— иррациональное число, равное 1.414213562.... Это число, квадрат которого равен двум. Оно обозначается еще $2^{1/2}$. Помимо данного выше арифметического определения имеет множество других — эквивалентных. Таковы

— геометрическое определение: $\sqrt{2}$ — отношение диагонали квадрата к его стороне;

— алгебраическое: $\sqrt{2}$ — решение уравнения $x^2 - 2 = 0$ (отсюда следует, что $\sqrt{2}$ — *алгебраическое число*);

— аналитическое: $\sqrt{2}$ есть предел итеративной последовательности: $x_{n+1} = \frac{1}{2}(x_n + \frac{2}{x_n}),\ n \geq 2,\ x_1$ — любое (если начать с $x_1 = 1$, то получается последовательность $x_2 = \frac{3}{2} = 1.5,\ x_3 = \frac{17}{12} = 1.41(6),\ x_4 = \frac{577}{408} = 1.414215686,\ x_5 = \frac{665557}{470832} = 1.414213562......$).

$\sqrt{2}$ разлагается в следующую цепную дробь: $1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + ...}}}$. Подходящие дроби образуются согласно правилу: $z_n = y_n + 1,\ y_{n+1} = \frac{1}{2+y_n},\ n \geq 2, y_1 = 0$; первые подходящие дроби таковы: $1,\ \frac{3}{2} = 1.5,\ \frac{7}{5} = 1.4,\ \frac{17}{12} = 1.41(6)$ и т. д. Описанная итеративная процедура ($x_{n+1} = f(x_n),\ f(x) = \frac{1}{2+x}$) получила очень далекое обобщение — так называемый принцип сжимающих отображений.

Иррациональность корня из двух была впервые доказана в школе Пифагора.

Одно из доказательств иррациональности корня из двух было приведено выше.