

Уравнения степени 5 и выше

Дубна, 2025

Г.Б. Шабат

Лекция 1, 21 июля

Уравнения степеней ≤ 4 .

Версия 22 июля 2025

1.0. Уравнения и их решения	1
...1.0.0. Понятие уравнения	1
...1.0.1. Что значит <i>решить уравнение</i> ?	3
...1.0.2. Многочлены	4
...1.0.3. Корни многочленов	6
...1.0.4. Степень многочлена	7
...1.0.5. Кольцо многочленов	8
...1.0.6. Расширения основного поля	9
...1.0.7. Случай полей $\mathbb{R}$ и $\mathbb{C}$	12
1.1. Линейные уравнения	13
...1.1.0. Общее обсуждение	13
...1.1.1. Примеры	14
1.2. Квадратные уравнения	15
...1.2.0. Что это такое?	15
...1.2.1. Выделение полного квадрата	16
...1.2.2. Дискриминант	16
...1.2.3. Основная теорема	17
...1.2.4. Об истории	18
1.3. Кубические уравнения	18
...1.3.0. Итальянское Возрождение	18
...1.3.1. Канонический вид	19
...1.3.2. Дискриминант	18
...1.3.4. Итальянское решение	19
...1.3.5. Анализ над $\mathbb{R}$	22
...1.3.6. Решение ВСЕХ кубических уравнений	23
1.4. Сведение уравнений степени 4 к кубическим	23
...1.4.0. Неразличимость корней	23
...1.4.1. Канонический вид	23
...1.4.2. Гениальная идея	23
Литература	24

1.0. Уравнения и их решения

1.0.0. Понятие уравнения. Давайте наивно называть *уравнением* любое выражение вида

$$f(x) = a, \quad (1.0.0a)$$

но считать, что это выражение имеет точный математический смысл, лишь если подразумевается четвёрка (X, Y, f, a) , в которой X и Y – множества,

$$f : X \longrightarrow Y \quad (1.0.0b)$$

– отображение, и фиксирован элемент $a \in Y$.

Мы в этом курсе будем заниматься *полиномиальными* уравнениями с одной *неизвестной* над полем¹ $\mathbb{k}$, то есть работать с четвёрками, в которых множества суть $X = Y = \mathbb{k}$, а отображение задаётся многочленом²; обычно будем считать, что $a = 0$.

Однако в настоящем разделе мы обсуждаем существенно более общие понятия. Так, мы можем рассмотреть множество людей $X = \mathbb{L}$, множество мужчин $Y = \mathbb{M}$ и отображение

$$\text{отец} : \mathbb{L} \longrightarrow \mathbb{M}. \quad (1.0.0c)$$

Уравнение (или *равенство*?) (1.0.0a) превращается в утверждение на естественном языке *этот мужчина – его (или её) отец*. Решения этого "уравнения" мы обсудим ниже.

Понимание наших (1.0.0a) и (1.0.0b) опирается на концепции, возникшие сравнительно недавно, тогда как уравнения – один из самых старых разделов математики (вскоре мы поговорим о примерах). Понятия "множество" и "отображение" появились лишь в XIX веке.

Знак же равенства = был введён в XVI веке. врачом и математиком Робертом Рекордом³ в книге [Record1557], содержащей, согласно Википедии, следующий текст:

Howbeit, for easie alteration of equations. I will propounde a fewe erâples, bicause the extraction of their rootes, maie the more aptly bee wroughte. And to avoid the tedious repetition of these woordes: is equalle to: I will sette as I doe often in worke use, a paire of paralleles, or Gemowe lines of one lengthe, thus: =, bicause noe. 2. thynges, can be moare equalle. And now marke these numbers.

Записанный современными буквами, он выглядит как

Howbeit, for easie alteration of equations. I will propounde a fewe examples, bicause the extraction of their rootes, maie the more aptly bee wroughte. And to avoid the tedious repetition of these woordes: is equalle to: I will sette as I doe often in worke use, a paire of paralleles, or Gemowe lines of one lengthe, thus: =, bicause noe. 2. thynges, can be moare equalle.

и переводится на современный английский следующим образом:

However, for easy manipulation of equations, I will present a few examples in order that the extraction of roots may be more readily done. And to avoid the tedious repetition of these words "is equal to", I will substitute, as I often do when working,

¹Слушатели, не знакомые с теорией полей, могут понять некоторую часть курса, считая, как в школе, что мы работаем над полем *действительных* чисел $\mathbb{R}$. Но и этим слушателям необходимо освоить поле *комплексных* чисел $\mathbb{C} \supset \mathbb{R}$.

²Некоторое время мы, как в школе, не будем различать многочлены и определяемые ими отображения. В дальнейшем обсудим разницу.

³Англ. Robert Recorde; около 1510 —1558.

a pair of parallels or twin lines of the same length, thus: = , because no two things can be more equal.

Первое уравнение, записанное новым тогда способом, выглядело почти современно:

$$14.\text{з.} - 15.\text{з.} = 71.\text{з.}$$

($14x + 15 = 71$ — правда, не все значки понятны...); хотя и названное в Википедии *first ever*, оно не заслуживает нашего обсуждения.

Некоторые хорошо известные уравнения тоже имеют имена.

Наши определения уравнений и решений (1.0.0a) и (1.0.0b) охватывают различные классы уравнений, например

дифференциальное уравнение *маятника*: $\ddot{x} = \sqrt{\frac{g}{\ell}} \sin x$,

функциональное уравнение *логарифма*: $x(t_1 t_2) = x(t_1) + x(t_2)$

и другие. Слушателям рекомендуется преобразовать их так, чтобы имели смысл наши X, Y, f, a и затем ввести эти объекты. Мы же в этом курсе заниматься ими не будем.

1.0.1. Что значит решить уравнение? В обозначениях предыдущего подраздела решение уравнения

$$f(x) = a \tag{1.0.1a}$$

представляет собой исследование множества⁴

$$f^{-1\circ}(a) := \{x \in X \mid f(x) = a\}.$$

Вопросы и задания, связанные с этим множеством, могут быть разные. Основные таковы:

I. Разрешимость уравнения:

$$f^{-1\circ}(a) \stackrel{?}{\neq} \emptyset.$$

Более общо,

II. Сколько⁵ решений имеет уравнение:

$$\#f^{-1\circ}(a) = ?$$

Остальные вопросы и задания имеют смысл лишь в предположении утвердительного ответа на вопрос I. А именно

III. Найти хотя бы одно решение

$$x_1 \in f^{-1\circ}(a).$$

IV. Найти (и упорядочить!) все решения

$$x_1, x_2, \dots \in f^{-1\circ}(a).$$

⁴Мы различаем *алгебраически* обратное f^{-1} и композиционно обратное $f^{-1\circ}$. Например, $\text{tg}^{-1} = \text{ctg}$, тогда как $\text{tg}^{-1\circ} = \text{arctg}$.

⁵В случае дифференциальных уравнений этот вопрос заменяется на *от скольких параметров зависит общее* решение уравнения?

Разумеется, выполнение задания IV перекрывает все остальные вопросы и задания. Как мы убедимся в основной части курса, одна из главных трудностей теории состоит в упорядочении, или, иначе говоря, индивидуализации решений; существенная часть проблемы окажется **ЯЗЫКОВОЙ**: на каком языке мы определяем решения уравнений высших степеней?

В случае "уравнений" на естественном языке эта проблема решается настолько просто, что почти незаметна. Например, в стихотворении Давида Самойлова "Смерть Ивана" по существу рассматривается "уравнение" (1.0.0с) для случая $a = \text{Иван Грозный}$:

«Где же то, Иване, дети твои?»
«Вот он старший – чернец,
Вот он младший – птенец.
Ни тому, ни другому не по чину венец...»

(царь опускает ещё одно "решение" – убитого им царевича Иоанна, которому *венец* был бы как раз *по чину*). Здесь "решения" фигурируют вместе с именами, как и обычные дети обычных, не венценосных мужчин. (В теории уравнений высших степеней, как мы увидим, всё иначе).

Если чуть-чуть изменить f из уравнения (1.00с), положив

$$f(x) := \text{тот, кого } x \text{ называет отцом,}$$

то к множеству решений добавился бы Григорий Отрепьев (Пушкин: *тень Грозного меня усыновила...*), а затем и другие самозванцы, и *венцы* на какое-то время оказывались им *по чину*.

Вернёмся к уравнениям произвольных степеней, в которых

$$f(x) = x^n + c_1 x^{n-1} + \dots + c_n. \quad (1.0.1b)$$

Если $X = Y = \mathbb{R}$, а $f \in \mathbb{R}[x]$, то ответ на вопросы I и II даётся *теорией Штурма* (см. [Шафаревич1954]). Однако в целом, как мы покажем, действительная теория уравнений высших степеней весьма неполна, а в случае $X = Y = \mathbb{C}$, а $f \in \mathbb{C}[x]$ задача упорядочивания в проблеме IV практически безнадежна.

1.0.2. Многочлены. Вряд ли понимание формулы (1.0.1b), как и сопутствующего уравнения

$$x^n + c_1 x^{n-1} + \dots + c_n = 0, \quad (1.0.2a)$$

вызывает у кого-нибудь из слушателей затруднения: к уравнениям этого класса все привыкли со школы, особенно при $n = 2$, а, раз уж вы слушаете этот курс, то, видимо, надеетесь что-то узнать про случай $n = 5$.

Тем не менее, обсудим не совсем приличный вопрос:

$$\text{ЧТО ТАКОЕ МНОГОЧЛЕН?} \quad (1.0.2b)$$

Начнём с очевидного *лингвистического* ответа: это – выражение в левой части уравнения (1.0.2a). Попробуем согласиться. Только сменим нумерацию коэффициентов, перепишем по возрастанию степени *переменной*... или *неизвестной*? Этот x всегда вызывал затруднения; вспомним чудовищную запись

ever first equation, про трудности итальянских алгебраистов мы поговорим ниже.

Попытаемся обойтись без x :

$$a_0 + a_1x + a_2x^2 + \dots + a_nx^n \longleftrightarrow (a_0, a_1, a_2, \dots, a_n). \quad (1.0.2c)$$

Мы подошли к сомнительному ответу на вопрос, отождествив многочлен с *последовательностью его коэффициентов*. Поскольку слово *последовательность* в математике занято (и к тому же обычно обозначает нечто *бесконечное*...), воспользуемся программистским словом *массив*.

Что мы потеряли, отождествив многочлен с массивом его коэффициентов? Обратимся к алгебре.

Мы умели *складывать* и *умножать* многочлены. Но мы ведь можем воспроизвести эти операции на уровне массивов!

Действительно, сложение определяется покомпонентно:

$$(a_0, a_1, a_2, \dots) + (b_0, b_1, b_2, \dots) := (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots) \quad (1.0.2d)$$

Здесь возникает небольшое затруднение, связанное со сложением многочленов разных степеней. Мы преодолеем его, договорившись дозаполнять массив коэффициентов многочлена меньшей степени нулями – для того и сменили традиционную школьную запись многочленов на запись по возрастанию степеней одночленов. Ещё более радикальное решение – считать все массивы имеющими бесконечную длину, но только заполненными, начиная с некоторого места, нулями.

Теперь человек, обладающий некоторым опытом работы с многочленами, определит и умножение массивов: зная тождество

$$\begin{aligned} (a_0 + a_1x + a_2x^2 + \dots)(b_0 + b_1x + b_2x^2 + \dots) &\equiv \\ &\equiv a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \dots, \end{aligned}$$

он или она определит

$$(a_0, a_1, a_2, \dots) \cdot (b_0, b_1, b_2, \dots) := (a_0b_0, a_0b_1 + a_1b_0, a_0b_2 + a_1b_1 + a_2b_0, \dots). \quad (1.0.2e)$$

Такое умножение массивов называется *свёрткой*.

Мы готовы предложить ответ на вопрос (1.02b):

$$\text{МНОГОЧЛЕН} - \text{ЭТО МАССИВ ЕГО КОЭФФИЦИЕНТОВ} \quad (1.0.2f)$$

с дополнением

СЛОЖЕНИЕ МАССИВОВ ОЧЕВИДНО,

$$\text{А УМНОЖЕНИЕ} - \text{СВЁРТКА}. \quad (1.0.2f')$$

Для уточнения этого ответа необходимо договориться, из какого множества берутся коэффициенты.

Чтобы формулы (1.0.2d) и (1.0.2e) имели смысл, на множестве коэффициентов должны быть определены сложение и умножение. Чтобы с многочленами в стандартной записи (то есть с x) можно было производить привычные операции, то есть *раскрывать скобки* и *приводить подобные члены*, эти операции должны обладать привычными свойствами – на языке современной алгебре

это означает, что множество коэффициентов с введёнными операциями должно представлять собой *коммутативное полукольцо*.

Список аксиом коммутативного полукольца отличается от списка аксиом кольца тем, что из него выброшена аксиома наличия аддитивно обратного элемента; примерами коммутативных полуколец служат $(\mathbb{N}, +, \cdot)$ и множество подмножеств любого множества с операциями $\cup$ и $\cap$. В задаче 1.1 предлагается поработать с соответствующей аксиоматикой.

Если мы хотим, как привыкли, свободно переносить одночлены из одной части уравнения в другую, то нам необходимо *вычитание*, так что о полукольцах до конца курса давайте забудем.

Итак,

КОЭФФИЦИЕНТЫ НАШИХ МНОГОЧЛЕНОВ ЛЕЖАТ В КОММУТАТИВНОМ КОЛЬЦЕ. (1.0.2g)

Начиная с уравнений 1-й степени, нам необходима также и четвёртая (наряду со сложением, умножением и вычитанием) операция – *деление*, такое мучительное для древних египтян – см. ниже. Мы пришли к аксиомам *поля*⁶, и до конца курса принимаем термин *основное поле*, из которого будем брать коэффициенты, и **всегда будем обозначать его**⁷ $\mathbb{k}$.

Для **кольца многочленов** с коэффициентами из поля $\mathbb{k}$ мы уже использовали обозначение

$$\mathbb{k}[x]$$

и будем продолжать им пользоваться. Отметим, однако, что **буква x в определении этого кольца не входит!** Она используется лишь при обосновании умножения-свёртки с помощью биекции (1.0.2c).

Итог подраздела: отвечая на вопрос (1.0.2b), мы построили сопоставление

$$\mathbb{k} \mapsto \mathbb{k}[x]$$

полю коммутативного кольца.

Знакомые с языком не-школьной математики легко проверят, что это – *функтор* из категории полей в категорию коммутативных колец.

(Можно было бы расширить область определения этого функтора до категории коммутативных колец, но, во-первых, нам это не понадобится, а, во-вторых, значениями этого функтора были бы кольца гораздо более сложные, чем кольца *главных идеалов* вида $\mathbb{k}[x]$, похожие на кольцо $\mathbb{Z}$).

Современная математика не выработала хорошего обозначения для этого функтора.

1.0.3. Корни многочленов. Буква x в основной конструкции предыдущего подраздела утратила смысл. Его надо восстановить как для того, чтобы вернуться к нашей основной теме, уравнениям вида $f(x) = 0$, так и для того,

⁶См. любой учебник современной алгебры.

⁷Из Википедии: *Р. Дедекинд в [DirichletDedekind1871] назвал множество действительных или комплексных чисел, замкнутое относительно четырёх арифметических операций, немецким словом $\mathbb{K}örrer$, означающим "тело" или "корпус" (чтобы подчеркнуть органическое единство вводимого объекта). Термин укоренился в немецком и французском (*corps*), тогда как в английском и русском вслед за [Moore1893] стал использоваться менее обоснованный термин "поле".*

чтобы не утратить наши школьные представления в случае $\mathbb{k} = \mathbb{R}$ — например, о *графиках* $y = f(x)$.

Здесь снова не хватает общепринятых обозначений, и нам придётся ввести свои. Воспользовавшись иногда фигурирующим обозначением

$$Y^X := \{\text{отображения } X \rightarrow Y\}$$

для произвольных множеств X, Y (его пониманию помогает задача 1.2), определим отображение

$$\text{func} : \mathbb{k}[x] \longrightarrow \mathbb{k}^{\mathbb{k}} : (a_0, a_1, a_2, \dots) \mapsto (x \mapsto a_0 + a_1x + a_2x^2 + \dots); \quad (1.0.3a)$$

в задаче 1.3 предлагается проверить, что это — *гомоморфизм колец*.

В школьной алгебре отображение `func` не замечают, отождествляя многочлен f с *функцией* `func(f)`. Это отождествление безвредно в основных для нас случаях $\mathbb{k} \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$ — в этих случаях, как и во всех других *нулевой характеристики*, отображение `func` инъективно. В случаях же *положительной характеристики* (мы им тоже уделим внимание) дела обстоят иначе, см. задачу 1.4.

Для краткости введём обозначение

$$\text{func}(f) =: \underline{f}. \quad (1.0.3b)$$

Как вы "знаете" из школы, *корнем* многочлена $f \in \mathbb{k}[x]$ называется любое

$$\text{решение уравнения } \underline{f}(x) = 0 \quad (1.0.3c)$$

или, повторимся, любой

$$\text{элемент множества } \underline{f}^{-1 \circ}(0). \quad (1.0.3d)$$

Приведённые определения, возможно, представляются очевидными; в любом случае, с точностью до $f \longleftrightarrow \underline{f}$, они абсолютно стандартны. Отметим, однако, **несуразность**, связанную всё с той же буквой x , которой можно придать три разных смысла:

- (1) ничего не значащая буква, использованная при определении кольца $\mathbb{k}[x]$;
- (2) в соответствии с (1.0.3d) — одно из "чисел" $x \in \mathbb{k}$;
- (3) при рассмотрении в кольце $\mathbb{k}[x]$ (наряду с $+$ и $\cdot$) третьей важной⁸ операции, *композиции* $\circ$, нейтральный элемент относительно этой операции есть $x \in \mathbb{k}[x]$.

Рассматривая конкретные уравнения, мы будем, как правило, придерживаться смысла (2). В дальнейшем, чтобы избежать указанной **трёхсмысленности**, мы поставим в центр обсуждений понятие, тоже известное со школы — разложение многочленов на множители.

1.0.4. Степень многочлена. Разумеется, слушатели знают или думают, что знают определение этого понятия. Но некоторые уточнения могут оказаться полезны.

На первый взгляд, степень — это отображение⁹

$$\deg : \mathbb{k}[x] \longrightarrow \mathbb{N}.$$

⁸Например, в теории *биквадратных* уравнений.

⁹Здесь и далее принимаем *французское* соглашение $\mathbb{N} := \{0, 1, 2, \dots\}$.

Попробуем дать соответствующее определение для обоих способов записи многочленов:

$$\deg(a_0 + a_1x + a_2x^2 + \dots) := \max\{n \mid a_n \neq 0\}, \quad (1.0.4a)$$

$$\deg(c_0x^n + c_1x^{n-1} + \dots + c_0) = n, \text{ если } c_0 \neq 0. \quad (1.0.4b)$$

Оба определения кажутся правильными, но... не работают для *нулевого* многочлена, то есть многочлена с массивом коэффициентов $(0, 0, 0, \dots)$ (он же – нейтральный элемент относительно сложения в кольце $\mathbb{k}[x]$).

Преодоление возникшего затруднения заключается в том, чтобы к *упорядоченному моноиду* $(\mathbb{N}, +; \leq)$ добавить интуитивно ясный элемент $-\infty$, получив *упорядоченную полугруппу* $(\mathbb{N} \amalg \{-\infty\}, +; \leq)$ – слушателям предлагается либо найти где-нибудь (или придумать) использованные определения, либо пропустить непонятные слова. Теперь предлагается положить

$$\deg(0, 0, 0, \dots) := -\infty$$

и чуть-чуть модифицировать приведенные ”определения”: по-прежнему

$$\deg(a_0 + a_1x + a_2x^2 + \dots) := \max\{n \mid a_n \neq 0\}, \quad (1.0.4a')$$

с соглашением $\max(\emptyset) = -\infty$,

$$\deg(c_0x^n + c_1x^{n-1} + \dots + c_n) = \begin{cases} n, & \text{если } c_n \neq 0 \\ -\infty, & \text{если } c_0 = c_1 = \dots = c_n = 0 \end{cases} \quad (1.0.4b')$$

Так введённая степень

$$\deg : \mathbb{k}[x] \longrightarrow \mathbb{N} \amalg \{-\infty\}$$

обладает свойствами *нормирования*:

$$[(f_1, f_2) \neq (0, 0)] \implies [\deg(f_1 \cdot f_2) = \deg(f_1) + \deg(f_2)],$$

$$\deg(f_1 + f_2) \leq \max(\deg(f_1), \deg(f_2)).$$

Нормирования играют важную роль в алгебраической теории чисел и в алгебраической геометрии.

1.0.5. Кольцо многочленов. Кольца $\mathbb{k}[x]$ похоже на кольцо целых чисел $\mathbb{Z}$; так, во всех них определён *алгоритм Евклида*.

В любом кольце многочленов есть также аналог понятия *простого числа*: многочлен $f \in \mathbb{k}[x]$ называется *неприводимым*, если он не представим в виде произведения многочленов меньших степеней. В кольце $\mathbb{k}[x]$ полезно ввести *подмножество неприводимых многочленов*:

$$\mathbb{k}[x] \supset \mathbb{k}[x]^{\text{irr}} := \left\{ f \in \mathbb{k}[x] \mid \forall f_1, f_2 \in \mathbb{k}[x] \left[f = f_1 f_2 \implies [(\deg(f_1) = \deg(f)) \vee (\deg(f_2) = \deg(f))] \right] \right\}$$

Уравнения $\underline{f}(x) = 0$ представляют интерес лишь для $\boxed{f \in \mathbb{k}[x]^{\text{irr}}}$, поскольку, очевидно,

$$(\underline{f_1 f_2})^{-1\circ}(0) = (\underline{f_1})^{-1\circ}(0) \cup (\underline{f_2})^{-1\circ}(0).$$

Кольца многочленов, однако, обладают свойством, не имеющим аналогов в кольце целых чисел.

Кольцо R называется *градуированным*, если его аддитивная группа так представима в виде прямой суммы своих подгрупп

$$R^+ = \bigoplus_{n=0}^{\infty} R_n,$$

что для любых $m, n \in \mathbb{N}$

$$R_m R_n \subseteq R_{m+n}.$$

Введя нестандартные обозначения

$$\mathbb{k}[x]_0 := \mathbb{k}^+ = \{f \in \mathbb{k}[x] \mid \deg(f) \leq 0\}$$

и для $n \in \mathbb{N}_{>0}$

$$\boxed{\mathbb{k}[x]_n := \{f \in \mathbb{k}[x] \mid \deg(f) = n\}}$$

(именно ради этого обозначения мы углубились в профессиональную алгебру), мы будем считать каждое кольцо $\mathbb{k}[x]$ градуированным:

$$\boxed{\mathbb{k}[x]^+ = \bigoplus_{n=0}^{\infty} \mathbb{k}[x]_n}.$$

Иногда нам будет удобно обозначение

$$\boxed{\mathbb{k}[x]_n^{\text{Irr}} := \mathbb{k}[x]^{\text{Irr}} \cap \mathbb{k}[x]_n}$$

множества неприводимых многочленов данной степени. Оно, видимо, не обладает никакой разумной алгебраической структурой.

1.0.6. Расширения основного поля. Вернёмся ненадолго к общим уравнениям вида

$$f(x) = a, \tag{1.06a}$$

где $f : X \rightarrow Y$ – отображение и $a \in Y$.

Здесь аналогом математической конструкции, которую мы собираемся рассмотреть, является пара вложений множеств¹⁰ $X \hookrightarrow Z, Y \hookrightarrow W$ с *расширением* отображения f , которое мы будем обозначать той же буквой; это означает, что теперь задано отображение

$$f : Z \longrightarrow W,$$

ограничение $f|_X$ которого на подмножество X совпадает с рассматриваемым ранее f . В этой ситуации имеет место *расширение множества решений* уравнения (1.06a):

$$f|_X^{-1\circ}(a) \subseteq f^{-1\circ}(a) \tag{1.06b}$$

(здесь подразумевается $f^{-1\circ}(a) := \{z \in Z \mid f(z) = a\}$; можно также уточнить $f|_X^{-1\circ}(a) = f^{-1\circ}(a) \cap X$).

¹⁰Выбранные обозначения множеств соответствуют традиционному переходу от функций действительной переменной $y = f(x)$ к функциям комплексной $w = f(z)$.

Например, в рассмотренной выше ситуации Иван Грозный интерпретировал обращённый к нему вопрос *где...дети твои?* как вопрос о живых детях, как будто бы речь шла об отображении

$$\text{отец} : X \longrightarrow M,$$

определённом лишь на множестве $X = \text{ЖЛ живых людей}$. Правдивый¹¹ ответ на вопрос, то есть решение уравнения $\boxed{\text{отец}(x) = \text{Иван Грозный}}$, состоял в 1584 в формуле

$$(\text{отец}|_X)^{-1\circ}(a) = \{\text{Фёдор, Дмитрий}\}.$$

На предстоящем же царю Страшном Суде должно было подразумеваться множество $Z = \text{Л всех людей}$, и ответ должен был расшириться до

$$(\text{отец})^{-1\circ}(a) = \{\text{Иоанн, Фёдор, Дмитрий}\}.$$

Вернёмся к математике. Теория полей – это в большой степени теория расширений полей, в нашем случае расширений

$$\mathbb{K} \supset \mathbb{k}.$$

В связи с полиномиальными уравнениями такие расширения рассматриваются для того, чтобы в больших полях найти корни многочленов, отсутствующие в меньших. Учитывая, что вложение полей

$$\mathbb{k} \hookrightarrow \mathbb{K}$$

согласно любому из рассмотренных определений многочленов индуцирует вложение колец многочленов

$$\mathbb{k}[x] \hookrightarrow \mathbb{K}[x],$$

введём центральные для всего курса обозначения.

Для каждого многочлена $f \in \mathbb{k}[x]$ и каждого расширения мы, как только что было отмечено, можем считать, что $f \in \mathbb{K}[x]$; выше мы определили соответствующее отображение

$$\underline{f} : \mathbb{K} \longrightarrow \mathbb{K}.$$

Поскольку теперь это отображение зависит от выбранного расширения, мы его обозначим $f_{\mathbb{K}}$. Таким образом, для массива коэффициентов $a_0, a_1, \dots \in \mathbb{k}$ мы определяем отображение

$$(a_0, a_1, \dots)_{\mathbb{k}} : \mathbb{K} \longrightarrow \mathbb{K} : (z \mapsto (a_0 + a_1 z + a_2 z^2 + \dots)).$$

Теперь для $\boxed{f \in \mathbb{k}[x]}$ и $\boxed{\mathbb{K} \supset \mathbb{k}}$ обозначим множество *лежащих в поле $\mathbb{K}$ корней многочлена f*

$$\boxed{\text{Roots}_f(\mathbb{K}) := \{\alpha \in \mathbb{K} \mid f_{\mathbb{K}}(\alpha) = 0\}}.$$

По определению,

$$\text{Roots}_f(\mathbb{K}) \supseteq \text{Roots}_f(\mathbb{k}).$$

Приведём три конструкции расширений исходного поля, позволяющие увеличить множество корней многочлена.

¹¹Речь идёт о законных детях властителя. В Википедии приводятся сведения о том, что сам он хвастался тысячами(!) незаконных.

Присоединение корня. Пусть $f \in \mathbb{k}^{\text{irr}}$. Для знакомых с идеалами и фактор-кольцами просто определим

$$\mathbb{K} := \frac{\mathbb{k}[x]}{\langle f \rangle}.$$

Из наличия алгоритма Евклида не очень трудно вывести (придумайте доказательство, найдите его где-нибудь или поверьте), что *фактор-кольцо* $\mathbb{K}$ *есть поле*; вложение $\mathbb{k} \hookrightarrow \mathbb{K}$ осуществляется на уровне свободных членов; наконец, образ (всё того же!) элемента $x \in \mathbb{k}[x]$ есть корень многочлена $f \in \mathbb{K}[x]$.

Для незнакомых с идеалами и фактор-кольцами рассмотрим два исторически важных примера в случаях $\deg(f) = 2$ (в меньших степенях всё тривиально).

(а) Перенесёмся в древнюю Грецию и обсудим тогдашнюю сенсацию: *несоизмеримость диагонали квадрата и его стороны*.

На современном языке это открытие формулируется короче:

$$\sqrt{2} \notin \mathbb{Q}.$$

Но $\sqrt{2}$ — это же несомненно ЧИСЛО! Оно представляет собой ОТНОШЕНИЕ ДЛИН ОТРЕЗКОВ, которые мы можем взять в руки. Так что требуется расширение поля¹² рациональных чисел.

Приведённая конструкция определяет это расширение как

$$\mathbb{k} = \mathbb{Q} \hookrightarrow \mathbb{Q}(\sqrt{2}) := \frac{\mathbb{Q}[x]}{\langle x^2 - 2 \rangle} =: \mathbb{K}.$$

Элементарное определение этого поля читателю предлагается осуществить в задаче **1.5**. Оно оказывается подполем поля действительных чисел $\mathbb{R}$, и его положительные числа легко построить циркулем и линейкой.

(б) *Мнимая единица* i . Теперь переместимся ближе к нашему времени, к формуле Эйлера

$$e^{it} \equiv \cos t + i \sin t$$

и к мемуару [Argand1806] об изображении комплексных чисел точками плоскости. Здесь

$$\mathbb{k} = \mathbb{R} \hookrightarrow \frac{\mathbb{R}[x]}{\langle x^2 + 1 \rangle} =: \mathbb{C}.$$

Этой конструкции посвящена задача **1.6**.

Хотя рассмотренные конструкции (а) и (б) связаны с разными эпохами развития математики и с разными интуитивными представлениями, их алгебраическая природа совпадает; в обоих случаях речь идёт о *присоединении корней квадратного уравнения*. В задаче **1.7** предлагается провести эти конструкции для случая общего квадратного трёхчлена $x^2 + px + q \in \mathbb{k}[x]_2^{\text{irr}}$.

Поле разложения многочлена. Эта конструкция представляет собой итерацию присоединения корней. На каждом шагу у многочлена появляется новый

¹²Тут мы сознательно допускаем историческую неточность. Древние греки (во всяком случае до Диофанта) не владели отрицательными числами.

корень, то есть многочлен, неприводимый в меньшем поле, оказывается приводимым в большем. За конечное число шагов, не превосходящее степень исходного многочлена, достигается поле, в котором исходный многочлен разлагается на линейные множители. Это поле, разумеется, и называется *полем разложения многочлена*.

Примеры будут разобраны ниже.

Алгебраическое замыкание поля. Существует процедура присоединения "всех" корней сразу. Иначе говоря, для любого поля $\mathbb{k}$ существует поле $\mathbb{K}_1$, в котором все многочлены из $\mathbb{k}[x]$ разлагаются на линейные множители. Однако могут появиться новые не разлагающиеся на линейные множители многочлены из $\mathbb{K}_1[x]$; строим поле $\mathbb{K}_2$, над которым они все разлагаются. Продолжая процедуру, получаем бесконечную башню полей

$$\mathbb{k} \subseteq \mathbb{K}_1 \subseteq \mathbb{K}_2 \subseteq \mathbb{K}_3 \subseteq \dots$$

Их объединение

$$\bar{\mathbb{k}} := \bigcup_{n=1}^{\infty} \mathbb{K}_n$$

Поле $\bar{\mathbb{k}}$ является *алгебраически замкнутым*; это значит, что все многочлены из $\bar{\mathbb{k}}[x]$ разлагаются на линейные множители). В $\bar{\mathbb{k}}$ существует по крайней мере одно минимальное содержащее $\mathbb{k}$ алгебраически замкнутое поле. Оно обозначается $\bar{\mathbb{k}}$; таким образом, имеется башня полей

$$\mathbb{k} \subseteq \bar{\mathbb{k}} \subseteq \bar{\bar{\mathbb{k}}},$$

в которой два большие поля алгебраически замкнуты. Оказывается, поле $\bar{\mathbb{k}}$ определено *однозначно с точностью до изоморфизма*. Оно и называется *алгебраическим замыканием* поля $\mathbb{k}$. См. задачи к первой главе исключительно компактной книги [АтьяМакдональд1972].

Бегло описанная конструкция, основанная на идеях Э. Артина, кажется очень абстрактной. Не все математики принимают её, поскольку при проведении более подробного доказательства приходится использовать неконструктивную *лемму Цорна*.

Однако не всё так плохо. Как-никак, ОСНОВНОЕ классическое поле — это, согласно *основной теореме алгебры*, алгебраически замкнутое поле $\mathbb{C}$. Оно же — алгебраическое замыкание $\bar{\mathbb{R}}$, так что для поля действительных чисел утомительная конструкция Артина не нужна. *Поле алгебраических чисел* $\bar{\mathbb{Q}}$ более загадочно, но благодаря (единственному!) вложению $\mathbb{Q} \hookrightarrow \mathbb{R}$ можно считать, что $\bar{\mathbb{Q}} \subseteq \mathbb{C}$.

С метаматематикой конечных полей и их алгебраических замыканий, а также связями этих полей с другими важными разделами математики, можно познакомиться по работе [Ах1968].

Цель расширений исходного поля всех рассмотренных видов — "найти" недостающие в основном поле корни.

Вопросы I и II из подраздела 1.0.1 теряют смысл (будем исходить из того, что слушателям известна теорема Безу), вопрос III требует уточнения, а вопрос IV, по мнению лектора, остаётся (почти) безнадёжным.

1.0.7. Случаи полей $\mathbb{R}$ и $\mathbb{C}$ выделяются возможностью использовать **геометрическую интуицию**. Для $\mathbb{R}$ она основана на рассмотрении ”школьных” графиков многочленов $y = f(x)$. Наглядные понятия для $\mathbb{C}$ будут по мере необходимости вырабатываться.

Основная теорема алгебры для $\mathbb{C}$ общеизвестна:

Любой многочлен с комплексными коэффициентами разлагается на множители первой степени.

Для $\mathbb{R}$ приведём более осторожную формулировку из [Gauss1799]:

Любой многочлен с действительными коэффициентами разлагается на множители первой и второй степени.

Формулировка Гаусса бесценна при анализе уравнений малых степеней с действительными коэффициентами.

Однако комплексная точка зрения даёт более глубокое понимание.

Приведём пример вне рамок нашего курса.

Логарифм и арктангенс изучаются в разных разделах школьной математики и обычно воспринимаются как не связанные между собой. Однако возможны чуть-чуть похожие определения:

$$\log x := \int_1^x \frac{du}{u},$$

$$\operatorname{arctg} x := \int_0^x \frac{du}{1+u^2}.$$

При переходе к комплексным числам возникает тождество

$$1+u^2 \equiv (1+ui)(1-ui)$$

и вытекающее из него

$$\frac{1}{1+u^2} \equiv \frac{1}{2} \left(\frac{1}{1+ui} + \frac{1}{1-ui} \right).$$

Можно ли с помощью этих тождеств связать логарифм с арктангенсом? Предоставляю слушателям продумать ответ на этот вопрос.

1.1. Линейные уравнения

1.1.0. Общее обсуждение. Согласно нашим определениям, линейное уравнение (правильнее было бы называть его уравнением *первой степени*) имеет вид

$$c_0x + c_1 = 0, \tag{1.1.0.a}$$

где подразумевается $c_0 \neq 0$ (иначе оно было бы уравнением нулевой степени или, как мы договорились, ещё и при $c_1 = 0$ степени $-\infty$).

Поскольку уравнение (1.1.0.a) мгновенно решается:

$$x = -\frac{c_1}{c_0}, \tag{1.1.0.b}$$

есть ли предмет для обсуждения?

Не могу уверенно ответить на этот вопрос.

Математика уравнений первой степени богата. Краткое решение (1.1.0.b) уравнения (1.1.0.a) основано на развившихся в течение многих столетий концепций числа и четырёх арифметических операций. Мы немного поговорили о

замечательном разделе математики, взявшем за основу эти четыре операции, о теории полей. Но аксиомы этой теории допускают многочисленные вариации.

Одной из них является теория *тел*, в которой отказываются от коммутативности умножения (в связи с квадратными уравнениями будет предложена задача, связанная с этой теорией). Уравнение (1.1.0.a) в теории тел также решается мгновенно, но формулу (1.1.0.b) приходится заменить на

$$x = -c_0^{-1}c_1 \quad (1.1.0.b')$$

Известны и другие направления отказа от привычных свойств чисел, например, развитие увлекательной теории *ассоциативных алгебр с делением*. Все они, однако, лежат на границе предмета нашего курса или вне его.

Как мы вскоре увидим, люди решали уравнения малых степеней в течение тысяч лет. Содержание задач на составление уравнений (даже первой степени) и методы их решений, ранние документы, эволюция представлений о числах, взаимодействие математических культур – всё это доставляет богатый материал и предметы исследований историков, археологов, лингвистов,... но нам придётся лишь бегло коснуться профессиональной жизни наших коллег из других эпох. См., например, [Варден1959].

Перейдём к конкретным задачам на составление уравнений первой степени.

1.1.1. Примеры. Современный человек легко извлекает из Интернета фрагменты "задачников" вроде такого:



Об этом осколке вавилонской математики (ему более трёх тысяч лет) можно почитать, например, в [Friberg1978].

Вот одна из задач (перевод Friberg→ГБШ), возможно, содержащаяся в этой глиняной табличке:

Предположим, что взято две трети от двух третей некоторого количества ячменя, затем добавлено сто единиц, и в результате получено исходное

количество. Сколько было ячменя?

Для нас сравнительно легко перевести эту задачу на современный алгебраический язык:

$$\frac{2}{3} \times \frac{2}{3}x + 100 = x$$

Хотя это не сразу бросается в глаза, коэффициенты подобраны так, что ответ – натуральное число $x = 180$.

До наших $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ оставались тысячи лет... Или дроби в этой школе писцов "ещё не проходили?" Или для них не было обозначений? Или не было понятий?

Специалистам по истории математики ответы, вероятно, известны.

Переместимся более чем на тысячу лет ближе к нашему времени и затронем **египетскую** математику, причём не самую древнюю.

Акхимский папирус относится к VII или VIII веку нашей эры, см. [Baillet1892].

Вот пример задачи из этого папируса, более близкой нам, чем предыдущая, и по времени, и по содержанию (перевод заимствован из [Чистяков1962])

Некто взял из сокровищницы $\frac{1}{13}$. Из того, что осталось, другой взял $\frac{1}{17}$, оставил же он в сокровищнице 150. Сколько было в сокровищнице изначально?

Сравнительно легко составить уравнение:

$$\frac{16}{17} \times \frac{12}{13}x = 150.$$

Наш современник легко решит его (вероятно, воспользовавшись находящимся под рукой вычислительным устройством):

$$x = \frac{5525}{32}.$$

В школе нас, однако, учат, что эта дробь – *неправильная*, и надо преобразовать её к виду¹³

$$x = 172 + \frac{21}{32}.$$

Древнеегипетские преподаватели в школах писцов шли на шаг дальше: они не признавали (или не знали?) произвольных дробей; годились только дроби с числителем 1, называемые *аликвотными* дробям, см. [Варден1959]). Поэтому требовалось представить ответ в виде

$$x = 172 + \frac{1}{2} + \frac{1}{8} + \frac{1}{48} + \frac{1}{96}.$$

Вряд ли многие из нас смогли бы сходу написать древнеегипетскую контрольную на "отлично"!

¹³В школе учат записывать ответ в виде $x = 172\frac{21}{32}$, но мне представляется недопустимым опускать КАК знак умножения, например, в $ab \equiv a \cdot b$, ТАК И знак сложения, например $172\frac{21}{32} \equiv 172 + \frac{21}{32}$.

Рекомендуется ответить на вопрос задачи **1.8**.

1.2. Квадратные уравнения

1.2.0. Что это такое? Согласно введённым обозначениям, *квадратное уравнение* имеет вид

$$f_{\mathbb{k}}(x) = 0,$$

где $f \in \mathbb{k}[x]_2$.

Это определение, вычурное с точки зрения школьной математики, имеет ряд преимуществ.

Во-первых, мы в самом определении фиксируем основное поле $\mathbb{k}$ – само собой, не подразумевая, что $\mathbb{k} = \mathbb{R}$.

Во-вторых, мы с самого начала ставим в центр внимания отображение

$$f_{\mathbb{k}} : \mathbb{k} \longrightarrow \mathbb{k},$$

будучи готовыми для расширений $\mathbb{K} \supset \mathbb{k}$ продолжить отображение до

$$f_{\mathbb{K}} : \mathbb{K} \longrightarrow \mathbb{K}.$$

В случае $\mathbb{k} = \mathbb{R}$ это отображение сопровождается привычным наглядным образом – графиком, представляющим собой параболу, а в случаях $\mathbb{k} = \mathbb{C}$ или $\mathbb{K} = \mathbb{C}$ – образами, которые мы ещё выработаем.

В-третьих, мы не привязываемся ни к какому распространённому набору букв, как в случае школьных определений

$$ax^2 + bx + c = 0,$$

$$ax^2 + 2bx + c = 0,$$

$$x^2 + px + q = 0,$$

$$x^2 - tx + n = 0,$$

Найти два числа
по их сумме m
и произведению n .

и наших

$$c_0x^2 + c_1x + c_2 = 0,$$

$$a_0 + a_1x + a_2x^2 = 0.$$

Основные вопросы о квадратных уравнениях формулируются не столько в терминах троек или пар букв, сколько в терминах множеств $f_{\mathbb{k}}^{-1\circ}(0)$ или $f_{\mathbb{K}}^{-1\circ}(0)$.

1.2.1. Выделение полного квадрата. Всё же выберем запись, например,

$$c_0x^2 + c_1x + c_2 = 0, \tag{1.2.1a}$$

где $c_0, c_1, c_2 \in \mathbb{k}$.

Порассуждав о коэффициенте c_0 , как в случае степени 1, сведём его к уравнению

$$x^2 + px + q = 0. \tag{1.2.1b}$$

Нас учили преобразовывать уравнение (1.2.1b) к уравнению

$$\left(x + \frac{p}{2}\right)^2 = \frac{p^2}{4} - q. \quad (1.2.1b')$$

Но сделать это можно **ЛИШЬ В ПРЕДПОЛОЖЕНИИ**

$$\boxed{\text{char}(\mathbb{k}) \neq 2}, \quad (1.2.1c)$$

которое мы и **принимает**.

Теория квадратных уравнений в случае $\text{char}(\mathbb{k}) = 2$ весьма интересна (как и вся математика над расширениями поля $\mathbb{F}_2$). У нас, к сожалению, нет времени ей заниматься, и я ограничиваюсь ссылкой на весьма серьёзную работу [CheGaVaW1998].

1.2.2. Дискриминант. Сначала рассмотрим два многочлена положительной степени со старшим коэффициентом 1 (По-английски такие многочлены называются *unital*; русского общепринятого термина, видимо, не существует)

$$f, g \in \mathbb{k}[x].$$

Теорема-определение. Для введённых многочленов имеет место равенство

$$\prod_{\beta \in \text{Roots}_g(\bar{\mathbb{k}})} f_{\bar{\mathbb{k}}}(\beta) = \prod_{\alpha \in \text{Roots}_f(\bar{\mathbb{k}})} g_{\bar{\mathbb{k}}}(\alpha) =: \boxed{\text{resultant}}(f, g). \quad (1.2.2a)$$

Результант двух многочленов лежит в $\mathbb{k}$ и обращается в 0 тогда и только тогда, когда многочлены имеют общий корень.

Доказательство этой теоремы можно найти в любом основательном учебнике "высшей" алгебры. Мы вскоре проверим её в интересующем нас частном случае.

Определение¹⁴. Дискриминантом многочлена $f \in \mathbb{k}[x]$ положительной степени, взаимно простой с $\text{char}(\mathbb{k})$, называется

$$\boxed{\text{discrim}}(f) := -\text{resultant}\left(f, \frac{f'}{\deg(f)}\right). \quad (1.2.2b)$$

Вычислим двумя способами дискриминант многочлена $f = x^2 + px + q$, введя

$$g := \frac{f'}{2} = x + \frac{p}{2}. \quad (1.2.2c)$$

Согласно левой части (1.2.2a),

$$\text{discrim}(f) = -\left(\left(-\frac{p}{2}\right)^2 + p\left(-\frac{p}{2}\right) + q\right) = \frac{p^2}{4} - q.$$

¹⁴Не вполне стандартное.

Согласно же правой части (1.2.2a),

$$\text{discrim}(f) = \left(-\frac{p}{2} + \sqrt{\frac{p^2}{4} - q} + \frac{p}{2}\right) \left(-\frac{p}{2} - \sqrt{\frac{p^2}{4} - q} + \frac{p}{2}\right) = \frac{p^2}{4} - q$$

Мы подтвердили (1.2.2a) и убедились, что наше определение совпадает со школьным.

1.2.3. Основная теорема. Итак, пусть дан многочлен

$$f \in \mathbb{k}[x]_2$$

и $\text{char}(\mathbb{k}) \neq 2$. Тогда

$$\begin{aligned} [\text{discrim}(f) = 0] &\iff [\exists m \in \mathbb{k}[x]_2 [f = m^2]]; \\ [\text{discrim}(f) \neq 0] &\implies \left[[\text{discrim}(f) \in (\mathbb{k}^\times)^2] \iff [\text{Roots}_f(\mathbb{k}) \neq \emptyset] \right]. \end{aligned}$$

Предлагается сопоставить со школьной формулировкой!

1.2.4. Об истории. К сожалению, у нас нет времени обсуждать богатую историю квадратных уравнений в различных древних цивилизациях. Помимо [Варден1959], можно порекомендовать интересный недавний препринт [Hungerbuhler2019].

1.3. Кубические уравнения

1.3.0. Итальянское Возрождение. Литература здесь необъятна, и трудно выбрать какой-то один источник для ссылок. Думая об этом важнейшем для мировой культуры периоде, можно постараться понять, почему

- именно в Италии возникла и укрепилась дерзкая мысль о том, что *древних можно превзойти*;
- Возрождение в математике началось позже, чем в живописи, архитектуре, литературе и т.д. – за исключением обогнавшего своё время Леонардо Пизанского (Фибоначчи).

1.3.1. Канонический вид. Отправляясь от нашего общего вида

$$c_0x^3 + c_1x^2 + c_2x + c_0 = 0, \tag{1.3.1a}$$

порассуждаем о $c_0 \neq 0$ и перейдем к виду

$$x^3 + b_1x^2 + b_2x + b_0 = 0 \tag{1.3.1b}$$

и применим замену

$$x \leftarrow x + \frac{b_1}{3}. \tag{1.3.1c}$$

Придем к виду

$$\boxed{x^3 + px + q = 0}, \tag{1.3.1d}$$

который и будем называть *каноническим*.

Но преобразование (1.3.1c) законно **ЛИШЬ В ПРЕДПОЛОЖЕНИИ**

$$\boxed{\text{char}(\mathbb{k}) \neq 3}, \tag{1.3.1e}$$

которое мы и **принимаем**. Более того, для дальнейших действий мы сохраняем уже принятое предположение и на весь оставшийся курс принимаем соглашение

$$\boxed{\text{char}(\mathbb{k}) \notin \{2, 3\}} \quad (1.3.1e').$$

Исследование кубических уравнений в этих характеристиках – весьма специальная проблема, и исчерпывающих ссылок нам найти не удалось.

1.3.2. Дискриминант. Чтобы вычислить дискриминант многочлена

$$f := x^3 + px + q$$

по данному выше определению, вводим

$$f_1 := \frac{f'}{2} = x^2 + \frac{p}{3} \quad (1.3.2a)$$

Предложение. *Имеет место равенство*

$$\text{discrim}(x^3 + px + q) = 4 \boxed{\left(\frac{p^3}{27} + \frac{q^2}{4}\right)} \quad (1.3.2b)$$

Доказательство. Имеем

$$\begin{aligned} \text{discrim}(f) &= -f\left(\sqrt{-\frac{p}{3}}\right)f\left(-\sqrt{-\frac{p}{3}}\right) = \\ &= -\left(\sqrt{-\frac{p}{3}}^3 + p\sqrt{-\frac{p}{3}} + q\right)\left(\sqrt{-\frac{p}{3}}^3 + p\sqrt{-\frac{p}{3}} + q\right) = \\ &= \left(q + \sqrt{-\frac{p}{3}}\left(1 + \frac{1}{3}\right)p\right)\left(q + \sqrt{-\frac{p}{3}}\left(1 + \frac{1}{3}\right)p\right) = \\ &= q^2 + \frac{4}{27}p^3 = 4 \boxed{\left(\frac{p^3}{27} + \frac{q^2}{4}\right)}. \blacksquare \end{aligned}$$

Обозначение. (Дискриминант многочлена определён с точностью до умножения на квадрат элемента основного поля). Будем иногда пользоваться сокращением

$$\frac{1}{4}\text{discrim}(f) = \boxed{\delta_f := \left(\frac{p^3}{27} + \frac{q^2}{4}\right)} \quad (1.3.2c)$$

В этой формуле знаменатели напоминают о принятых ограничениях на характеристику основного поля. Возможно, она лучше запоминается в виде

$$\delta_f = \left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2.$$

1.3.4. Итальянское решение. Приведём его формально.

$$x =: u + v. \quad (1.3.4d)$$

Преобразуем уравнение $0 = f_{\mathbb{k}}(x)$:

$$0 = (u + v)^3 + p(u + v) + q =$$

$$= u^3 + v^3 + 3(u + v) \boxed{(3uv + p)} + q \quad (1.3.4e)$$

”Переменные” u и v были введены произвольно; подчиним их соотношению

$$3uv + p = 0. \quad (1.3.4f)$$

Уравнение преобразуется в систему

$$\begin{cases} uv = -\frac{p}{3} \\ u^3 + v^3 = -q \end{cases} \quad (1.3.4g)$$

Возводя первое уравнение в куб (при $\mathbb{k} = \mathbb{R}$ эта операция обратима!), придём к системе

$$\begin{cases} u^3 + v^3 = -q \\ u^3 v^3 = -\frac{p^3}{27} \end{cases} \quad (1.3.4h)$$

Решение таких систем было под силу итальянским алгебраистам XVI века. Тарталья отразил всю процедуру звучными стихами:

Quando chel cubo con le cose appresso
 Se acquaglia á qualche numero discreto
 Trouan duo altri differenti in esso
 Dapoi terrai questo per consueto
 Che'llor productto sempre sia equale
 Alterzo cubo delle cose neto,
 El residuo poi suo generale
 Delli lor lati cubi ben sottrati
 Varra la tua cosa principale.
 In el secondo de cotestiatti
 Quando chel cubo restasse lui solo
 Tu osseruarai quest'altri contratti,
 Del numer farai due tal part''a uolo
 Che luna in l'altra si produca schietto
 El terzo cubo delle cose in stolo
 Delle qual poi, per communprecetto
 Torrai li lati cubi insieme gionti
 Et cotal somma sara il tuo concetto.
 El terzo poi de questi nostri conti
 Se solue col secondo se ben guardi
 Che per natura son quasi congionti.
 Questi trouai, non con passi tardi
 Nel mille cinquecent'e, quatroe trenta
 Con fondamenti ben sald'e gagliardi
 Nella citta dal marintorno centa.

В Интернете можно найти английский подстрочник:

When the cube and the things together
 Are equal to some discrete number,
 Find two other numbers differing in this one.
 Then you will keep this as a habit
 That their product should always be equal
 Exactly to the cube of a third of the things.
 The remainder then as a general rule
 Of their cube roots subtracted
 Will be equal to your principal thing.
 In the second of these acts,
 When the cube remains alone
 You will observe these other agreements:
 You will at once divide the number into two parts
 So that the one times the other produces clearly
 The cube of a third of the things exactly.
 Then of these two parts, as a habitual rule,
 You will take the cube roots added together,
 And this sum will be your thought.
 The third of these calculations of ours
 Is solved with the second if you take good care,
 As in their nature they are almost matched.
 These things I found, and not with sluggish steps,
 In the year one thousand five hundred, four and thirty
 With foundations strong and sturdy
 In the city girdled by the sea

Вместе с разъяснением: Тарталья рассматривает чуть-чуть другое уравнение,

$$x^3 + ax = b,$$

и ищет решение в виде $c = \sqrt[3]{u} - \sqrt[3]{v}$.

Рискую предложить вольный прозаический перевод на русский:

Пусть куб неизвестной вещи, сложенный с произведением неизвестной вещи на заданное число и ещё с одним заданным числом, обращается в ничто.

Представьте неизвестную вещь в виде суммы двух неизвестных вещей. Подберите произведение двух неизвестных так, чтобы от исходного уравнения осталось только значение сумм их кубов. Тогда уравнение сведётся к нахождению кубов двух неизвестных вещей по их сумме и произведению, а находить эти кубы вас учили в школе.

От лета две тысячи двадцать пятого, составлено согласно алгебре этих времён там, где река Дубна впадает в Волгу.

Вернувшись в XXI, составим квадратное уравнение, корни которого – кубы ”неизвестных вещей”.

$$\boxed{(\lambda - u^3)(\lambda - v^3) \equiv_{\mathbb{K}[\lambda]} \lambda^2 + q\lambda - \frac{p^3}{27}} \quad (1.3.4i)$$

Приходим к *формуле Кардано*:

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}. \quad (1.3.2j)$$

В каком-то смысле это – ответ, аналогичный общеизвестной формуле корней квадратного уравнения.

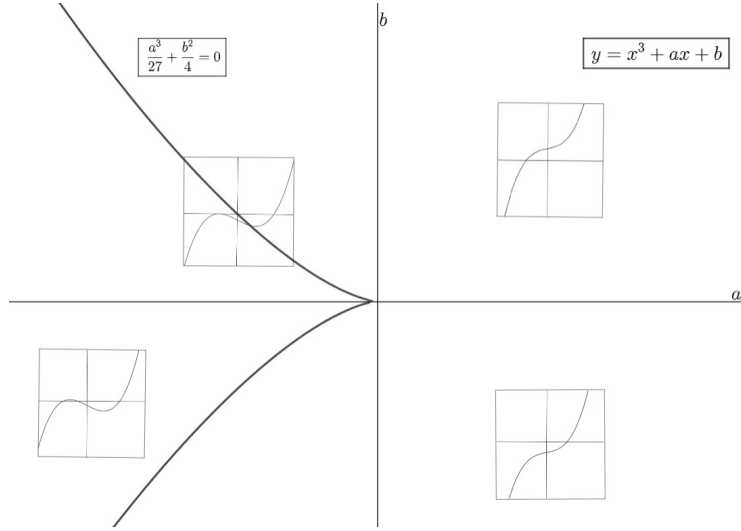
По знаками кубических корней в формуле (1.3.2j) узнаем дискриминант и, пользуясь (1.3.2c), перепишем формулу Кардано в виде

$$\boxed{x = \sqrt[3]{-\frac{q}{2} + \sqrt{\delta_f}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\delta_f}}} \quad (1.3.2k)$$

В таком виде она лучше поддаётся анализу; над полем действительных чисел, как и в случае квадратного уравнения, *знак дискриминанта* играет основную роль.

Рекомендуется решить задачи **1.11** и **1.12**.

1.3.4. Анализ над $\mathbb{R}$. Ограничимся графическим разбором возможных случаев.¹⁵



NB (утро 23 июля 2025). Здесь будет произведена замена $(a, b) \leftarrow (p, q)$.

¹⁵Я признателен П. Киму, создавшему эту картинку.

1.3.6. Решение ВСЕХ кубических уравнений. Введём ещё одно нестандартное определение

$$\mathbb{k}_1[z] := \{z^n + c_1 z^{n-1} + \dots + c_n\}.$$

Главное действующее лицо теории полиномиальных уравнений – разветвлённое накрытие¹⁶

$$\mathbb{k}^{n \times} \xrightarrow{/S_n} \mathbb{k}_1[z]_n : (z_1, \dots, z_n) \mapsto \prod_{i=1}^n (z - z_i),$$

забывающее порядок корней многочлена. Под решением *семейства* уравнений степени n понимается локальное обращение этого накрытия.

В случае $n = 3$ группа S_n разрешима, и накрытие $/S_3$ раскладывается в композицию

$$\begin{array}{ccc} & \mathbb{k}^{3 \times} & \\ \swarrow /A_3 & \downarrow /S_3 & \\ \mathbb{k}^{3 \times} / A_3 & & \\ \searrow /C_2 & \downarrow & \\ & \mathbb{k}_1[z]_3 \cong \text{Sym}^3(\mathbb{k}) & \end{array}$$

Слушателям предоставляется выписывание соответствующей башни циклических расширений полей, обеспечивающих разрешимость кубических уравнений в радикалах.

1.4. Сведение уравнений степени 4 к кубическим

1.4.0. Неразличимость корней. Мы приходим к пониманию того, что главное действующее лицо в теории полиномиальных уравнений – группа перестановок корней. Случай степени 4 – последний, когда она разрешима, и можно это использовать для решения уравнений 4-й степени в радикалах.

1.4.1. Канонический вид. Как и выше, мы сводим его к

$$x^4 + ax^2 + bx + c = 0.$$

Ограничений на характеристику не добавляется.

1.4.2. Гениальная идея. Эпиморфизм

$$S_4 \twoheadrightarrow S_3$$

реализуется заменой переменных

$$\begin{cases} y_1 := x_1 x_2 + x_3 x_4 \\ y_2 := x_1 x_3 + x_2 x_4 \\ y_3 := x_1 x_4 + x_2 x_3 \end{cases}.$$

¹⁶Вводим нестандартное определение декартовой степени поля $\mathbb{k}^{n \times} := \underbrace{\mathbb{k} \times \dots \times \mathbb{k}}_n$, чтобы отличить его от *множества степеней* $\mathbb{k}^{n \cdot} := \{\alpha^n \mid \alpha \in \mathbb{k}\}$.

Возникает кубическое уравнение

$$0 = (\lambda - y_1)(\lambda - y_2)(\lambda - y_3) \in \mathbb{k}[a, b, c][\lambda],$$

которое мы уже умеем решать в радикалах.

Неизвестные $\{x_i\}$ восстанавливаются по $\{y_i\}$ простыми алгебраическими операциями.

СПИСОК ЛИТЕРАТУРЫ

- [Argand1806] Jean-Robert Argand, *Essai sur une manière de représenter des quantités imaginaires dans les constructions géométriques*. Annales de mathématiques pures et appliquées, tome 4 (1813-1814), p. 133-147.
- [Ax1968] James Ax, *The Elementary Theory of Finite Fields*. Annals of Mathematics, Second Series, Vol. 88, No. 2 (Sep., 1968), pp. 239-271.
- [Baillet1892] Jules Baillet, *Le papyrus mathématique d'Akhmîm*. Volume 9 of Mémoires publiés par les membres de la Mission archéologique française au Caire Publisher Ernest Leroux, 1892.
- [CheGaVaW1998] Jørgen Cherly, Luis Gallardo, Leonid Vaserstein, and Ethel Wheland, *Solving quadratic equations over polynomial rings of characteristic two*. Publ. Mat., 42(1):131-142, 1998.
- [DirichletDedekind1871] Gustav Lejeune Dirichlet, Richard Dedekind (ed.), *Vorlesungen über Zahlentheorie*. Translation: Lectures on Number Theory, American Mathematical Society, 1999.
- [Friberg1978] J. Friberg, *The third millenium roots of Babylonian mathematics. I. A method for the decipherment, through mathematical and metrological analysis, of proto-Sumerian and proto-Elamite semipictographic inscriptions*. Braunschweig, Germany: Friedrich Vieweg und Sohn.
- [Gauss1799] C. F. Gauss, *Demonstratio nova theorematis omnem functionem algebraicam rationalem integram unius variabilis in factores reales primi vel secundi gradus resolvi posse*. Диссертация.
- [Hungerbuhler2019] Norbert Hungerbühler, *An alternative quadratic formula*. arXiv, 2019.
- [Moore1893] E. Hastings Moore, *A doubly-infinite system of simple groups*. Bulletin of the American Mathematical Society, 3 (3): 73-78.
- [Record1557] Robert Recorde, *The Whetstone¹⁷ of Witte¹⁸*. Department of Mathematics, University of Göteborg No. 9 (Göteborg, 1978).
- [АтьяМакдональд1972] М. Атья, И. Макдональд, *Введение в коммутативную алгебру*. Москва, "Мир" 1972.
- [Варден1959] Б.Л. ван дер Варден, *Пробуждающаяся наука*. Москва, Государственное Издательство физико-математической литературы, 1959.
- [Чистяков1962] В.Д. Чистяков, *Сборник старинных задач по элементарной математике с историческими экскурсами и подробными решениями*. Минск, Изд.-во Мин. Обр. БССР, 1962.
- [Шафаревич1954] И.Р. Шафаревич, *О решении уравнений высших степеней (метод Штурма)*. — М.: Гостехиздат, 1954.

¹⁷Гочилка.

¹⁸Чего-то вроде изворотливого ума.