ГЛАВА

ТЕОРИЯ ГАЛУА И ТФКП

9. Неразрешимость сложных алгебраических уравнений при помощи решения более простых алгебраических уравнений

Вопрос разрешимости уравнений в радикалах можно сформулировать следующим образом. Можно ли выразить все корни заданного уравнения через элементы исходного поля коэффициентов, используя лишь арифметические и операции извлечения корней. Последняя операция означает, что если элемент a уже выражен в нужном виде, а элемент x удовлетворяет уравнению $x^n = a$, где n — натуральное, то элемент x тоже считается выраженным в нужном виде. Можно обобщить вопрос о разрешимости уравнений в радикалах, увеличив множество допустимых операций, т.е. разрешая решать те или иные алгебраические уравнения с уже построенными коэффициентами. Например, можно к числу допустимых операций можно добавить операцию решения алгебраических урщвнений степени не выше k. Использование этой опереции означает, что если элементы $a_1, \dots, a_k$ уже выражены в нужном виде, а элемент x удовлетворяет уравнению $x^k + a_1 x^{k-1} + \cdots + a_k = 0$, то элемент x тоже считается выраженым в нужном виде. Можно ли решить заданное алгебраическое уравнение, используя лишь арифметические операции, радикалы и решая алгебраические уравнения степени не выше k? Ниже мы приведем исчерпывающий ответ на этот вопрос. Но сначала обсудим более общие определения.

Можно рассматривать и другие вопросы о разрешимости (сложных) алгебраических уравнений, в которых в качестве допустимых операций используются другие (более простые) алгебраические уравнения. Алгебраическое уравнение $x^k + a_1 x^{k-1} + \cdots + a_k = 0$ определено над полем K, если его коэффициенты a_i лежат в поле K. Если уравнение определено над полем K, то оно определено и над любым большим полем K_1, $K \subset K_1$.

Пусть B — некоторая совокупность алгебраических уравнений.

Определение. Уравнение $x^k + a_1 x^{k-1} + \cdots + a_k = 0$ над полем K называется разрешимым при помощи алгебраических уравнений из совокупности B или, короче, называется B-разрешимым, если существует последовательность полей $K = K_0 \subset K_1 \subset \cdots \subset K_n$ такая, что все корни уравнения лежат в поле K_n и для каждого $i = 0, \dots, n-1$ поле K_{i+1} получается из поля K_i присоединением всех корней некоторого алгебраического уравнения из совокупности B, определенного над полем K_i.

Разрешимость уравнений в радикалах является частным случаем B-разрешимости. Чтобы это показать, нужно рассмотреть совокупность

Typeset by $\mathcal{AMS}$-TEX

всех уравнений вида $x^n - a = 0$, где n — натуральное число и a — любой элемент любого поля. Является ли заданное алгебраическое уравнение B-разрешимым? Теория Галуа доставляет необходимое условие для B-разрешимости уравнений. Сформулируем его.

Сопоставим совокупности уравнений B множество $G(B)$ групп Галуа этих уравнений.

Утверждение 1. *Множество конечных групп $G(B)$ с каждой группой содержит все ее подгруппы.*

Доказательство. Дело в том, что совокупность уравнений B вместе со всяким уравнением, определенным над некоторым полем K, содержит то же самое уравнение над всяким большим полем K_1, $K \subset K_1$. При увеличении основного поля группа Галуа уравнения заменяется ее подгруппой. Обратно, пусть некоторое уравнение, определенное над полем K принадлежит совокупности уравнений B. Пусть P — расширение Галуа поля K, полученное присоединением к полю K всех корней рассматриваемого уравнения. Пусть G — группа Галуа этого расширения и G_1 — любая ее подгруппа. Возьмем в качестве большего поля промежуточное поле K_1, $K \subset K_1 \subset P$, соответствующее подгруппе G_1 группы G. Группа Галуа рассматриваемого уравнения над большим полем K_1 совпадает с подгруппой G_1.

Теорема (необходимое условие B-разрешимости). *Если алгебраическое уравнение над полем K является B-разрешимым, то у его группы Галуа G существует цепочка подгрупп $G = G_0 \supset G_1 \cdots \supset G_1 = e$, в которой группа G_n тривиальна и для любого $i = 0, \ldots, n-1$ группа G_{i+1}является нормальным делителем группы G_i, причем, факторгруппа G_i/G_{i+1} является одновременно факторгруппой одной из групп $G(B)$.*

Доказательство. Действительно, B-разрешимость уравнения над полем K означает существование цепочки расширений $K = K_0 \subset K_1 \cdots \subset K_n$, в которой поле K_{i+1} получается из поля K_i, $i = 0, \ldots, n-1$ присоединением всех решений некоторого алгебраического уравнения из совокупности B, а последнее поле K_n содержит все корни исходного алгебраического уравнения. Обозначим через G_i группу Галуа исходного уравнения над полем K_i. Покажем, что полученная цепочка подгрупп G_i удовлетворяет требованиям теоремы. Действительно, согласно теореме [] группа G_{i+1} является нормальной подгруппой в группе G_i, причем, факторгруппа G_i/G_{i+1} является одновременно факторгруппой группы Галуа поля K_{i+1} над полем K_i. Так как поле K_{i+1} получается из поля K_i присоединением всех корней алгебраического уравнения из совокупности B, то группа Галуа поля K_{i+1} над полем K_i принадлежит множеству $G(B)$. Поскольку поле K_0 совпадает с полем K, группа G_0 совпадает с группой G. Так как все корни алгебраического уравнения лежат в поле K_n, то группа Галуа G_n алгебраического уравнения над полем K_n тривиальна.

Необходимое условие B-разрешимости — прямое обобщение необходимого условия разрешимости в радикалах. Чтобы это увидеть, нужно в качестве совокупности B рассмотреть все уравнения вида $x^n - a = 0$ и отсенить их группу Галуа. Повторим еще раз вывод необходимого условия разрешимости уравнения в радикалах, немного его изменив.

Лемма. *Группа Галуа G уравнения $x^n - a = 0$, $a \in K$, над полем K обладает коммутативным нормальным делителем G_2, факторгруппа G/G_1 относительно которого коммутативна.*

Доказательство. Пусть P — расширение поля K, полученное добавлением к этому полю всех корней уравнения $x^n = a$. Отношение любых двух корней уравнения $x^n = a$ является корнем n-й степени из единицы. оцюда видно, что поле P содержит все корни степени n из единицы. Обозначим через K_1 расширение поля K, полученное добавлением к этому полю всех корней степени n из единицы. Мы имеем включения $K \subset K_1 \subset P$. Обозначим через G_1 группа Галуа уравнения $x^n = a$ над полем K_1. Согласно утверждению [] группа G_1 коммутативна. Группа G_1 является нормальным делителем группы G, т.к. поле K_1 является расширением Галуа поля K. Факторгруппа G/G_1 коммутативна, т.к. согласно утверждению [] коммутативна группа Галуа поля K_1 над полем K.

Следствие. *1. Для совокупности B уравнений вида $x^n - a = 0$ множество $G(B)$ содержит лишь разрешимые группы.*

2. Если уравнение решается в радикалах, то его группа Галуа разрешима.

Доказательство. Пункт 1 вытекает из леммы. Пункт 2 вытекает из пункта 1 и необходимого условию B-разрешимости.

Вернемся к вопросу о разрешимости алгебраического уравнения при помощи радикалов и решения уравнения степени не выше k. Этот вопрос совпадает с вопросом о B-разрешимости уравнения для совокупности B, состоящей из всех уравнений вида $x^n - a = 0$ для $n = 1, 2 \ldots$, и всех уравнений $x^m + a_1 x^{m-1} + \cdots + a_m = 0$ при $m \leq k$.

Утверждение. *Группа Галуа уравнения степени $m \leq k$ изоморфно подгруппе группы $S(k)$.*

Доказательство. Любой элемент группа Галуа лишь переставляет корни уравнения и вполне определяется возникшей перестановкой корней. Поэтому группа Галуа уравнения степени m изоморфна подгруппе группы $S(m)$. При $m \leq k$ группа $S(m)$ является подгруппой группы $S(k)$.

Нам понадобится следующая лемма.

Лемма 1. *Группа Γ изоморфна подгруппе $S(k)$, если и только если группа Γ обладает набором подгрупп Γ_i, $i = 1, \ldots, m$, таким, что*

1) группа $\bigcap_{i=1}^{m} \Gamma_i$ не содержит нормальных делителей группы Γ, отличных от тривиального;

2) $\sum_{i=1}^{m} \operatorname{ind}(\Gamma, \Gamma_i) \leq k$.

Доказательство. Пусть Γ является подгруппой $S(k)$. Рассмотрим представление группы Γ как некоторой подгруппы перестановок множества M, содержащего k элементов. Пусть под действием группы Γ множество M распадается на m орбит. Выберем в каждой орбите по точке x_i. Набор стационарных подгрупп Γ_i точек x_i удовлетворяет условиям леммы.

Обратно, пусть группа Γ обладает набором подгрупп, удовлетворяющим условиям леммы. Обозначим через P непересекающееся объединение

множеств $P_i = \{P_i^j\}$ — множеств правых классов смежности P_i^j группы Γ по подгруппе Γ_i. Группа Γ обладает естественным действием на множестве P. Возникающее представление группы Γ в группу $S(P)$ точное, т.к. ядро этого представления лежит в группе $\bigcap_{i=1}^{m} \Gamma_i$. Группа $S(P)$ вкладывается в группу $S(k)$, т.к. в множестве P содержится $\sum_{i=1}^{m} \mathrm{ind}(\Gamma, \Gamma_i) \leq k$ элементов.

proclaimСледствие1. Факторгруппа подгруппы симметрической группы $S(k)$ изоморфна подгруппе симметрической группы $S(k)$.

2. Если группа G является подгруппой группы $S(k)$, то у группы G су7ествует вложенная цепочка подгрупп $G = G_0 \supset G_1 \supset \cdots \supset G_n = e$, в которой группа G_n тривиальна, а для каждого $i = 0, 1, \ldots, n-1$ группа G_{i+1} явлтается нормальным делителем группы G_i глубины не превосходящей k. (см. п.[]) endproclaim

Доказательство. 1. Пусть группа G изоморфна подгруппе группы $S(k)$, и G_i — набор ее подгрупп, удовлетворяющих условию леммы. Пусть π — произвольный гомоморфизм группы G. Тогда совокупность подгрупп $\pi(G_i)$ в группе $\pi(G)$ тоже удовлетворяет условиям леммы.

2. Пусть G_i — совокупность подгрупп в группе G, удовлетворяющих условиям леммы. Обозначим через F_i нормальный делитель группы G, равный пересечению всех подгрупп, сопряженных группе G_i. Цепочка подгрупп $D_0 = B_0$, $D_1 = B_1, \ldots, D_l = B_0 \cap B_1 \cap \cdots \cap B_l$ удовлетворяет требованиял следствия.

Теорема (критерий разрешимости уравнения при помощи радикалов и решений вспомогательных уравнений степени, не превосходящей k). *Алгебраическое уравнение над полем характеристики нуль решается при помощи радикалов и решения вспомогательных уравнений степени не выше k, если и только если его группа G обладает цепочкой подгрупп*

$$G = H_0 \supset H_1 \supset \cdots \supset H_n = e$$

такой, что

1) *для каждого i, $0 < i \leq n$, подгруппа H_i является нормальным делителем подгруппы H_{i-1};*
2) *для каждого i, $0 < i \leq n$, либо глубина нормального делителы H_i в группе H_{i-1} не превосходит k, либо факторгруппа H_{i-1}/H_i коммутативна;*
3) *подгруппа H_0 совпадает с группой G, а подгруппа H_n совпадает с единичным элементом e группы G.*

Доказательство. 1. Необходимое условие разрешимости. В теореме идет речь о B-разрешимости уравнений, в которых совокупность B состоит из всех уравнений степени меньшей или равной k и уравнений вида $x^n - a = 0$. Множество $G(B)$ групп Галуа уравнений совокупности B содержит лишь разрешимые группы и подгруппы группы $S(k)$ (см. []-[]). Согласно необходимому условию для B-разрешимости группа Галуа G уравнения, разрешимого при помощи радикалов и вспомогательных уравнений, обладает нормальной цепочкой подгрупп такой, что все соответствующие факторгруппы принадлежат множеству $G(B)$. Согласно [] []

каждая группа из множества $G(B)$, в свою очередь, обладает нормальной цепочкой подгрупп, в которой либо факторгруппы коммутативны,...

2. Достаточность. Индукция по длине n цепочки подгрупп в группе G. Группа G имеет нормальный делитель H_1, а группа H_1 обладает тем же свойством, что и группа G, но с цепочкой подгрупп

$$H_1 = H_1 \supset H_2 \supset \cdots \supset H_n = e$$

длины $n-1$. Обозначим через P_1 поле инвариантов группы H_1. Согласно индукционному предположению поле P получается из поля P_1 при помощи присоединений радикалов и корней уравнений степени не выше k. Факторгруппа G/H_1 действует на поле P_1 с полем инвариантов P_0. Если факторгруппа G/H_1 коммутативна, то поле P_1 получается из поля P_0 при помощи присоединеня радикалов (см. утверждение ?). Если факторгруппа G/H_1 имеет глубину, не превосходящую k, то поле P_1 получается из поля P присоедимемием всех корней алгебраического уравнения степени не выше k (см. утверждение выше).

* * *

Определение. Пусть M — некоторое множество конечных групп. *Пополнением* $\mathcal{K}(M)$ множества M называется минимальное множество конечных групп, содержащее множество M и обладающее следующими свойствами:

1) если группа G содержится в множестве $\mathcal{K}(M)$, а G_1 — подгруппа группы G, то G_1 принадлежит множеству $\mathcal{K}(M)$;

2) если группа G содержится в множестве $\mathcal{K}(M)$, а G_1 — факторгруппа группы G, то G_1 принадлежит множеству $\mathcal{K}(M)$;

3) если у группы G существует нормальный делитель H такой, что группа H и фактор группа G/H принадлежат множеству $\mathcal{K}(M)$, то группа G принадлежит множеству $\mathcal{K}(M)$.

Доказанная выше теорема делает актуальной следующую задачу: для заданного множества M конечных групп описать его поплнение $\mathcal{K}(M)$. Прежде всего напомним теорему Жордана-Гельдера (см. []). Нормальная башня группы Γ, т.е. цепочка вложенных подгрупп $\Gamma = \Gamma_0 \supset \Gamma_1 \supset \cdots \supset \Gamma_n =$, в которой каждая группа Γ_{i+1} является нормальным делителем предыдущей группы Γ_i, называется *неуплотняемой*, если все факторгруппы Γ_i/Γ_{i+1} относительно этой нормальной башни, являются простыми группами, группа Γ_n тривиальна (т.е. состоит из единичного эсемента группы Γ). Теорема Жордана-Гельдера утверждает, что для всякой конечной группы Γ множество факторгрупп Γ_i/Γ_{i+1} относительно неуплотняемой нормальной басгни группы Γ определен инвариантно, т.е. не зависит от выбора неуплотняемой башни.

Утверждение. *Группа* Γ *принадлежит пополнению* $\mathcal{K}(M)$ *множества конечных групп* M, *если и только если каждая факторгруппа* Γ_i/Γ_{i+1} *относительно неуплотняемой нормальной башни группы* Γ *является факторгруппой подгруппы некоторой группы из множества* M.

Доказательство. Во-первых, согласно определению пополнения $\mathcal{K}(M)$ каждая группа Γ, удовлетворяющая условиям утверждения, лежит в пополнении $\mathcal{K}(M)$. Во-вторых, несложно проверить, что группы Γ, удовлетворяющие

условиям утверждения, обладают свойствами 1–3 из определения пополнения множества M.

Следствие. *1. Пополнение множества всех конечных абелевых групп является множеством всех конечных разрешимых групп.*

2. Теорема [], доставляющая необходимые условия разрешимости алгебраических уравнений в радикалах, является частным случаем теоремы [].

Доказательство. Остановимся на пункте 2. Разрешимость уравнения в радикалах – это то же самое, что B-разрешимость, где B — совокупность уравнений вида $x^n - a = 0$. Так как группа Галуа уравнения $x^n = a$ абелева, то из теоремы [] и пункта 1 настоящего следствия вытекает, что группа Галуа уравнения, разрешимого в радикалах, является разрешимой группой.