Georgii Potoshin, 2024

Высшая Алгебра, Николай Вавилов

0.1 Предыстория

Определить, что такое современная алгебра трудно. Всё, что рассказывалось в школе – вещи очень древние 1000 лет. Один польский математик в своей книге "Математический калейдоскоп"описывал распространение математических знаний следующим образом. Человечество по отношению к математическим знаниям образует очень растянутую процессию. Математические знания, которыми располагает большинство людей предшествует эпохи строительства египетских пирамид. Что по сути изучают в школе (по алгебре, анализ конечно ушел чуть дальше, к экспонентам и логарифмам).

- $$ax + b = 0$$
- $$ax^2 + bx + c = 0$$
- $$\begin{cases} ax + by = 0 \\ cx + by = 0 \end{cases}$$

Есть египетские тексты, что давали методы решения этих проблем. Так же есть китайский тексты 5 века до нашей эры, что описывают решение произвольных линейных систем методом, что сегодня носит имя Гаусса (за 22 века до него). В этом направлении алгебра долго развивалась в античные века и апофеозом стала книга Диофанта "Арифметика правда там решалась иная задача, а именно решение уравнений в целых числах.

В 3-4 веках греческие ученые побежали в Индию, Иран (от христианства). Именно поэтому большинство математических текстов этого периода написано на арабском. Так книга, в честь которой названа это дисциплина, хоть и написана на арабском, но её автор – Арихизмий был персом.

Переломным моментом для европейской науки (в частности по мнению Феймана, его тогда спросили об этом на одном из интервью и он назвал изобретение комплексных чисел) – конец 15 века, стал первый прогресс, была решена задача, непосильная грекам.

$$ax^3 + bx^2 + cx + d = 0 \ ()$$

Была решена Итальянским алгебраистом, а сама история совершенно криминальная.

Мы говорим, что математика – это наука, но это сильное преувеличение. Математика – это совершенно иной вид деятельности, гораздо больше свободы, чем в науке.

Так вот, оказалось, что при решении кубических уравнений с действительными коэффициентами необходимо проводить вычисления в комплексных числах. Это был переломный момент европейской цивилизации. До этого считалось, что всё знали древние, но $\mathbb{C}$ – реальный прорыв. Любая современная электроника, правда как стало понятно в 19 веке, основана на $\mathbb{C}$. Затем математика начала набирать обороты. Виет ввёл буквы, Де Ферма ввел двойные числа, другое расширение $\mathbb{R} \cup \{d | d^2 = 0\}$, алгебризация актуальных бесконечно малых (17 век) [такое даже в стандартных курсах анализа не изучают]. Фон Лейбниц придумал детерминант (17 век). В 18 веке решались любые линейные системы, но уравнения более высоких степеней – нет. В 18 веке аналитически доказали основную теорему Алгебры. Началась алгебраическая теория чисел с работ Лежандра и Гаусса. В области решения уравнений Абелем и Руфини было доказано, что общее уравнение не решается в радикалах, то есть нет общей формулы. Затем Галуа придумал теорию Галуа, конечные поля, простые группы и эллиптические интегралы. Он дал ответ на вопрос, когда уравнения любой степени решаются в радикалах. Он ввел понятие группы и поля и с этого момента понимание алгебры стало меняться. В целом теория Галуа решает многие классические задачи, как трисекция угла например, так что является общекультурной вещью и странно, что она не вошла в стандартные курсы, хотя есть один учебник, которой предлагает рассказывать теорию Галуа школьникам. "Я не верю, что образование развивается. Если вы зайдете в лабораторию алгебры и теории чисел в Париже, там вы увидите учебник для гимназий, написанный Д.А.Граве в 5 году. В этом учебнике излагалась теория Галуа (1830 г.) Как образование оторвано от науки!".

После теории Галуа содержание алгебры стало немного смещаться. На самом деле любое алгебраическое уравнение может быть решено, не в радикалах разумеется. Формула для 5 степени была известна Гамельтону и Изенштейну. В некотором смысле, через базисы Грёбнера можно решать системы алгебраических уравнений любой степени (на компьютере разумеется). В 20 веке была решенв проблема, которой 35 веков, любая система алгебраических уравнений может быть решена. Но изменился и сам предмет. На какое-то время алгебра стала пониматься как изучение множеств с операциями. Этим занимались немецкие математики Дедекинд – кольцами, Форбениус, Жарданова форма и т.д. Потом происходило ещё несколько революций. 1920 Гильберт и Нётер. 1940-50 теория категорий и гомологическая Алгебра. 1960 современная алгебраическая геометрия. Собственно книги по темам:

- Шавалье "Введение в алгебру"
- Вандер Варден (1 перевод лучше второго)

Шавалье говорил "Алгебра играет такую же роль по отношению к математике, какую математика играет по отношению к физике."Алгебра – язык, инструмент, специфика которого в том, как что изучается. Сами математики разделяются по чувству комфорта:

- работают с числами – аналитики
- с картинами – геометры
- со словами – алгебраисты

0.2 План

Первый год алгебра будет играть служебную роль для остальных дисциплин. Так как "всё"выражается через линейную алгебру. Те же дифференциальные уранения могут быть хорошо аппроксимированы 1000000 линейных уравнений, как показал Фадеев в 60х годах, этот метод используется и по сегодняшний день.

0.2.1 I-ый семестр

1. Кольца и Арифметика
2. Многочлены и Поля
3. Модули и Векторные пространства (начала линейной алгебры)
4. Группы
5. Определители

0.2.2 II-ой семестр

1. Линейные операторы
2. Квадратичные и Эрмитовы формы
3. Кваторнионы
4. Теория Групп
5. Представления конечных групп

многие вещи стали прикладной математикой

0.2.3 III-ий семестр

1. Полилинейная алгебра
2. Теория категорий
3. Гомологическая алгебра

0.2.4 IV-ый семестр

??

Глава 1

Кольца и Арифметика Коммутативных Колец

1.1 Алгебраические операции

Пусть $X \neq \emptyset$ – множество.

Опр: *Бинарная алгебраическая операция* на X – это отображение $X \times X \longrightarrow X$.

Мы также можем рассматривать:

- $X \times Y \longrightarrow Z$ внешние операции
- $X \times X \times X \longrightarrow X$ тринарные
- $* \longrightarrow X$ нулярные
- $X \longrightarrow X$ унарные

И так, пусть у нас задано некое отображение $f : X \times X \longrightarrow X$. Тогда функциональная запись может быть префиксной $f(x, y)$ или fxy, инфиксной xfy, постфиксной $(x, y)f$ или xyf или интерфиксная $< x, y >$ ещё много как. Собственно в основном мы будем пользоваться инфиксной записью либо аддитивной со значком $+$ или мультипликативной со значками $\times$ или $\cdot$ или $*$.

Опр: *Нейтральным элементом* относительное некой операции $*$ называется элемент e, что $\forall x \in X, e * x = x = x * e$. Первая запись означает, что элемент левый нейтральный, а вторая, что элемент – правый нейтральный. В аддитивной записи нейтральный элемент обозначается 0_X, а в мультипликативной 1_x.

Опр: Элемент x' называется симметричным к x, если $x' * x = e = x * x'$. В аддитивной записи симметричный обычно называется противоположным, а в мультипликативной – обратным.

Заметим, что часта обратный элемент может быть обратим только с одной стороны. Элемент x называется обратимым слева (справа), если существует элемент y, называемый левым (правым) обратным, что выполняется $y * x = e$ $(x * y = e)$.

Опр: Операция $*$ называется ассоциативной, если $\forall x, y, z \in X (x * y) * z = x * (y * z)$. Раньше этот закон называли сочетательным. На самом деле он обозначает функциональное уравнение $f(f(x, y), z) = f(x, f(y, z))$.

Опр: Операция $*$ называется коммутативной, если $x * y = y * x$, устаревшее название – "переместительный закон".

На самом деле большая часть математики не коммутативна и мы будем отказываться от неё. Многие обычные формулы за некоторым исключением существуют в некоммутативном варианте и заучивать и использовать лучше сразу его. Например $(1/f)' = -f^{-1}f'f^{-1}$ [проверьте].

Абинкар писал, что есть 3 алгебры:

1. Школьная – уравнение и многочлены
2. Коледжная – группы, кольца, векторные пространства
3. Университетская – категории, функторы, комплексы, гомологии и когомологии

Мы же постараемся дойти до университетского уровня.

Давайте посмотрим чем же важны ассоциативные операции???. $e = e * e' = e' \Rightarrow e = e'$ единственность единицы? В общем случае ассоциативность есть не везде, бесконечные матрицы умножаются не ассоциативно. В анализе на такие бесконечные объекты накладывается условие сходимости, что делает операции вновь ассоциативными.

Ассоциативность ещё хороша тем, что правые и левые обратные совпадают, то есть $x * y = e$ и $x * z = e$, тогда $y = y * (x * z) = (y * x) * z = z$.

Про расстановку скобок есть замечательный пример. Количество способов посчитать неассоциативую операцию из n множителей называется n-ым числом Каталана. Предлагаю вам найти формулу для таких чисел или можете прочитать про них в книге "Не совсем наивная теория множеств". С числами Каталана также связаны числа Родригеса.

На самом деле в школе уже были неассоциативные операции, например деление и вычитание, но обычно их не используют как основные операции, хотя существуют логические извращения, когда для групп задают только операцию разности, но мы таким не будем заниматься. Другое не ассоциативной операцией было возведение в степень. Причем нужно отметить, что устоявшаяся запись левонормирована (скобки расставляют с начала с лева), а не более общепринятая правонормированная.

Другой знакомой вам не ассоциативной операцией является векторное произведение (cross product). Но она удовлетворяет иному тождеству, которое часто заменяет ассоциативность. *Тождество Якоби* $(u \times v) \times w + (v \times w) \times u + (w \times u) \times v = 0$. Об этом тождестве Арнольд говорил следующее "Это тождество означает, что высоты треугольника пересекаются в одной точке."

1.2 Моноиды

Опр: $(X, *, e)$ называется *мноидом*, если:

1. $*$ ассоциативна
2. существует нейтральный элемент e

Опр: *Полугруппа* – это моноид без единицы.

Примеры: $(\mathbb{N}, \times, 1)$, $(\mathbb{N}_0, +, 0)$, $(\mathbb{N}, \vee, 1)$, $(\mathbb{N}_0, \wedge, 0)$, $(2^Y, \cap, Y)$, $(2^Y, \cup, \emptyset)$, $(2^Y, \triangle, \emptyset)$ – это всё моноиды.

Так как формально всегда можно присоединить единицу, то с алгебраической точки зрения нет особой разницы изучать структуры без неё или с.

1.2.1 Сокращения

Опр: Элемент $x \in X$ называется **регулярным слева (справа)**, если на него можно сокращать слева (справа).

$$\forall x, z \in X,\ x * y = x * z \Rightarrow y = z\ (y * x = z * x \Rightarrow y = z)$$

Лемма: Элемент $x \in X$ обратимый слева/справа, регулярен слева/справа.

Прошу заметить, что в доказательстве СУЩЕСТВЕННУЮ роль играет ассоциативность. В общем неассоциатвном случае это вообще говоря не верно. В продолжении мы докажем теорему Фробениуса, которая покажет где нам нужно будет остановится в построении расширений действительных чисел. Всем известны 4 тела, последнее из которых неассоциативно $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, $\mathbb{O}$. Так в $\mathbb{O}$, несмотря на отсутствие ассоциативности, любые два элемента пораждают ассоциативную

алгебру, то есть они альтернативны. Неассоциативность всё же ограничена. Так что обычно этот ряд не продолжают. Теорема говорит, что кроме первых трёх, нет других ассоциативных тел, а её обобщенная версия показывает, что други конечномерных тел над $\mathbb{R}$ кроме этих 4х нет. Мы получим последовательность $1, 2, 4, 8$. На самом деле для 16 есть сединионы Диксона, но хоть каждый элемент там обратим, но там также есть делители нуля. Это показывает, что в неассоциативном случае наша интуиция перестаёт действовать. На самом деле все наши обычные рассуждения основаны на ассоциативности. А если её нет, то всему нужно учится с нуля.

Докозательство: Пусть $u * x = e$ и $x * y = x * z$, тогда $y = e * y = (u * x) * y = u * (x * y) = u * (x * z) = (u * x) * z = e * z = z$. С другой стороны аналогично.

Но регулярный не обязательно обратим. Важнейшим классом моноидов являются те, в которых каждый элемент обратим. Такие моноиды называются группами. [Теорема Руфини-Абеля]. Моноиды, в которых операция коммутативна, называются коммутативными, но группы называются абелевыми. Есть и Кайновы группы, кстати.

1.3 Группы

Группы – один из важнейших и первейший исторический пример алгебраических систем. Формально группы были определены впервые Галуа, причем было видно как это понятие у него в работах возникает. В начале он просто говорил "Grouper les permutation то есть группировать перестановки. Потом возник термин группа перестановок, а в конце 19 века уже была развита теория групп, в первую очередь конечных групп, но на самом деле не только. Так вот это одно из важнейших математических понятий, структур. Придумать аксиом можно сколько угодно, важность структур, которые реально изучают, определяется не их сложностью и многообразием. Важность и определение структуры для работающего математика – это не набор свойств или аксиом, а набор содержательных не тривиальных примеров. И такое замечательный алгебраист Адреан Альберт, русский кстати, но он работал в Чикаго, хотя при этом был русским, так вот Адреан Алберт говорил, что математическую структуру имеет смысл изучать, если есть 3 разных содеражательных пример. Но вот у групп больше совершенно чем 3 разных содержательных примеров.

Опр: $(G, \cdot(=\text{mult}), .^{-1}(=\text{inv}), 1)$ – группа, где
$i)$ mult $: G \times G \longrightarrow G,\ (x, y) \mapsto x \cdot y$
$ii)$ inv $: G \longrightarrow G,\ x \mapsto x^{-1}$
$iii)$ $1 \in G$
для которых выполнено:
1) ассоциатиность $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
2) нейтральный элемент $1 \cdot x = x = x \cdot 1$.
3) обратный $\forall x \exists x',\ x \cdot x' = x' \cdot x = 1$

Многие буквы на самом деле говорящие. G – group, R – ring, K – Körper, F - field, A - anneau, M - module, V - vector space.

Переход от элемента к обратному является антиавтоморфизмом группы порядка 2. $(xy)^{-1} = x^{-1}y^{-1}$ и $(x^{-1})^{-1}$. Очень важно помнить правильные формулы. Мы надеваем педжак, а потом пальто, снимают их обычно в ином порядке. Если $xy = yx$, то мы говорим, что они коммутируют.

Мы не будем заниматься ослаблением свойств групп, так как это абсолютно бессмысленная деятельность.

1.3.1 Элементарный свойства групп

1. Сокращение $xy = xz \Rightarrow y = z$ и $yx = zx \Rightarrow y = z$.

2. Деление $\forall h, g \exists! x$ т.ч.$hx = g$, (а именно $x = h^{-1}g$) $\exists! y$ т.ч. $xh = g$ (–//– $x = gh^{-1}$). Деление бывает справа и слева и это не одно и тоже.

На самом деле есть всякие интересные обобщения группы. Если вы присмотретесь, то нигде выше единица не фигурирует, в возможностях сокращения и деления. Так вот можно изучать, и собственно изучались и очень важны структуры в которых операция не ассоциативна, но тем не менее сокращение всегда возможно и деление всегда возможно, это так называемые квази

группы. Тогда огромная часть того, что доказывается для групп имеет смысл и для квазигрупп. Например латинские квадраты и есть квазигруппы.

[$\mathbb{Z}/(10)$ при обычном сложении мы отдельно смотрим на единицы и отдельно на десятки и гомологии помогают из двух групп по модулю 10 получить по модулю 100.]

Так что то, чем мы занимаемся, так это напоминание в Платоновском смысле. До рождения человек знает всё, но вовремя забывает. И всё что он делает в жизни, так это не учит, а вспоминает.

Примеры:

- $(\mathbb{Z}, +)$ бесконечная циклическая группа
- повороты n угольника $C_n \cong \mathbb{Z}/(n) \cong \mu_n$ конечная циклическая группа, классы вычитов по n и группа n-ых корней из 1 в $\mathbb{C}$ $|C_n| = n$ – порядок группы.
- D_n – диэдральная группа, группа симметрий правильного n-угольника. $|D_n| = 2n$
- S_n – симметрическая группа степени n. Основное, что нужно знать из теории множеств, так это то, что композиция ассоциативна. Bij(X, X) – симметрическая группа биекций X. Так как мы обычно пишем функции слева, то композиция направлена в обратную сторону! Редко кто пишет в категорном стиле $(x)sin$. (Bij$(X), \circ, .^{-1}, id_X$). Если f – биективно $\Leftrightarrow$ f – обратимо. [Вы должны читать не то, что здесь написанно, а то, что я думаю.] Пусть $\underline{n} = \{1, 2, ..., n\}$. Так вот $S_n = S_{\underline{n}}$. $|S_n| = n!$. Интересная книжка "Три поросёнка"Мацумаса, где обсуждается сколько способов рассадить 3 парасёнка по 3–м домикам. Разные случаи там могут быть, поросята могут сидеть вместе, в каком порядке их съедает волк итд. Это всё обсуждают волк и его друг жаб Сократ. Когда мы увидим действие групп, то поймём, что любая конечная группа вкладывается в некотрый S_n.
- $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, ...
- $(\mathbb{R}^*, \cdot)$, $(\mathbb{R}_{>0}, \cdot)$
- π группа углов. Её можно получить на окружности, зафиксировав 1 и проводя параллельные прямые. Возьмём две точки на окружности, проведем через них прямую, проведём параллельную к ней через 1. Эта прямая пересечет окружность в новой точке, назавём её произведение двух предыдущих. Эта операция образует топологическую группу изоморфную $\mathbb{R}/\mathbb{Z}$.

Опр: G – абелева, если умножение коммутативно.

Опр: $\varphi : H \longrightarrow G$ – гомоморфизм групп, если $\varphi(xy) = \varphi(x)\varphi(y)$.

Пример: exp $: (\mathbb{R}, +) \longrightarrow (\mathbb{R}_{>0}, \cdot)$ - гомоморфизм и более того изоморфизм. Аналогично про логарифм.

На самом деле разные классы морфизмов имеют разные названия. Инъективный гомоморфизм групп называется мономорфизмом, но в общем случае это совершенно не тоже самое, что инъективный гомоморфизм. Это не так например для колец. Сюрьективный называвает эпиморфизмом, биективный называется изоморфизмом. В предыдущем примере мы видели именно изоморфизм. В топологии это совершенно не так, поэтому она существенно сложнее. Обратное тоже должно быть морфизмом! Если между двумя объектами есть изморфизм, то говорят, что они изоморфны. В этом случае объекты не различаются. Гомоморфизм на себя называется эндоморфизмом. Изоморфизм – автоморфизмом. Приставка анти- означает замену порядка.