записанно by Georgii Potoshin

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 permutations 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 Адриан Альберт, русский кстати, но он работал в Чикаго, хотя при этом был русским, так вот Адриан Альберт говорил, что математическую структуру имеет смысл изучать, если есть 3 разных содержательных 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) ассоциативность $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
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 пиджак, 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 присмотритесь, 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 квазигруппы. 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 вычетов 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 поросёнка 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 некоторый 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, назовём 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 называется 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.

1.4 Кольца. Первые примеры

Кольца тоже одно из основных понятий алгебры и математики в целом, так как очень много различных объектов, возникающих в разных ситуациях, имеют структуру кольца.

Опр: Кольцо – это множество с двумя операциями сложением и умножением. Относительно сложения кольцо образует абелеву группу, а умножение дистрибутивно (с двух сторон) относительно сложения.

$.^+$ – функтор из категории колец в категорию абелевых групп. То есть R^+ это тоже самое множество, только без умножения. Функторы, грубо говоря, это срелки которые все объекты одной категории превращают в объекты другой. А морфизмы одной категории согласовано превращаются в морфизмы другой.

Обычно рассматриваются ассоциативные кольца с единицей. То есть умножение ассоциативно, и есть нейтральный элемент относительно умножения. Так как мы хотим в будущем вкладывать область целостности в поле частных, то нам нужно, чтобы нуль и один не совпадали. Иначе вложение не удастся. В этой главе большинство колец ещё будут коммутативными (умножение).

Бывают ли коммутативные не ассоциативные кольца? Да, например Грайс использовал такое при построении большого монстра.

Опр: Ассоциативное кольцо с 1 называется телом (fr. corp, en. skew-field), если каждый элемент, кроме нуля, обратим. То есть моноид получаемый из кольца выкидыванием нуля и сохранением только умножения $R^\bullet = R\backslash\{0\}$ является группой. Также будет ещё один функтор R^* – группа обратимых элементов.

Опр: R называется полем, если оно коммутативное тело.

Примеры:

- $\mathbb{Z}$ – целые числа (Zahlen)
- $\mathbb{Z}[1/2]$ – кольцо двоичных дробей
- $\mathbb{Z}[1/2, 1/3, 1/5] \subseteq \mathbb{Q}$ (quotient)
- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ – поля
- $\mathbb{Z}/n\mathbb{Z}$ – кольцо классов вычитов по модулю n

Мы писали фактор кольцо по идеалу $I \trianglelefteq R$. Математике вам нужно учиться, как маленькие дети учатся языку. Маленьким детям не объясняют каждое слово, им говорят "Вот посмотри, это фактор кольцо, вот это к-цикл". И когда вы услышите 5 раз использование этих слов, то вы будете понимать, что они значат, даже если вы не будете знать определения. Определение можно будет выучить уже позже, потому что за всем этим должно стоять понимание, если его не будет, то все слова и формулы – это просто дым. Математика живет только в понимании, сами последовательности буковок ничего не значат.

1.4.1 Таблицы Кэли Cayley (≠ Келли Kelley)

Артур Кэли провел детство в Петербурге до 12 лет, (но Кантор там родился). Кэли разумеется Британский математик, и по началу он был юристом, поверенным в наследственных делах, но за это время написал порядком 200 работ и конечно потом стал профессором в Кембридже. Он был одним из классиков алгебры и многие вещи из линейной алгебры, теории групп восходят к нему.

Как заметил Галуа, $\mathbb{Z}/4\mathbb{Z} \ncong \mathbb{F}_4$. Поэтому посмотрим на $\mathbb{Z}/4\mathbb{Z} = \{[0], [1], [2], [3]\} = \{0, 1, 2, 3\}$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Мы выполняем операции над представителями классов, а затем берём остаток и записываем класс через его представителя. Можно заметить, что первая таблица является латинским квадратом! То есть в каждой строке и столбце элементы различны. Это ровно означает, что эта операция задаёт квазигруппу, то есть, что можно сокращать. В группе мы можем сокращать, а значит всё верно и у нас должен был получиться латинский квадрат.

Простейший следствия аксиом кольца $0 * x = 0 = x * 0$. В элементарных учебниках любят такие теоремы, я не буду говорить где такое есть, но если вы поищете, то найдете такого много.

Обратите внимание! $2 \neq 0$, но $2 * 2 = 0$. Ненулевые числа, что не являются нулями, но в произведении дают нуль называются *делителями нуля*, а те, что в некоторой целой степени дают нуль, *нильпотентами*. Нильпотенты, это то, что в анализе называется бесконечно малым некоторого порядка, их впервые начали рассматривать в 17 веке де Ферма и фон Лейбниц. [проверьте или проверьте] Они начали рассматривать буковку d, что в некоторой степени равна нулю. А потом

следующий поколения забыли, что эта буковка значит и стали писать d от x и начали говорить, что это какой-то дифференциал и так далее.

Если из таблицы умножения мы выкинем нулевые строки, то не получим латинского квадрата, а значит умножение не образует группу и $\mathbb{Z}/4\mathbb{Z}$ не поле.

На самом деле на любой абелевой группе можно ввести структуру кольца ассоциативного и коммутативного, но при этом без единицы. Условие существования единицы – очень сильное условие, хотя к любому кольцу можно добавить 1.

1.4.2 Кольцо с нулевым умножением

Если A это у нас любая абелева группа по сложению, тогда определим умножение следующим образом $x \cdot y \mapsto 0$. Вопрос какие операции можно ввести – отдельный.

1.4.3 Булево кольцо множеств

Пусть X – любое множество, тогда можем рассмотреть $R = 2^X$ множество всех подмножеств X, тогда на R можно ввести следующие операции сложения и умножения. Для $Y, Z \subseteq X$, то положим $Y + Z = Y \triangle Z$, что называется или Булевой суммой или симметрической разностью. Тогда нетрудно осознать, что такая сумма коммутативна, ассоциативна, $0 = \emptyset$. В нём $2y = 0$, то есть характеристика равна 2. В качестве произведения возьмём пересечение, тогда в этом кольце $1 = X$. Такое умножение, кстати, коммутативно, ассоциативно, дистрибутивно относительно сложения. Заметим, что в этом кольце $y^2 = y$, то есть любой элемент является *идемпотентом*. Есть целый раздел, теория решеток, где такие кольца играют большую роль.

1.4.4 Следствия и аксиом

Так как сложение образует группу, то в кольце определено вычитание. Тогда все обычные свойства будут выполнятся.

$$x(y-z) = xy - xz$$
$$(x-y)z = xz - yz$$
$$(-1)x = -x$$
$$(-x)(-y) = xy$$
$$\dots$$

Моральный смысл такое, что коммутативное ассоциативное кольцо с единицей – это то место, где выполняются все правила школьной алгебры, кроме деления и сокращения. С делением всё сложнее, так как в отсутствие коммутативности деление слева и справа это совсем не одно и тоже $x/y = xy^{-1} \neq y \backslash x = y^{-1}x$.

Давайте на кое-что посмотрим что можно в кольце $(x+y)(x-y) = x^2 + yx - xy - y^2$. Назовём аддитивным коммутатором следующее $[y,x] = yx - xy$. Если элементы коммутируют, то получится школьная формула, но вообще это может быть неверным. Точно также в коммутативном кольце выполняется формула бинома Ньютона, но не верна в некоммутативном! $(x+y)^2 = x^2+xy+yx+y^2$. В частности подставлять матрицы в школьные формулы НЕЛЬЗЯ! Так многие формулы во многих курсах даются неверными. $(fg)' = f'g + fg'$ обратите внимание на верный порядок! Если операция не коммутативна, то нужно очень аккуратно следить за порядком сомножителей. И тогда гораздо лучше учить сразу правильные некоммутативные формулы.

1.5 Простейшие конструкции колец

1.5.1 Конструкция многочленов

Из коммутативного ассоциативного кольца с 1 R можно построить кольцо многочленов от одной переменной $R[t]$. Коммутативность нам нужна, чтобы подстановка была гомоморфизмом. Произведения переходили в произведения и так далее. В противном случае многочлены бесполезны и ничего не значат. Элементами кольца являются следующие выражения $f = a_n t^n + a_{n-1} t^{n-1} +$

$... + a_0$, где $a_i \in R$. Многочлены равны, когда они равны формально, то есть когда равны их коэффициенты. Сложение происходит покоэффициентно, а умножения такое же как в школе, но на самом деле является простым случаем свертки (свертка впервые была придумана Фадеевым в Питере). $R[t]$ хорошо устроено и удолетворяет всем аксиомам коммутативного ассоциативного кольца с 1. То есть мы получили способ по одному кольцу строить другое кольцо. Дальше можно строить многочлены от нескольких переменный $R[t_1, ..., t_m]$, кольца многочленов от некоммутирующих переменных $R\langle x, y\rangle$, то есть xy и yx линейно независимы. Так как мы хотим потом вместо t подставлять что угодно, то нам требуется, чтобы кольцо коэффициентов было коммутативным. Формальное определение будет дано в следующей главе.

1.5.2 Конструкция матриц

Следующий пример, важнейший, кольца, это кольцо матриц. Этот пример – один из первых некоммутативных примеров, который в математике стал систематически изучаться, который формально определил Кэли в 1842 году. Хотя конечно формулы умножений матриц, это формулы линейных замен переменных и эти формулы вы найдёте у Эйлера за 100 лет до этого. Кольцо матриц это следующая конструкция, мы стартуем с любого ассоциативного кольца с 1, не обязательно коммутативного. Коммутативность важна только для определения транспонированной матрицы, так обычное определение работает только для коммутативных колец, то есть кольца матриц над коммутативными кольцами обладают некоторой спецификой, но правильно определить можно для любого кольца. Возьмём ещё натуральное число. Тогда по этим двум данным мы строим $M(n, R)$ – кольцо квадратных матриц степени n над R. Что это такое мы будем обсуждать в 3-й главе. Матрица, пока не важно что это такое, изображается следующей картинкой

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}, a, b, c, d \in R$$

Сложение устроено следующим образом, они складываются поэлементно

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}$$

Вы хотите сказать, что матрицы умножаются тоже поэлементно?

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} * \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae & bf \\ cg & dh \end{pmatrix}$$

Так конечно будет очень круто, это вовсю используется в вычислительной математике на каждом шагу, но только это называется *умножение матриц по Адамару или по Шуру*. Шур кстати величайший белорусский математик времен и народов Иссая Шур, действительно великий алгебраист. Это поэлементное умножение матриц настоящая очень хорошая и важная операция, но в действительности в кольце матриц умножение другое. Это будет охвачено в конструкции прямых сумм, а умножение матриц в действительности – композиция линейных отображений. Ну а в терминах того, что мы скоро узнаем, умножение матриц – ещё один пример свертки. Собственно матрицы умножаются следующим образом:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}$$

Мы смотрим на строки первой матрицы и на столбцы второй, как мы умножаем строчку на столбец.

$$\begin{pmatrix} x_1 & ... & x_n \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = x_1y_1 + ... + x_ny_n$$

Мы также можем умножать столбец на строчку

$$\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \begin{pmatrix} x_1 & ... & x_n \end{pmatrix} = \begin{pmatrix} y_1x_1 & \cdots & y_1x_n \\ \vdots & \ddots & \vdots \\ y_nx_1 & \cdots & y_nc_n \end{pmatrix}$$

В итоге получиться матрица ранга 1. Причем тут мы не определяем ранг, а именно матрицу ранга 1. Те определения, что вам даются должны восприниматься nominal value, то есть если что-то определяют, то не определяют слова, по отдельности входящие во что-то, мы определяем целую фразу. Оно совпадает с обычным определением ранга, если в итоге матрица не будет нулевой, а наш ранг называется тензорным рангом, для поля определения совпадают (нет делителей нуля?!). По сложению матрицы образуют абелеву группу, но в действительности они образуют R-модуль. Матрицы можно умножать и слева и справа на скаляры и там будут выполнятся свойства, такие же как для векторных пространств, сложение векторов и умножение векторов на скаляры. Умножение матриц очевидно дистрибутивно относительно сложения, чуть сложнее проверяется ассоциативность умножения, это конечно можно было бы сделать здесь, но так как в дальнейшем мы узнаем, что вообще любая свертка ассоциативна, то мы этого делать не будем. Умножение матриц НЕ КОММУТАТИВНО, пример для неквадратных мы только что видели. В квадратных же есть *стандартные матричные единицы.* Для случая 2×2 они следующие:

$$e_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},\ e_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},\ e_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix},\ e_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Ну вот легко проверить, что $e_{ij}e_{hk} = \delta_{jh}e_{ik}$, где $\delta_{jh} = \begin{cases} 1, & j = h \\ 0, & j \neq h \end{cases}$ дельта Крòнекера, для ударения поищите стишок Манина. Тогда например $e_{12}e_{21} = e_{11} \neq e_{22} = e_{21}e_{12}$. К тому же вы можете обнаружить, что в кольце матриц есть нильпотенты $e_{12}^2 = 0$. Нетривиальные идемпотенты $e_{11}^2 = e_{11}$. Тогда мы получили способ строить по ассоциативному кольцу с единицей новые ассоциативные кольца с единицей. Единицей кольца матриц как нетрудно заметить является

$$1_{M(n,R)} = e_{11} + \ldots + e_{nn} = \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix} = e \quad \text{(от Einheit)}$$

1.5.3 Непример кольца!

Философская шутка Венгенштейна "предположим, что n не есть число овец". Посмотрим на $(R[t], +, \circ)$, где $\circ$ – композиция многочленов, то есть $f \circ g = f(g)$. Например $t^2 \circ (t+1) = (t+1)^2 = t^2 + 2t + 1$, а $(t+1) \circ t^2 = t^2 + 1$. По сложению, это абелева группа, композиция ассоциативна, ну потому что это почти что композиция соответствующих полиномиальных отображений, будет у нас и нейтральный элемент t относительно композиции. А теперь дистрибутивность $(f_1 + f_2) \circ g = (f_1 + f_2)(g) = f_1(g) + f_2(g) = f_1 \circ g + f_2 \circ g$, и в этот момент хочется сказать, что это кольцо. Но что на счёт второй дистрибутивности? Что означает, что $f \circ (g_1 + g_2) = f \circ g_1 + f \circ g_2$? Это ровно значит, что это линейный многочлен. Для поля характеристики p это конечно будет чем-то послабее, то есть, что это многочлен от t^p, но в общем случае вторая дистрибутивность выполняется очень редко. Для некоммутативной ситуации левая дистрибутивность и правая дистрибутивность не зависима и нужно проверять обе! И это очень существенно.

1.5.4 Конструкция прямой суммы

Пусть R, S – два кольца. Тогда их прямая сумма $R \oplus S$ – это по сути их декартого произведение со следующими покомпонентными операциями $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$ и $(x_1, y_1) \cdot (x_2, y_2) = (x_1 x_2, y_1 y_2)$. Все знают, что у пар нет элементов, вернее что является их элементами не известно, у них есть компоненты. Пары конечно же модулируются в теории множеств, но модулируются разными способами и именно пары. В такой конструкции все тождества, выполняющиеся для компонент прямой суммы выполняются и для неё самой, например коммутативность, ассоциативность или обладание единицей. Аналогично определяется прямая сумма конечного числа колец $R_1 \oplus \ldots \oplus R_t$. Для бесконечного числа колец возникают разные нюансы, которые мы пока не будем обсуждать, мы будем их обсуждать для модулей, различие прямого произведения и прямой суммы и так далее. Грубо говоря прямая сумма сводит своё изучение к изучению её компонент. Почему не рассматривается конструкция матриц с поэлементным умножением, так мы получим просто прямую сумму.

1.6 Противоположное кольцо

Очень важная конструкция для некоммутативных колец, которая на понадобится, например при определении транспонировании матриц, потому что обычно транспонирование матриц определяется неправильно в учебниках, то есть оно определяется правильно только для случая, когда коэффициенты коммутативны. Это конструкция противоположного кольца.

R^o - (opposite) противоположное кольцо. К его построению можно подходить двояко. Пусть $R^o = R$ как множество с тем же сложением, но с другим умножением, $x \circ y = yx$. Тогда R – коммутативно $\Leftrightarrow R^o = R$ как кольцо. Вторая конструкция следующая, часто удобно считать, что мы создаём копию кольца R, то есть не те же элементы, а элементы, находящиеся в взаимно однозначном соответствии, $R \leftrightarrow R^o,\ x \leftrightarrow x^o$. Тогда мы определяем сумму двух элементов противоположного кольца, как элемент противоположный к сумме этих двух $x^o + y^o = (x+y)^o$, а произведение, как образ произведения в противоположном порядке $x^o \cdot y^o = (yx)^o$. Тогда $R \longrightarrow R^o,\ x \mapsto x^o$ – антиизоморфизм колец. Я ещё формально не определил гомоморфизм колец, но я надеюсь, что все понимают что это такое. Гомоморфизм колец – это отображение из одного кольца в другое, что переводит сумму в сумму, произведение в произведение, 0 в 0 автоматически, а 1 в 1 это нужно постулировать. Таких примеров я вам приведу в большом количестве, например вложение прямого слагаемого в прямую сумму не переводит единицу в единицу. Если мы рассмотрим $R \hookrightarrow R \bigoplus S \hookleftarrow S$, то тогда мы получим $x \mapsto (x, 0)$ и $(0, y) \mapsfrom y$. И тогда например при первом отображении единица кольца R переходит в не единицу кольца $R \oplus S$ $(1_R, 0)$, потому что единиц будет пара единиц $1_{R \oplus S} = (1_R, 1_S)$. Это пример гомоморфизма колец без единицы, при котором сумма переходит в сумму, произведение в произведение, так как это так определяется, то есть это гомоморфизм колец, но единица не переходит в единицу, поэтому это неунитальный гомоморфизм (unital ≠ unitary). Вернёмся к операции перехода к противоположному кольцу, там тоже самое, но только произведение переходит в произведение, но в обратном порядке. Такие отображения тоже очень часто встречаются и естественным образом возникают. Я пока намекну, что транспонирование матриц $M(n, R) \longrightarrow ...$, если мы хотим, чтобы оно обладало обычными свойствами, то есть чтобы матрица, транспонированная к произведению, будет произведением транспонированных, в обратном порядке $(xy)^t = y^t x^t$. Почему в обратном порядке, ну там скажем матрицы - это отбражения правых линейных пространств, а транспонированная матрица будет матрицей линейного отображения левых векторных пространств. Поэтому композиция в одном порядке должна заменятся на композицию в другом порядке. Так вот чтобы это выполнялось, транспонирование должно бить из кольца матриц над R не в само же кольцо, а в кольцо матриц над противоположным кольцом. То есть $M(n, R) \longrightarrow M(n, R^o)$. Но если кольцо коммутативно, то противоположное совпадает с самим кольцом, а значит транспонирование будет обычным.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^t = \begin{pmatrix} a^o & c^o \\ b^o & d^o \end{pmatrix}$$

Рассматривание противоположных колец, кстати, позволяет полностью избавится от антигомоморфизмов, так как антигомоморфизм – это просто гомоморфизм в противоположное кольцо, так что можно рассматривать только гомоморфизмы.

1.6.1 Формальное присоединение единицы

Последняя конструкция, это присоединение единицы, которая делает возможным рассматривание только колец с единицей. Но в действительности не все гомоморфизмы переводят единицы в единицы, с чем сопряжены некоторые проблемы. Пусть R – любое кольцо, вообще говоря без 1. Рассмотрим прямую сумму абелевых групп $\mathbb{Z} \oplus R = \{(m, x) | m \in \mathbb{Z}, x \in R\}$ со следующими операциями $(m, x) + (n, y) = (m + n, x + y)$ и $(m, x)(n, y) = (mn, my + nx + xy)$. Вы могли задастся вопросом, а как мы умножаем целое число на элемент кольца, и это хороший вопрос. Тогда для $n \in \mathbb{Z}, x \in R$ определим $nx = x + ... + x$ (n раз).

$$\cdots,\ 2x = x + x,\ 1x = x,\ 0x = 0,\ (-1)x = -x,\ (-2)x = 2(-x),\ \cdots$$