15.5.21 / 18.9.19

Независимый Московский Университет, Алгебра-1, осень 2018

АЛГЕБРА, ПЕРВЫЙ СЕМЕСТР

Лекция 1 (20 сентября 2018):
Введение. От уравнений к современной алгебре

1.0. С чего начиналась алгебра?

С незапамятных времён – в сильном и точном смысле этих слов – люди решали уравнения. Мы начнём наш курс с самых древних, которые вам знакомы со школы (и в дальнейшем школьной математикой заниматься не будем), а затем расширим горизонт, обсудив класс уравнений, которые в силу своего юного возраста (составляющего всего несколько сотен лет) в школьные программы пока не вошли.

Мы не знаем, кто и когда составил и решил первое уравнение, но знаем, что это случиось очень давно.

С тех пор по планете распространяется идея работать с *неизвестными количествами* так, как будто это числа. Но понятие *числа* уточняется (математиками, философами, физиками и прочими) вот уже несколько тысячелетий, и нет никакой уверенности в том, что выработана окончательная точка зрения. В нашем курсе, впрочем, словам *неизвестная/переменная* будет придаваться современный, алгебраический смысл.

1.1. Системы линейных уравнений

1.1.0. Об истории. Задачи, которые мы бы решали с помощью систем линейных уравнений, встречаются в самых ранних из доступных нам сегодня математических документах, то есть в вавилонских клинописных табличках, созданных около четырёх тысяч лет назад – см., например, **[Sesiano2009]**. Древневавилонские задачи нелегко расшифровать и понять, даже с помощью историков и лингвистов; к счастью, задачи этого класса встречаются во всех значительных математических культурах, и некоторые из них преобразуются в системы линейных уравнений легко. Пример из арабского раннего средневековья: на 458-ю ночь из *тысячи и одной*[1] рассматривалась следующая задача[2]:

Стая голубей подлетела к высокому дереву. Часть голубей села на ветвях, а другая расположилась под деревом. Сидевшие на ветвях голуби говорят расположившимся внизу: «Если бы один из вас взлетел к нам, то вас стало бы втрое меньше, чем нас всех вместе, а если бы один из нас слетел к вам, то нас с вами стало бы поровну». Сколько голубей сидело на ветвях и сколько под деревом?

Сведя эту задачу к системе уравнений

$$\begin{cases} 3(y-1) = x+y \\ x-1 = y+1 \end{cases}$$

или пользуясь какими-то иными соображениями, Шахерезада на вопрос ответила.

1.1.1. Правило Крамера. Решим теперь общую систему

[1] См., например, **[Irwin2005]**

[2] перевод заимствован из книги **[БавринФрибус1994]**

двух линейных уравнений с двумя неизвестными

$$\begin{cases} a_1x + b_1y = c_1 & (1) \\ a_2x + b_2y = c_2 & (2) \end{cases}$$

Здесь шесть коэффициентов $a_1, b_1, c_1; a_2, b_2, c_2$ предполагаются заданными, а найти надо "неизвестные" x, y; природой этих *чисел* мы пока не интересуемся.

Идея давать уравнениям (а также другим формулам и утверждениям) *имена* (и затем работать с ними по законам алгебры) не менее важна, чем идея обозначать числа буквами. Она лишь менее разрекламирована.

Чтобы истребить y, вычислим $b_2(1) - b_1(2)$:

$$(b_2a_1 - b_1a_2)x = b_2c_1 - b_1c_2 \qquad (3)_x$$

Чтобы истребить x, вычислим $a_2(1) - a_1(2)$:

$$(a_2b_1 - a_1b_2)y = a_2c_1 - a_1c_2. \qquad (3)_y$$

По-прежнему не уточняя класса чисел, с которыми мы работаем, мы примем важное ограничение: $\underline{\text{умножение коммутативно}}$, то есть *от перемены мест сомножителей произведение не меняется.*

В древних математических цивилизациях и в современной школьной математике это ограничение принимается как само собой разумеющееся, тогда как в нашем курсе встретятся и некоммутативные умножения.

В предположении коммутативности перепишем полученные уравнения чуть-чуть по-другому – в частности, *изменив знак* у уравнения $(3)_y$:

$$(a_1b_2 - a_2b_1)x = b_2c_1 - b_1c_2, \qquad (3)'_x$$

$$(a_1b_2 - a_2b_1)y = -a_2c_1 + a_1c_2. \qquad (3)'_y$$

Эти несложные преобразования позволяют выявить главное действующее лицо рассматриваемой системы уравнений – её *определитель*[3], для которого мы вводим специальное обозначение

$$\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} := a_1b_2 - a_2b_1.$$

Достижение (радость от которого – верный признак склонности к занятиям алгеброй) заключается в том, что коэффициенты, стоящие перед *изолированными* переменными в уравнениях $(3)'_x$ и

[3]вводя который, мы впервые *делинеаризуем* наши формулы: они перестают быть *последовательностями* знаков

$(3)'_y$, совпали – так определитель и возник.

Сразу выделяется класс *вырожденных* систем уравнений с нулевым определителем; их мы сегодня обсуждать не будем. Что же касается *не*вырожденных систем, то на ненулевые определители принято *делить*. Это законно без дальнейших оговорок в *полях*, которым будет посвящена существенная часть нашего курса; однако общая система линейных уравнений формулируется только в терминах сложения и умножения, поэтому (хотя мы по-прежнему не уточняем природы рассматриваемых чисел – как коэффициентов, так и неизвестных) естественно получить ответы на языке *колец*. Тогда наиболее естественно формулируемое свойство системы уравнений (1), (2) – *обратимость определителя*:

$$\boxed{\exists\delta; (a_1b_2 - a_2b_1)\delta = 1} \tag{$\bigstar$}$$

Это свойство в кольцах, разумеется, сильнее свойства определителя быть ненулевым. Так, над[4] кольцом целых чисел выделяются системы линейных уравнений с определителем ±1. Кстати, к этому классу относится упомянутая выше задача, предложенная Шахерезаде: действительно, в стандартном виде эта задача превращается в

$$\begin{cases} -x + 2y = \dots \\ x - y = \dots \end{cases}$$

(правые части не важны) и

$$\begin{vmatrix} -1 & 2 \\ 1 & -1 \end{vmatrix} := (-1)\cdot(-1) - 1\cdot 2 = -1,$$

так что независимо от правых частей нецелые количества голубей в ответ не попадут.

Вернёмся к общей системе двух линейных уравнений с двумя неизвестными. В предположении обратимости определителя – *деление* на него совпадает с умножением на δ из формулы ($\bigstar$) – уравнения (3)' разрешаются относительно изолированных переменных:

$$x = \frac{b_2c_1 - b_1c_2}{a_1b_2 - a_2b_1}, \tag{$(3)''_x$}$$

$$y = \frac{-a_2c_1 + a_1c_2}{a_1b_2 - a_2b_1}. \tag{$(3)''_y$}$$

[4]именно этот предлог используют специалисты по коммутативной алгебре и алгебраической геометрии, выражая намерение считать все встречаемые "числа"элементами какого-то определённого

Замечательно то, что с помощью понятия определителя мы можем выразить не только знаменатели, но и числители этих формул:

$$x = \frac{\begin{vmatrix} c_1 & b_1 \\ c_2 & b_2 \end{vmatrix}}{\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix}}, \ y = \frac{\begin{vmatrix} a_1 & c_1 \\ a_2 & c_2 \end{vmatrix}}{\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix}}.$$

Это и есть *правило Крамера*[5] для системы двух линейных уравнений с двумя неизвестными (1), (2).

Суть правила понятна при всматривании в *столбцы* и становится ещё понятнее при переходе к системе трёх уравнений с тремя неизвестными: решения системы

$$\begin{cases} a_1x + b_1y + c_1z = d_1 \\ a_2x + b_2y + c_2z = d_2 \\ a_3x + b_3y + c_3z = d_3 \end{cases}$$

суть

$$x = \frac{\begin{vmatrix} d_1 & b_1 & c_1 \\ d_2 & b_2 & c_2 \\ d_3 & b_3 & c_3 \end{vmatrix}}{\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix}}, \ y = \frac{\begin{vmatrix} a_1 & d_1 & c_1 \\ a_2 & d_2 & c_2 \\ a_3 & d_3 & c_3 \end{vmatrix}}{\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix}}, \ z = \frac{\begin{vmatrix} a_1 & b_1 & d_1 \\ a_2 & b_2 & d_2 \\ a_3 & b_3 & d_3 \end{vmatrix}}{\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix}}.$$

Остаётся понять, что представляет собой 3×3-определитель; можно вычислить вручную

$$\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} = a_1b_2c_3 + a_2b_3c_1 + a_3b_1c_2 - a_1b_3c_2 - a_3b_1c_2 - a_2b_1c_3.$$

Сложность определителей бо́льших порядков очень быстро возрастает.

Одна из задач этого семестра – понять *природу* определителей (а не только вывести общую формулу). Для этого нам придётся развить достаточно общие взгляды на алгебру.

1.1.2. О вычислительной практике. Как можно прочитать во многих источниках, использование правила Крамера

[5] Габриэль Крамер (1704 — 1752) — швейцарский математик; известен также перепиской с Л. Эйлером по теории алгебраических кривых

непрактично – при значительном количестве неизвестных и уравнений оно требует неоправданно большого количества операций. Более экономные методы разрабатывались с древности; наиболее известным является *метод Гаусса* – см., например, **[ИльинПозняк2004]**. Сравнительно недавно, около полувека назад оказалось, что существуют и дальнейшие усовершенствования – см. **[Strassen1969]**; стремление к совершенству продолжается, см., например, **[BDHT2013]**.

Следует, впрочем, отметить, что современные инженеры, экономисты и другие люди, которым приходится для своей работы решать обширные системы линейных уравнений, интересуются методами решения этих систем существенно меньше, чем их предшественники: для получения ответа достаточно вызвать стандартную компьютерную программу. Размеры систем, доступных современным компьютерам, зависят, конечно, от применяемых изощрённых алгоритмов, но не в меньшей степени зависят от технического прогресса. Не исключено, что в обозримом будущем появление новых поколений компьютеров – например, квантовых – снизит практическую значимость упомянутых оптимальных методов.

1.2. Квадратные уравнения

1.2.0. Вавилонское наследие. От древневавилонской математики сохранился огромный материал по квадратным уравнениям. Он тщательно упорядочен и проанализирован – см., например, **[Beriman1956]**.

Один из главных (с точки зрения нашего курса) выводов заключается в том, что вавилонская алгебра существовала. Например, вавилоняне сводили умножение к возведению в квадрат, сложению, вычитанию и делению пополам – пользуясь тождеством, которое тысячи лет спустя записывается в виде

$$ab \equiv \frac{(a+b)^2 - (a-b)^2}{4}.$$

В ходу были таблицы квадратов[6], сохранившиеся до наших дней! Как утверждают историки, эти таблицы широко использовались при решении задач практического характера; замечательные

[6]в 1854 году на Евфрате была найдена таблица квадратов от 8^2 до 59^2; естественно объяснить число 59 используемой вавилонянами *шестидесятиричной* системой счисления

приближения $\sqrt{2}$ были получены (см. **[FowlerRobson1998]**) более чем за полторы тысячи лет до того, как древнегреческие мыслители заинтересовались соизмеримостью квадрата и его диагонали.

Что же касается *обучения* решениям квадратных уравнений – занятия, вплоть до наших дней составляющего существенную часть школьной математики – то вавилонские педагоги, видимо, владели техникой составления уравнений, дискриминанты которых – квадраты рациональных чисел. До нас дошла, например, такая задача[7]:

Длину и ширину я перемножил и площадь получил. Затем избыток длины над шириной я прибавил к площади; 183 получилось у меня[8]*. Затем я длину и ширину сложил: 27. Спрашивается длина, ширина и площадь.*

Тысячи лет оттачивались навыки перевода этого текста в уравнение

$$x(27-x)+x-(27-x)=183.$$

Наше понимание древних математических текстов основано на текстовых задачах; концепции ЧИСЛА, УРАВНЕНИЯ и РЕШЕНИЯ связывают нас с безвестными авторами этих текстов.

1.2.1. Выделяется ли полный квадрат? Всеобщее знакомство с квадратными уравнениями позволяет нам быть очень краткими. Рассмотрим уравнение

$$x^2+px+q=0, \qquad (\mathbf{1})$$

опять (временно) не уточняя природы коэффициентов и неизвестного.

Как известно, первый шаг в упрощении уравнения **(1)** требует прибавления к обеим частям $\frac{p^2}{4}$. Для этого в "числах" , с которыми мы работаем, должна быть определена *процедура деления на* 2 – иначе говоря,

$$\exists \frac{1}{2}.$$

---

[7]из так называемого текста *AO 8862* эпохи династии Гаммурапи, см. **[Варден1959]**

[8]числа переведены в десятичную систему счисления

Это – нетривиальное предположение; вскоре мы кратко обсудим возможность его невыполнения.

В "обычных" же случаях, то есть когда оно выполнено, уравнение **(1)**, как известно с вавилонских времён, равносильно уравнению

$$(x+\frac{p}{2})^2 = \frac{p^2}{4} - q. \qquad \textbf{(2)}$$

1.2.2. Квадратен ли дискриминант? Уравнение **(2)** говорит о том, что для разрешимости уравнения **(1)** необходимо и достаточно, чтобы *дискриминант* его левой части был квадратом:

$$\exists d; d^2 = \frac{p^2}{4} - q. \qquad (\bigstar\bigstar)$$

В отличие от непреодолимого препятствия $\nexists\frac{1}{2}$, *неквадратность* дискриминанта излечивается *расширением числовых множеств.* Важные вехи этого процесса – легализация числа $\sqrt{2}$ и введение *мнимой единицы* $\mathbf{i}$, удовлетворяющей "невозможному" равенству $\mathbf{i}^2 = -1$.

Каждое такое расширение приводило к тому, что квадратные уравнения, неразрешимые в меньших числовых множествах, становились разрешимыми в бóльших.

1.2.3. Случай 2=0. Имеются в виду "числа" , в которых 1+1=0. Наименьшим таким "числовым" множеством является поле из двух элементов $\mathbb{F}_2 = \{0, 1\}$ со сложением и умножением

+	0	1
0	0	1
1	1	0

,

·	0	1
0	0	0
1	0	1

.

Существуют и поля из 4,8,16,... элементов; в каждом из них 1+1=0.

При анализе уравнения $x^2 + px + q = 0$ надо различать два случая – более близкий к обычному и экзотический.

Случай $p = 0$. Уравнение $x^2 + q = 0$ переписывается в виде

$$x^2 = q \qquad \textbf{(3)}$$

(когда 2=0, *минусов* в алгебре нет...), и оно, очевидно, разрешимо тогда и только тогда, когда q – квадрат.

Отметим, что в полях $\mathbb{F}_2, \mathbb{F}_4, \mathbb{F}_8, \ldots$ *все* элементы – квадраты (на традиционном алгебраическом языке, *конечные поля совершенны*). Однако поле $\mathbb{F}_2(q)$ *рациональных функций с коэффициентами в* $\mathbb{F}_2$ <u>не</u>совершенно: q – не квадрат в нём.

Забавным свойством уравнения **(3)** в предположении 2=0 является *кратность* его (единственного) корня. Это следует из любого из тождеств $(x+Q)^2 \equiv x^2+Q^2$ и $\frac{\mathrm{d}}{\mathrm{d}x}(x^2+q) \equiv 0$.

<u>Случай $p \neq 0$</u>. Замена $x = py$ с последующим делением на p^2 превращает уравнение **(1)** в $y^2 + y = \frac{q}{p^2}$, так что в исходном уравнении можно положить $p = 1$, то есть рассматривать уравнение

$$x^2 + x = q. \tag{4}$$

Это – простейший случай так называемого уравнения *Артина-Шрайера*. Мы проанализируем это уравнение позже, развив соответствующую технику, а пока лишь подчеркнём, что оно <u>не</u> решается извлечением квадратных корней.

В случае, когда уравнение **(4)** разрешимо, оно имеет *разные* корни $\{\alpha, \alpha+1\}$. В этом же можно убедиться с помощью тождества $\frac{\mathrm{d}}{\mathrm{d}x}(x^2+x+q) \equiv 1$.

1.3. Кубические уравнения

Сейчас мы выйдем за пределы школьной математики. Кратко описав обстановку, в которой работали итальянские алгебраисты XVI-го века, мы не будем вдаваться в детали приоритетных споров.

1.3.0. Предыстория. Ещё древние вавилоняне умели решать <u>некоторые</u> кубические уравнения; во всяком случае, ими были составлены таблицы значений $n^3 + n^2$, пригодные для решения методом *подглядывания в ответ*. Во многих других культурах были получены разнообразные частные результаты – связанные с *удвоением куба* и другие. По этим вопросам существует обширная литература; весьма живописно, в частности, освещается работа поэта-математика Омара Хайяма. См, например, **[Земляков2007]**.

Завершающий (и в некотором смысле *отрицательный*) результат был получен последним выдающимся математиком средневековой Европы *Леонардо Пизанским* (ок. 1175–ок. 1250), известным также под именем *Фибоначчи.* При его представлении императору Фридриху Второму придворный математик Джон Палермский предложил Фибоначчи три задачи[9], в их числе – решить уравнение

$$x^3 + 2x^2 + 10x = 20$$

(это уравнение, согласно **[Kasir1931]**, было заимствовано у Омара Хайяма). Леонардо <u>доказал</u>, что (единственный вещественный) корень этого уравнения *не* может быть выражен в виде *евклидовых иррациональностей.* Затем он нашёл *приближённое* решение с невероятной точностью! См. **[Cajori1893]**.

Два столетия после Фибоначчи в Европе не было ни выдающихся математиков, ни ярких математических достижений. Однако шли медленные процессы, подготавливающие будущий расцвет: укреплялась позиционная система счисления, возникали первые университеты, переводы античных авторов на латынь распространялись среди образованных людей.

1.3.1. Возрождение в алгебре. В математике возможность превзойти древних была осознана позже, чем в литературе, живописи и архитектуре. В средневековых университетах студенты <u>клялись</u> в прочтении шести (из тринадцати!) книг Евклида и "проходили" *Введение в арифметику* Никомаха **[Никомах2006]** – вряд ли особенно вдумчиво, поскольку в течение столетий содержащиеся в этой книге интересные результаты[10] не анализировались и не обобщались. Видимо, удовольствие от чистого счёта было чуждо средневековым европейцам, столкнувшимся с математикой – за замечательным исключением упомянутого выше Фибоначчи.

Но средневековье сменялось возрождением, нравы смягчались,

---

[9]Помимо обсуждаемой, одна из оставшихся двух задач рутинна и относится к средневековой коммерции, а другая – замечательна: *найти три рациональных квадрата, образующих арифметическую прогрессию с разностью* 5. Историки полагают, что Фибоначчи, хорошо знавший математику арабского Востока, владел переформулировкой этого вопроса как задачи нахождения пифагорова треугольника с площадью $5d^2$, где $d \in \mathbb{N}$. Он нашёл такой треугольник со сторонами $a = 9, b = 40, c = 41$, а требуемая прогрессия (при $d = 6$) состоит из квадратов длин $\frac{b-a}{2d}, \frac{c}{2d}, \frac{b+a}{2d}$. Проблема *конгруэтных чисел*, то есть описания *площадей пифагоровых треугольников*, в решение которой внёс вклад Фибоначчи (развивший своё решение в книге **[Fibonacci1225]**), до сих пор открыта – точнее, решена лишь по модулю одной из проблем (нашего) тысячелетия, *гипотезы Бёрча – Свиннертона-Дайера.* См. **[Коблиц1988]**.

[10]например, $1 = 1^3$, $3 + 5 = 2^3$, $7 + 9 + 11 = 3^3$, $\ldots$

рыцарские турниры уступали место математическим состязаниям при дворах вельмож, и *решения уравнений* выходили на первый план. Поскольку квадратные уравнения были общеизвестны, остро стоял вопрос о решении *кубических*. Предыстория первого алгебраического прорыва Нового времени завершалась публично выраженной убеждённостью авторитетного Луки Пачоли в неразрешимости этой задачи – в **[Пачоли1494]** он сравнил решения кубических уравнений с *квадратурой круга.*

Для опровержения этой пессимистической точки зрения потребовалось меньше полувека. Книга **[Cardano1545]** содержала решение не только кубических уравнений, но и уравнений 4-й степени. Соответствующие формулы называют *формулами Кардано*, и им будет уделено значительное место в нашем курсе.

Мы не будем касаться приоритетных вопросов, связанным с обсуждаемыми результатами – им посвящена обширная литература. Приведём лишь возражение против распространённой точки зрения, заключающейся в том, что название *формул Кардано* некорректно, поскольку он выманил их у *Тартальи*[11], поклявшись держать в тайне. Однако несомненная заслуга Кардано заключается в том, что он в них разобрался и их опубликовал в замечательной книге **[Cardano1545]**, оказавшей огромное влияние на развитие математики; в частности, там были высказаны соображения о *квадратных корнях из отрицательных чисел*, на 2-3 столетия обогнавшие существовавшие понятия. Это – заслуга гораздо более существенная, чем хранение в черновиках тайных методов решения.

Перейдём теперь от истории к математике.

1.3.2. Общий вид кубического уравнения; упрощение. Как все, будем рассматривать уравнение

$$ax^3 + bx^2 + px + q = 0, \qquad (\mathbf{1.3.2a})$$

[11]Тарталья закодировал свой метод в стихотворении, один из английских переводов которого начинается словами
When the cube and the things together
Are equal to some discrete number,
Find two other numbers differing in this one...
Итальянский оригинал и его комментированные переводы легко найти в современном Интернете.

подразумевая, что *коэффициенты* a, b, p, q даны, а *неизвестное* x надо найти. Природу коэффициентов и неизвестной мы снова не оговариваем, но предполагаем, что с ними можно производить все четыре арифметические действия, обладающие всеми обычными свойствами.

Если $a = 0$, то уравнение (**1.3.2a**) – **не кубическое, а** *квадратное,* поэтому предположим, что $a \neq 0$, и поделим уравнение (**1.3.2a**) на a. Получится уравнение того же вида, но с $a = 1$:

$$x^3 + bx^2 + px + q = 0, \tag{\textbf{1.3.2b}}$$

Для дальнейшего упрощения подберём подходящую замену вида$x = y + m$. Уравнение (**1.3.2b**) примет вид

$$y^3 + (b+3m)y^2 + (p+3m^2+2bm)y + q + m^3 + bm^2 + pm + q. \tag{\textbf{1.3.2c}}$$

Теперь придётся рассмотреть два случая.

(I) $1 + 1 + 1 \neq 0$. Тогда можно делить на 3, и, положив в уравнении (**1.3.2c**) $m = -\frac{b}{3}$, мы после соответствующих переобозначений придём к уравнению (**1.3.2b**), в котором $b = 0$, то есть

$$\boxed{x^3 + px + q = 0} \tag{\textbf{1.3.2d}}$$

Именно это уравнение мы будем решать.

(II) $1 + 1 + 1 = 0$. Имеются в виду "числа" , в которых 3=0. Наименьшим таким "числовым" множеством является поле из трёх элементов $\mathbb{F}_3 = \{0, 1, 2\}$ со сложением и умножением

$$\begin{array}{|c|c|c|c|} \hline + & 0 & 1 & 2 \\ \hline 0 & 0 & 1 & 2 \\ 1 & 1 & 2 & 0 \\ 2 & 2 & 0 & 1 \\ \hline \end{array}, \quad \begin{array}{|c|c|c|c|} \hline \cdot & 0 & 1 & 2 \\ \hline 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 \\ 2 & 0 & 2 & 1 \\ \hline \end{array}.$$

Существуют и поля из 9, 27, 81,...элементов; в каждом из них 1+1+1=0.

В таких полях уравнение (**1.3.2c**) принимает вид

$$y^3 + by^2 + (p + 2bm)y + q + m^3 + bm^2 + pm + q = 0. \tag{\textbf{1.3.2e}}$$

Если $b = 0$, то перед нами опять уравнение (**1.3.2d**).

Если же $b \neq 0$, то никакое значение m не уничтожает член с

y^2. Однако, если $3 = 0$, то $2 \neq 0$[12], так что можно положить $m = -\frac{p}{2b}$, и уравнение (**1.3.2e**) после очевидного переобозначения превращается в

$$y^3 + by^2 + r = 0. \qquad (\mathbf{1.3.2f})$$

Если $r = 0$, то это уравнение имеет тривиальное решение $y = 0$. Если же $r \neq 0$, то допустима замена $y = \frac{1}{z}$, приводящая уравнение (**1.3.2f**) к виду

$$rz^3 + bz + 1 = 0, \qquad (\mathbf{1.3.2g})$$

которое после деления на r снова превращается в уравнение (**1.3.2d**).

1.3.3. Формула Кардано. Итак, мы убедились, что все кубические уравнения будут решены, если будет решено уравнение (**1.3.2d**)

$$\boxed{x^3 + px + q = 0} \qquad (\mathbf{1.3.3a})$$

Воспроизведём в современных терминах решение итальянских алгебраистов XVI-го века. Положим

$$x = u + v, \qquad (\mathbf{1.3.3b})$$

ненадолго оставляя себе свободу в выборе новых вспомогательных неизвестных u и v. Уравнение (**1.3.3a**) превратится в

$$u^3 + v^3 + (3uv + p)(u + v) + q = 0. \qquad (\mathbf{1.3.3c})$$

Теперь реализуем упомянутую свободу: чтобы истребить произведение скобок в левой части, потребуем

$$3uv + p = 0; \qquad (\mathbf{1.3.3d})$$

уравнение (**1.3.3c**) примет вид

$$u^3 + v^3 = -q. \qquad (\mathbf{1.3.3e})$$

Здесь нам всё-таки придётся предположить, что $3 \neq 0$, отложив на будущее разбор экзотического случая 3=0. Принятое предположение позволяет преобразовать (**1.3.3d**) в

$$uv = -\frac{p}{3}, \qquad (\mathbf{1.3.3f})$$

и мы можем перейти к "словесной алгебре"в духе XVI-го века:

найти два числа по сумме их кубов и их произведению.

[12] иначе $1 = 0$, и в такой математике есть единственное число; хотя в дальнейшем эта математика будет упоминаться, сейчас мы считаем её невозможной

Произведение можно возвести в куб, и задача сведётся к (известной с глубокой древности) задаче нахождения неизвестных (в данном случае – кубов вспомогательных неизвестных) по сумме и произведению.

Вернувшись к буквенным обозначениям, подытожим наши действия системой

$$\begin{cases} u^3 + v^3 = -q & \textbf{(1.3.3e)} \\ u^3v^3 = -\dfrac{p^3}{27}. & \textbf{(1.3.3f)}^{\mathbf{3}} \end{cases}$$

равносильной полиномиальному тождеству

$$(\lambda - u^3)(\lambda - v^3) \equiv \lambda^2 + q\lambda - \frac{p^3}{27}. \qquad \textbf{(1.3.3g)}$$

Формально используя значок кубического корня для операции, обратной возведению в куб, из **(1.3.3b)** и **(1.3.3g)** получаем *формулу Кардано*

$$\boxed{x = \sqrt[3]{-\frac{q}{2} + \sqrt{-\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{-\frac{q^2}{4} + \frac{p^3}{27}}}} \qquad \textbf{(1.3.3h)}$$

1.3.4. Обсуждение. Можно ли сказать, что, "выведя" формулу Кардано, мы *решили все кубические уравнения*?

Попытка вдуматься в этот вопрос приводит к выводу о его не очень точной постановке. Возникают встречные законные вопросы:

• Из какого множества берутся коэффициенты?
• В каком множестве ищутся решения?
• С помощью каких функций хочется выразить решения через коэффициенты?

В курсе эти вопросы будут рассмотрены с позиций "взрослой" алгебры и, будем надеяться, прояснены.

Частный вопрос, относящийся к формуле Кардано – *какие из кубических корней брать*? Здесь традиция считать все числа вещественными оказывает плохую услугу: со школьной точки зрения функция $\mathbb{R} \to \mathbb{R} : r \mapsto \sqrt[3]{r}$ корректно определена, и можно попытаться прочитать формулу Кардано буквально. Итальянцам

XVI-го века эти попытки доставили массу проблем[13]; современные же математики понимают, что "функция" $r \mapsto \sqrt[3]{r}$ *трёхзначна*, так что формула Кардано **(1.3.3h)** задаёт *девятизначную* "функцию" (могло бы показаться, что даже 18-значную из-за двузначности $r \mapsto \sqrt[2]{r}$, но $\pm\sqrt[2]{\ldots}$ входят в формулу Кардано *симметрично*). В курсе будет показано, что три (надлежащим образом понимаемых...) *ветви* из этих девяти определяют настоящие корни уравнения **(1.3.3d)**, так что формула Кардано при правильных определениях действующих лиц даёт <u>все</u> решения этого уравнения в довольно сильном смысле.

1.4. Обобщения

1.4.0. Системы полиномиальных уравнений. Пусть даны положительные натуральный числа m и n и многочлены $f_1, \ldots, f_m$ от переменных $x_1, \ldots, x_n$ положительных степеней. В этой лекции мы обсудили несколько частных случаев *систем полиномиальных уравнений*

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \ldots \\ f_m(x_1, \ldots, x_n) = 0 \end{cases}$$

Степенью системы полиномиальных уравнений называется <u>произведение</u> степеней

$$d := \deg f_1 \cdot \deg f_2 \cdot \cdots \cdot \deg f_m.$$

В этой лекции мы сначала рассмотрели системы *линейных*, то есть с $d = 1$, систем уравнений при $m = n = 2$ (и чуть-чуть поговорили о случае $m = n = 3$), а затем перешли к *полиномиальным уравнениям*, то есть "системам" с $m = n = 1$ при $d = 2$ и $d = 3$.

В курсе будут полностью исследованы общие (то есть с произвольными m и n) системы линейных уравнений; относительно уравнений ($m = n = 1$, а d произвольно) будут получены результаты, в определённом смысле окончательные.

Вряд ли современная алгебра может претендовать на полное понимание систем полиномиальных уравнений с какими-то другими наборами (m, n, d) – за возможным исключением случая $d = 2$, которому мы тоже уделим некоторое внимание.

---

[13] усугублённых традицией работать только с *положительными* числами

1.4.1. Об уравнениях высших степеней. Как уже было упомянуто, уравнения степени 4 были решены вскоре после кубических уравнений, и результат отражён в **[Cardano1545]**. Идея заключается в следующем.

Надо искать не один корень, а все четыре, то есть для общего многочлена 4-й степени стремиться к разложению на множители

$$x^4 + ax^3 + bx^2 + cx + d \equiv (x - x_1)(x - x_2)(x - x_3)(x - x_4).$$

В терминах "чисел" это означает, что при заданных a, b, c, d следует найти такие x_1, x_2, x_3, x_4, что

$$\begin{cases} x_1 + x_2 + x_3 + x_4 = -a \\ x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 = b \\ x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 = -c \\ x_1x_2x_3x_4 = d. \end{cases}$$

Главный шаг – введение

$$\begin{cases} y_1 := x_1x_2 + x_3x_4, \\ y_2 := x_1x_3 + x_2x_4, \\ y_3 := x_1x_2 + x_3x_4; \end{cases}$$

устанавливается, что коэффициенты многочлена

$$(y - y_1)(y - y_2)(y - y_3)$$

от y *полиномиально* выражаются через коэффициенты a, b, c, d. Поскольку кубические уравнения мы решать умеем, некоторые *комбинации* корней x_1, x_2, x_3, x_4 тоже могут быть выражены (на этот раз с помощью радикалов 2-й и 3-й степени) через эти коэффициенты. Остальное сравнительно несложно.

Все упомянутые вычисления будут проведены в курсе после того, как будет развита концепция *симметрии* – в данном случае *равноправия* корней многочлена.

Что касается уравнений степени ≥ 5, сильнейшие математики безуспешно искали аналогичные формулы ещё три века, пока в первой половине XIX-го века не было установлено, что эти попытки обречены на провал. Поскольку теоремы *не*существования требуют гораздо более точных формулировок, чем применяющиеся в этой лекции, мы откладываем обсуждение этого вопроса.

1.4.2. Случай целых коэффициентов. Сохраняем обозначения предыдущего раздела, и пусть рассматриваемые многочлены имеют целые коэффициенты; в курсе это будет обозначаться как

$$f_1, \ldots, f_m \in \mathbb{Z}[x_1, \ldots, x_n].$$

Такими системами занимается *диофантова геометрия*. Как правило, основные вопросы в этой науке – *существуют ли решения данной системы полиномиальных уравнений?* Иногда – помимо очевидных или почему-то неинтересных, иногда уравнения зависят от параметров.

Пример: Великая теорема Ферма. *При натуральном $n > 2$ не существует целочисленных решений уравнения*

$$x^n + y^n = z^n,$$

для которых $xy \neq 0$. Доказательство потребовало сотни лет и стимулировало развитие разнообразных разделов математики, см. **[Ribenboim2000]**.

Пример: конгруэнтные числа. *Какие числа – площади пифагоровых треугольников?* Вопрос в том, для каких $S \in \mathbb{N}$ разрешима в целых числах система уравнений

$$\begin{cases} a^2 + b^2 = c^2 \\ ab = 2S \end{cases}$$

(обозначения неизвестных a, b, c необычны в теории уравнений, но традиционны в геометрии треугольника). Преобразование

$$x = \frac{a-c}{b}S, \; y = \frac{a(a-c)}{b}S$$

(его можно найти стандартными средствами алгебраической геометрии, которые будут разобраны в нашем курсе) сводит этот вопрос к классическому и вместе с тем крайне современному: изучению *рациональных* точек на плоской кривой, заданной уравнением

$$y^2 = x(x-S)(x+S);$$

треугольник восстанавливается по такой точке с помощью формул

$$a = \frac{y}{x}, \; b = \frac{2Sx}{y}, \; c = -\frac{x^2 + S^2}{y} \;.$$

Как было отмечено в примечании к рассказу о подвигах Фибоначчи, понимание теории рациональных точек на таких кривых достигнуто современной математикой лишь условно, по модулю одной из нерешённых проблем недавно начавшегося тысячелетия.

1.4.3. Десятая проблема Гильберта. Как мы только что упомянули, главный вопрос, связанный с *целочисленными системами* полиномиальных уравнений – их совместность, то есть наличие хотя бы одного решения (в отличие, например, от теории вещественных кубических уравнений, в которой существование корней не вызывает сомнений, а задача заключается в том, чтобы выразить их через коэффициенты).

Среди знаменитых двадцати трёх проблем Гильберта (см. **[Болибрух1999]**) десятая заключалась в том, чтобы научиться определять указанную совместность *алгоритмически*.

Проблемы Гильберта формулировались в 1900 году, за несколько десятилетий и до математической теории алгоритмов, и до реальных компьютеров. Поэтому неудивительно, что Гильберт не мог предусмотреть будущее "решение": проблема целочисленных систем полиномиальных уравнений *алгоритмически неразрешима*. Этот результат был получен в 1970-м году Ю.В. Матиясевичем[14]; см. **[Матиясевич1993]**.

Алгоритмическая неразрешимость центральной проблемы диофантовой геометрии – прежде всего, конечно, свидетельство огромной сложности этого раздела математики. Но именно у этой теоремы несуществования есть поразительные *положительные* аспекты – см. **[DMR1976]**. Совсем описательно выражаясь, Матиясевичем обнаружена сводимость вопросов о работе алгоритмов к вопросам о совместности систем целочисленных полиномиальных уравнений. На техническом языке – доказано совпадение классов *перечислимых* и *диофантовых* множеств.

Благодаря достижениям, связанным с 10-й проблемой Гильберта, статус диофантовой геометрии сменился: из чуть ли не развлекательного[15] раздела чистой математики она превратилась в не менее "серьёзную" область, чем, скажем, уравнения в частных производных.

В течение курса мы будем регулярно возвращаться к алгоритмическим проблемам.

[14] с использованием результатов М. Дэвиса, Х. Патнем и Дж. Робинсон

[15] важную роль в развитии диофантовой геометрии сыграла книга Баше де Мезириака "Приятные и занимательные задачи" **[Meziriac1624]**

Заключение

В этой лекции мы обсудили несколько видов алгебраических уравнений, а также отдельные уравнения – в основном с исторических позиций, иногда добавляя современные комментарии. Мы увидели, что с древних времён до наших дней изучение уравнений вносит важнейший вклад в развитие математики.

Однако эта вводная лекция занимает в курсе исключительное положение и по материалу, и по стилю. Начиная со следующей, мы будем точно определять действующие лица, вводить определения и формулировать (а иногда доказывать...) теоремы.

Иначе говоря, мы перейдём к изучению *множеств со структурами*, что характерно для устоявшихся разделов современной математики.

К уравнениям мы регулярно будем возвращаться, причём окажется, что получаемые с современных точек зрения результаты сильнее и полнее, чем результаты первопроходцев.

Литература

[BDHT2013] M. Baboulin, J. Dongarra, J. Herrmann, and S. Tomov, *Accelerating linear system solutions using randomization techniques.* ACM Trans. Math. Softw., 39(2), 2013.
[Beriman1956] A.E. Beriman, *The Babylonian quadratic equation.* Math. Gaz. 40 (1956), 185 — 192.
[Cajori1893] Florian Cajori, *A History of Mathematics.* Gutenberg EBook #31061.
[Cardano1545] Cardano, The Great Art or The Rules of Algebra (Ars Magna), Trans, and ed., T. Richard Witmer, with a foreword by Oystein Ore. Cambridge, Massachusetts, and London, England: The M.LT. Press, 1968.
[DMR1976] Martin Davis, Yuri Matijasevic and Julia Robinson, *Hubert's tenth problem. Diophantine equations: Positive aspects of a negative solution.* Proc. Sympos. Pure Math., vol. 28, Amer. Math. Soc., Providence, R. I., 1976, pp. 323-378.
[Fibonacci1225] Fibonacci, Leonardo Pisano. *The Book of Squares (Liber Quadratorum).* An annotated translation into modern English by L. E. Sigler. (1987) Orlando, FL: Academic Press.
[FowlerRobson1998] David Fowler and Eleanor Robson, *Square*

Root Approximations in Old Babylonian Mathematics: YBC 7289 in Context. HISTORIA MATHEMATICA 25 (1998), 366–378 ARTICLE NO. HM982209.
[Irwin2005] Robert Irwin, *The Arabian Nights: A Companion.* Tauris Parke, 2005.
[Kasir1931] D. S. Kasir, *The Algebra of Omar Khayyam.* Teachers College Press, New York, 1931. Reprinted AMS, 1972.
[Meziriac1624] Claude Gaspard Bachet, sieur de Méziriac, *Problemes plaisants et délectables…* . 2nd ed., Lyons, France: Pierre Rigaud et Associates, 1624. **[Ribenboim2000]** Ribenboim, Paulo, *Fermat's Last Theorem for Amateurs.* Springer, 2000.
[Sesiano2009] Jacques Sesiano, *An Introduction to the History of Algebra: Solving Equations from Mesopotamian Times to the Renaissance.* Providence, R.I. : American Mathematical Society, 2009.
[Strassen1969] Strassen V., *Gaussian Elimination is not Optimal.* Numer. Math — Springer Science+Business Media, 1969. — Vol. 13, Iss. 4. — P. 354—356
[БавринФрибус1994] И. И. Баврин, Е. А. Фрибус, *Старинные задачи. Книга для учащихся.* М., Просвещение, 1994.
[Болибрух1999] Болибрух А. А., *Проблемы Гильберта (100 лет спустя).* МЦНМО, 1999.
[Варден1959] Б. Л. ван дер Варден. *Пробуждающаяся наука. Математика древнего Египта, Вавилона и Греции.* М., Гос. издательство физико-математической литературы, 1959.
[Земляков2007] А.Н. Земляков, *Введение в алгебру и анализ. Культурно-исторический дискурс.* Элективный курс. "Озон" , 2007.
[ИльинПозняк2004] Ильин В. А., Позняк Э. Г., *Линейная алгебра: Учебник для вузов.* — 6-е изд., стер. — М.: ФИЗМАТЛИТ, 2004.
[Коблиц1988] Коблиц Н. *Введение в эллиптические кривые и модулярные формы.* М.: Мир, 1988.
[Матиясевич1993] Ю. В. Матиясевич, *Десятая проблема Гильберта.* М., Наука, 1993.
[Никомах2006] Никомах Геразский. *Введение в арифметику.* Пер., вступит. статья и комм. А. И. Щетникова. Новосибирск: АНТ, 2006.
[Пачоли1494] Пачоли Л.*Трактат о счетах и записях.* Под ред. Я. В. Соколова. — М.: Финансы и статистика, 1994.