ГЛАВА

ТЕОРИЯ ГАЛУА И ТФКП

8. Основная теорема теории Галуа и критерий разрешимости уравнений в радикалах

В предыдущих параграфах мы уже, фактически, доказали центральные теоремы теории Галуа. В этом параграфе мы подведем итог и докажем критерий разрешимости уравнений в радикалах. Как и во всей книге, мы ограничваемся полями характристики нуль.

Определение 1. Поле P называется *расширением Галуа* поля K, если существует алгебраическое уравнение с коэффициентами в поле K, все корни которого лежат в поле P, причем, поле P получается присоединением к полю K всех корней этого уравнения.

Приведем другое эквивалентное определение.

Определение 2. Поле P является *расширением Галуа* своего подполя K, если существует конечная группа автоморфизмов G поля P такая, что

а) все элементы подполя K остаются на месте при действии любого группы G;

б) лишь элементы подполя K остаются на месте при действии всех элементов группы G.

Утверждение 1. *1. Если поле P является расширением Галуа поля K в смысле определения 1, то P является расширением Галуа K в смысле определения 2.*

2. Если поле P является расширением Галуа поля K в смысле определения 2, то P является ресширением Галуа поля K в смысле определения 1. Группа G из определения 2 совпадает с группой всех автоморфизмов поля P над полем K. Следовательно, группа G определена однозначно.

Доказательство. 1. Если поле P является расширением Галуа поля K в смысле определения 1, то согласно теореме [] из параграфа [] существует группа автоморфизмов поля P, единственными неподвижными элементами относительно действия которой являются элементы поля K, т.е. поле K является расширением Галуа в смысле определения 2.

2. Пусть теперь поле P является расширением Галуа поля K в смысле определения 2. Согласно теореме [] из параграфа [], в поле P найдется элемент a, которого сдвигает с места любой нетривиальный элемент группы G. Возьмем элемент a и рассмотрим его орбиту O относительно действия группы G. Согласно утверждению [] параграфа [] существует алгебраическое уравнение с коэффициентами в поле K, множество корней

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

которого совпадает с O. Согласно теореме [] из параграфа [] любой из элементов орбиты, т.е. любой из корней построенного уравнения порождает поле P над полем K. Тем самым поле P является расширением Галуа поля K в смысле определения 1.

Любой автоморфизм σ поля P над полем K переводит элемент a в некоторый элемент множества O, т.к. множество O является множеством решения уравнения с коэффициентами в поле K. Поэтому для σ найдется элемент g группы G такой, что $\sigma(a) = g(a)$. Автоморфизм σ совпадает с этим элементом g, т.к. элемент a порождает поле P над полем K. Значит, группа G совпадает с группой всех автоморфизмов поля P над полем K.

Определение 3. *Группой Галуа расширения Галуа P* поля K называется группа всех автоморфизмов поля P над полем K. *Группой Галуа алгебраического уравнения* с коэффициентами в поле K называется группа Галуа расширения Галуа поля K, полученного присоединением к этому полю всех корней алгебраического уравнения.

Пусть поле P является расширением Галуа поля K. Теория Галуа описывает все промежуточные поля, т.е. все поля, лежащие в поле P и содержащие поле K. Сопоставим каждой подгруппе L группы Галуа поля P над полем K подполе P_L всех элементов, остающихся неподвижными при действии подгруппы L. Итак, каждой подгруппе группы Галуа мы поставили в соответствие промежуточное поле. Это соответствие называется *соответствием Галуа.*

Основная теореме теории Галуа. *Соответствие Галуа устанавливает взаимнооднозначное соответствие между множеством подгрупп группы Галуа и множеством промежуточных полей.*

Доказательство. Во-первых, различные подгруппы имеют различные поля инвариантов. Действительно, если две группы различаются, то в одной из этих групп, которую для определенности мы будем называть первой, найдется элемент, не содержащийся во другой группе, которую мы будем называть второй. Согласно теореме [] из[] найдется элемент поля P, который остается на месте лишь при действии автоморфизмов из второй группы. Этот элемент не может быть неподвижным относительно всех преобразований первой группы автоморфизмов, поэтому различные подгруппы группы Галуа, действительно, имеют различные поля инвариантов. Во-вторых, каждое промежуточное поле является соответствует некоторой подгруппе группы Галуа. Действительно, если поле P является расширением Галуа поля K, то оно является расширением Галуа и всякого промежуточного поля. Это совершенно очевидно, если воспользоваться первым определением расширения Галуа. Из второго определения расширения Галуа видно, что промежуточное поле является неподвижным полем для некоторой группы автоморфизмов поля P над полем K. Теорема доказана.

Утверждение 2. *Промежуточное поле является расширением Галуа поля коэффициентов, если и только если при соответствии Галуа этому промежуточному полю сопоставляется нормальный делитель группы Галуа. При этом группа Галуа промежуточного расширения Галуа над полем коэффициентов изоморфна факторгруппе группы Галуа исходного расширения группы Галуа по нормальному делителю, соответствующему промежуточному расширению Галуа.*

Доказательств. 1. Пусть промежуточное поле K_1 соответствует нормальному делителю H группы Галуа G расширения Галуа P поля K. Поле K_1 переходит в себя при действии автоморфизмов из группы Галуа G, т.к. множество неподвижных точек относительно действия нормального делителя инвариантно относительно действия (см. утверждение [] пункта []). Группа автоморфизмов поля K, индуцированная действием группы G, изоморфна факторгруппе G/H. При этом поле инвариантов относительно действия на поле K_1 индуцированной группы автоморфизмов, совпадает с полем K. Итак, если H — нормальный делитель группы G, то K_1 — расширение Галуа поля K с группой Галуа G/H.

2. Пусть H — любая подгруппа группы Галуа G и P_H — поле неподвижных элементов относительно действия подгруппы. Ясно, что элемент g группы G переводит поле P_H в поле $P_{gHg^{-1}}$ — поле неподвижных элементов относительно действия сопряженной подгруппы gHg^{-1}.

Промежуточное расширение Галуа K_1 получается из поля K присоединением всех корней некоторого алгебраического уравнения. Любой автоморфизм g из группы Галуа G лишь переставляет между собой корни этого уравнения и поэтому переводит поле K_1 в себя.

Поэтому, если промежуточное расширение Галуа K_1 соответствует подгруппе H, то для всякого элемента $g \in G$ справедливо равенство $H = gHg^{-1}$. Другими словами, группа H, соответствующая промежуточному расширению Галуа, является нормальным делителем группы Галуа G.

Утверждение 3. *Пересечение двух расширений Галуа является расширением Галуа. Группа Галуа пересечения является факторгруппой группы Галуа каждого из исходных расширений Галуа.*

Доказательство. Рассмотрим наименьшее поле, содержащее оба расширения Галуа. Это поле можно получить следующим образом. Если первое поле получается добавлением к полю коэффициентов всех корней полинома $Q_1(x)$, а второе поле — всех корней полинома $Q_2(x)$, то наименьшее поле, их содержащее, получается присоединением к полю коэффициентов всех корней полинома $Q_1Q_2(x)$. Поэтому это поле также является расширением Галуа поля K. Группа Галуа этого расширения Галуа поля K оставляет инвариантными как первое, так и второе расширение поля K. Следовательно, пересечение двух расширений Галуа также будет инвариантно относительно действия этой группы. Следовательно, согласно утверждению 2, пересечение двух расширений Галуа будет расширение Галуа. Согласно тому же утверждению группа Галуа этого расширения является факторгруппой группы Галуа каждого из исходных расширений Галуа.

Пусть

$$(*) \qquad a_0 + a_1x + \cdots + a_nx^n = 0$$

— алгебраичеслое уравнение с коэффициентами в поле K и P — расширение Галуа поля K, полученное присоединением к полю K всех корней уравнения $*$. Рассмотрим новое большее поле коэффициентов $\tilde{K}$, $\tilde{K} \subset K$, и его расширение Галуа $\tilde{P}$, полученное присоединением к полю $\tilde{K}$ всех корней уравнения $*$. Как связаны группы Галуа G и $\tilde{G}$ полей P над K и

$\tilde{P}$ над $\tilde{K}$? Или, другими словами, что происходит с группой Галуа уравнения $*$ при увеличении основного поля (т.е. при переходе от поля K к полю $\tilde{K}$)?

Достаточно ясно, что при увеличении поля коэффициентов группа Галуа уравнения уменьшается, т.е. заменяется некоторой подгруппой Галуа уравнения над исходным полем коэффициентов. Сформулируем это утверждение более точно и докажем его.

Обозначим через K_1 пересечение полей P и $\tilde{K}$. Поле K_1 — промежуточное поле между полями K и P, т.е. $K \subset K_1 \subset P$. Согласно основной теореме теории Галуа полю K_1 соответствует некоторая подгруппа G_1 группы Галуа G.

Теорема 1. *Группа Галуа поля $\tilde{P}$ над полем $\tilde{K}$ изоморфна подгруппе G_1 в группе Галуа G поля P над полем K, которая при соответствии Галуа (для расширения Галуа P поля K) сопоставляется промежуточному полю $K_1 = P \cap \tilde{K}$.*

Доказательство. Группа Галуа $\tilde{G}$ оставляет элементы поля K неподвижными (т.к. $K \subset \tilde{K}$) и переставляет корни уравнения $*$. Поэтому поле P переводится автоморфизмами группы $\tilde{G}$ в себя. Неподвижными элементами относительно индуцированной группы автоморфизмов поля P являются в точности те элементы поля P, которые содержатся в поле $\tilde{K}$, т.е. элементы поля $K_1 = P \cap \tilde{K}$. Поэтому индуцированная группа автоморфизмов поля P совпадает с подгруппой G_1 группы Галуа G поля P над полем K. Осталось показать, что описанный выше гомоморфизм группы $\tilde{G}$ в группу G_1 не имеет ядра. Действительно, ядро этого гомомрфизма оставляет неподвижными все корни уравнения $*$, т.е. ядро гоморфизма содержит лишь тривиальный элемент группы $\tilde{G}$. Теорема доказана.

Пусть теперь в условиях предыдущей теоремы поле $\tilde{K}$ само является расширением Галуа поля K. Согласно утверждению 3 поле K_1 в этом случае также является расширением Галуа поля K. Обозначим через Γ_1 группу Галуа расширения K_1 поля K.

Теорема 2 (об изменении группы Галуа при расширении Галуа поля коэффициентов). *При расширении Галуа поля коэффициентов группа Галуа G исходного уравнения заменяется своим нормальным делителем G_1. Факторгруппа G/G_1 группы G относительно этого нормального делителя изоморфна факторгруппе группы Галуа нового поля коэффициентов $\tilde{K}$ над старым полем коэффитиентов K.*

Доказательство. Действительно, группс G_1 соответствует полю $P \cap \tilde{K}$, которое является расширением Галуа поля K. Поэтому группа G_1 является нормальным делителем группы G, а ее факторгруппа G/G_1 изоморфна группе Галуа поля K_1 над полем K. Но группа Галуа поля K_1 над полем K изоморфна факторгруппе Γ/Γ_1. Теорема доказана.

Теория Галуа была создана для ответа на следующий вопрос: решается ли заданное уравнение в радикалах или нет. Опишем, как теория Галуа решает этот вопрос. Нанчнем с уравнений, определенных над полями коэффициентов, которые содержат все корни из единицы. Этот случай

немного проще общего, а для нас основной интерес представляют различные поля мероморфных функций, которые содержат не только все корни из единицым но и вообще все комплексные константы.

Утверждение 4. *Группа Галуа уравнения $x^n - a = 0$ над полем K, $a \in K$, содержашим все корни степени n из единицы является подгруппой циклической группы из n элементов.*

Доказательство. Фиксируем любой корень x_0 уравнения $x^n - a = 0$ и любой первообразный корень ξ степени n из единицы. Занумеруем корни уравнения $x^n - a = 0$ вычетами i по модулю n, положив x_i равным $\xi^i x_0$. Пусть преобразование g из группы Галуа переводит корень x_0 в корень x_i. Тогда $g(x_k) = g(\xi^k x_0) = \xi^{k+i} x_0 = x_{k+i}$. То есть всякое преобразование группы Галуа задает циклическую перестановку корней. Следовательно, группа Галуа вкладывается в циклическую группу из n элементов.

Если поле коэффициентов K содержит все корни из единицуы, то все готово для доказательства критерия разрешимости уравнений в радикалах. Впрочем, это дополнительное ограничение на поле коэффициентов K легко устраняется. Для этого нам понадобятся следующие леммы 1–3.

Лемма 1. *Пусть расширение Галуа P поля K получается из поля K присоединением некоторых корней из единицы. Тогда группа Галуа поля P над полем K коммутативна.*

Доказательство. Все корни из единицы, лежащие в поле P, образуют коммутативную группу по умножению. В этой группе присутствует не более чем одна циклическая подгруппа любого фиксированного порядка k. Действительно, такую подгруппу может образовать лишь множество всех корней уравнения $x^k = 1$. Любое преобразование группы Галуа задает автоморфизм группы всех корней из единицы. Преобразование из группы Галуа целиком определяется заданным им автоморфизмом. Следовательно, описанное отображение группы G в группу автоморфизмов является вложением. Теперь лемма 1 вытекает из следующей леммы 2.

Лемма 2. *Группа всех автоморфизмов абелевой группы, содержащей не более одной циклической подгруппы любого фиксированного порядка, коммутативна.*

Доказательство. Каждый автоморфизм группы, удовлетворяющий условиям леммы, переводит любую циклическую подгруппу в себя и поэтому индутсирует автоморфизм любой циклической подгруппы. Поэтому группа автоморфизмов группы, удовлетворяющей условиям леммы, отображается в прямую сумму группы автоморфизмов всех ее циклических подгрупп. Это отображение является вложением. Циклическую группу из k элементов можно отождествить с аддитивной группой кольца $\mathbb{Z}/k\mathbb{Z}$, где $\mathbb{Z}$ — кольцо целых чисел. Группа автоморфизмов этой группы изоморфна мультипликативной группе обратимых элементов кольца $\mathbb{Z}/k\mathbb{Z}$ и поэтому коммутативна.

Лемма 3. *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. В частности, группа галуа G разрешима.*

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 4 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 лемме 1 коммутативна группа Галуа поля K_1 над полем K.

Теорема 3 (критерий разрешимости уравнений в радикалах). *Алгебраическое уравнение решается в радикалах, если и только если его группа Галуа разрешима.*

Доказательство. 1. Пусть уравнение решается в радикалах. Разрешимость уравнения в радикалах 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, $i = 0, 1, \ldots, n-1$, присоединением радикала, а поле K_n содержит все корни исходного алгебраического уравнения. Проследим, что происходит с группой Галуа уравнения при переходе от поля коэффициентов K_i к полю коэффициентов K_{i+1}. Обозначим через G_i группу Галуа нашего уравнения над полем K_i. Тогда согласно теореме 2 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 радикала, то согласно лемме 3, группа Галуа поля K_{i+1} над полем K_i разрешима. (В случае, если поле K содержит все корни из единицы, вместо леммы 3 можно воспользоваться более простым утверждением 4, согласно которому группа Галуа поля K_{i+1} над полем K_i коммутативна.) Так как все корни алгебраического уравнения по условию лежат в поле K_n, то группа Галуа G_n алгебраического уравнения над полем K_n тривиальна. Итак, если уравнение решается в радикалах, то у его группы Галуа G существует цепочка подгрупп $G = G_0 \supset G_1 \supset \cdots \supset G_n$, в которой группа G_{i+1} является нормальным делителем группы G_i с разрешимой факторгруппой G_i/G_{i+1}, а группа G_n тривиальна. (Если поле K содержит все корни из единицы, то факторгруппы G_i/G_{i+1} коммутативны.) То есть, если уравнение решается в радикалах, то его группа Галуа разрешима.

2. Пусть группа Галуа G алгебраического уравнения над полем K разрешима. Обозначим через $\tilde{K}$ поле, полученное из поля K присоединением всех корней из единицы. Группа Галуа $\tilde{G}$ алгебраического уравнения над большим полем $\tilde{K}$ является подгруппой группы G. Поэтому группа Галуа $\tilde{G}$ разрешима. Обозначим через $\tilde{P}$ поле, полученное из поля $\tilde{K}$ присоединением всех корней алгебраического уравнения. Разрешимая группа $\tilde{G}$ действует на поле $\tilde{P}$ с полем инвариантов $\tilde{K}$. Согласно теореме [] каждый элемент поля $\tilde{P}$ выражается в радикалах через элементы поля $\tilde{K}$. По определению поля $\tilde{K}$ каждый элемент этого поля выражается через корни из единицы и елементы поля K. Теореме доказана.