О трёх составляющих понимания определений, утверждений и доказательств

Г.Б. Шабат

3 июля 2020

Конструктивное знание – 12:
формальные доказательства и человеческое понимание

План

0.0. Сопоставление взглядов с Н.А. Вавиловым

Текст [**Vavilov2019**] написан интересно (оторваться невозможно!), талантливо, с замечательным знанием предмета и любовью к нему. Вот типичная цитата:

Here is what philosophers and popularisers declare:

• Proof is a formal text written according to rigorously defined rules. Essentially, a sequence of elementary steps each of them consisting of applying inference rules to axioms and previous steps.

• It is sometimes difficult to find a proof; this process may require intuition and inventiveness, but **checking a proof is an entirely mechanical process** that can be delegated to low-skilled personnel, and, ultimately, to a computer.

• Mathematics can be completely formalized, that is reduced to deriving consequences of explicitly given axioms according to explicitly listed inference rules.

...

• To understand and consciously use any mathematical result is possible only after its proof is fully understood. All results in all educational courses at any sufficiently advanced level should be accompanied by complete and detailed proofs.

I believe that such a simplistic propagandist picture is infinitely remote from reality.

Автор подробно и очень убедительно развенчивает перечисленные точки зрения наивных, далёких от математики людей. Возразить почти нечего, если бы не одно важное обстоятельство.

Доказательства эволюционируют! Будут приведены примеры кардинальных упрощений доказательств со временем; при этом и возражения о формализации и т. п. постепенно отпадают.

Мы не знаем, как будут выглядеть доказательства Воеводского и Перельмана через 100 лет...

0.1. Доказательства в развитии: примеры

Tartaglia, 1539

Quando chel cubo con le cose appresso
Se agguaglia a qualche numero discreto
Trouan dui altri differenti in esso
...

$[\mathbb{K} : \Bbbk] = 3 \Longrightarrow \mathrm{Gal}(\mathbb{K}/\Bbbk) \subseteq \mathsf{S}_3$

Euler, 1760, *De seriebus divergentibus*

$$\boxed{1 + 2 + 3 + \cdots = -\frac{1}{12}}$$

Предыстория: *Базельская задача*
(поставлена Пьетро Менголи ок. 1650):
$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots = ??$
Эйлер, 1734: $?? = \frac{\pi^2}{6}$: действительно,
$\frac{\sin(\pi x)}{\pi x} = \left(1 - \frac{x^2}{1^2}\right)\left(1 - \frac{x^2}{2^2}\right)\left(1 - \frac{x^2}{3^2}\right) \ldots,$
ряд Тейлора и теорема Виета.
А заодно уж введём $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$,
и после небольшого усложнения
$\xi(s) := \Gamma(\frac{s}{2})\pi^{-\frac{s}{2}}\zeta(s)$
установим $\xi(s) = \xi(1 - s)$

1.0. Формальная составляющая доказательств

Proof checking

Разбиение рассуждение на мелкие шаги,
механическая проверка,
Coq,
...

Общепризнанные правила??

Тезис Чёрча...

1.1. Естественно-языковая составляющая

Речь о <u>формулировках</u> и <u>определениях</u>.

Сумма квадратов катетов равна квадрату гипотенузы.
...(см. [**KreydlinShabat2020**])

$$\int_a^b F'(x)\mathrm{d}x = F(b) - F(a) \quad \text{вряд ли...}$$

$$\int_c \mathrm{d}\omega = \int_{\partial c} \omega \quad \text{можно.}$$

А чем занимается алгебраическая геометрия?

Alexander Grothendieck: *схемы – это окольцованные пространства, локально изоморфные спектрам коммутативных колец.*

1.2. Визуальная составляющая доказательств

Формула Эйлера

$$\boxed{d^2 = R^2 - 2Rr}$$

См. динамические чертежи.
Детали: [**СгибневШабат2009**].

2.0. Снятие и навешивание квантора общности

См. [**KreydlinShabat2012**].

Обобщение: от $\mathcal{F}(x_1), \mathcal{F}(x_2), \ldots$ к $\forall x \mathcal{F}(x)$

$$1^3 = 1^2, 1^3 + 2^3 = (1+2)^2, 1^3 + 2^3 + 3^3 = (1+2+3)^2, \ldots$$

Помогает нахождению прозрачных доказательств!

Специализация: от $\forall x \mathcal{F}(x)$ к $\mathcal{F}(a)$

1+2+4+8+...+1024=???

Необходимо при КОНТРОЛЕ понимания!

2.1. Снятие и навешивание квантора существования

См. [**KreydlinShabat2012**].

Элиминация деталей: от $\mathcal{F}(a)$ к $\exists x \mathcal{F}(x)$

$$\exists x [x^2 > 999 x^{1.99} \log x]$$

Конкретный a часто не нужен.

Конструктивная математика: от $\exists x \mathcal{F}(x)$ к $\mathcal{F}(a)$

Гипотеза Морделла, доказанная Фальтингсом:
Пусть $\mathbf{X}$ *– кривая над* $\mathbb{Q}$*.*
Если род $\mathbf{X}(\mathbb{C})>1$, то $\#\mathbf{X}(\mathbb{Q}) < \infty$
Но *конструктивный Фальтингс* неизвестен! (2020).

2.2. Другие когнитивные операции

Аннотирование, комментирование, написание исторических обзоров, ... требует неформального (и не обязательно полного...) понимания.

Научное руководство (на этапе представления диссертаций учеников), оппонирование, рецензирование требуют К ТОМУ ЖЕ ответственной **проверки** и результатов, и их доказательств.

И в XXI веке неизбежна и идея computer checking (тоже своего рода когнитивная операция), и какие-то формы её общественного признания.

2.0. Формальное и неформальное понимание

Совсем разные вещи!

Несколько уровней формального понимания:
- Я тщательно проверил этот результат и ручаюсь за него.
- Я проверил этот результат и нашёл несколько ошибок в промежуточных рассуждениях, но знаю, как их исправить. Результат верен.
- Я проверил этот результат с точностью до нескольких деталей. Он мне кажется правдоподобным.
- Я проверил этот результат с точностью до ссылок на некоторые другие работы (или результаты, которые кто-то обещает вскоре опубликовать). Результат, возможно, верен.
- Мне не удалось понять некоторые рассуждения. Не знаю, верен ли результат.
- В доказательстве серьёзная ошибка. Не знаю, верен ли результат.
- Я знаю контрпример. Результат неверен.

Несколько уровней неформального понимания:
- Результат меня заинтересовал. Буду разбираться в частных случаях и искать обобщения.
- Я понял этот результат вместе с доказательством и он стал "моим". Готов рассказывать его.
- Результат мне нравится, но доказательство противное. Буду искать другое.
- Я проследил за всеми рассуждениями, но что-то не укладывается у меня в голове и продолжает удивлять. Придётся дальше разбираться.
- Мне стало скучно разбираться в этом доказательстве, и я готов ему поверить.
- Доказательство отвратило меня от этого предмета, и я в дальнейшем буду его избегать.
- Ничего не понял, и больше заниматься математикой не буду.

3.1. Об идеальных доказательствах

Компьютерная проверяемость + что-то ещё?

- Красота (можно объективно, с экспертными оценками);
- Естественность

(теорему о простых в арифметической прогрессии $\#\{7, 17, 37, 47, 67, \dots\} = \infty$ Дирихле вывел из $\lim_{s\to 1}\sum_{p\in\{7,17,37,47,67,\dots\}}\frac{1}{p^s} = \infty$."Элеменарное" доказательство Сельберга гораздо труднее понять);

- Перспективность

(снова теорема Дирихле: продумывание и обобщение его доказательства легло в основу нескольких теорий XX века);

- Понимаемость и проверяемость <u>человеком</u> (банальность).

3.2. Фрагментарное vs цельное понимание

Элементарный пример: Зачем классифицировать алгебры Ли?
Курьёз с Колмогоровым, Арнольдом и высотами сферического треугольника.

Продвинутый пример: За что Воеводскому дали филдсовскую премию?
Кратко малая часть ответа: За гипотезу Милнора. А зачем тополог Милнор стал для полей $\mathbb{F}$ рассматривать полилинейные отображения в абелевы группы

$$\mathbb{F}^{\times} \times \cdots \times \mathbb{F}^{\times} \longrightarrow A,$$

удовлетворяющие условию $(..., x, ..., 1 - x, ...) \mapsto 0$?

Условие можно понять только в контексте *законов взаимности* – от Ферма-Эйлера до настоящего времени. А причуда Милнора объясняется существованием K-теории, в которой почему-то топологическая интуиция оказывается применима к арифметике и позволяет предсказывать арифметические результаты...

3.3. Ещё об эволюции

(Взгляд в прошлое) Некоторые доказательства, бывшие когда-то длинными и трудными, стали короткими и прозрачными. Таковы

- основная теорема алгебры;
- лемма Жордана;
- формула Эйлера В-Р+Г=2-2g;
- … .

Стремление прояснить тёмные доказательства сыграло важную роль в построении соответствующих понятийных аппаратов.

(Взгляд в будущее) И в наше время существуют **непризнанные доказательства**. Пример: Mochizuki утверждает, что abc-гипотеза (*if a and b are composed from large powers of primes, then a+b is usually not divisible by large powers of primes*) вытекает из его Inter-universal Teichmuller Theory. Теория ОЧЕНЬ интересна, и Mochizuki пишет много длинных текстов, но их не понимают.

Литература

- Grigory Kreydlin, George Shabat, *The cognitive operations over the texts.* Пятая международная конференция по когнитивной науке: тезисы докладов, стр.101 – 102. Калининград, 2012.
- Grigory Kreydlin, George Shabat, *Mathematical theorems in natural languages.* Advances in Mathematics Research. Volume 28(2020) Editor: Albert R. Baswell https://novapublishers.com/shop/advances-in-mathematics-research-volume-28.
- Nikolai Vavilov, *Reshaping the metaphor of proof.* Philosophical Transactions of the Royal Society A. Mathematical, Physical, and Engineering Sciences, 2019.
- А.И. Сгибнев, Г.Б. Шабат, *Формула Эйлера и теорема Понселе.* Полином. 2009. N 2. С. 22-27.