



Гильмуллин, М. Ф. Зачем нужна алгебра? О книге «Библия математика» // Математика с Мансур-абый. 2025. URL: <https://history-math.org/ru/publications/hm-tt-ea92383ab5d3-ru/>. Дата публикации: 03.02.2025.

ОЧЕРК

Зачем нужна алгебра? О книге «Библия математика»

Вышла новая книга Мансура Гильмуллина: «Библия математика. Основы высшей и линейной алгебры». Рассказываем, о чём эта книга и зачем нужна алгебра.

Мансур Гильмуллин · 03.02.2025 · RU

[Статья на сайте журнала](#)



Автор Мансур Гильмуллин и тираж его книги «Библия математика. Основы высшей и линейной алгебры» (2024) · [Источник](#)

В декабре 2024 года мы поделились с вами радостной [новостью о публикации новой книги](#) Мансура Гильмуллина «Библия математика. Основы высшей и линейной алгебры». Её можно найти на сайте издательства Ridero.ru поиском: [«Гильмуллин Библия математика»](#). А в этой статье подробнее расскажем, о чём эта книга и зачем нужна алгебра.

Об алгебре

Происхождение термина «алгебра» связывают с сочинением Мухаммеда аль-Хорезми (ок. 787–850, Багдад) «Хисаб аль-джабр ва-л мукабала» («Исчисление восполнения и противопоставления»). Эта книга стала известна в латинском переводе, и слово «аль-джабр» (algebra) стало употребляться как синоним всей науки алгебры, которая до XIX в. была наукой о решении уравнений. «Аль-джабр» означает «восполнение», то есть перенос вычитаемых членов в другую часть уравнения.



Изображение Мухаммеда аль-Хорезми (ок. 787–850) на специальной марке СССР номиналом 4 копейки от 6 сентября 1989 г. по случаю 1200-летия со дня рождения, а также титульный лист его книги «Хисаб аль-джабр ва-л мукабала» · [Источник](#)

В наши дни происходит «алгебраизация» математики: то есть идеи и методы алгебры проникают в теоретические и в прикладные разделы математики. Естественные науки XX века резко расширили сферу применения алгебры. Например, почти все методы линейной алгебры превратились в аппарат, который используют при формулировке фундаментальных законов природы и алгоритмов решения прикладных задач.

Алгебраические методы также весьма полезны при моделировании задач экономики и конструировании архитектуры современных компьютеров. Алгоритмы теории чисел получили новую жизнь в связи с развитием компьютерной алгебры и её приложений: анализа сложности алгоритмов и криптографии.

Современная алгебра определяется как наука об алгебраических системах — множествах с операциями и отношениями над их элементами. Классическая алгебра — это наука о задачах, которые сводятся к решению алгебраических уравнений. Она также является частью современной алгебры.

Зачем нужна алгебра

Под абстрактной оболочкой большинства алгебраических теорий стоят конкретные задачи теоретического или практического характера. В своё время они дали импульс к созданию новых теорий и средства к решению новых задач.

Сложное взаимодействие теоретических и прикладных аспектов математики, и особенно алгебры, оправдывает принятый нами концентрический стиль её развёртывания — к вводимым понятиям мы возвращаемся несколько раз на разных уровнях.

Сформулируем несколько прикладных задач математического моделирования, которые будут мотивировать изучение теоретических методов алгебры, используя книгу [«Библия математика»](#).

Методы шифрования

На алгебре, конкретнее на теории сравнений, которая излагается в главе 10 книги, основаны многие современные методы шифрования информации. Например, RSA (аббревиатура от фамилий Rivest, Shamir и Adleman, 1978) — популярный криптографический алгоритм с открытым ключом, основанный на вычислительной сложности факторизации, то есть разложения на простые множители, больших полупростых чисел. Это такие натуральные числа, которые представляются в виде произведения двух простых чисел.

RSA является системой, пригодной для шифрования, дешифрования и цифровой подписи. Основными средствами в ней являются функция Эйлера и основанная на ней малая теорема Ферма: $a^{p-1} \equiv 1 \pmod{p}$. Малая теорема Ферма является также основным инструментом в теории конечных колец и полей, которые встречаются в материалах главы 8 книги.

Таким образом, алгебра помогает решению прикладных задач теории информации.

Уменьшение размерности данных

Один из основных способов уменьшить размерность данных, потеряв наименьшее количество информации, — это метод главных компонент (Principal Component Analysis, PCA). Хотя метод был изобретён Карлом Пирсоном ещё в 1901 году, он с каждым годом расширяет приложения: сжатие данных, обработка изображений, эконометрика и биоинформатика.

Этот метод используется теперь в науке о данных (Data Science) и в машинном обучении (Machine Learning). В анализе данных обычно создают некую упрощённую модель, максимально точно описывающую реальное положение дел. Часто бывает так, что статистические признаки объекта довольно сильно зависят друг от друга и их одновременное наличие избыточно. Но гораздо чаще бывает так, что они зависят не так строго и явно. Зная зависимости и корреляцию между ними, можно выразить несколько признаков объекта через один. Избежать потерю информации не удастся, но минимизировать её помогает как раз метод PCA.

Вычисление главных компонент сводится к разложению эмпирической ковариационной матрицы данных и к вычислению собственных векторов и собственных значений этой матрицы: $Mx = \lambda x$. О них можно узнать из главы 7 книги.

Таким образом, алгебра помогает решению статистических задач.

Эллиптические кривые

Эллиптические кривые используются в качестве основы для построения криптосистем с середины 80-х годов прошлого века и инструмента решения некоторых теоретико-числовых задач, например, для факторизации и тестирования чисел на простоту. Также в теории чисел они были использованы Эндрю Уайлсом при доказательстве великой теоремы Ферма. Об этих понятиях можно узнать из глав 8–10. Исторически термин «эллиптическая кривая» происходит от термина «эллиптический интеграл», что показывает связь методов алгебры и математического анализа.

Если характеристика поля не равна 2 или 3, что включает поля нулевой характеристики, например, числовые поля, то общее уравнение эллиптической кривой с помощью замены координат приводится к канонической форме: $y^2 = x^3 + ax + b$, которая называется нормальной формой Вейерштрасса.

Сегодня криптосистемы на эллиптических кривых используются в важнейших технологиях, на которых базируется вся современная защита в интернете, крипто- и цифровые валюты, алгоритмы формирования и проверки электронной цифровой подписи (ЭЦП).

Интеллектуальный анализ данных

Одной из фундаментальных задач при анализе больших данных является упрощение структуры данных с максимальным сохранением нужной информации. В подходах к её решению принято выделять методы сокращения размерности пространства данных и методы классификации и кластеризации.

Методы интеллектуального анализа больших данных обычно используют алгоритмы умножения AB и обращения A^{-1} квадратных матриц больших порядков. Также используются новые алгебраические системы, такие как бигрупповые алгебры, некоммутативные $ab \neq ba$ и неассоциативные $(ab)c \neq a(bc)$ алгебраические структуры. Про эти базовые понятия можно узнать из глав 2, 4 и 5 книги.

Таким образом, синтез алгебраических и геометрических подходов, а также методов топологической, линейной и компьютерной алгебр, способствует разработке эффективных алгоритмов решения сложных задач в различных научных и прикладных областях средствами искусственного интеллекта (ИИ).

О курсе алгебры в «Библии математика»

С 90-х годов XX века программы по алгебре в вузах постоянно меняются. Это связано с тем, что в различных направлениях подготовки к выпускникам предъявляются разные требования, связанные с их будущей профессиональной деятельностью.

В программах обучения, которые предлагались в разные годы в вузах педагогического, экономического, технического профиля, вопросы введения в алгебру, общей и линейной алгебры, теории чисел объединялись.

Главная цель курса, например, для педагогических направлений подготовки (математики, информатики, физики) — изучение основных алгебраических систем и воспитание алгебраической культуры, которая необходима будущему учителю, чтобы глубоко понимать цели и задачи школьного курса математики и дополнительного математического образования.

Цель дисциплины для направлений информационных технологий — получить базовые знания по алгебре, сформировать представления о её понятиях и методах, её месте в системе компьютерных наук и использовании в приложениях.

Курс можно использовать модульно, обращаться к необходимым разделам в соответствии с программой конкретной специальности. Этому помогает и концентрическое изложение основных понятий и методов: к ним возвращаются в различных главах с разных точек зрения, более детально или обобщённо.

Структура курса

Условно можно считать, что курс состоит из четырёх частей, тесно связанных между собой.

К первой, вводной части алгебры (главы 1–2), относятся:

- элементы теории множеств и логики;
- бинарные отношения (эквивалентности, порядка и функциональные);
- начальные сведения об алгебрах и алгебраических системах (группы, кольца, поля);
- основные числовые системы (натуральные числа и метод математической индукции, алгебраическая и тригонометрическая форма комплексных чисел).

Элементы теории множеств и математической логики даются на содержательном уровне и в дальнейшем существенным образом используются в курсе алгебры. Начальные сведения об алгебрах и алгебраических системах, о группах, кольцах и полях, данные во второй главе, более подробно продолжают в следующих главах на более широком классе новых примеров.

Во второй части (главы 3–4) излагается базовая линейная алгебра (арифметическое векторное пространство, линейная зависимость, базис и ранг системы векторов, матрица и её ранг, системы линейных уравнений). Вводятся понятия векторного пространства над полем, его базиса и размерности, подпространства и линейного многообразия. Глава 4 посвящается операциям над матрицами, вычислению определителей и их приложениям. Определитель матрицы произвольного порядка определяется через подстановки.

В главе 5 излагается вся классическая теория групп на основе примеров групп, построенных в предыдущих главах. В свою очередь на ней основывается всё дальнейшее изложение алгебры. В первую очередь в 6–7 главах линейная алгебра продолжается до операций над подпространствами, евклидовых пространств, изоморфизма пространств. Теория линейных операторов доводится до вычислений собственных значений и собственных векторов. Естественным образом возникают примеры линейных алгебр (линейных операторов и матриц).

Третья часть курса (главы 8–10) начинается с классической теории колец (глава 8) от примеров колец, подколец и идеалов до вопросов факторизации. На её примере будет излагаться теория делимости и сравнений в кольцах целых чисел и многочленов. Возникающие в них теоретико-числовые вопросы тесно связаны со школьной программой и могут служить основой для школьных элективных курсов. Теория делимости дополняется числовыми функциями, систематическими числами, цепными дробями. Теория сравнений дополняется теоретико-числовыми приложениями: теория остатков, функция Эйлера, признаки делимости и длина периода бесконечной дроби.

В последних главах 11–13 изучаются кольца многочленов от одной и от нескольких переменных. В главе 12 уделяется внимание предмету классической алгебры — решению алгебраических уравнений над основными числовыми полями. Классическая алгебра завершается главой 14, в которой изложена теория расширений полей и её приложений в школе: иррациональность, трансцендентность, разрешимость уравнений в радикалах, проблемы построения циркулем и линейкой.

В последнюю главу 15 выделена теория систем линейных неравенств (основные понятия, следствия, критерий несовместности) и элементы линейного программирования (стандартные и канонические задачи, двойственные задачи, симплекс-метод, транспортная задача). Эти вопросы можно отнести к примерам приложений линейной алгебры.

Курс завершается дополнительной главой «История развития алгебры». Мы считаем, что при изучении курса алгебры, как и любой другой научной или учебной теории, важна актуализация её истории. Приводится периодизация истории развития алгебры, основанная на изменении понимания предмета алгебры. Материал этой главы может быть использован соответствующим образом при систематическом изложении курса алгебры или её частей.

Все главы делятся на параграфы. Определения, теоремы, следствия не нумеруются. При необходимости ссылок на них даётся соответствующее разъяснение. Ко всем понятиям, алгоритмам приводятся примеры. Почти все утверждения теорем доказываются, но при первом знакомстве их можно опускать. При этом нужно учитывать, что доказательства часто дают и методы решения практических задач.

Выше изложен общий план курса, а зависимость глав и связь между ними может быть представлена как на схеме ниже.

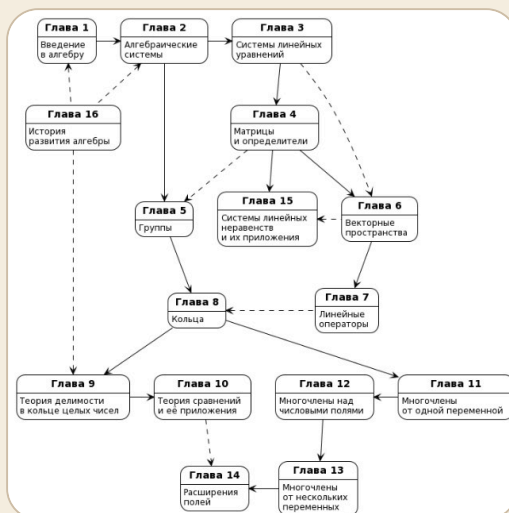


Схема зависимости глав из курса алгебры в книге «Библия математика. Основы высшей и линейной алгебры» (2024) · [Источник](#)

Опираясь на данную схему подготовленный читатель может начинать с любой главы и выбрать свою траекторию изучения материала. Пунктирными стрелками показаны альтернативные траектории движения и существующие связи между главами через теорию и примеры в них.

Список источников в книге также составлен с учётом методической целесообразности. Указанная литература может быть любого года издания. Конечно же, имеются и другие подходящие источники, которые вы можете найти самостоятельно.



Макет печатной книги Гильмуллина М. Ф. «Библия математика. Основы высшей и линейной алгебры» (2024). Её можно найти на сайте издательства Ridero.ru через поиск: «Гильмуллин Библия математика» · [Источник](#)

Современная алгебра играет ту же роль, что и язык в общении человека с внешним миром. Насколько важно научиться языку алгебры, можно понять, лишь попробовав обойтись без него в самостоятельных занятиях математикой. Поэтому желаем всем развития своего алгебраического вкуса. Пусть между духом и материей посредником выступает алгебра!