# Министерство общего и профессионального образования РФ

## Кубанский государственный технологический университет

**Кафедра общей математики**

ОБ АЛГЕБРАИЧЕСКИХ УРАВНЕНИЯХ ВЫСШИХ СТЕПЕНЕЙ

Белокопытов А.Ю., Морозов В.О.

группа 20-КТ-61

**Краснодар, 2001**

Уравнения! Можно утверждать наверняка, что не найдется ни одного человека, который бы не был знаком с ними. Дети сызмала начинают решать «задачи с иксом». Дальше – больше. Правда, для многих знакомство с уравнениями и заканчивается школьными делами. Известный немецкий математик Курант писал: «На протяжении двух с лишним тысячелетий обладание некоторыми, не слишком поверхностными, знаниями в области математики входило необходимой составной частью в интеллектуальный инвентарь каждого образованного человека». И среди этих знаний было умение решать уравнения.

Уже в древности люди осознали, как важно научиться решать алгебраические уравнения вида

*a0xn + a1xn – 1 + … + an = 0*

– ведь к ним сводятся очень многие и очень разнообразные вопросы практики и естествознания (конечно, здесь можно сразу предполагать, что *а0 ≠ 0*, так как иначе степень уравнения на самом деле не *n*, а меньше). Многим, разумеется, приходила в голову заманчивая мысль найти для любой степени *n* формулы, которые выражали бы корни уравнения через его коэффициенты, т.е., решали бы уравнение в радикалах. Однако «мрачное средневековье» оказалось как нельзя более мрачным и в отношении обсуждаемой задачи – в течение целых семи столетий требуемых формул никто не нашел! Только в XVI веке итальянским математикам удалось продвинуться дальше – найти формулы для *n = 3* и *4*. История их открытий и даже авторство найденных формул достаточно темны по сей день, и мы не будем здесь выяснять сложные отношения между Ферро, Кардано, Тартальей и Феррари, а изложим лучше математическую суть дела.

Рассмотрим сначала уравнение

*a0x3 + a1x2 + a2x + a3 = 0.*

Легко проверить, что если мы положим , где *y* – новое неизвестное, то дело сведется к решению уравнения



*y3 + py + q = 0,*

где *p, q* – новые коэффициенты. Счастливая догадка итальянцев состояла в том, чтобы искать *y* в виде суммы *y = u + v,* где *u, v* – **д в а** новых неизвестных. Для них наше уравнение перепишется – после небольшой перегруппировки слагаемых – так:

*u3 + v3 + (3uv + p)(u + v) + q = 0.*

Так как неизвестных теперь два, на них можно наложить еще какое-нибудь условие – лучше всего

*3uv + p = 0,*

тогда исходное уравнение примет совсем простой вид

*u3 + v3 + q = 0.*

Это означает, что сумма кубов *u3, v3* должна равняться – *q,* а их произведение . Следовательно, сами *u3, v3* должны быть конями квадратного уравнения



*t2 + qt* – p3/27 = 0,

а для него формула уже известна. В итоге получается формула



причем из девяти пар значений входящих в нее кубических радикалов надо брать только пары, дающие в произведении –p/3, как вытекает из нашего рассуждения. Исторически за этой формулой закрепилось название формулы Кардано, хотя вопрос о ее авторстве так до конца и не выяснен.

Для *n = 4* формулу открыл Феррари, она выглядит сложнее, но тоже использует только четыре арифметических действия и извлечение радикалов. Вот набросок вывода формулы Феррари. Прежде всего, подобно предыдущему, положим , тогда дело сведется к решению уравнения вида



*y4 + py2 + qy + r = 0.*

Дополнив *y4* до *(y2 + z)2*, т.е. прибавив и вычтя в левой части *2zy2 + z2*, где *z* – вспомогательное неизвестное, получим

*(y2 + z)2 – [(2z – p) y2 – qy + (z2 – r)] = 0.*

Подберем теперь *z* так, чтобы квадратный трехчлен в квадратных скобках оказался полным квадратом; для этого нужно, чтобы его дискриминант равнялся нулю, т.е. чтобы было

q2 – 4(2z – p) (z2 – r) = 0.

Можем ли мы решить это уравнение относительно *z*? Да, можем, так как оно кубическое. Пусть *z0* – какой-нибудь его корень (даваемый формулой Кардано) тогда исходное уравнение перепишется в виде

[(y2 + z0) – (…)] \* [(y2 + z0) + (…)] = 0,

где многоточия означают многочлен не более чем первой степени от *y*, оба раза один и тот же.

;



;



При этом знаки перед радикалами выбирают так, чтобы выполнялось равенство .



В 1770-71 гг. знаменитый французский математик Лагранж (1736-1819) публикует в Мемуарах Берлинской Академии свой мемуар «Мысли над решением алгебраических уравнений», в котором делает критический пересмотр всех решений уравнений 3-й и 4-й степеней, данных его предшественниками, и замечает, что все они в сущности основаны на следующем принципе. Пусть *x1, x2, …, xn* будут корни заданного уравнения, и пусть *ϕ (x1, x2, …, xn)* будет их рациональная функция, принимающая при всевозможных *n!* перестановках между корнями *v* значений. Тогда эта функция удовлетворяет уравнению степени *v* с рациональными коэффициентами. Согласно точке зрения Лагранжа, задача заключается в том, чтобы подобрать функцию *ϕ (x1, x2, …, xn)* таким образом, чтобы *v* было меньше *n*. И вот оказалось, что при *п>4* невозможно.

Эти исследования Лагранжа дали для последующих алгебраистов весьма удобный аппарат. Кроме того, они указали путь, по которому следовало искать доказательства невозможности общего решения уравнений в радикалах.

Дальнейшим этапом в выяснении проблемы решения уравнений в радикалах послужили работы Руффини (P. Ruffini, 1765-1822) и Абеля (N.-H. Abel, 1802 - 1829). Руффини (1799) предложил доказательство неразрешимости в радикалах уравнений 5-й степени, коэффициенты которого являются независимыми переменными. Однако его доказательство окончилось неудачей.

Нужен был принципиально новый подход. На этот раз он не заставил себя долго ждать – уже в 1824 году молодой (и в возрасте 27 лет умерший) норвежский математик Нильс Генрик Абель, опираясь на идеи Лагранжа, связанные с перестановками корней уравнения, доказал, что требуемых формул, которые решали бы в радикалах уравнение общего вида, при *n≥5* действительно не существует. Теорема Абеля дала отрицательный ответ только для уравнений общего вида, т.е. с буквенными коэффициентами *a0, a1, …, an*, но, разумеется, многие конкретные уравнения сколь угодно высокой степени вполне могут решаться в радикалах (пример: уравнение *x90 + 5x45 + 7 = 0).* Поэтому сразу же встал вопрос о полном решении задачи – нахождении *критерия разрешимости уравнений в радикалах,* т.е. необходимого и достаточного условия, которое по коэффициентам *a0, a1, …, an* любого заданного уравнения позволяло бы судить, решается уравнение в радикалах или нет.

Вопрос о разрешимости уравнений в радикалах был окончательно разобран, во всяком случае принципиально, в работах Галуа (Evariste Galois, 1811-1832). Личность Галуа представляет собой совершенно исключительное в истории науки явление. Жизнь Галуа, умершего всего на 21 году, протекала крайне бурно. Дважды провалившись на вступительных экзаменах в знаменитую Политехническую школу, Галуа поступил в Подготовительную школу (преобразованную из Высшей нормальной школы во время реакционного правления Карла IX), откуда вскоре после июльского переворота был уволен за печатное выступление против школы. После этого Галуа открыл «публичный курс» по алгебре, но политическая жизнь страны быстро вовлекла его в свой водоворот. Имея репутацию ярого республиканца и активного врага Луи-Филиппа, он два раза сидел в тюрьме за политические выступления и в мае 1832 года был убит на дуэли, причины которой остаются до сих пор загадочными.

За свою короткую жизнь Галуа успел создать теорию, которая до сих пор стоит в фокусе математической мысли. Рассматривая численные уравнения, он установил понятие их *группы*, т.е. совокупности таких подстановок между их корнями, которые не нарушают рациональных соотношений между ними. Эта группа определяет для каждого уравнения алгебраическую структура его корней. В частности, уравнение разрешимо в радикалах тогда и только тогда, если его группа принадлежит к числу так называемых *разрешимых групп*. Таким образом вопрос о разрешимости каждого данного уравнения в радикалах может быть решен при помощи конечного числа действий.

Обратимся теперь к исходному объекту исследования – уравнению

*a0xn + a1xn – 1 + … + an = 0,*

где *a0, a1, …, an* - заданные числа. Еще Гаусс в конце XVIII века доказал «основную теорему алгебры», гласящую, что при любых *a0, a1, …, an* данное уравнение имеет в поле комплексных чисел *п* корней, точнее, стоящий в его левой части многочлен *f(x)* может быть разложен на линейные множители

*f(x) = a0(x - α1)…(x - αn),*

где *α1 … αn* – некоторые комплексные числа (называемые корнями уравнения). Задача состоит в том, чтобы узнать, существуют ли формулы, выражающие корни *α1, …, αn* через коэффициенты *a0, a1, …, an* с помощью четырех арифметических действий и извлечения радикалов? Прежде всего, сразу можно считать, что все числа *α1, …, αn* различны, иначе мы поделили бы многочлен *f* на наибольший общий делитель этого *f*  и его производной *f’*, что дало бы нам новый многочлен с теми же самыми корнями, но уже без повторений.

Ключевой идеей, поистине прозрением Галуа, явилась мысль связать с каждым алгебраическим уравнением группу всех автоморфизмов его «поля корней» **Q**(*α1, …, αn*), которые оставляют неподвижным «поле коэффициентов» **Q(***a0, a1, …, an*). Понятно, что это действительно группа, так как если ϕ, ψ - два таких автоморфизма, то автоморфизмы ϕψ и ϕ -1 тоже оставляют числа *a0, a1, …, an* неподвижными.

Как действует любой такой автоморфизм ϕ на корни нашего уравнения? Если α - корень, т.е.

*a0αn + a1αn – 1 + … + an = 0,*

то, применив ϕ к обеим частям, получим

*a0(αϕ)n + a1(αϕ)n – 1 + … + an = 0,*

т.е. *αϕ* – *корень того же уравнения!* Другими словами, автоморфизм ϕ просто переставляет корни *α1, …, αn* между собой, определяя тем самым некоторую перестановку

*α1 … αn*

*α1 … αin*

легко сообразить, что произведению автоморфизмов будет отвечать произведение соответствующих перестановок, так что все получающиеся при этом перестанвоки сами составляют группу. Она называется *группой симметрий* или *группой Галуа* уравнения *f*=0 и обозначается Gal(*f*). Понятно, что Gal(*f*) – подгруппа группы Sn всех перестановок *п* символов. Оказывается, свойствами группы Галуа и определяется ответ на вопрос о разрешимости данного уравнения в радикалах.

Вот этот знаменитый

**Критерий Галуа.** *Уравнение f=0 тогда и только тогда разрешимо в радикалах, когда его группа* Gal(*f*) *обладает полициклической матрёшкой.*

Прежде всего, может возникнуть недоумение: «Как можно манипулировать перестановками корней, когда сами корни неизвестны? А если корни будут найдены, то никакие перестановки уже не понадобятся. В чем здесь достижение?»

Оказывается, что группу Gal(*f*) действительно можно вычислить, *не зная* корней уравнения *f* = 0, а пользуясь лишь, так сказать, соображениями симметрии.

Рассмотрим уравнение

x4 – x2 + 1 = 0.

Конечно, без всякого критерия Галуа видно, что оно биквадратное и легко решается в радикалах, но наша цель сейчас в другом продемонстрировать на этом простеньком примере, как, не пользуясь знанием корней уравнения, найти его группу Галуа. Сейчас мы убедимся, что это вполне возможно. Прежде всего заметим, что многочлен

*f = x4 – x2 + 1,*

стоящий в левой части, не разлагается на множители меньшей степени с рациональными коэффициентами. Для выяснения этого имеется несложный общей прием, на котором мы не будем останавливаться.

Пусть α какой-нибудь корень нашего уравнения. Понятно, что тогда -α, 1/α, -1/α - тоже корни, причем все они попарно различны. Занумеруем их, пусть

α1 = α, α2 = - α, α3 = 1/α, α4 = -1/α

Очевидно,

**Q (**α1, α2, α3, α4 )= **Q** (α)

Какие перестановки войдут в группу Gal(*f*)? Разумеется, далеко не все 24 перестановки четырех символов. В самом деле, если при каком-то автоморфизме поля **Q** (α) число α переходит в α1, т.е. остается на месте, то легко понять, числа α2, α3, α4 тоже останутся на месте. Другими словами, получится единичная перестановка *е*. Далее, если α перейдет в α2, то по той же причине получится перестановка

α1  α2 α3 α4

*а*=

α2  α1 α4 α3

Наконец, при α α3 и α α3 получатся перестановки

α1  α2 α3 α4

*b*=

α3 α4 α1 α2

α1  α2 α3 α4

*c*=

α4 α3 α2  α1

Так как все возможности для образа корня α мы перебрали, никакие другие перестановки появиться не могут.

С другой стороны, можно убедиться, что все четыре перестановки *е, а, b, с* действительно возникают из автоморфизмов поля **Q** (α), так что они и составляют группу Gal(*f*) нашего уравнения. В самом деле, рассмотрим, например, подстановку *а* (для подстановок *b, c* рассуждение абсолютно аналогично). Если, как мы собираемся доказать, автоморфизм поля **Q** (α), соответствующий подстановке *a*, существует, то он обязан действовать так:

,



где *g, h* произвольные многочлены с рациональными коэффициентами, причем *h(α)* ≠ 0 (учтите, что автоморфизм обязан переводить сумму в сумму и произведение в произведение). Ясно, что это формулу и следует взять за определение искомого автоморфизма. Тонкость состоит в том, что число может быть записано многими разными способами:



и нужно убедиться, что при замене α на α2 все эти равенства сохранятся. Иначе говоря, если *p = gh1 – g1h* и *p(α) = 0*, то и *p(α2) = 0*. Чтобы доказать это, поделим *р* на исходный многочлен *f* с остатком:

p(x) = f(x)q(x) + r(x);

остаток *r(x)* – это многочлен степени не выше третьей. Так как *p(α) = f(α) = 0*, то и *r(α) = 0*. Предположим на время, что *r(x) ≠ 0*. По школьной теореме Безу многочлены *f(x), r(x)* имеют общий делитель *x - α;* пусть *d(x)* – их наибольший общий делитель. Очевидно, *d(x)* имеет степень не ниже первой и не выше третьей и делит многочлен *f(x)*, а это противоречит неразложимости на множители. Полученное противоречие означает, что *r(x)=0*, т.е.

p(x) = f(x)q(x).

Положив здесь *x = α2*, получаем требуемое равенство *p(α2) = 0* (а вместе с ним и два других равенства *p(α3) = p(α4) = 0).* Точно так же из *h(α)≠ 0* следует *h(α2)≠ 0* и т.д. Итак,

Gal(f) = {e, a, b, c}.

Как видите, группа Галуа найдена, и значения корней при этом не понадобились!

В заключение несколько слов об общем уравнении

*a0xn + a1xn – 1 + … + an = 0,*

где *a0, a1, …, an* - буквенные коэффициенты. Можно показать (опять-таки не пользуясь значениями корней), что группой Галуа этого уравнения будет группа всех перестановок Sn. обладает ли она полициклической матрешкой подгрупп? Если *п*≤4, то да. Если же *п≥*5, то группа Sn  не имеет полициклических матрёшек, - это уже довольно трудная теорема, также доказанная Эваристом Галуа. Следовательно, общее уравнение степени *п≥*5 неразрешимо в радикалах.

Заканчивая этот краткий очерк идей Галуа, скажем, что шестьдесят страниц, написанных Эваристом Галуа накануне роковой дуэли явилось одним из истоков современной теории групп – основного и наиболее развитого раздела алгебры, изучающего в общем виде глубокую закономерность реального мира – симметрию.

Преобразование ϕ поля К называется его **автоморфизмом**, если оно сумму переводит в сумму, а произведение в произведение, т.е.

(а + в) ϕ = аϕ + вϕ, (АВ) ϕ = аϕвϕ

для любых *а,в* из К; здесь *аϕ* обозначает образ элемента *а* и т.д.

**Поле** – это множество К с двумя двуместными операциями, называемыми сложением и умножением, причем отностительно сложения оно является коммутативной группой, относительно умножения его элементы, отличные от нулевого, тоже составляют коммутативную группу и, наконец, в К выполняется обычное правило для раскрытия скобок *(а + в)с=ас + вс* для любых *а, в, с* из К.

Рассмотрим последовательность вложенных друг в друга подгрупп; всякая такая последовательность

М: G=H0 ≥ H1 ≥ … ≥Hm=E,

содержащая G и E, называется **матрёшкой** подгрупп группы G. Допустим теперь, что в каждом члене Hi данной матрёшки М выделено по элементу аi, причем для каждого элемента х из Нi + 1 «сопряженный элемент» а­i –1 xai снова лежит в Нi + 1 и каждый элемент у из Hi записывается в виде произведения некоторой степени аim на некоторый элемент из Нi + 1; тогда матрешка М называется **полициклической.**

**Группой** называется любое множество G, на котором задана двуместная алгебраическая операция, т.е. правило, сопоставляющее каждым двум элементам из G определенный третий элемент из G, причем выполняются следующие аксиомы:

а) операция *ассоциативна*, т.е. *(аb)c=a(bc)*

б) G содержит *единичный элемент*

в) для всякого а из G существует обратный элемент.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

1. В. Чеботарев, «Основы теории Галуа» Москва, 1934.
2. А. Дальма, « Эварист Галуа. Революционер и математик» Москва, 1984.
3. Ван дер Варден, «Алгебра»
4. И.Н. Бронштейн, К.А. Семендяев, «Справочник по математике для инженеров и учащихся ВТУЗов» Москва, 1986.