ГЛАВА

ТЕОРИЯ ГАЛУА И ТФКП

2. Разрешимость алгебраических уравнений в радикалах

Решать уравнения легче, чем доказывать их неразрешимость. Согласно теории Галуа алгебраическое уравнение решается в радикалах, если и только если его группа Галуа разрешима. Конструкция решений алгебраических уравнений с разрешимой группой Галуа фактически не использует основных теорем теории Галуа и основана на простой линейной алгебре, а именно, на теории представлений конечных коммутативных групп. Здесь мы напомним соответствующую линейную алгебру, алгоритм выражения в радикалах элементов алгебры через инварианты относительно действия разрешимой группы автоморфизмов и восходящий к Лагранжу анализ решений в радикалах уравнений второй, третьей и четвертой степени.

2.1. Комплексные представления конечных коммутативных групп. Конструкция явного решения уравнений в радикалах основана на тех или иных вариантах следующей классической теореме из линейной алгебры.

Теорема. *Матрицы всех операторов конечной коммутативной группы линейных преобразований конечномерного комплексного векторного пространства в некотором базисе приводятся к диагональному виду.*

Лемма 1. *Пусть A — линейное преобразование конечномерного векторного пространства над полем K, и пусть все собственные числа A лежат в поле K. Пусть $A \neq \lambda I$, где I — тождественное преобразование. Тогда все линейные преобразования, коммутирующие с преобразованием A, имеют общее нетривиальное инвариантное подпространство.*

Доказательство. В качестве общего инвариантного подпространства достаточно взять собственное подпространство L_λ преобразования A с любым собственным числом λ этого преобразования. Действительно, если вектор $x \in L_\lambda$ и преобразование B коммутирует с A, то

$$ABx = BAx = \lambda Bx,$$

Поэтому вектор Bx тоже принадлежит пространству L_λ.

Лемма 2. *Комплексное представление конечной группы вполне приводимо, т.е. для всякого инвариантного подпространства най дется дополнительное*

Typeset by $\mathcal{AMS}$-TEX

инвариантное подпространство такое, что прямая сумма этих инвариантных подпространств совпадает со всем пространством.

Доказательство. В комплексном векторном пространстве существует эрмитово скалярное произведение, инвариантное относительно действия конечной группы G. Действительно, такое скалярное произведение можно построить следующим образом. Пусть $\langle x, y\rangle$ — любое эрмитово скалярное произведение в пространстве. Тогда новое скалярсное произведение, определенное формулой

$$[x, y] = \sum_{A\in G} \langle Ax, Ay\rangle,$$

будет невырожденно и инвариантно относительно группы G. В качестве дополнительного пространства достаточно взять ортогональное дополнение инвариантного подпространства относительно этого скалярного произведения.

Теорема непосредственно вытекает из лемм 1,2.

2.2.Резольвенты Лагранжа.

Для дальнейшего нам нужно уметь представлять всякий вектор x в виде линейной комбинации общих собственных векторов относительно действия конечной коммутативной группы G. Это можно сделать явным образом, даже не использую приведенной выше теоремы. Приведем эту явную явную конструкцию, восходящую к Лагранжу. Начнем со случая циклической группы порядка n.

Пусть L — векторное пространство над полемнулевой характеристики, содержащим все корни n-й степени из единицы, и пусть A — образующая циклической группы G порядка n, действующая на пространстве L. Другими словами, пусть $A\colon L \to L$ — оператор, удовлетворяющий тождеству $A^n = I$, где I — тождественное преобразование. Для всякого корня ξ n-й степени из единицы, $\xi^n = 1$, определим ξ-ю резольвенту Лагранжа вектора x формулой: $R_\xi(x) = \sum_{0\le k<n} \xi^k A^k(x)$. Мы будем пользоватья следующим очевидным утверждением 1.

Утверждение 1. *При $0 < k < n$ сумма k-х степеней всех корней степени n из единицы равна нулю. При $k = 0$ эта сумма равна n.*

Утверждение 2. *Для всякого вектора x его резольвента Лагранжа $R_\xi(x)$ либо равна нулю, либо является собственным вектором оператора A с собственным числом ξ^{-1}, при этом вектор x является средним арифметическим всех своих резоьвент Лагранжа.*

Доказательство. 1. $A(R_\xi(x)) = \sum_{0\le k<n} \xi^k A^{k+1}(x) = \xi^{-1} \sum_{0<k\le n} \xi^{k+1} A^{k+1}(x) = \xi^{-1} R_\xi(x)$.

2. $1/n \sum_{\xi^n=1} R_\xi(x) = 1/n \sum_{0\le k<n} \left(\sum_{\xi^n=1} \xi^k\right) A^k(x)$. Воспользовавшись утверждением 1, получаем искомое тождество

$$\frac{1}{n} \sum_{\xi^n=1} R_\xi(x) = x.$$

Конструкция из утверждения 2 обобщается для любых конечных коммутативных групп. *Характером* χ конечной группы G называется ее гомоморфизм $\chi\colon G \to \mathbb{C}^*$, где $\mathbb{C}^*$ — группа комплексных чисел по умножению. Характер можно рассматривать как комплекснозначную функцию на группе.

Лемма. *Среднее арифметическое всех характеров конечной коммутативной группы — это функция на группе, тождественно равная нулю всюду, кроме единицы группы. Значение этой функции в единице группы равно единице.*

Доказательство. Всякая конечная коммутативная группа G является, как известно, прямым произведением циклических групп. Всякий характер прямого произведения групп является произведением характеров этих групп. Сумма значений характера по всем элементам прямого произведения групп равна произведению сумм значений соответствующих характеров по элементам этих групп. Характер циклической группы из n элементов с образующей a сопоставляет элементу a^k число ξ^k, где ξ — корень n-й степени из единицы. Поэтому лемма сводится к утверждению 1.

Пусть конечная коммутативная группа порядка n действует линейными преобразованиями на векторном пространстве L над полем нулевой характеристики, содержащем все корни n-й степени из единицы. Для всякого характера χ определим χ-ю резольвенту Лагранжа вектора x формулой: $R_\chi(x) = \sum_{g\in G} \chi(g)g(x)$.

Утверждение 3. *Для всякого вектора x его резольвента Лагранжа $R_\chi(x)$ либо равна нулю, либо является собственным вектором для всякого оператора A с собственным числом $\chi^{-1}(A)$. Вектор x является средним арифметическим всех своих резоьвент Лагранжа.*

Доказательство. 1) $AR_\chi(x) = A\sum_{g\in G} \chi(g)g(x) = \sum_{g\in G} \chi(g)Ag(x) = \chi^{-1}(A)\sum_{g\in G} \chi(Agg)Ag(x) = \chi^{-1}(A)R_\chi(x)$;

2) $\dfrac{1}{|G|}\sum_{\chi\in G^*} R_\chi(x) = \dfrac{1}{|G|}\sum_{g\in G}\left(\sum_{\chi\in G^*}\chi(g)\right)g(x) = x.$

2.3. Явное выражение элементов алгебры через инварианты действия разрешимой группы. Пусть группа G действует на множестве X, пусть H — нормальный делитель группы G, и пусть X_0 — подмножество X, состоящее из неподвижных точек относительно действия группы G.

Утверждение 1. *Подмножество X_H множества X, состоящее из неподвижных точек относительно действия нормального делителя H, инвариантно относительно действия группы G. На множестве X_H естественно действует факторгруппа G/H с неподвижным множеством X_0.*

Доказательство. Пусть $g \in G$ и $h \in H$. Тогда элемент $g^{-1}hg$ принадлежит нормальному делителю H. Пусть $x \in X_H$. Тогда $g^{-1}hg(x) = x$, или $h(gx) = g(x)$, что означает, что элемент $g \in X$ неподвижен при действии нормального делителя H. Итак, множество X_H инвариантно относительно действия группы G. При этом действии элементам нормального делителя H соответствуют тождественные преобразования. Поэтому действие группы G на X_H сводится к действию факторгруппы G/H.

Конструкция явных решений алгебраических уравнений, в основном, относится к линейной алгебре. Она очень слабо использует то обстоятельство, что мы имеем дело с полями. Чтобы подчеркнуть это, мы опишем эту конструкцию, взяв вместо поля алгебру V, которая может быть и некоммутативной. В дальнейшем нам даже не понадобится перемножать разные элементы этой алгебры. Мы будем использовать лишь операцию возведения в целую неотрицательную степень k и однородность этой операции относительно умножения на элементы основного поля $(\lambda a)^k = \lambda^k a^k$ при $a \in V$, $\lambda \in K$. Итак, пусть V — алгебра над полем K.

Утверждение 2. *Пусть A — автоморфизм конечного порядка n алгебры V, $A^n = I$, и V_0 — подалгебра инвариантов. Пусть поле нулевой характеристики K содержит все корни степени n из единицы. Тогда каждый элемент x алгебры V представим в виде суммы $x = x_1 + \cdots + x_n$ элеменов $x_i \in V$ таких, что $x_i^n \in V_0$.*

Доказательство. Рассмотрим конечномерное линейное пространство в алгебре V, натянутое на орбиту $x, A(x) \ldots, A^{n-1}(x)$ элемента x относительно действия автоморфизма A и его степеней. Согласно утверждению 1 из 2.1 элемент x является средним арифметическим своих резольвент Лагранжа относительно действия оператора A:

$$\frac{1}{n}\sum_{\xi^n=1} R_\xi(x) = x.$$

Достаточно положить $x_k = \dfrac{1}{n} R_{\xi_k}(x)$, где ξ_k, $1, \ldots, n$ — все корни n-й степени из единицы. Действительно, согласно утверждению 1 имеем $A(x_k) = \xi_k x_k$. Поэтому $A(x_k^n) = \xi_k^n x_k = x_k$. То есть элемент x_k^n принадлежит алгебре инвариантов автоморфизма A.

Введем следующее

Определение. Скажем, что элемент x алгебры V получается *операцией извлечения n-й степени из элемента a*, если выполняется равенство $x^n = a$.

Пользуясь этим определением, утверждение 1 можно интерпретировать следующим образом: каждый элемент x в алгебре V представляется в виде сумы корней n-й степени из элементов алгебры инвариантов. Утверждение 1 легко обобщается на случай действия конечной коммутативной группы автоморфизмов.

Утверждение 3. *Пусть G — конечная коммутативная группа порядка n автоморфизмов алгебры V над полем нулевой характеристики K, содержащем все корни степени n из единицы, и пусть V_0 — подалгебра инвариантов. Тогда каждый элемент x алгебры V представим в виде суммы $x = x_1 + \cdots + x_n$ элементов $x_i \in V$ таких, что $x_i^m \in V_0$, где m — наименьшее общее кратное порядков элементов группы G.*

Доказательство утверждения 3 почти дословно повторяет доказательства утверждения 2, нужно только ссылку на утверждение 3 из 2.1, относящуюся к циклической группы, заменить ссылкои на утверждение 3 из того же пункта, относящейся к конечной коммутативной группе.

Теорема. *Пусть G — конечная разрешимая группа порядка n автоморфизмов алгебры V над полем нулевой характеристики K, содержащем все корни n-й степени из единицы, и пусть V_0 — подалгебра инвариантов. Тогда каждый элемент x алгебры V получается из элементов алгебры инвариантов V_0 при помощи извлечения корней и суммирований.*

Доказательство. Пусть $G_0 \supset G_1 \supset \cdots \supset G_m$ — цепочка вложенных подгрупп группы G такая, что

1) группа G_0 совпадает с G, а группа G_m совпадает с единичным элементом e: $G_0 = G$, $G_m = e$;

2) при $i = 1, \ldots, m$ группа G_i является нормальным делителем группы G_{i-1}, причем факторгруппа G_{i-1}/G_i коммутативна.

Такая цепочка подгрупп существует ввиду коммутативности группы G.

Обозначим через $V_0 \subset \cdots \subset V_m = V$ цепочку подалгебр инвариантов алгебры V относительно действия групп $G_0, \ldots, G_m$. Согласно утверждению ??? коммутативная факторгруппа G_{i-1}/G_i естественно действует на алгебры инвариантов V_i, оставляя неподвижной подалгебру инвариантов V_{i_1}. Согласно утверждению 3 каждый элемент алгебры V_i выражается при помощи суммирования и извлечения корней через элементы алгебры V_{i-1}. Последовательно повторяя это рассуждение, мы выразим каждый элемент алгебры V через элементы подалгебры V_0 цепочкой извлечения корней и суммирования.

Замечание. Цепочку нормальных делителей конечной разрешимой группы G можно выбрать таким образом, что все факторгруппы G_i/G_{i-1} буудут не только коммутативными, но циклическими. Поэтому для доказательства теоремы утверждение 3 в полном объеме не нужно, а вполне достаточно использовать утверждение 2.

2.4. Решения в радикалах уравнений второй, третьей и четвертой степени.

В этом пункте мы опишем как уравнения маленькой степени явно решаются в радикалах при помощи теоремы из предыдущего пункта.

Пусть $K[x_1, \ldots, x_n]$ — кольцо многочленов от переменных $x_1, \ldots, x_n$ над полем нулевой характеристики K, содержащим все корни из единицы. Группа $S(n)$ перестановок n элементов действует на этом кольце, переставляя переменные $x_1, \ldots, x_n$ в многочленах из этого лольца. Алгебра инвариантов $K_S[x_1, \ldots, x_n]$ относительно этого действия состоит из симметричных многочленов. Каждый многочлен этой алгебры явным образом представляется в виде многочлена от переменных $\sigma_1, \ldots, \sigma_n$, где $\sigma_1 = x_1 + \cdots + x_n$, $\sigma_2 = \sum_{i<j} x_i x_j$, ... ,$\sigma_n = x_1 \ldots x_n$. При $n = 2, 3, 4$ группа $S(n)$ разрешима. Применяя теорему предыдущего пункта, получаем, что каждый полином от $x_1, \ldots, x_n$ при $n \leq 4$ выражается через основные симметрические многочлены $\sigma_1, \ldots, \sigma_n$ при помощи извлечения корней и суммирования. Рассмотрим алгебраическое уравнение

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0. \tag{3}$$

Согласно формулам Виета коэффициенты этого уравнения с точностью до знака совпадают с основными симметрическими функциями от его корней $x_1, \ldots, x_n$, поэтому описанная в пункте 2.2 теорема при $n = 2, 3, 4$

дает явное выражение корня x_1 уравнения (3) через коэффициенты этого уравнения при помощи суммирования и извлечения корней. Рассмотрим этот алгоритм подробнее для уравнений степени два, три и четыре.

Уравнение второй степени. На кольце многогчленов $K[x_1, x_2]$ действует группа $S(2) = \mathbb{Z}_2$ перестановок двух элементов. Линейное пространство, натянутое на орбиты многочлена x_1 относительно этого действия, будет состоять из линейных многочленов. Относительно этого действия у элемента x_1 есть две резольвентуы Лагранжа:

$$R_1 = x_1 + x_2 = \sigma_1,$$
$$R_2 = x_1 - x_2.$$

Квадрат резольвенты Лагрнжа $x_1 - x_2$ является симметричным многочленом. Имеем

$$(x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = \sigma_1^2 - 4\sigma_2.$$

Получаем представление полинома x_1 через симметрические многочлены $x_1 = 1/2(R_1 + R_2) = \dfrac{\sigma_1 \pm \sqrt{\sigma_1^2 - 4\sigma_2}}{2}$. что и дает обычную форму решения квадратного уравнения.

Уравнение третьей степени. На кольце многогчленов $K[x_1, x_2, x_3]$ действует группа $S(3)$ перестановок трех элементов. Группа $S(3)$ имеет нормальным делителем знакопеременную группу $A(3)$, которая является циклической группой порядка 3, $A(s) = \mathbb{Z}_3$. Факторгруппа $S(3)/A(3)$ является циклической группой порядка 2. Обозначим через $K_A[x_1, x_2, x_3]$ кольцо инвариантов группы $A(3)$ (которое состоит из многочленов не меняющихся при четных перестановках переменных) и через $K_S[x_1, x_2, x_3]$ алгебру симметричных многочленов. Многочлен x_1 имеет три резольвенты Лагранжа относительно действия группы $A(3)$

$$R_1 = x_1 + x_2 + x_3,$$
$$R_2 = x_1 + \xi x_2 + \xi^2 x_3,$$
$$R_3 = x_1 - \xi x_2 - xi^2 x_3,$$

где ξ — кубический корень из единицы, $\xi = \dfrac{-1 + \sqrt{3}i}{2}$.

Имеем $x_1 = 1/3(R_1 + R_2 + R_3)$ и R_1^3, R_2^3, R_3^3 лежат в алгебре $K_A[x_1, x_2, x_3]$. Более того, резольвента $R_1 = \sigma_1$ является симметричным многочленом, а полиномы R_2^3 и R_3^3 переставляются друг с другом при действии группы $\mathbb{Z}_2 = S(3)/A(3)$ на кольце $K_A[x_1, x_2, x_3]$. Повторяя для полиномов R_2^3 и R_3^3 конструкцию, которую мы использовали при решении квадратного уравнения, получим, что эти полиномы выражаются через симметричные полиномы $R_2^3 + R_3^3$ и $(R_2^3 - R_3^3)^2$. Окончательно получаем, что многочлен x_1 выражается через симметричные многочлены R_1, $R_2^3 + R_3^3$ и $(R_2^3 - R_3^3)^2$ при помощи извлечения корней второи и третьей степени и арифметических операций. Для написания явной формулы для решения осталось лишь явно выразить эти симметрические многочлены через основные симметрические многочлены.

Уравнение четвертой степени. Причина разрешимости уравнений четвертой степени заключается в разрешимости группы $S(4)$. Группа $S(4)$ разрешима,

потому что существует гомоморфизм $\pi\colon S(4)\to S(3)$, ядром которого является коммутативная группа $Kl=\mathbb{Z}_2+\mathbb{Z}_2$. Гоморфизм π описывается следующим образом. Существует ровно три способа разбить множество, содержащее четыре элемента, на два подмножества, содержащие по паре элементов. Каждой перестановке множества из четырех элементов соответствует перестановка этих трех разбиений. Описанное соответствие и задает гомоморфизм π. Ядро этого гомоморфизма Kl — нормальный делитель группы $S(4)$, состоящий из четырех перестановок: тождественной перестановки и трех перестановок, каждая из которых является произведением транспозиций двух непересекающихся пар элементов.

На кольце полиномов $K[x_1,x_2,x_3,x_4]$ действует группа $S(4)$. Обозначим через $K_{Kl}[x_1,x_2,x_3,x_4]$ подкольцо инвариантов нормального делителя Kl группы $S(4)$. Итак, на кольце $K[x_1,x_2,x_3,x_4]$ действует коммутативная группа Kl с кольцом инвариантов $K_{Kl}[x_1,x_2,x_3,x_4]$. На кольце $K_{Kl}[x_1,x_2,x_3,x_4]$ действует разрешимая группа $S(3)=S(4)/Kl$, и алгеброй инвариантов относительно ээтого действия является кольцо симметричных многочленов.

Элемент x_1 имеет четыре резольвенты Лагранжа относительно действия группы Kl

$$\begin{aligned}R_1&=x_1+x_2+x_3+x_4,\\R_2&=x_1-x_2+x_3-x_4,\\R_3&=x_1+x_2-x_3-x_4,\\R_4&=x_1-x_2-x_3+x_4.\end{aligned}$$

Имеем $x_1=1/4(R_1+R_2+R_3+R_4)$ и R_1^2, R_2^2, R_3^2 и R_4^2 принадлежат $K_{Kl}[x_1,x_2,x_3,x_4]$. Поэтому x_1 при помощи арифметических операций и извлечения квадратных корней выражается через элементы алгебты $K_{Kl}[x_1,x_2,x_3,x_4]$. В свою очередь элементы алгебры $K_{Kl}[x_1,x_2,x_3,x_4]$ выражаются через симметричные многочлены, т.к. на этой алгебре действует группа $S(3)$, относительно которой инвариантны симметричные многочлены (см выше решение кубических уравнений).

Отметим, что приведенное выше рассуждение доказывают нечто большее: оно дает явное сведение уравнения четвертой степени к кубическому уравнению. Действительно, резольвента $R_1=\sigma_1$ является симметричным многочленом, а квадраты резольвент R_2, R_3 и R_4 переставляются между собой при действии группы S_4 (смотри выше описание гомоморфизма $\pi\colon S(4)\to S(3)$). Так как элементы R_2^2, R_3^2, R_4^2 лишь переставляются, то основные симметрические многочлены от них инвариантны относительно действия группы $S(4)$. Итак многочлены

$$\begin{aligned}b_1&=R_2^2+R_3^2+R_4^2,\\b_2&=R_2^2R_3^2+R_3^2R_4^2+R_4^2R_2^2,\\b_3&=R_2^2R_3^2R_4^2\end{aligned}$$

являются симметрическими многочленами от x_1, x_2, x_3 и x_4, следовательно, b_1, b_2 и b_3 явно выражаются через коэффициенты уравнения

$$x^4+a_1x^3+a_2x^2+a_3x+a_4=0. \tag{4}$$

Итак, чтобы решить уравнение (4) достаточно составить и решить уравнение

$$r^3 - b_1 r^2 + b_2 r - b_3 = 0 \tag{5}$$

и положить $x = 1/4(-a_1 + \sqrt{r_1} + \sqrt{r_2} + \sqrt{r_3})$, где r_1, r_2 и r_3 — корни уравнения 5.