ЛЕКЦИИ ПО АЛГЕБРЕ

1 СЕМЕСТР

2021–2022 УЧЕБНЫЙ ГОД

БУНИНА ЕЛЕНА ИГОРЕВНА

helenbunina@gmail.com

Часть 1 — ОСНОВНЫЕ ПОНЯТИЯ АЛГЕБРЫ

ЛЕКЦИЯ 1

КРАТКАЯ ИСТОРИЯ АЛГЕБРЫ.

ВАЖНЫЕ ПРИКЛАДНЫЕ ЗАДАЧИ.

СИСТЕМЫ ЛИНЕЙНЫХ УРАВНЕНИЙ.

ЧТО ТАКОЕ АЛГЕБРА И КАК ОНА РАЗВИВАЛАСЬ

Сегодня многие говорят об алгебраизации математики, то есть о проникновении идей и методов алгебры как в теоретические, так и в прикладные разделы математики. Так поменялось положение вещей в математике примерно в середине прошлого века.

Алгебра с древних времен составляла довольно существенную часть математики.

Что есть алгебра? Это наука об алгебраических операциях, выполняемых над элементами различных множеств. При этом исходно алгебраические операции выросли их элементарных операций на числами (сложение, умножение и т.п.). Дальше элементарные понятия обобщаются на более широкие классы множеств, после его про них доказываются какие-то теоремы, которые помогают при рассмотрении примеров получать полезные результаты.

Попробуем кратко рассказать основные шаги развития алгебры в предыдущих веках.

Древние цивилизации Вавилона и Египта. Греческая цивилизация. "Арифметика" Диофанта, III век н.э.:

— Арифметические действия над множествами целых и рациональных положительных чисел;

— Алгебраические формулы в геометрических и астрономических расчетах;

— Формулировка задач на построение (удвоение куба и трисекция угла)

Восточная цивилизация средних веков, VIII–X века:

— Алгебраические уравнения первой и второй степени;

— Возникновение термина “алгебра”.

Эпоха Возрождения, XV–XVI века, Ферро, Тарталья, Кардано, Феррари, Бомбелли, Виет:

— Решение общих алгебраических уравнений третьей и четвертой степени;

— Создание современной алгебраической символики.

XVII–XVIII века, Декарт, Ферма, Ньютон, Лейбниц, Эйлер, Даламбер, Лагранж, Крамер, Лаплас, Вандермонд:

— Возникновение аналитической геометрии;

— Оживления деятельности в теории чисел;

— Развитие алгебры многочленов;

— Поиски общих формул для решения алгебраических уравнений;

— Первые подходы к доказательству существования корня уравнения с числовыми коэффициентами;

— Начало теории определителей.

XIX–начало XX века, Гаусс, Дирихле, Куммер, Кронекер, Дедекинд, Золотарев, Вороной, Марков:

— Доказательство основной теоремы о существований корней уравнений с числовыми коэффициентами;

— Интенсивное развитие теории алгебраических чисел.

XIX–начало XX века, Чебышев, Эрмит, Лобаческий, Гурвиц:

— Поиски методов приближенного решения алгебраических уравнений;

— Условия на коэффициенты, обеспечивающие заданное расположение корней.

XIX–начало XX века, Руффини, Абель, Якоби, Галуа, Риман, Коши, Жордан, Силов:

— Решение проблемы о неразрешимости общих уравнений степени $\geqslant 5$ в радикалах;

— Развитие теории алгебраических функций;

— Создание теории Галуа;

— Начала теории конечных групп, преимущественно на базе групп перестановок.

XIX–начало XX века, Грассман, Сильвестр, Кэли, Гамильтон, Буль, Ли, Фробениус, Серр, Нетер, Граве, Пуанкаре, Клейн, Бернсайд, Молин, Шур, Вейль, Энриквес:

— Интенсивное развитие методов линейной алгебры;

— Открытие кватернионов;

— Теория алгебр и групп Ли;

— Алгебраическая геометрия и теория инвариантов.

XIX–начало XX века, Нейман, Гильберт, Картан, Гензель, Штейниц, Эмми Нетер, Артин, Бурбаки:

— Коренная перестройка всего здания математики;

— Переход алгебры на более абстрактный и аксиоматический путь развития.

Начало–середина XX века, Чеботарев, Шмидт, Мальцев, Курош, Новиков, Фаддеев и другие:

— Вошел в обиход язык теории колец, модулей, категорий, гомологий;

— Многие разрозненные теории оказались уложены в общую схему универсальной алгебры;

— На стыке алгебры и математической логики родилась теория моделей;

— Яркие взлеты теории конечных групп.

НЕКОТОРЫЕ ВАЖНЫЕ ПРИКЛАДНЫЕ ЗАДАЧИ

1. Задача о разрешимости уравнений в радикалах.

Из школьной алгебры известна формула

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

для решений квадратного уравнения $ax^2 + bx + c = 0$.

Уравнение третьей степени

$$x^3 + ax^2 + bx + c = 0$$

подстановкой $x \mapsto x - a/3$ приводится к виду

$$x^3 + px + q = 0.$$

Корни x_1, x_2, x_3 этого уравнения следующим образом выражаются через его коэффициенты. Если положить

$$D = -4p^3 - 27q^3, \quad \varepsilon = \frac{-1 + \sqrt{-3}}{2},$$
$$u = \sqrt[3]{-\frac{27}{2}q + \frac{3}{2}\sqrt{-3D}}, \quad v = \sqrt[3]{-\frac{27}{2}q - \frac{3}{2}\sqrt{-3D}}$$

(кубические корни выбираются так, чтобы $uv = -3p$), то можно показать, что

$$x_1 = \frac{1}{3}(u + v), \quad x_2 = \frac{1}{3}(\varepsilon^2 u + \varepsilon v), \quad x_3 = \frac{1}{3}(\varepsilon u + \varepsilon^2 v).$$

Эти формулы называются *формулами Кардано* (1545 г.) и связаны также с именами других итальянских математиков эпохи

Возрождения (Ферро, Тарталья). Эти формулы справедливы при любых значениях коэффициентов.

Аналогичные формулы были найдены для уравнений четвертой степени, и на протяжении почти трехсот лет предпринимались безуспешные попытки "решить в радикалах" общее уравнение пятой степени. Лишь в 1813 году Руффини (в первом приближении) и Абель (независимо и уже совсем строго) доказал теорему о том, что общее алгебраическое уравнение

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

при $n > 4$ не разрешимо в радикалах.

В 1831 году двадцатилеьний Эварист Галуа сделал фундаментальное открытие в этой области, которое стало известно только через 15 лет. Он дал универсальный критерий для разрешмости в радикалах любого уравнения с рациональными коэффициентами. при этом критерий формулируется совершенно в терминах современной алгебры, а не алгебры XIX века, когда эту теорию мало кто мог понять. Мы в курсе дойдем до этой теории и соответствующих доказательств, но только к самому концу 3 семестра. Эта теория (называемая *теорией Галуа*) удивительным образом включает в себя большую часть теории полей и теории групп.

Давайте для начала немного обсудим, что такое эти самые поля и группы, так они будут большой частью предмета нашего изучения.

Примерами полей являются привычные нам рациональные числа (которые обозначаются буквой $\mathbb{Q}$) и действительные числа (обозначение: $\mathbb{R}$).

Что можно делать с этими числами? Складывать, вычитать, умножать, делить (только не ноль!).

Давайте формализуем это понятие.

Полем называется множество $\mathbb{F}$, на котором введены две операции $+$ (*сложение*) и $\times$ (*умножение*) так, что

(1) $\forall a, b, c \in \mathbb{F}\ (a+b)+c = a+(b+c)$ (*ассоциативность*);

(2) $\forall a, b \in \mathbb{F}\ a+b = b+a$ (*коммутативность*);

(3) существует такой элемент $0 \in \mathbb{F}$ (называемый *нулем*), что $\forall a \in \mathbb{F}\ a+0 = a$;

(4) $\forall a \in \mathbb{F}\ \exists b \in \mathbb{F}\ a+b = 0$, элемент b называется *противоположным* к a и обозначается через $-a$;

(5) $\forall a, b, c \in \mathbb{F}\ (a \times b) \times c = a \times (b \times c)$;

(6) $\forall a, b \in \mathbb{F}\ a \times b = b \times a$;

(7) существует такой элемент $1 \neq 0 \in \mathbb{F}$ (называемый *единицей*), что $\forall a \in \mathbb{F}\ a \times 1 = a$;

(8) $\forall a \neq 0 \in \mathbb{F}\ \exists b \in \mathbb{F}\ a \times b = 1$, элемент b называется *обратным* к a и обозначается через a^{-1} или $1/a$;

(9) $\forall a, b, c \in \mathbb{F}\ a \times (b+c) = a \times b + a \times c$ (*дистрибутивность*).

Заметим, что рациональные и действительные числа являются полями, но вообще полей (и даже очень полезных!) очень много. В этом семестре мы будем подробно проходить поле комплексных чисел $\mathbb{C}$, которое содержит все корни всех алгебраических уравнений с действительными коэффициентами, а также приведем примеры еще некоторых полезных полей. В третьем семестре у нас будет отдельная большая тема “поля”, в том числе, мы полностью поймем, какими бывают поля с конечным числом элементов.

Теперь давайте выясним, что такое группа.

Все поля по сложению, и поля по умножению без нуля являются группами. Также группой являются целые числа.

Формально, группа — это множество $\mathbf{G}$ с операцией $\times$ или $\cdot$ (*умножение*), для которой выполняются следующие аксиомы:

(1) $\forall a, b, c \in \mathbf{G}\ (a \times b) \times c = a \times (b \times c)$;

(2) существует такой элемент $e \in \mathbf{G}$ (называемый *единицей*), что $\forall a \in \mathbf{G}\ a \cdot e = e \cdot a = a$;

(3) $\forall a \in \mathbf{G}\ \exists b \in \mathbf{G}\ a \cdot b = e$, элемент b называется *обратным* к a и обозначается через a^{-1}.

Оказывается, поля и группы тесно связаны с теорией Галуа, благодаря которой мы сможем доказать теорему о неразрешимости алгебраических уравнений степени $\geqslant 5$, а также доказать, что неразрешимы следующие две древние задачи:

(1) Циркулем и линейкой разделить данный угол на три равные части;

(2) Циркулем и линейкой построить куб, объем которого в два раза больше объема данного куба.

2. Задача о состояниях многоатомной молекулы

Пусть у нас имеется какая-то фигура на плоскости или в пространстве. Рассмотрим все ее движения (то есть отображения точек этой фигуры в себя, сохраняющие расстояния). На множестве таких движений можно ввести операцию композии (еще ее называют суперпозицией) $\circ$. Множество всех движений будет удовлетворять аксиоме ассоциативности (композиция всегда ассоциативна).

Кроме того, всегда существует тождественное движение (ни одна точка фигуры не двигается), композиция которого с любым другим движением не меняет это движение.

Наконец, к любому движению можно подобрать обратное: возьмем наше движение и отобразим все точки в обратную сторону.

Таким образом, множество движений любой фигуры является группой относительно операции композиции. Эта группа также называется *группой симметрий* данной фигуры.

Теперь рассмотрим некоторую молекулу — это система частиц (атомных ядер, окруженных электронами). Если в начальный момент времени конфигурация системы близка к равновесной, то частицы, входящие в систему, всегда будут оставаться около положения равновесия и не будут приобретать больших скоростей. Движения такого типа называются колебаниями относительно равновесной конфигурации, а система — устойчивой.

Любое малое колебание молекулы вблизи положения устойчивого равновесия является композицией так называемых нормальных колебаний. Часто можно определить все параметры молекулы (потенциальную энергию, нормальные частоты), зная внут-

ренние симметрии молекулы.

Внутренние симметрии — это группа, как мы уже знаем. Изучение данной группы (ее представления, например) очень полезно, так как дает нам возможность посчитать параметры колебания молекулы.

Таким образом, на сегодняшний день развитие структурной теории молекул невозможно себе представить без теории групп.

Гораздо более ранние (но до сих пор идущие) применения теории групп относятся к кристаллографии.

Еще в 1891 году русский кристаллограф Е.С. Федоров, а затем немецкий ученый А.Шенфлис нашли 230 пространственных кристаллографических групп, описывающих все имеющиеся в природе симметрии кристаллов.

3. Задача о кодировании сообщения

В конструировании автоматических систем связи, наземных или космических, обычно в качестве элементарного сообщения берется упорядоченная последовательность — строка (или слово)

$$a = (a_1, a_2, \ldots, a_n)$$

длины n, где $a_i = 0$ или 1.

Так как операции сложения и умножения по модулю два совершенно естественны для компьютера, то поле из двух элементов $\mathbb{F}_2$ или $\mathbb{Z}_2$ — необходимый атрибут специалиста по обработке информации.

Это поле с такими правилами сложения:

$$0 + 0 = 1 + 1 = 0 \text{ и } 0 + 1 = 1 + 0 = 1$$

умножения —

$$0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0 \text{ и } 1 \cdot 1 = 1.$$

Иногда удобно использовать в качестве символов a_i элементы других конечных полей (например, поля $\mathbb{F}_{2^k}$ из 2^k элементов, которое существует для любого натурального k).

С целью исключения помех, способных превратить 0 в 1 или наоборот, приходится брать a досаточно длинным и использовать специальную систему кодирования — выбор такого подмножества (кода) S_0 передаваемых строк из всего множества S, чтобы было возможно восстановить слово a по искаженному передаваемому слову a' при условии, что произошло не слишком много ошибок. Так возникают *коды, исправляющие ошибки.*

Алгебраическая теория кодирования, которая развивается последние несколько десятилетий, очень в большой степени основана на теории полей. Она будет проходится на старших курсов в курсе дискретной математики, когда теория полей уже может немного забыться.

Кроме приведенных примеров использования теории групп и теории полей хочется сказать, что очень важной для практических задач дисциплиной является линейная алгебра — сейчас она нужна как для абсолютно всех других предметов высшей математики (функциональный анализ, теория вероятностей и математическая статистика, дифференциальные уравнения и уравнения в частных производных, вычислительная математика, дифференциальная геометрия и т.д.), так и для совершенно практических задач (например, машинного обучения).

В этом семестре мы в основном будем заниматься изучением самых первых основ линейной алгебры, базовыми понятиями теории групп и теории полей, а также многочленами.

Второй семестр будет полностью посвящен линейной алгебре, третий — теории групп, теории полей и колец, представлениям групп, а также основам теории Галуа.

СИСТЕМЫ ЛИНЕЙНЫХ УРАВНЕНИЙ

Линейные уравнения $ax = b$ и системы вида

$$\begin{cases} ax + by = e, \\ cx + dy = f \end{cases}$$

с вещественными коэффициентами решаются в средней школе. Наша цель — научиться оперировать с системой линейных алгебраических уравнений самого общего вида

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1, \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m. \end{cases}$$

Здесь m и n — произвольные натуральные числа.

Для удобства всегда будем считать, что элемент a_{ij} находится в i-м уравнении при переменной x_j. Число b_i называется *свободным членом* i-го уравнения. Система называется *однородной*, если все $b_i = 0$, $i = 1, 2, \ldots, m$.

при любых b_i линейную систему

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = 0, \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = 0 \end{cases}$$

называют *однородной системой, ассоциированной* с исходной.

Коэффициенты при неизвестных составляют прямоугольную таблицу

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix},$$

называемую *матрицей* размера $m \times n$ и сокращенно обозначаемую символом (a_{ij}) или просто A. Естественно говорить об i-й строке или j-м столбце этой матрицы, а в случае квадратной матрицы $(m = n)$ — еще и о главной диагонали, состоящей из элементов $a_{11}, a_{22}, \dots, a_{nn}$.

Матрица, у которой все элементы вне главной диагонали равны нулю, обозначается иногда через

$$\operatorname{diag}(a_{11}, a_{22}, \dots, a_{nn})$$

и называется *диагональной* матрицей, а при $a_{11} = a_{22} = \dots = a_{nn} = a$ обозначается aE — *скалярная* матрица.

Наряду с матрицей коэффициентов рассматривают и *расширенную* матрицу $(a_{ij}|b_i)$, получающуюся из исходной добавлением столбца свободных членов.

Если каждое из уравнений нашей линейной системы обращается в ноль после замены неизвестных x_i числами x_i^0, то упорядоченный набор n чисел $x_1^0, x_2^0, \dots, x_n^0$ называется *решением* системы.

Система, не имеющая ни одного решения, называется *несовместной*. Если у системы есть решение, то она называется *совместной*. Если при этом оно единственно, то система называется

определенной. Если у системы больше одного решения, то она называется *неопределенной*.

ЭКВИВАЛЕНТНОСТЬ ЛИНЕЙНЫХ СИСТЕМ

Пусть нам дана еще одна линейная система того же размера

$$\begin{cases} a'_{11}x_1 + a'_{12}x_2 + \cdots + a'_{1n}x_n = b'_1, \\ a'_{21}x_1 + a'_{22}x_2 + \cdots + a'_{2n}x_n = b'_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a'_{m1}x_1 + a'_{m2}x_2 + \cdots + a'_{mn}x_n = b'_m. \end{cases}$$

Будем говорить, что штрихованная система получена из исходной с помощью *элементарного преобразования типа* (I), если в новой системе все уравнения остались прежними, только какие-то два поменялись местами.

Если же в штрихованной системе все уравнения те же, что и в исходной, и только i-е уравнение выглядит как

$$(a_{i1} + ca_{k1})x_1 + (a_{i2} + ca_{k2})x_2 + \cdots + (a_{in} + ca_{kn})x_n = b_i + cb_k,$$

где c — какое-то число, то полагаем, что к системе применено элементарное преобразование типа (II).

Линейные системы называются *эквивалентными*, если они либо обе несовместны, либо совместны и обладают одним и тем же множеством решений.

Если обозначать эквивалентность систем как $(a) \sim (b)$, то можно заметить, что

(1) $(a) \sim (a)$;

(2) из $(a) \sim (b)$ следует $(b) \sim (a)$;

(3) из $(a) \sim (b)$ и $(b) \sim (c)$ следует $(a) \sim (c)$.

Достаточный признак эквивалентности систем содержится в следующем утверждении:

Теорема 1. *Две линейные системы эквивалентны, если одна получается из другой путем применения конечной последовательности элементарных преобразований.*

Доказательство. Достаточно доказать, что если система $(**)$ получена из системы $(*)$ применением одного элементарного преобразования, то системы $(**)$ и $(*)$ эквивалентны.

Заметим, что система $(*)$ получается из системы $(**)$ также применением одного элементарного преобразования: в случае первого типа нужно снова поменять местами два уравнения, в случае второго типа — прибавив к i-му уравнению в $(**)$ k-ое, умноженное на $(-c)$, мы получим i-е уравнение системы $(*)$.

Докажем теперь, что любое решение $(x_1^0, x_2^0, \ldots, x_n^0)$ системы $(*)$ является также решением системы $(**)$, этого благодаря замечанию будет достаточно.

Действительно, пусть у нас есть решение системы $(*)$, тогда при подставление его в каждое уравнение системы $(*)$ мы получаем верное равенство. Если система $(**)$ получилась из системы $(*)$ с помощью элементарного преобразования первого типа, то все уравнения в ней те же (только местами переставлены), поэтому тоже при подставлении набора $(x_1^0, x_2^0, \ldots, x_n^0)$ обращаются в верные равенства. Если система $(**)$ получена из системы $(*)$ элементарным преобразованием второго типа, то все уравнения, кроме i-го, автоматически обращаются в верные равенство, а i-е обращается, потому что является суммой верного равенства и еще одного врного равенства, умноженного на число c. $\square$