ГЛАВА 2.
РАЗРЕШИМОСТЬ АЛГЕБРАИЧЕСКИХ УРАВНЕНИй В РАДИКАЛАХ И ТЕОРИЯ ГАЛУА

Решается ли заданное алгебраическое уравнение в радикалах? Можно ли решать заданное алгебраическое уравнение степени n, используя решение вспомогательных алгебраических уравнений меньшей степени и используя радикалы? В этой главее мы обсуждаем, как теория Галуа (по крайней мере, в принципе) решает эти вопросы.

Сформулированные вопросы по своей природе являются чисто алгебраическими и могут быть поставлены над любым полем K. *Мы будем предполагать, что поле K имеет нулевую характеристику. В этой главе "поле" означает "поле характеристики нуль".* Случай полей нулевой характеристики немного проще общего, а для нас основной интерес представляют функциональные дифференциальные поля, которые содержат все комплексные константы. Другие интересные примеры полей, к которым полностью применимы результаты этой главы, доставляют подполя поля комплексных чисел (в частности, поле рациональных чисел $\mathbb{Q}$).

"Разрешительная" часть теории Галуа (см. §1), позволяющая решать уравнение в радикалах, весьма проста. Она не использует ни основную теорему теории Галуа, ни вообще теорию полей и относится, по существу, к линейной алгебре. Только эти линейно-алгебраические соображения применяются в топологической теории Галуа при обсуждении вопроса о представимости алгебраических функций в радикалах. Однако достаточное условие разрешимости уравнения с помощью решения вспомогательных уравнений меньшей степени и радикалов опирается не только на линейную алгебру, но и на основную теорему теории Галуа. Это одна из причин, почему мы приводим полное доказательство основной теоремы теории Галуа.

Без доказательства используются хорошо известные свойства разрешимых групп и группы $S(k)$. В пункте 9.1 доказывается значительно менее известное характеристическое свойство подгрупп группы $S(k)$. Эти факты из теории групп применяются как в обычной теории Галуа, так и в ее дифференциальном и топологическом вариантах.

Нам часто нужно расширять поле, присоединяя к нему один корень или неколько корней алгебраического уравнения. Для функциональных дифференциальных полей конструкция таких расширений проста и уже описана в §2 главы 1. Для подполей поля комплексных чисел $\mathbb{C}$ конструкция таких расширений очевидна. Так как нас в основном интересуют поля

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

именно этих двух типов, *ниже мы будем использовать такие расширения, не останавливаясь на их конструкции.*

Несколько слов о расположении материала. В параграфах 1–4 рассматривается поле P, на котором действует конечная группа автоморфизмов G. Элементы поля P, неподвижные относительно действия группы G, образуют подполе $K \subseteq P$, называемое полем инвариантов.

В параграфе 1 показано, что если группа G разрешима, то элементы поля P представимы в радикалах через элементы поля инвариантов K. (Здесь надо дополнительно предполагать, что поле K содержит все корни из единицы степени, равной порядку n группы G.) В случае, когда P — поле рациональных функций от n переменных, G — группа перестановок n переменных и K — поле симметричных рациональных функций от n переменных, этот результат объясняет, почему уравнения 2–4-й степеней решаются в радикалах.

В параграфе 2 показано, что для любой подгруппы G_0 группы G существует элемент $x \in P$, стационарная группа которого равна G_0. Результаты параграфов 1 и 2 основаны на простых соображениях теории групп и используют явную формулу для интерполяционного полинома Лагранжа.

В параграфе 3 показано, что всякий элемент поля P алгебраичен над полем K. Доказано, что если стационарная группа точки $z \in P$ содержит стационарную группу точки $y \in P$, то z является значением в точке y некоторого полинома над полем K. Это доказательство тоже основано на исследовании интерполяционного полинома Лагранжа (см. п. 3.3).

В параграфе 4 введен класс k-разрешимых групп. Показано, что если группа G k-разрешима, то элементы поля P представимы в k-радикалах (т.е. представимы с использованием радикалов и решений вспомогательных уравнений степени $\leq k$) через элементы поля K. Здесь тоже нужно дополнительно предполагать, что поле K содержит все корни из единицы степени, равной порядку n группы G.

Рассмотрим теперь другую ситуацию. Пусть поле P получено из поля K присоединением всех корней полиномиального уравнения над полем K, имеющего лишь некратные корни. В этом случае существует конечная группа G автоморфизмов поля P, полем инвариантов которой является поле K. Для построения группы G исходное уравнение заменяется эквивалентным уравнением Галуа, т.е. уравнением, каждый корень которого выражается через любой другой из его кореней (см. §5). Группа автоморфизмов G строится в §6.

Таким образом, в параграфах 2, 3, 5 и 6 доказаны центральные теоремы теории Галуа. В параграфе 7 подводится итог, формулируется и доказывается основная теорема теории Галуа.

Алгебраическое уравнение над некоторым полем решается в радикалах, если и только если его группа Галуа разрешима (см. §8), решается в k-радикалах, если и только если его группа Галуа k-резрешима (§9). В параграфе 10 обсуждается вопрос о разрешимости сложных алгебраических уравнений при помощи решения более простых уравнений. Здесь дается необходимое условие для подобной разрешимости в терминах группы

Галуа уравнения.

В этой главе большое внимание уделено приложениям теории Галуа к задачам о разрешимости алгебраических уравнений в явном виде. Для построения самой теории Галуа эти приложения не нужны. Главные положения теории Галуа содержатся в параграфах 2, 3, 5–7. Их можно читать отдельно.

Конструкция разрешения уравнений в радикалах (включающая решения общих уравнения степени 2–4) содержится в §1 и не зависит от остального текста.

§1. Действие разрешимой группы и представимость в радикалах

В этом параграфе доказано, что если на поле P действует конечная разрешимая группа автоморфизмов G, то (при некоторых дополнительных предположениях о поле P) все элементы поля P выражаются через элементы поля инвариантов K при помощи радикалов и арифметических операций.

Конструкция представления элемента в радикалах основана на линейной алгебре (п. 1.1). В пункте 1.2 результат применяется для доказательства разрешимости уравнений маленьких степеней. Чтобы написать явные формулы для решений, конструкцию из линейной алгебры нужно проделать явно. В пункте 1.3 мы описываем технику резольвент Лагранжа, позволяющую явно диагонализировать конечную коммутативную группу линейных операторов. В пункте 1.4 мы объясняем, как резольвенты Лагранжа помогают написать формулы решений в радикалах для уравнений 2–4-й степеней.

Результаты настоящего параграфа применимы в общей ситуации, рассматриваемой в теории Галуа. Если поле P получено из поля K присоединением всех корней алгебраического уравнения над полем K, имеющего лишь некратные корни, то существует группа G автоморфизмов поля P, полем инвариантов которой является поле K (п. 7.1). Эта группа называется *группой Галуа уравнения*. Из результатов настоящего параграфа вытекает, что уравнение, группа Галуа которого разрешима, решается в радикалах (достаточное условие разрешимости в радикалах из теоремы 8.7). Существование группы Галуа никак не самоочевидно и представляет собой один из центральных фактов теории Галуа. Здесь мы эту теорему не доказываем (доказательство имеется в п. 7.1), а изначально предполагаем, что группа G существует.

В ряде важных случаев группа G задана априори. Так, например, обстоит дело, если K — поле рациональных функций одной переменной, P — поле, полученное присоединением к K всех решений алгебраического уравнения и G — группа монодромии алгебраический функции, определенной этим уравнением (см. главу 4).

1.1. Достаточное условие разрешимости в радикалах. Конструкция представления элемента в радикалах 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. (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 $a \in V$, $\lambda \in K$.)

Пусть V — алгебра над полем K, содержащим все корни из единицы. Конечная коммутативная группа линейных преобразований конечномерного векторного пространства над полем K в некотором базисе приводится к диагональному виду (см. п. 1.3).

Утверждение 1.1. *Пусть G — конечная коммутативная группа порядка n автоморфизмов алгебры V. Пусть поле K содержит все корни степени n из единицы. Тогда каждый элемент x алгебры V представим в виде суммы $k \leq n$ элеменов $x_i \in V$, $i = 1, \ldots, k$, таких, что x_i^n лежит в алгебре инвариантов V_0.*

Доказательство. Рассмотрим конечномерное векторное пространство L в алгебре V, натянутое на орбиту элемента x относительно действия группы G. Пространство L раскладывается в прямую сумму $L = L_1 \oplus \cdots \oplus L_k$ подпространств, собственных для всех операторов группы G (см. п. 1.3). Поэтому вектор x представим в виде суммы $x = x_1 + \cdots + x_k$ векторов $x_1, \ldots, x_n$, собственных для всех операторов группы. Собственные числа этих операторов — корни степени n из единицы. Поэтому элементы $x_1^n, \ldots, x_k^n$ принадлежат алгебре инвариантов V_0.

Введем следующее

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

Пользуясь этим определением, утверждение 1.1 можно интерпретировать следующим образом: каждый элемент x в алгебре V представляется в виде суммы корней n-й степени из элементов алгебры инвариантов.

Теорема 1.2. *Пусть G — конечная разрешимая группа порядка n автоморфизмов алгебры V. Пусть поле K содержит все корни степени n из единицы. Тогда каждый элемент x алгебры V получается из элементов алгебры инвариантов V_0 при помощи извлечения корней и суммирований.*

Докажем сначала следующее простое утверждение о действии группы на множестве.

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 1.3. *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 фактор-группа 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 фактор-группы G/H.

Перейдем теперь к доказательству теоремы 1.2.

Доказательство. Так как группа G разрешима, то у нее существует цепочка вложенных подгрупп $G = G_0 \supset \cdots \supset G_m = e$, такая, что группа G_m совпадает с единичным элементом e и при $i = 1, \ldots, m$ группа G_i является нормальным делителем группы G_{i-1}, причем фактор-группа G_{i-1}/G_i коммутативна.

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 1.3, коммутативная фактор-группа G_{i-1}/G_i естественно действует на алгебры инвариантов V_i, оставляя неподвижной подалгебру инвариантов V_{i-1}. Порядок m_i фактор-группы G_{i-1}/G_i является делителем порядка n группы G. Поэтому к этому действию применимо утверждение 1.1. Следовательно, 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.

1.2. Группа перестановок переменных и уравнения 2–4-й степеней. Теорема 1.2 объясняет, почему уравнения маленькой степени решаются в радикалах.

Пусть алгебра V — кольцо многочленов от переменных $x_1, \ldots, x_n$ над полем K. Группа $S(n)$ перестановок n элементов действует на этом кольце, переставляя переменные $x_1, \ldots, x_n$ в многочленах из этого кольца. Алгебра инвариантов V_0 относительно этого действия состоит из симметричных многочленов. Каждый многочлен этой алгебры явным образом представляется в виде многочлена от $\sigma_1, \ldots, \sigma_n$, где $\sigma_1 = x_1 + \cdots + x_n$, $\sigma_2 = \sum_{i<j} x_i x_j$, ... ,$\sigma_n = x_1 \ldots x_n$. Рассмотрим общее алгебраическое уравнение $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ степени n. Согласно формулам Виета, коэффициенты этого уравнения с точностью до знака совпадают с основными симметрическими функциями от его корней $x_1, \ldots, x_n$. Именно, $\sigma_1 = -a_1, \ldots, \sigma_n = (-1)^n a_n$.

При $n = 2, 3, 4$ группа $S(n)$ разрешима. Пусть поле K содержит все корни из единицы степени ≤ 4. Применяя теорему 1.2, получаем, что каждый многочлен от $x_1, \ldots, x_n$ при $n \leq 4$ выражается через основные симметрические многочлены $\sigma_1, \ldots, \sigma_n$ при помощи извлечения корней, суммирования и умножения на рациональные числа. Поэтому *теорема 1.2 при* $n = 2, 3, 4$ *доказывает представимость корней уравнения степени* n *через*

коэффициенты уравнения при помощи извлечения корней, суммирования и умножения на рациональные числа.

Чтобы получить явные формулы для корней этих уравнений, нужно повторить снова все рассуждения, делая все необходимые конструкции явно. Мы это сделаем в п.п. 1.3 и 1.4.

1.3. Полиномы Лагранжа и коммутативные матричные группы. Пусть T — полином степени n с единичным старшим коэффициентом над произвольным полем K. Пусть полином T имеет в поле K ровно n различных корней $\lambda_1, \dots, \lambda_n$. С каждым корнем λ_i связан полином $T_i(t) = T(t)/T'(\lambda_i)(t - \lambda_i)$. Полином T_i — единственный полином степени $\leq (n-1)$, равный единице в корне λ_i и обращающийся в нуль в остальных корнях полинома T. Пусть $c_1, \dots, c_n$ — произвольная последовательность элементов поля K. Полином $L(t) = \sum c_i T_i(t)$ называется интерполяционным полиномом Лагранжа с узлами интерполирования $\lambda_1, \dots, \lambda_n$ и начальными данными $c_1, \dots, c_n$. Это единственный полином степени $\leq (n-1)$, принимающий в точке λ_i значение c_i при $i = 1, \dots, n$.

Рассмотрим векторное пространство V (возможно, бесконечномерное) над полем K и линейный оператор $A : V \to V$. Пусть оператор A удовлетворяет полиномиальмому уравнению $T(A) = A^n + a_1 A^{n-1} \cdots + a_{n-1}A + a_n E = 0$, где $a_i \in K$ и E — тождественный оператор. Допустим, что полином $T(t) = t^n + a_1 t^{n-1} + \cdots + a_{n-1}t + a_n$ имеет n различных корней $\lambda_1, \dots, \lambda_n$ в поле K. Оператор $L_i = T_i(A)$, где T_i — полином вида $T_i(t) = T/T'(\lambda_i)(t - \lambda_i)$, назовем *обобщенной резольвентой Лагранжа* оператора A, соответствующей корню λ_i. Для каждого вектора $x \in V$ вектор $x_i = L_i x$ будем называть обобщенной резольвентой Лагранжа (соответствующей корню λ_i) вектора x.

Утверждение 1.4. *1. Обобщенные резольвенты Лаграмжа L_i оператора A удовлетворяют следующим соотношениям: $L_1 + \cdots + L_n = E$, $L_i L_j = 0$ при $i \neq j$, $L_i^2 = L_i, AL_i = \lambda_i L_i$.*

2. Всякий вектор $x \in V$ представим в виде суммы своих обобщенных резольвент Лагранжа, т.е. $x = x_1 + \ldots + x_n$. При этом ненулевые резольвенты x_i вектора x линейно независимы и являются собственными векторами оператора A с собственными числами λ_i.

Доказательство. 1. Пусть $\Lambda = \{\lambda_i\}$ — множество корней полинома T. По определению, полином T_i равен единице в точке $\lambda_i \in \Lambda$ и обращается в нуль в остальных точках этого множества. Очевидно, что на множестве Λ обращаются в нуль следующие полиномы: $T_1 + \cdots + T_n - 1$, $T_i T_j$ при $i \neq j$, $T_i^2 - T_i$, $tT_i - \lambda_i T_i$. Поэтому каждый из перечисленных полиномов делится на полином T, имеющий простые корни в точках множества Λ. Поскольку полином T аннулирует оператор A, т.е. $T(A) = 0$, отсюда вытекают соотношения $L_1 + \cdots + L_n = E$, $L_i L_j = 0$ при $i \neq j$, $L_i^2 = L_i, AL_i = \lambda_i L_i$.

2. Вторая часть утверждения является формальным следствием первой части. Действительно, т.к. $E = L_1 + \cdots + L_n$, то для всякого вектора x

имеем $x = L_1x + \cdots + L_ix = x_1 + \ldots + x_n$. Допустим, что вектор x_i не равен нулю и что некоторая линейная комбинация $\sum \mu_j x_j$ векторов $x_1, \ldots, x_n$ обращается в нуль. Тогда $0 = L_i \sum \mu_j L_j x = \sum L_i L_j \mu_j x_j = \mu_i x_i$, т.е. ненулевой вектор x_i входит в линейную комбинацию с нулевым коэффициентом $\mu_i = 0$. Из равенства $AL_i = \lambda_i L_i$ вытекает, что $AL_ix = \lambda_i L_i x$, т.е. что либо вектор $x_i = L_ix$ — собственный вектор оператора A с собственным числом λ_i, либо $x_i = 0$.

Приведенная явная конструкция разложения вектора x по собственным векторам оператора A автоматически переносится на случай нескольких коммутирующих операторов. Остановимся подробнее на случае двух коммутирующих операторов. Пусть в пространсве V, кроме оператора A, задан еще один линейный оператор $B : V \to V$, коммутирующий с оператором A и удовлетворяющий полиномиальмому уравнению $Q(B) = B^k + b_1B^{k-1} + \cdots + b_{k-1}B + b_kE = 0$, где $b_i \in K$. Допустим, что полином $Q(t) = t^k + b_1t^{k-1} + \cdots + b_{k-1}t + b_k$ имеет k различных корней $\mu_1, \ldots, \mu_k$ в поле K. С корнем μ_j связаны полином $Q_j(t) = Q/Q'(\mu_j)(t - \mu_j)$ и оператор $Q_j(B)$ — обобщенная резольвента Лагранжа оператора B, соответствующая корню μ_j. Оператор $L_{i,j} = T_i(A)Q_j(B)$ назовем обобщенной резольвентой Лагранжа операторов A и B, соответствующей паре корней λ_i, μ_j. Вектор $x_{i,j} = L_{i,j}x$ будем называть обобщенной резольвентой Лагранжа вектора $x \in V$ (соответствующей паре корней λ_i и μ_j) относительно операторов A и B.

Утверждение 1.5. *1. Обобщенные резольвенты Лагранжа $L_{i,j}$ коммутирующих операторов A и B удовлетворяют следующим соотношениям: $\sum L_{i,j} = E$, $L_{i_1,j_1}L_{i_2,j_2} = 0$ при $(i_1, j_1) \neq (i_2, j_2)$, $L_{i,j}^2 = L_{i,j}$, $AL_{i,j} = \lambda_i L_{i,j}$. $BL_{i,j} = \mu_j L_{i,j}$.*

2. Всякий вектор $x \in V$ представим в виде суммы своих обобщенных резольвент Лагранжа, т.е. $x = \sum x_{i,j}$. При этом ненулевые резольвенты $x_{i,j}$ вектора x линейно независимы и являются собственными векторами операторов A и B с собственными числами λ_i и μ_j соответственно.

Для доказательства первой части утверждения достаточно перемножить соответствующие соотношения для обобщенных резольвент операторов A и B. Вторая часть утверждения является формальным следствием первой части.

Применим доказанные утверждения для оператора A конечного порядка n, $A^n = E$. Обобщенные резольвенты Лагранжа для таких операторов особенно важны для решения уравнений в радикалах. Именно эти резольвенты были открыты Лагранжем, и мы будем называть их резольвентами Лагранжа (опуская слово "обобщенными"). Пусть поле K содержит n корней $\xi_1, \ldots, \xi_n$ степени n из единицы, $\xi_i^n = 1$. По условию $T(A) = 0$, где $T(t) = t^n - 1$. Вычислим резольвенту Лагранжа, соответствующую корню $\xi_i = \xi$. Имеем $T_i(t) = \dfrac{t^n - \xi^n}{n\xi^{n-1}(t - \xi)} = \dfrac{1}{n\xi^{n-1}}(t^{n-1} + \cdots + \xi^{n-1}) = \dfrac{1}{n}((\xi^{-1}t)^{n-1} + \cdots + 1)$. Резольвенту Лагранжа $T_i(A)$ оператора A, соответствующую корню $\xi_i = \xi$, будем обозначать $R_\xi(A)$. Имеем: $R_\xi(A) = \dfrac{1}{n}\sum_{0 \leq k < n} \xi^{-k}A^k$.

Следствие 1.6. *Рассмотрим векторное пространство V над полем K, содержащим все корни степени n из единицы. Пусть оператор $A : V \to V$ удовлетворяет уравнению $A^n = E$. Тогда для всякого вектора $x \in V$ его резольвента Лагранжа $R_\xi(A)(x)$ либо равна нулю, либо является собственным вектором оператора A с собственным числом ξ. Вектор x является суммой всех своих резольвент Лагранжа.*

Замечание 1. Справедливость следствия 1.6 легко проверить непосредственно, не ссылаясь на предыдущие утверждения.

Пусть G — конечная коммутативная группа линейных операторов на векторном пространстве V над полем K. Обозначим через n порядок группы G. Пусть поле K содержит все корни степени n из единицы. Тогда пространство V является прямой суммой подпространств, собственных для всех операторов группы G. Уточним это утверждение. Пусть группа G является прямой суммой k циклических групп порядков $m_1, \dots, m_k$. Пусть операторы $A_1 \in G, \dots, A_k \in G$ порождают эти циклические подгруппы. В частности, $A_1^{m_1} = E, \dots, A_k^{m_k} = E$. Для всякого набора $\lambda = \lambda_1, \dots, \lambda_k$ корней из единицы степеней $m_1, \dots, m_k$ рассмотрим *совместную резольвенту Лагранжа* $L_\lambda = L_{\lambda_1}(A_1) \dots L_{\lambda_k}(A_k)$ образующих $A_1, \dots, A_k$ группы G.

Следствие 1.7. *Всякий вектор $x \in V$ представим в виде $x = \sum L_\lambda x$. Каждый из векторов $L_\lambda x$ — либо нуль, либо общий собственный вектор операторов $A_1, \dots, A_k$ с собственными числами $\lambda_1, \dots, \lambda_k$.*

1.4. Решение в радикалах уравнений 2–4-й степеней. В этом пункте мы снова вернемся к уравнениям маленьких степеней (см. п. 1.2). Мы воспользуемся техникой резольвент Лагранжа и объясним, как довести схему решения уравнений из п. 1.2 до явных формул. Сами формулы при этом мы выписывать не будем. Здесь используются обозначения п.п. 1.2, 1.3. Резольвенты Лагранжа операторов мы будем нумеровать собственными числами этих операторов. Совместные резольвенты Лагранжа пар операторов мы будем нумеровать парами собственных чисел этих операторов.

Уравнение второй степени. На кольце многочленов $K[x_1, x_2]$ линейно действует группа $S(2) = \mathbb{Z}_2$ перестановок двух элементов. Она состоит из тождественного преобразования и оператора второго порядка. Элемент x_1 относительно действия этого оператора имеет две резольвенты Лагранжа:

$$R_1 = \frac{1}{2}(x_1 + x_2) = \frac{1}{2}\sigma_1,$$
$$R_{-1} = \frac{1}{2}(x_1 - x_2).$$

Квадрат резольвенты Лагрнжа R_{-1} является симметричным многочленом. Имеем

$$R_{-1}^2 = \frac{1}{4}((x_1 + x_2)^2 - 4x_1x_2) = \frac{1}{4}(\sigma_1^2 - 4\sigma_2).$$

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

Уравнение третьей степени. Предположим, что поле K содержит все три кубических корня из единицы. На кольце многогчленов $K[x_1, x_2, x_3] = V$ действует группа $S(3)$ перестановок трех элементов. Группа $S(3)$ имеет нормальным делителем знакопеременную группу $A(3)$, которая является циклической группой порядка 3. Группа $A(3)$ порождена оператором B, задающим перестановку x_2, x_3, x_1 переменных x_1, x_2, x_3. Фактор-группа $S(3)/A(3)$ является циклической группой порядка 2. Обозначим через V_1 кольцо инвариантов группы $A(3)$ (которое состоит из многочленов, не меняющихся при четных перестановках переменных) и через V_2 алгебру симметрических многочленов. Элемент x_1 имеет три резольвенты Лагранжа относительно оператора B, порождающего группу $A(3)$

$$\begin{aligned} R_1 &= \frac{1}{3}(x_1 + x_2 + x_3), \\ R_{\xi_1} &= \frac{1}{3}(x_1 + \xi_2 x_2 + \xi_2^2 x_3), \\ R_{\xi_2} &= \frac{1}{3}(x_1 + \xi_1 x_2 + \xi_1^2 x_3), \end{aligned}$$

где ξ_1, ξ_2 — неединичные кубические корни из единицы, $\xi_1, \xi_2, = \dfrac{-1 \pm \sqrt{-3}}{2}$.

Имеем $x_1 = R_1 + R_{\xi_1} + R_{\xi_2}$ и R_1^3, $R_{\xi_1}^3$, $R_{\xi_2}^3$ лежат в алгебре V_1. Более того, резольвента R_1 является симметрическим многочленом, а полиномы $R_{\xi_1}^3$ и $R_{\xi_2}^3$ переставляются друг с другом при действии группы $\mathbb{Z}_2 = S(3)/A(3)$ на кольце V_1. Повторяя для полиномов $R_{\xi_1}^3$ и $R_{\xi_2}^3$ конструкцию, которую мы использовали при решении квадратного уравнения, получим, что эти полиномы выражаются через симметрические полиномы $R_{\xi_1}^3 + R_{\xi_2}^3$ и $(R_{\xi_1}^3 - R_{\xi_2}^3)^2$. Окончательно получаем, что многочлен x_1 выражается через симметрические многочлены $R_1 \in V_2$, $(R_{\xi_1}^3 + R_{\xi_2}^3) \in V_2$ и $(R_{\xi_1}^3 - R_{\xi_2}^3)^2 \in V_2$ при помощи извлечения корней второй и третьей степени и при помощи 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 $Kl = \mathbb{Z}^2 \oplus \mathbb{Z}^2$. Гомоморфизм 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 Kl этого гомоморфизма —

нормальный делитель группы $S(4)$, состоящий из четырех перестановок: тождественной перестановки и трех перестановок, каждая из которых является произведением транспозиций двух непересекающихся пар элементов.

Предположим, что поле K содержит все три кубических корня из единицы. На кольце полиномов $K[x_1, x_2, x_3, x_4] = V$ действует группа $S(4)$. Обозначим через V_1 подкольцо инвариантов нормального делителя Kl группы $S(4)$. Итак, на кольце $V = K[x_1, x_2, x_3, x_4]$ действует коммутативная группа Kl с кольцом инвариантов V_1. На кольце V_1 действует разрешимая группа $S(3) = S(4)/Kl$, и алгеброй инвариантов относительно этого действия является кольцо V_2 симметрических многочленов.

Пусть A и B — операторы, соответствующие перестановкам x_2, x_1, x_4, x_3 и x_3, x_4, x_1, x_2 переменных x_1, x_2, x_3, x_4. Операторы A и B порождают группу Kl. Справедливы тождества $A^2 = B^2 = E$. Корни полинома $T(t) = t^2 - 1$, аннулирующего операторы A и B, равны $+1, -1$. Группа Kl является суммой двух экземпляров группы из двух элементов, первое слагаемое порождено оператором A, второе — оператором B.

Элемент x_1 имеет четыре резольвенты Лагранжа относительно действия коммутирующих операторов A, B, порождающих группы Kl:

$$
\begin{aligned}
R_{1,1} &= \frac{1}{4}(x_1 + x_2 + x_3 + x_4),\\
R_{-1,1} &= \frac{1}{4}(x_1 - x_2 + x_3 - x_4),\\
R_{1,-1} &= \frac{1}{4}(x_1 + x_2 - x_3 - x_4),\\
R_{-1,-1} &= \frac{1}{4}(x_1 - x_2 - x_3 + x_4).
\end{aligned}
$$

Элемент x_1 равен сумме этих резольвент $x_1 = R_{1,1} + R_{-1,1} + R_{1,-1} + R_{-1,-1}$ и $R_{1,1}^2$, квадраты $R_{-1,1}^2$, $R_{1,-1}^2$ и $R_{-1,-1}^2$ резольвент Лагранжа принадлежат алгебре V_1. Поэтому x_1 при помощи арифметических операций и извлечения квадратных корней выражается через элементы алгебры V_1. В свою очередь, элементы алгебры V_1 выражаются через симметрические многочлены, т.к. на этой алгебре действует группа $S(3)$ с алгеброй инвариантнов V_2 (см. выше решение кубических уравнений).

Покажем, что приведенное выше рассуждение дает явное сведение уравнения четвертой степени к кубическому уравнению. Действительно, резольвента $R_{1,1} = \frac{1}{4}\sigma_1$ является симметрическим многочленом, а квадраты резольвент $R_{-1,1}$, $R_{1,-1}$ и $R_{-1,-1}$ переставляются между собой при действии группы S_4 (см. выше описание гомоморфизма $\pi\colon S(4) \to S(3)$). Так как элементы $R_{-1,1}^2$, $R_{1,-1}^2$, $R_{-1,-1}^2$ лишь переставляются, то основные симметрические многочлены от них инвариантны относительно действия группы

$S(4)$ и принадлежат кольцу V_2. Итак, многочлены

$$b_1 = R^2_{-1,1} + R^2_{1,-1} + R^2_{-1,-1},$$
$$b_2 = R^2_{-1,1}R^2_{1,-1} + R^2_{1,-1}R^2_{-1,-1} + R^2_{-1,-1}R^2_{-1,1},$$
$$b_3 = R^2_{-1,1}R^2_{1,-1}R^2_{-1,-1}$$

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

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

Чтобы решить уравнение (4), достаточно составить и решить уравнение

$$r^3 - b_1r^2 + b_2r - b_3 = 0 \tag{5}$$

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).

В заключение приведем еще одно красивое явное сведение уравнения четвертой степени к уравнению третьей степени, основанное на рассмотрении пучка плоских квадрик [Бер].

Координаты точек пересечения двух плоских квадрик $P = 0$ и $Q = 0$, где P и Q — заданные полиномы второй степени от x и y, можно найти, решая одно кубическое и несколько квадратных уравнений. Действительно, каждая квадрика пучка $P + \lambda Q = 0$, где λ — произвольный параметр, проходит через искомые точки. При некотором значении λ_0 параметра λ квадрика $P + \lambda Q = 0$ распадается на пару прямых. Это значение удовлетворяет кубическому уравнению $\det(\tilde{P} + \lambda\tilde{Q}) = 0$, где $\tilde{P}$ и $\tilde{Q}$ — (3×3)-матрицы квадратичных форм, соответствующих уравнениям квадрик в однородных координатах. Уравнения каждой из двух прямых, составляющих квадрику $P + \lambda_0 Q = 0$, можно найти, решая квадратное уранение: каждая такая прямая проходит через центр симметрии квадрики, координаты которого выражаются через коэффициенты квадрики при помощи арифметических орерации, и через одну из точек пересечения квадрики с любой фиксированной прямой. Для нахождения координат этой точки нужно решить квадратное уравнение. Уравнение прямой, проходящей через две заданные точки, находится с помощью арифметических операций. Если известны уравнения прямых, на которые распадается квадрика $P + \lambda_0 Q = 0$, то для нахождения искомых точек остается лишь решить квадратные уравнения для точек перечения квадрики $P = 0$ и каждой из двух прямых, составляющих квадрику.

Поэтому общее уравнение четвертой степени с помощью арифметических операций и извлечения квадратных корней сводится к кубическому уравнению. Действительно, корни уравнения $a_0x^4 + a_1x^3 + a_2x^2 + a_3x + a_4 = 0$ являются проекциями на ось x точек пересечения квадрик $y = x^2$ и $a_0y^2 + a_1xy + a_2y + a_3x + a_4 = 0$.

§2. Неподвижные точки действия конечной группы и ее подгрупп

Здесь доказывается одна из центральных теорем теории Галуа, согласно которой различные подгруппы конечной группы автоморфизмов поля имеют различные поля инвариантов. Доказательство опирается на простую явную конструкцию, использующую интерполяционный полином Лагранжа, и на геометрически очевидное утверждение, согласно которому векторное пространство нельзя покрыть конечным числом подпространств.

Начнем с геометрического утверждения. Пусть V — аффинное пространство (может быть, бесконечномерное) над некоторым полем.

Утверждение 2.1. *Пространство V не может быть представлено в виде объединения конечного числа своих собственных аффинных подпространств.*

Доказательство. Индукция по числу аффинных подпространств. Пусть утверждение доказано для объединения менее чем n собственных аффинных подпространств. Допустим, что пространство V представимо в виде объединения n собственных аффинных подпространств $V_1, \ldots, V_n$. Рассмотрим любую собственную аффинную гиперплоскость $\hat{V}$ в пространстве V, содержащую первое из этих подпространств V_1. Пространство V является объединением бесконечного семейства непересекающихся аффинных гиперплоскостей, параллельных гиперплоскости $\hat{V}$. Не более чем n гиперплоскостей этого семейства содержат одно из пространств $V_1, \ldots, V_n$. Возьмем любую другую гиперплоскость из семейства. К этой гиперплоскости и ее пересечениям с аффинными плоскостями $V_2, \ldots, V_n$ применимо индукционное предположение. Что и доказывает утверждение.

Следствие 2.2. *Пусть на векторном пространстве V действует конечная группа линейных преобразований. Тогда найдется вектор a, на орбите которого группа действует свободно.*

Доказательство. Множество неподвижных точек линейного преобразования является векторным подпространством. Для нетождественного линейного преобразования это подпространство является собственным. В качестве вектора a достаточно взять любой вектор, не принадлежащий объединению неподвижных подпространств нетривиальных преобразований группы.

Стационарной подгруппой $G_a \subset G$ вектора $a \in V$ называется подгруппа, состоящая из всех элементов $g \in G$, оставляющих вектор a неподвижным, т.е. таких, что $g(a) = a$.

Вообще говоря, не каждая подгруппа G_0 конечной группы G линейных преобразований является стационарной подгруппой некоторого вектора a. В качестве примера достаточно рассмотреть циклическую группу линейных преобразований комплексной прямой, порожденную оператором умножения на первообразный корень степени n из единицы. Если число n не является простым, то эта циклическая группа имеет нетривиальную подгруппу, но стационарные подгруппы всех элементов тривиальны (тождественная подгруппа для каждого элемента $a \neq 0$ и вся циклическая группа

для $a = 0$). Таким образом, существование вектора a, неподвижного лишь для преобразований из подгруппы G_0, не очевидно и верно не для всех представлений группы G.

Лемма 2.3. *Пусть G_a и G_b — стационарные подгруппы векторов a и b некоторого векторного пространства V. Тогда в подпространстве L, порожденном векторами a и b, существует вектор c, стационарная группа G_c которого равна $G_a \cap G_b$.*

Доказательство. Подгруппа $G_a \cap G_b$ оставляет неподвижными все векторы подпространства L. Однако каждый элемент $g \notin G_a \cap G_b$ нетривиально действует либо на вектор a, либо на вектор b. Векторы из L, неподвижные относительно действия фиксированного элемента $g \notin G_a \cap G_b$, образуют собственное подпространство в L. По утверждению 2.1, такие подпространства не могут покрыть все пространство L.

Пусть G — некоторая группа автоморфизмов поля P. Неподвижные элементы относительно действия группы G образуют подполе, которое мы обозначим через K. Поле P можно рассматривать как векторное пространство над полем K.

В теории Галуа важную роль играет следующая

Теорема 2.4. *Пусть G — некоторая конечная группа автоморфизмов поля P. Тогда для всякой подгруппы G_0 группы G существует элемент $x \in P$, стационарная подгруппа которого совпадает с подгруппой G_0.*

Для доказательства удобно воспользоваться пространством полиномов $P[t]$ с коэффициентами из поля P. Каждый элемент f пространства $P[t]$ имеет вид $f = a_0 + \cdots + a_m t^m$, где $a_0, \ldots, a_m \in P$. Полином $f \in P[t]$ задает отображение $f : P \to P$, переводящее точку $x \in P$ в точку $f(x) = a_0 + \cdots + a_m x^m$. Каждому автоморфизму σ поля P соответствует индуцированный автоморфизм кольца $P[t]$, переводящий полином $f = a_0 + \cdots + a_m t^m$ в полином $f^\sigma = \sigma(a_0) + \cdots + \sigma(a_m)t^m$. Для каждого элемента $x \in P$ справедливо тождество $f^\sigma(\sigma x) = \sigma(f(x))$. Итак, группа автоморфизмов G поля P действует на кольце $P[t]$. Для всякого $k \geq 0$ пространство $P_k[t]$ полиномов степени $\leq k$ инвариантно относительно этого действия.

Лемма 2.5. *Пусть группа автоморфизмов G поля P содержит m элементов. Тогда для всякой подгруппы G_0 группы G существует полином f степени, меньшей чем m, стационарная подгруппа которого совпадает с подгруппой G_0.*

Доказательство. Действительно, согласно следствию 2.2, существует элемент $a \in P$, на орбите O которого группа G действует свободно. В частности, орбита O содержит ровно m элементов. Пусть подгруппа G_0 содержит k элементов. Тогда в группе G есть $q = m/k$ правых классов смежности по подгруппе G_0. Под действием подгруппы G_0 множество O разбивается на q орбит O_j, $j = 1, \ldots, q$. Фиксируем q попарно различных элементов $b_1, \ldots, b_q$ поля инвариантов K и построим полином Лагранжа f степени $< m$, принимающий на всех элементах множества O_j значение b_j для $j = 1, \ldots, q$. Полином f удовлетворяет условиям леммы.

Действительно, полином f инвариантен относительно автоморфизма σ, если и только если для каждого элемента x поля P выполняется равенство $f(\sigma(x)) = \sigma(f(x))$. Так как полином f имеет степень $< m$ и множество O содержит m элементов, то равенство достаточно проверить для всех элементов x множества O. По построению полинома f, на всех элементах множества O выполняется равенство $f(\sigma(x)) = \sigma(f(x))$, если и только если $\sigma \in G_0$.

Вернемся к доказательству теоремы. Рассмотрим полином $f = a_0 + \cdots + a_{m-1}t^{m-1}$, стационарная погруппа которого равна G_0. Пересечение стационарных подгрупп коэффициентов $a_0, \ldots, a_{m-1}$ этого полинома совпадает с подгруппой G_0. Рассмотрим векторное пространство L над полем $K \subset P$ инвариантов относительно действия группы G, натянутое на коэффициенты $a_0, \ldots, a_{m-1}$. Согласно лемме 2.3, существует вектор $c \in L$, стационарная подгруппа которого равна G_0.

§3. Автомофризмы поля и соотношения между его элементами

В этом параграфе рассматривается конечная группа автоморфизмов поля. Доказываются две следующие теоремы теории Галуа.

Первая теорема (п. 3.2) утверждает, что каждый элемент поля алгебраичен над полем инвариантов.

Пусть y и z — два элемента поля. При каких условиях существует полином T с коэффициентами из поля инвариантов, такой, что $z = T(y)$? Вторая теорема (п. 3.4) утверждает, что полином T существует, если и только если стационарная группа элемента y принадлежит стационарной группе элемента z.

3.1. Уравнения с некратными корнями. Пусть $T(t)$ — полином над полем K, $T'(t)$ — его производная, $D(t)$ — наибольший общий делитель этих полиномов и $\tilde{T}$ — полином, определенный формулой $\tilde{T} = T/D$.

Утверждение 3.1. *1) Корень кратности $k > 0$ полинома $T(t)$ является корнем кратности $(k-1)$ полинома D. 2) Полином $\tilde{T}$ имеет те же корни, что и полином T, причем все корни полинома $\tilde{T}$ некратны.*

Доказательство. Пусть $T(t) = (t-x)^k Q(t)$ и $Q(x) \neq 0$. Тогда $T'(t) = k(t-x)^{k-1}Q(t) + (t-x)^k Q'(t)$. Отсюда следуют оба пункта утверждения 3.1.

Пусть мы хотим расширить некоторое поле K, добавив к нему один или несколько корней полинома T над полем K. Заменяя, если надо полином T на полином $\tilde{T}$, можно не ограничивая общности считать, что все корни полинома простые.

3.2. Алгебраичность над полем инвариантов. Пусть P — коммутативная алгебра без делителей нуля, на которой действует группа автоморфизмов π, и K — подалгебра инвариантов. Мы не предполагаем, что группа π конечна (хотя для теории Галуа достаточно рассматривать лишь действия конечных групп).

Теорема 3.2. *1) Стационарная подгруппа элемента $y \in P$, алгебраического над K, имеет конечный индекс в группе π. 2) Если стационарная подгруппа элемента $y \in P$ имеет индекс n в группе π, то y удовлетворяет над K неприводимому уравнению степени n с равным единице старшим коэффициентом.*

Доказательство. 1) Допустим, что элемент y удовлетворяет алгебраическому уравнению

$$p_0 y^n + \cdots + p_n = 0 \tag{6}$$

с коэффициентами p_i из алгебры инвариантов K. Тогда всякий автоморфизм алгебры P, оставляющий на месте элементы алгебры K, переводит элемент y в один из корней уравнения (6), а этих корней не более чем n, поэтому индекс в группе π стационарной подгруппы элемента y не превосходит n.

2. Пусть стационарная подгруппа G элемента y имеет индекс n в группе π. Тогда орбита элемента y относительно действия группы π содержит ровно n различных элементов. Обозначим через $y_1, \ldots, y_n$ элементы этой орбиты. Пусть $\sigma_1 = y_1 + \cdots + y_n$, $\sigma_2 = \sum_{i<j} y_i y_j$, $\ldots$, $\sigma_n = y_1 \ldots y_n$ — основные симметрические функции от элементов орбиты. Элементы $\sigma_1, \ldots, \sigma_n$ не меняются при перестановке точек $y_1, \ldots, y_n$ и принадлежат поэтому алгебре инвариантов K. Элемент y удовлетворяет алгебраическому уравнению

$$T(y) = y^n - \sigma_1 y^{n-1} + \sigma_2 y^{n-2} + \cdots + (-1)^n \sigma_n = 0.$$

Это уравнение неприводимо (т.е. полином T не раскладывается в произведение двух полиномов положительных стеней, коэффициенты которых лежат в алгебре K). Действительно, если оно приводимо, то y удовлетворяет уравнению меньшей степени над алгеброй K и орбита элемента y содержит меньше чем n элементов.

3.3. Подалгебра, содержащая коэффициенты полинома Лагранжа. В этом пункте рассматривается полином Лагранжа, построенный по специальным начальным данным, и оценивается подалгебра, содержащая его коэффициенты. Результаты применяются в пункте 3.4.

Пусть P — коммутативная алгебра без делителей нуля, $y_1, \ldots, y_n$ — различные элементы алгебры P и $Q \in P[y]$ — полином степени n с единичным старшим коэффициентом, обращающийся в нуль в точках $y_1, \ldots, y_n$, т.е. $Q(y) = (y - y_1) \ldots (y - y_n)$. Рассмотрим следующую задачу. Для заданных элементов $z_1, \ldots, z_n$ алгебры P найти полином Лагранжа T, принимающий в точках y_i значения $z_i Q'(y_i)$. (По определению, полином Q имеет некратные корни, т.е. $Q'(y_i) \neq 0$, и степень полинома Лагранжа T меньше, чем n.) Для формулировки ответа удобно воспользоваться рациональной функцией F, определенной тождеством $F(y) = \sum \dfrac{z_i}{y - y_i}$. Из явной формулы для полинома Лагранжа вытекает следующее

Утверждение 3.3. *Искомый полином Лагранжа T равен произведению QF полинома Q на рациональную функцию F. Коэффициенты полинома T принадлежат алгебре P, т.е. $T \in P[y]$.*

Замечание. При $P = \mathbb{C}$ задача допускает следующую переформулироку: найти полином T степени $< n$, такой, что 1-форма $\omega = T\dfrac{dy}{Q}$ имеет в точках $y_1, \dots, y_n$ вычеты $z_1, \dots, z_n$. Ясно, что форма ω равна $F(y)dy$. Поэтому $T = QF$.

Нам понадобится другая формула для полинома T, позволяющая точнее оценить подалгебру, содержащую его коэффициенты. Введем нужные обозначения. Для $k = 0, 1, \dots$ положим $m_k = \sum z_i y_i^k$. Обозначим через M полином от переменной y^{-1}, равный $\sum\limits_{k=0}^{n-1} m_k y^{-1-k}$. Представим произведение полиномов Q и M от переменных y и y^{-1} в виде $QM = L + L_-$, где L и L_- — суммы мономов полинома Лорана $QM \in K[y, y^{-1}]$, имеющих, соответственно, неотрицательные степени и строго отрицательные степени по переменной y.

Утверждение 3.4. *Полином T совпадает с определенным выше полиномом L.*

Доказательство. В кольце формальных рядов Тэйлора по степеням переменной y^{-1} с коэффициентами в алгебре P выполняются следующие равенства:

$$F(y) = y^{-1}\sum_{i=1}^{n} z_i(1 - y_i y^{-1})^{-1} = y^{-1}\sum_{k=0}^{\infty}\sum_{i=1}^{n} z_i y_i^k y^{-k} = y^{-1}\sum_{i=0}^{\infty} m_k y^{-k}.$$

(Если $P = \mathbb{C}$, то выписанный ряд является рядом Тэйлора рациональной функции F в точке ∞.) В кольце формальных рядов Лорана по переменной y^{-1} с коэффициентами в алгебре P выполняется равенство $T(y) = Q(y)y^{-1}\sum\limits_{i=0}^{\infty} m_k y^{-k}$, из которого вытекает, что $T = L$.

Из утверждения 3.4 вытекает следующее

Следствие 3.5. *Пусть подалгебра K алгебры P содержит коэффициенты полинома Q и элементы $m_0, \dots, m_{n-1}$, где $m_k = \sum z_i y_i^k$. Тогда коэффициенты полинома T принадлежат подалгебре K, т.е. $T \in K[y]$.*

3.4. Представимость одного элемента через другой над полем инвариантов. Пусть P — поле, на котором действует группа автоморфизмов π, и K — поле инвариантов. Пусть y и z — элементы поля P, алгебраические над полем K, и G_y, G_z — их стационарные подгруппы. Согласно теореме 3.2, элемент y (элемент z) алгебраичен над полем K, если и только если группа G_y (группа G_z) имеет конечный индекс в группе π. При каком условии z принадлежит расширению $K(y)$ поля K элементом y? Ответ на этот вопрос дает следующая

Теорема 3.6. *Элемент z принадлежит полю $K(y)$, если и только если стационарная подгруппа G_z элемента z содержит стационарную подгруппу G_y элемента y.*

Доказательство. В одну сторону теорема очевидна: каждый элемент поля $K(y)$ неподвижен при действии группы G_y. Другими словами, стационарная подгруппа каждого элемента поля $K(y)$ содержит группу G_y.

Обратное утверждение мы докажем в более сильной форме. Ослабим предположения в теореме 3.6. Будем предполагать, что P — коммутативная алгебра без делителей нуля (необязательно являющаяся полем), π — группа автоморфизмов алгебры P, K — алгебра инвариантов, y и z — элементы алгебры P, стационарные подгруппы G_y и G_z которых имеют конечный индекс в группе π. Обозначим через Q неприводимое целое алгебраическое уравнение над алгеброй K, которому удовлетворяет элемент y, $Q(y) = 0$ (см. пункт 2 теоремы 3.2).

Утверждение 3.7. *Если $G_z \supseteq G_y$, то существует полином T с коэффициентами в алгебре K, такой, что выполняется тождество $zQ'(y) = T(y)$.*

Доказательство. Обозначим через S множество правых классов смежности группы π по подгруппе G_y. Пусть множество S содержит n элементов. Занумеруем элементы $s_1, \ldots, s_n$ этого множества, присвоив классу единичного элемента группы π номер 1. Пусть g_i — любой представитель класса s_i в группе π. Образы $g_i(y)$, $g_i(z)$ элементов y, z при действии автоморфизма $g_1 \in \pi$ не зависят от выбора элемента g_i в классе s_i. Обозначим эти образы через y_i и z_i, соответственно. Все элементы $y_1, \ldots, y_n$ различны по построению, в то время как некоторые из элементов $z_1, \ldots, z_n$ могут совпадать. Для всякого целого неотрицательного k элемент $m_k = z_1 y_1^k + \cdots + z_n y_1^k$ инвариантен относительно действия группы π и, следовательно, принадлежит алгебре K. Для завершения доказательства осталось сослаться на следствие 3.5. Утверждение 3.7 и теорема 3.6 доказаны.

§4. Действие k-разрешимой группы и представимость в k-радикалах

В этом параграфе рассматривается поле P, на котором действует конечная группа автоморфизмов G с полем инвариантов K. Мы будем предполагать, что поле P содержит все корни из единицы. Вводится определение k-разрешимой группы. Мы докажем, что если группа G k-разрешима, то каждый элемент поля P выражается через элементы поля K с помощью радикалов и решения вспомогательных алгебраичеких уравнений, степень которых не превосходит k. Доказательство опирается на теоремы предыдущих пунктов.

Определение. Конечная группа G называется *k-разрешимой*, если у нее существует цепочка подгрупп

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{e\},$$

такая, что для каждого i, $0 < i \leq n$, либо индекс подгруппы G_i в группе G_{i-1} не превосходит k, либо подгруппа G_i — нормальный делитель в группе G_{i-1} и фактор-группа G_{i-1}/G_i коммутативна.

Теорема 4.1. *Пусть G — конечная k-разрешимая группа автоморфизмов поля P, содержашего все корни из единицы. Тогда каждый элемент x поля P выражается через элементы поля инвариантов K при помощи арифметических операций, извлечения корней и решения алгебраических уравнений степени, не выше чем k.*

Доказательство. Пусть $G = G_0 \supset \cdots \supset G_m = \{e\}$ — цепочка вложенных подгрупп, удовлетворяющая условиям, перечисленным в определении k-разрешимой группы. Обозначим через $K = K_0 \subset \cdots \subset K_m = P$ цепочку инвариантных полей относительно действия групп $G_0, \ldots, G_m$.

Пусть группа G_i является нормальным делителем группы G_{i-1}, и фактор-группа G_{i-1}/G_i коммутативна. Коммутативная фактор-группа G_{i-1}/G_i естественно действует на поле инвариантов K_i, оставляя неподвижным поле инвариантов K_{i-1}. Следовательно, каждый элемент поля K_i выражается при помощи суммирования и извлечения корней через элементы поля K_{i-1} (см. теорему 1.2 из пункта 1.1).

Пусть группа G_i является подгруппой индекса $m \leq k$ в группе G_{i-1}. Существует элемент $a \in P$, стационарная подгруппа которого равна G_i (теорема 2.4). На поле K действует группа автоморфизмов G_{i-1} с полем инвариантов K_{i-1}. Так как индекс стационарной подгруппы G_i элемента a в группе G_{i-1} равен m, то элемент a удовлетворяет алгебраическому уравнению степени $m \leq k$ над полем K_{i-1}. Согласно теореме 3.6, каждый элемент поля K_i является полиномом от a с коэффициентами из поля K_{i-1}.

Последовательно повторяя эти рассуждения, мы выразим каждый элемент поля P через элементы поля K с помощью арифметических операций, извлечения корней, решения алгебраических уравнений степени $\leq k$.

§5. Уравнения Галуа

Алгебраическое уравнение над полем K называется *уравнением Галуа*, если расширение поля K, полученное присоединением к K любого одного корня этого уравнения, содержит все остальные его корни. В этом параграфе доказывается, что для любого алгебраического уравнения над полем K существует уравнение Галуа, такое, что расширения поля K, полученные присоединением всех корней исходного уравнения, совпадает с расширением, полученным присоединением уравнения Галуа. Доказательство опирается на теорему 3.6 из п. 3.4. Уравнения Галуа удобны для построения группы Галуа (см. параграфы 6, 7).

Пусть K — любое поле. Обозначим через $\tilde{P}$ алгебру $K[x_1, \ldots, x_m]$ многочленов над полем K от переменных $x_1, \ldots, x_m$. На алгебре $\tilde{P}$ действует группа автоморфизмов π, изоморфная группе $S(m)$ перестановок m элементов: действие группы заключается в одновременной перестановке переменных $x_1, \ldots, x_m$ во всех многочленах из кольца $K[x_1, \ldots, x_m]$. Алгебра

инвариантов $\tilde{K}$ относительно этого действия состоит из симметрических многочленов от переменных $x_1, \ldots, x_m$.

Пусть $y \in \tilde{P}$ — некоторый многочлен от m переменных, орбита которого под действием группы $S(m)$ содержит ровно $n = m!$ различных элементов $y = y_1, \ldots, y_n$. Обозначим через Q полином над алгеброй $\tilde{K}$, корнями которого являются элементы $y_1, \ldots, y_n \in \tilde{P}$ (см. теорему 3.2). Производная полинома Q не обращается в нуль в его корнях $y_1, \ldots, y_n$. Применяя утверждение 3.7 к действию группы $S(m)$ на алгебре $\tilde{P}$ с алгеброй инвариантов $\tilde{K}$, получаем следующее

Следствие 5.1. *Для всякого элемента $F \in \tilde{P} = K[x_1, \ldots, x_m]$ существует полином T, коэффициенты которого — симметрические многочлены от переменных $x_1, \ldots, x_m$, такой, что выполняется тождество*

$$FQ'(y) = T(y).$$

Пусть $b_0 + b_1 x + \cdots + b_m x^m = 0$ — алгебраическое уравнение над полем K, $b_i \in K$, корни $x_1^0, \ldots, x_m^0$ которого попарно различны между собой. Пусть P — поле, полученное присоединением к полю K всех корней этого уравнения. Рассмотрим отображение $\pi\colon K[x_1, \ldots, x_m] \to P$, сопоставляющее каждому многочлену его значение в точке $(x_1^0, \ldots, x_m^0) \in P^m$.

Следствие 5.2. *Пусть $y \in K[x_1, \ldots, x_m]$ — такой многочлен, что все $n = m!$ многочленов, полученных из y всевозможными перестановками переменных, принимают различные значения в точке $(x_1^0, \ldots, x_m^0) \in P^m$. Тогда значение многочлена y в точке $(x_1^0, \ldots, x_m^0) \in P^m$ порождает поле P над полем K.*

Доказательство. Действительно, алгебраические элементы $x_1^0, \ldots, x_m^0$ порождают поле P над полем K. Поэтому каждый элемент поля P является значением некоторого многочлена из кольца $K[x_1, \ldots, x_m]$ в точке $x_1^0, \ldots, x_m^0$. Но согласно следствию 5.2, каждый многочлен F после умножения на $Q'(y)$ представляется в виде полинома T от y с коэффициентами из алгебры $\tilde{K}$. Подставим в соответствующее тождество $F(x_1, \ldots, x_m) = Q'(y)T(y)$ точку $(x_1^0, \ldots, x_m^0)$. По условию все $n = m!$ корней полинома Q в точке $(x_1^0, \ldots, x_m^0)$ различны между собой. Поэтому функция $Q'(y)$ в этой точке отлична от нуля, а значение симметрических полиномов в точке $(x_1^0, \ldots, x_m^0)$ принадлежат полю K (т.к. симметрические полиномы от корней уравнения выражаются через его коэффициенты).

Лемма 5.3. *Для любых попарно различных элементов $x_1^0, \ldots, x_m^0$ поля $P \supseteq K$ существует линейный многочлен $y = \lambda_1 x_1 + \cdots + \lambda_m x_m$ с коэффициентами $\lambda_1, \ldots, \lambda_m$ из поля K, такой, что все $n = m!$ многочленов, полученных из многочлена y перестановками переменных, принимают различные значения в точке $(x_1^0, \ldots, x_m^0) \in P^m$.*

Доказательство. Рассмотрим $n = m!$ точек, полученных из точки $(x_1^0, \ldots, x_m^0)$ всевозможными перестановками координат. Для каждой пары точек линейные многочлены, принимающие равные значения в этих точках, образуют собственное подпространство в пространстве линейных многочленов

с коэффициентами в поле K. Подпространства, соответствующие всевозможным парам точек, не могут покрывать всего пространства (утверждение 2.1). Любой линейный полином y, не лежащий в объединении описанных собственных подпространств, удовлетворяет условиям леммы.

Определение. Уравнение $a_0 + a_1 x + \cdots + a_m x^m = 0$ над полем K называется *уравнением Галуа*, если его корни $x_1^0, \ldots, x_m^0$ обладают следующим свойством: для любой пары корней x_i^0, x_j^0 найдется полином $P_{i,j}(t)$ над полем K, такой, что $P_{i,j}(x_i^0) = x_j^0$.

Теорема 5.4. *Пусть поле P получается из поля K при помощи присоединения всех корней алгебраического уравнения над полем K, не имеющего кратных корней. Тогда то же самое поле P можно получить из поля K, присоединяя один корень некоторого (вообще говоря, другого) неприводимого уравнения Галуа над полем K.*

Доказательство. По условию, все корни $x_1^0, \ldots, x_m^0$ уравнения попарно различны. Рассмотрим однородный линейный многочлен y с коэффициентами в поле K, такой, что все $n = m!$ линейных многочленов, полученных из многочлена y перестановкой переменных, принимают в точке $(x_1^0, \ldots, x_m^0)$ различные значения. Рассмотрим уравнение степени n над полем K, корнями которого являются эти значения. Согласно доказанному выше следствию, полученное уравнение является уравнением Галуа, а его корни порождают поле P. Полученное уравнение Галуа может оказаться приводимым. Приравнивая к нулю любой из неприводимых сомножителей, получим искомое неприводимое уравнение Галуа.

§6. Автоморфизмы, связанные с уравнением Галуа

В этом параграфе строится группа автоморфизмов расширения, полученного из исходного поля присоединением всех корней некоторого уравнения Галуа. Показывается (теорема 6.2), что поле инвариантов этой группы совпадает с полем коэффициентов.

Пусть $Q = b_0 + b_1 x + \cdots + b_n$ — неприводимый многочлен над полем K. Тогда все поля, порожденные над полем K одним корнем уравнения Q, изоморфны между собой и допускают следующее абстрактное описание: каждое такое поле изоморфно фактору кольца $K[x]$ по простому идеалу I_Q, порожденному неприводимым многочленом Q. Обозначим это поле через $K[x]/I_Q$.

Пусть M — расширение поля K, содержащее все n корней $x_1^0, \ldots, x_n^0$ уравнения $Q(x) = 0$. С каждым корнем x_i^0 свяжем поле K_i, являющееся расширением поля K при помощи корня x_i^0. Все поля K_i, $i = 1\ldots, n$, изоморфны между собой и изоморфны полю $K[x]/I_Q$. Обозначим через σ_i изоморфное отображение поля $K[x]/I_Q$ в поле K_i, оставляющее на месте элементы поля коэффициентов K и переводящее многочлен x в элемент x_i^0.

Лемма 6.1. *Пусть уравнение $Q = b_0 + b_1 x + \cdots + b_n x^n = 0$ неприводимо над полем K. Тогда образы $\sigma_i(a)$ элемента a поля $K[x]/I_Q$ в поле M при всех*

изоморфизмах σ_i, $i = 1, \ldots, n$, совпадают между собой, если и только если элемент a лежит в поле коэффициентов K.

Доказательство. Если $b = \sigma_1(a) = \cdots = \sigma_n(a)$, то $b = (\sigma_1(a) + \cdots + \sigma_n(a))n^{-1}$ (в рассматриваемом случае $n \neq 0$ в поле K). Поэтому элемент b является значением симметрического многочлена от корней $x_1^0, \ldots, x_n^0$ уравнения $Q(x) = 0$, т.е. элемент b принадлежит полю коэффициентов K.

Теперь все готово для доказательства основного утверждения этого пункта.

Теорема 6.2. *Пусть поле P полученно из поля K присоединением всех корней неприводимого алгебраического уравнения над полем K. Тогда элемент $b \in P$ неподвижен при всех автоморфизмах поля P, оставляющих неподвижными все элементы поля K, если и только если $b \in K$.*

Доказательство. Согласно теореме 5.4, можно считать, что поле P получено из поля K присоединением всех корней (или, что то же самое, одного корня) неприводимого уравнения Галуа. По определению уравнения Галуа, все поля K_i, о которых идет речь в доказанной выше лемме 6.1, совпадают между собой и совпадают с полем P. Изоморфизм $\sigma_j\sigma_i^{-1}$ поля K_i в поле K_j является автоморфизмом поля P, оставляющим неподвижными все элементы поля K. Согласно лемме, элемент $b \in P$ неподвижен при всех таких автоморфизмах, если и только если $b \in K$.

§7. Основная теорема теории Галуа

В параграфах 2, 3, 5 и 6, фактически, уже были доказаны центральные теоремы теории Галуа. В этом параграфе подводятся итоги. Определяются расширения Галуа (п. 7.1), группы Галуа (п. 7.2), доказывается основная теорема теории Галуа (п. 7.3), обсуждаются свойства соответствия Галуа (п. 7.4) и поведение группы Галуа при увеличении поля коэффициентов.

7.1. Расширения Галуа. Приведем два эквивалентных определения.

Определение 1. Поле P, полученное из поля K присоединением всех корней некоторого алгебраического уравнения над полем K, называется *расширением Галуа* поля K.

Определение 2. Поле P является *расширением Галуа* своего подполя K, если существует конечная группа автоморфизмов G поля P, полем инвариантов которой является поле K.

Утверждение 7.1. *Определения 1 и 2 эквивалентны. Группа G из определения 2 совпадает с группой всех автоморфизмов поля P над полем K. Следовательно, группа G определена однозначно.*

Доказательство. Если поле P является расширением Галуа поля K в смысле определения 1, то по теореме 6.2 поле P является расширением Галуа

поля P в смысле определения 2. Пусть теперь поле P является расширением Галуа поля K в смысле определения 2. Согласно следствию 2.2, существует элемент $a \in P$, который сдвигается с места любым нетривиальным элементом группы G. Рассмотрим орбиту O элемента a относительно действия группы G. Согласно теореме 3.2, существует алгебраическое уравнение над полем K, множество корней которого совпадает с O. Согласно теореме 3.6, любой из элементов орбиты, т.е. любой из корней этого алгебраического 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 решений 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.

7.2. Группы Галуа. Перейдем к группам Галуа — центральному объекту теории Галуа.

Группой Галуа расширения Галуа P поля K (или короче, группой Галуа поля P над полем K) называется группа всех автоморфизмов поля P над полем K. *Группой Галуа алгебраического уравнения* над полем K называется группа Галуа расширения Галуа P поля K, полученного присоединением к этому полю всех корней данного алгебраического уравнения.

Пусть поле P получается из поля K присоединением всех корней уравнения

$$a_0 + a_1 x + \cdots + a_n x^n = 0 \tag{7}$$

над полем K.

Каждый элемент σ из группы Галуа поля P над полем K переставляет корни уравнения (7). Действительно, применяя автоморфизм σ к равенству (7), получаем

$$\sigma(a_0 + a_1 x + \cdots + a_n x^n) = a_0 + a_1 \sigma(x) + \cdots + a_n (\sigma(x))^n = 0.$$

Таким образом, группа Галуа поля P над полем K имеет предствление в группе перестановок корней уравнения (7). Это представление точное: если автоморфизм оставляет неподвижными все корни уравнения (7), то он сохраняет на месте все элементы поля P и, следовательно, является тривиальным.

Определение. *Соотношением* между корнями уравнения (7), определенным над полем K, называется любой полином Q, принадлежащий кольцу $K[x_1, \ldots, x_n]$, который обращается в нуль в точке $(x_1^0, \ldots, x_n^0)$, где $x_1^0, \ldots, x_n^0$ — набор корней уравнения (7).

Утверждение 7.2. *Всякий автоморфизм из группы Галуа сохраняет все соотношения над полем K между корнями уравнения (7). Обратно, всякая перестановка корней, сохраняющая все соотношения между корнями, определенные над полем K, продолжаются до автоморфизма из группы Галуа.* (Таким образом, группу Галуа поля P над полем K можно отождествить с группой всех перестановок корней уравнения (7), сохраняющих все соотношения между корнями, определенные над полем K.)

Доказательство. Если перестановка $\sigma \in S(n)$ соответствует элементу группы Галуа, то полином σQ, полученный из соотношения Q перестановкой σ переменных $x_1, \ldots, x_n$, тоже обращается в нуль в точке $x_1^0, \ldots, x_n^0$. Обратно, пусть перестановка σ сохраняет все соотношения между корнями, определенные над полем K. Продолжим перестановку σ до автоморфизма поля P над полем K. Всякий элемент поля P является значением некоторого полинома Q_1, принадлежащего кольцу $K[x_1, \ldots, x_n]$, в точке $(x_1^0, \ldots, x_n^0)$. Значение автоморфизма σ на этом элементе естественно определить как значение полинома σQ_1, полученного из полинома Q_1 перестановкой переменных σ, в точке $(x_1^0, \ldots, x_n^0)$. Нужно проверить, что это определение корректно. Пусть Q_2 — другой полином из кольца $K[x_1, \ldots, x_n]$, значение которого в точке $(x_1^0, \ldots, x_n^0)$ совпадает со значением в этой точке полинома Q_1. Но тогда полином $Q_1 - Q_2$ является соотношением над полем K между корнями. Поэтому полином $\sigma Q_1 - \sigma Q_2$ тоже должен обратиться в нуль в точке $(x_1^0, \ldots, x_n^0)$, но это и означает, что автоморфизм σ определен корректно.

7.3. Основная теорема. 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. Это соответствие называется *соответствием Галуа.*

Теорема 7.3 (основная теорема теории Галуа). *Соответствие Галуа расширения Галуа является взаимно однозначным соответствием между множеством подгрупп группы Галуа и множеством промежуточных полей.*

Доказательство. Во-первых, согласно теореме 2.4, различные подгруппы группы Галуа имеют различные поля инвариантов. Во-вторых, если поле P является расширением Галуа поля K, то оно является расширением Галуа и всякого промежуточного поля. Это очевидно, если воспользоваться определением 1 расширения Галуа из п. 7.1. Из определения 2 расширения Галуа (там же) видно, что промежуточное поле является неподвижным полем для некоторой группы автоморфизмов поля P над полем K. Теорема доказана.

7.4. Свойства соответствия Галуа. Обсудим простейшие свойства соответствия Галуа.

Утверждение 7.4. *Промежуточное поле является расширением Галуа поля коэффициентов, если и только если при соответствии Галуа этому полю сопоставляется нормальный делитель группы Галуа. Группа Галуа промежуточного расширения Галуа над полем коэффициентов изоморфна факторгруппе группы Галуа исходного расширения по нормальному делителю, соответствующему промежуточному расширению Галуа.*

Доказательство. Пусть H — нормальный делитель группы Галуа G, и L_H — промежуточное поле, соответствующее подгруппе H. Поле L_H переходит в себя при действии автоморфизмов из группы G, т.к. множество неподвижных точек действия нормального делителя инвариантно относительно действия группы (утверждение 1.3). Группа автоморфизмов поля L_H, индуцированная действием группы G, изоморфна факторгруппе G/H. Поле инвариантов относительно действия на поле L_H индуцированной группы автоморфизмов совпадает с полем K. Итак, если H — нормальный делитель группы G, то L_H — расширение Галуа поля K с группой Галуа G/H.

Пусть K_1 — промежуточное расширение Галуа поля K. Поле K_1 получается из поля K присоединением всех корней некоторого алгебраического уравнения над полем K. Любой автоморфизм g из группы Галуа G лишь переставляет между собой корни этого уравнения и поэтому переводит поле K_1 в себя. Пусть поле K_1 соответствует подгруппе H, $K_1 = L_H$. Элемент g группы G переводит поле L_H в поле $L_{gHg^{-1}}$. Итак, 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 является нормальным делителем группы Галуа G.

Утверждение 7.5. *Наименьшее алгебраическое расширение поля K, содержашее два заданных расширения Галуа поля K, является расширением Галуа поля K.*

Доказательство. Наименьшее поле P, содержащее оба расширения Галуа, можно построить следующим образом. Пусть первое поле получается добавлением к полю K всех корней полинома Q_1, а второе поле — всех корней полинома Q_2. Поле P получается присоединением к полю K всех корней полинома $Q = Q_1Q_2$ и, следовательно, является расширением Галуа поля K.

Утверждение 7.6. *Пересечение двух расширений Галуа является расширением Галуа. Группа Галуа пересечения является фактор-группой группы Галуа каждого из исходных расширений Галуа.*

Доказательство. Пусть P — наименьшее поле, содержащее оба расширения Галуа. Как мы доказали, P — расширение Галуа поля K. Группа Галуа поля P над полем K переводит в себя как первое, так и второе расширение поля K. Следовательно, пересечение двух расширений Галуа также будет переводиться в себя действиями группы G. Поэтому, согласно утверждению 7.4, пересечение двух расширений Галуа будет расшире-

нием Галуа. Из того же утверждения вытекает, что группа Галуа пересечения является фактор-группой группы Галуа каждого из исходных расширений Галуа.

7.5. Изменение поля коэффициентов. Пусть

$$a_0 + a_1 x + \cdots + a_n x^n = 0 \tag{8}$$

— алгебраическое уравнение над полем K, и P — расширение Галуа поля K, полученное присоединением к полю K всех корней уравнения (8). Рассмотрим большее поле $\tilde{K} \supset K$ и его расширение Галуа $\tilde{P}$, полученное присоединением к полю $\tilde{K}$ всех корней уравнения (8). Как связана группа Галуа поля $\tilde{P}$ над $\tilde{K}$ с группой Галуа G поля P над K? Или, другими словами, что происходит с группой Галуа уравнения (8) при увеличении основного поля (т.е. при переходе от поля K к полю $\tilde{K}$)?

При увеличении поля коэффициентов группа Галуа уравнения, вообще говоря, уменьшается, т.е. заменяется некоторой подгруппой Галуа уравнения над исходным полем. Действительно, над бóльшим полем может быть больше соотношений между корнями уравнения (8). Приведем более точное утверждение.

Обозначим через K_1 пересечение полей P и $\tilde{K}$. Поле K_1 содержит поле K и лежит в поле 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 7.7. *Группа Галуа поля $\tilde{P}$ над полем $\tilde{K}$ изоморфна подгруппе G_1 в группе Галуа G поля P над полем K.*

Доказательство. Группа Галуа $\tilde{G}$ оставляет элементы поля K неподвижными (т.к. $K \subset \tilde{K}$) и переставляет корни уравнения (8). 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 гомоморфизма оставляет неподвижными все корни уравнения (8), т.е. ядро гомоморфизма 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 7.6, поле K_1 в этом случае также является расширением Галуа поля K. Обозначим через Γ_1 группу Галуа расширения K_1 поля K.

Теорема 7.8 (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 по этому нормальному делителю изоморфна факторгруппе группы Галуа нового поля коэффициентов $\tilde{K}$ над старым полем коэффитиентов K.*

Доказательство. Действительно, группа 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 фактор-группа G/G_1 изоморфна группе Галуа поля K_1 над полем K. Но группа Галуа поля K_1 над полем K изоморфна фактор-группе Γ/Γ_1. Теорема доказана.

§8. Критерий разрешимости уравнений в радикалах

Алгебраическое уравнение над полем K *разрешимо в радикалах*, если существует цепочка расширений $K = K_0 \subset K_1 \cdots \subset K_n$, в которой поле K_{j+1} получается из поля K_j, $j = 0, 1, \ldots, n-1$, присоединением радикала, а поле K_n содержит все корни исходного алгебраического уравнения. Решается ли заданное алгебраическое уравнение в радикалах? Теория Галуа была создана для ответа на этот вопрос.

В пункте 8.1 рассматривается группа корней n-й степени из единицы, лежащих в заданном поле K. В пункте 8.2 рассматривается группа Галуа уравнения $x^n = a$. В пункте 8.3 приводится критерий разрешимости алгебраического уравнения в радикалах (в терминах группы Галуа этого уравнения).

8.1. Корни из единицы. Пусть K — некоторое поле. Обозначим через K_E^* мультипликативную группу всех корней из единицы поля K (т.е. $a \in K_E^*$, если и только если $a \in K$ и для некоторого натурального n выполнено равенство $a^n = 1$).

Утверждение 8.1. *Если в группе K_E^* существует подгруппа, содержащая l элементов, то уравнение $x^l = 1$ имеет в поле K ровно l различных корней и рассматриваемая подгруппа образована всеми этими корнями.*

Доказательство. Каждый элемент x в любой группе порядка l удовлетворяет уравнению $x^l = 1$. В поле есть не более чем l корней такого уравнения, а группа по условию имеет ровно l элементов.

Из утверждения 8.1, в частности, вытекает, что в группе K_E^* есть не более одной циклической подгруппы любого заданного порядка l.

Утверждение 8.2. *Конечная абелева группа G, имеющая не более одной циклической подгруппы любого заданного порядка, является циклической группой. В частности, любая конечная подгруппа в группе K_E^* является циклической группой.*

Доказательство. Из классификации конечных абелевых групп легко видеть, что абелева группа, удовлетворяющая условию утверждения, с точностью до изоморфизма определяется числом m своих элементов: если $m = p_1^{k_1} \ldots p_n^{k_n}$ — разложение числа m на простые множители, то $G = (\mathbb{Z}/p_1^{k_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_n^{k_n}\mathbb{Z})$. Поэтому (см. утверждение 8.1) группы корней из единицы, содержащие заданное число элементов m, в различных полях изоморфны между собой. Но в поле комплексных чисел группа порядка m, состоящая из всех корней из единицы порядка m, очевидно, является циклической.

Циклическую группу из m элементов можно отождествить с аддитивной группой кольца вычетов по модулю m.

Утверждение 8.3. *Группа автоморфизмов группы $\mathbb{Z}/m\mathbb{Z}$ изоморфна мультипликативной группе обратимых элементов кольца вычетов по модулю m. В частности, эта группа автоморфизмов коммутативна.*

Доказательство. Автоморфизм F группы $\mathbb{Z}/m\mathbb{Z}$ однозначно определяется элементом $F(1)$, который, очевидно, должен быть обратим в мультипликативной группе кольца вычетов. Этот автоморфизм совпадает с умножением на $F(1)$.

Лемма 8.4. *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 циклическую группу по умножению. Преобразование из группы Галуа задает автоморфизм этой группы и целиком определяется этим автоморфизмом, т.е. группа Галуа вкладывается в группу автоморфизмов циклической группы. Теперь лемма 8.4 вытекает из утверждения 8.3.

8.2. Уравнение $x^n = a$.

Утверждение 8.5. *Пусть поле K содержит все корни степени n из единицы. Тогда группа Галуа уравнения $x^n - a = 0$ над полем K, где $0 \neq a \in K$, является подгруппой циклической группы из n элементов.*

Доказательство. Группа корней n-й степени из единицы циклическая (см. утверждение 8.2). Пусть ξ — любая образующая этой группы. Фиксируем любой корень x_0 уравнения $x^n - a = 0$. 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 $g(x_k) = g(\xi^k x_0) = \xi^{k+i} x_0 = x_{k+i}$ (напомним, что по предположению $\xi \in K$, поэтому $g(\xi) = \xi$). То есть всякое преобразование группы Галуа задает циклическую перестановку корней. Следовательно, группа Галуа вкладывается в циклическую группу из n элементов.

Лемма 8.6. *Группа Галуа G уравнения $x^n - a = 0$, $0 \neq a \in K$, над полем K обладает коммутативным нормальным делителем G_1, фактор-группа 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. Отсюда 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 группу Галуа уравнения $x^n = a$ над полем K_1. Согласно

утверждению 1.4, группа G_1 коммутативна. Группа G_1 является нормальным делителем группы G, т.к. поле K_1 является расширением Галуа поля K. Фактор-группа G/G_1 коммутативна, т.к. согласно лемме 8.4, группа Галуа поля K_1 над полем K коммутативна.

8.3. Разрешимость в радикалах. Спаведлив следующий критерий разрешимости алгебраических уравнений в радикалах.

Теорема 8.7 (критерий разрешимости уравнений в радикалах). *Алгебраическое уравнение над некоторым полем решается в радикалах, если и только если его группа Галуа разрешима.*

Доказательство. 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_{j+1} получается из поля K_j, $j = 0, 1, \ldots, n-1$, присоединением радикала, а поле K_n содержит все корни исходного алгебраического уравнения. Обозначим через G_j группу Галуа нашего уравнения над полем K_j. Проследим, что происходит с группой Галуа уравнения при переходе от поля K_i к полю K_{i+1}. Согласно теореме 7.8, группа G_{i+1} является нормальной подгруппой в группе G_i, причем, фактор-группа G_i/G_{i+1} является одновременно фактор-группой 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 8.6, группа Галуа поля K_{i+1} над полем K_i разрешима. (В случае, когда поле K содержит все корни из единицы, 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 фактор-группой G_i/G_{i+1}, а группа G_n тривиальна. (Если поле K содержит все корни из единицы, то фактор-группы G_i/G_{i+1} коммутативны.) Таким образом, если уравнение решается в радикалах, то его группа Галуа разрешима.

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 1.2, 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 элементы поля K. Теореме доказана.

§9. Критерий разрешимости уравнений в k-радикалах

Скажем, что алгебраическое уравнение над полем K *разрешимо в* k-

радикалах, если существует цепочка расширений $K = K_0 \subset K_1 \cdots \subset K_n$, такая, что для каждого j, $0 < j \leq n$, либо поле K_{j+1} получается из поля K_j присоединением радикала, либо поле K_{j+1} получается из поля K_j присоединением корня уравнения степени $\leq k$, а поле K_n содержит все корни исходного алгебраического уравнения. Решается ли заданное алгебраическое уравнение в k-радикалах? В этом параграфе дается ответ на этот вопрос. В пункте 9.1 обсуждаются свойства k-разрешимых групп. В пункте 9.2 доказывается критерий разрешимости уравнений в k-радикалах.

Начнем со следующего простого утверждения.

Утверждение 9.1. *Группа Галуа уравнения степени $m \leq k$ изоморфна подгруппе группы $S(k)$.*

Доказательство. Любой элемент группы Галуа 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 $S(k)$.

9.1. Свойства k-разрешимых групп. В этом пункте мы покажем, что k-разрешимые группы (см. §4) имеют свойства, аналогичные свойствам разрешимых групп. Начнем с леммы 9.2, характеризующей подгруппы группы $S(k)$.

Лемма 9.2. *Группа изоморфна подгруппе группы $S(k)$, если и только если у нее есть набор из $m \leq k$ подгрупп, такой, что: 1) пересечение подгрупп не содержит нормальных делителей группы, отличных от тривиального; 2) сумма индексов всех подгрупп не превосходит k.*

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

Обратно, пусть группа G обладает набором подгрупп, удовлетворяющим условиям леммы. Обозначим через P объединение множеств $P_i = \{P_i^j\}$ — множеств правых классов смежности P_i^j группы G по подгруппе G_i. Группа G обладает естественным действием на множестве P. Возникающее представление группы G в группу $S(P)$ точное, т.к. ядро этого представления лежит в пересечении подгрупп G_i. Группа $S(P)$ вкладывается в группу $S(k)$, т.к. число точек в множестве P равно сумме индексов подгрупп G_i.

Следствие 9.3. *Фактор-группа подгруппы симметрической группы $S(k)$ изоморфна подгруппе симметрической группы $S(k)$.*

Доказательство. 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.

Скажем, что *нормальный делитель* H в группе G *имеет глубину, не превосходящую* k, если в группе G существует подгруппа G_0 индекса, не превосходящего k, такая, что H является пересечением всех подгрупп, сопряженных с G_0.

Будем говорить, что *группа имеет глубину, не превосходящую* k, если ее единичный нормальный делитель имеет глубину $\leq k$.

Нормальной башней группы G называется вложенная цепочка подгрупп $G = G_0 \supset \cdots \supset G_n = \{e\}$, в которой каждая следующая группа является нормальным делителем в предыдущей группе.

Следствие 9.4. *Если группа G является подгруппой группы $S(k)$, то у группы G существует 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} является нормальным делителем группы G_i глубины, не превосходящей k.*

Доказательство. 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 $\Gamma_0 = F_0$, $\Gamma_1 = F_0 \cap F_1, \ldots, \Gamma_m = F_0 \cap F_1 \cap \cdots \cap F_m$ удовлетворяет требованиям следствия.

Лемма 9.5. *Группа G является k-разрешимой группой, если и только если у нее существует нормальная башня подгрупп $G = G_0 \supset G_1 \supset \cdots \supset G_n = \{e\}$, в которой для каждого i, $0 < i \leq n$, либо нормальный делитель G_i имеет в группе G_{i-1} глубину, не превосходящую k, либо фактор-группа G_{i-1}/Γ_i коммутативна.*

Доказательство. 1. Пусть у группы G есть нормальная башня $G = G_0 \supset G_1 \supset \cdots \supset G_n = \{e\}$, удовлетворяющая условиям леммы. Если для некоторого i нормальный делитель G_i в группе G_{i-1} имеет глубину $\leq k$, то у группы G_{i-1}/G_i есть цепочка подгрупп $G_{i-1}/G_i = \Gamma_0 \cdots \supset \Gamma_n = \{e\}$, такая, что индекс каждой следующей подгруппы в предыдущей не превосходит k. Для каждого такого номера i между группами G_{i-1} и G_i вставим цепочку подгрупп $G_{i-1} = \Gamma_{0,i} \supset \cdots \supset \Gamma_{0,i}$. Мы получим цепочку подгрупп группы G, удовлетворяющую определению k-разрешимой группы.

2. Пусть группа G — k-разрешима и $G = G_0 \supset G_1 \supset \cdots \supset G_n = \{e\}$ — цепочка подгрупп, удовлетворяющая условиям, перечисленным в определении k-разрешимой группы. Мы будем последовательно уменьшать подгруппы в цепочке. Пусть i — первый номер, для которого группа G_i не является нормальным делителем в группе G_{i-1}, а является подгруппой индекса i в этой группе. В этом случае у группы G_{i-1} есть нормальный делитель H, лежащий в подгруппе G_i, такой, что группа G_{i-1}/H изоморфна подгруппе группы $S(k)$. Действительно, в качестве H достаточно взять пересечение всех подгрупп в группе G_{i-1}, сопряженных с группой G_i. Изменим цепочку подгрупп $G = G_0 \supset G_1 \supset \cdots \supset G_n = \{e\}$ следуюшим образом: подгруппы с номерами, меньшими чем i, оставим без изменения. Каждую подгруппу G_j, $i \leq j$ заменим на группу $G_j \cap H$. Применим ту же процедуру к полученной цепочке подгрупп, и т.д. В

результате мы получим нормальную башню подрупп, удовлетворяющую условиям леммы.

Теорема 9.6. *1) Подгруппа и фактор-группа k-разрешимой группы являются k-разрешимыми группами. 2) Если группа имеет k-разрешимый нормальмый делитель, фактор-группа по которому k-разрешима, то группа тоже k-разрешима.*

Доказательство. Единственное неочевидное утверждение теоремы — это утверждение о фактор-группе. Оно легко вытекает из леммы 9.5.

9.2. Разрешимости в k-радикалах. Справедлив следующий критерий разрешимости уравнений в k-радикалах)

Теорема 9.7 (критерий разрешимости уравнений в k-радикалах). *Алгебраическое уравнение над некоторым полем решается в k-радикалах, если и только если его группа Галуа k-разрешима.*

Доказательство. 1. Пусть уравнение решается в k-радикалах. Нам надо показать, что группа Галуа уравнения k-разрешима. Это доказывается в точности так же, как разрешимость группы Галуа уравнения, решаемого в радикалах.

Пусть $K = K_0 \subset K_1 \subset \cdots \subset K_n$ — цепочка полей, связанная с решением уравнения в k-радикалах, и $G_0 \supset \cdots \supset G_n$ — цепочка групп Галуа уравнения над этими полями. Поле K_n, по условию, содержит все корни уравнения, поэтому группа G_n тривиальна и, следовательно, является k-разрешимой. Предположим, что группа G_{i+1} k-разрешима. Надо доказать, что группа G_i тоже k-разрешима.

Если поле K_{i+1} получается из поля K_i присоединением радикала, то группа Галуа поля K_{i+1} над полем K_i разрешима, и, следовательно, k-разрешима.

Если поле K_{i+1} получается из поля K_i присоединением всех корней уравнения степени $\leq k$, то то группа Галуа поля K_{i+1} над полем K_i — подруппа группы $S(k)$ (утверждение 9.1), и, следовательно, k-разрешима.

Согласно теореме 1.2, группа G_{i+1} является нормальной подгруппой в группе G_i, причем, фактор-группа G_i/G_{i+1} является одновременно фактор-группой группы Галуа поля K_{i+1} над полем K_i. Группа G_{i+1} k-разрешима по предположению. Группа Галуа поля K_{i+1} над полем K_i, как мы только что показали, k-разрешима. Воспользовавшись теоремой 9.6, получаем, что группа G_i k-разрешима.

2. Пусть группа Галуа G алгебраического уравнения над полем K 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 $\tilde{G}$ k-разрешима. Обозначим через $\tilde{P}$ поле, полученное из поля $\tilde{K}$ присоединением всех корней алгебраического уравнения. Группа $\tilde{G}$ действует на поле $\tilde{P}$ с полем инвариантов $\tilde{K}$. Согласно теореме 4.1, каждый элемент поля $\tilde{P}$ выражается через элементы поля $\tilde{K}$ при помощи

радикалов, арифметических операций и решения алгебраических уравнений степени $\leq k$. По определению поля $\tilde{K}$ каждый элемент этого поля выражается через корни из единицы и элементы поля K. Теореме доказана.

9.3. Неразрешимость общего уравнения степени $(k+1) > 4$ в k-радикалах. Пусть K — некоторое поле. Общее алгебраическое уравнение степени k с коэффициентами из поля K — это уравнение

$$x^k + a_1 x^{k-1} + \cdots + a_0 = 0, \tag{9}$$

коэффициенты которого — 'достаточно общие элементы' из поля K. Существуют ли формулы, включающие радикалы (k-радикалы) и переменные $a_1, \ldots, a_k$, которые при подстановке вместо переменных конкретных элементов $a_1^0, \ldots, a_k^0$ поля K дают решения уравнения $x^k + a_1^0 x^{k-1} + \cdots + a_0^0 = 0$?

Этот вопрос можно формализовать так. Общее алгебраическое уравнение можно рассматривать как уравнение над полем $K\{a_1, \ldots, a_k\}$ рациональных функций от k независимых переменных $a_1, \ldots, a_k$ с коэффициентами в поле K (при таком рассмотрении коэффициенты уравнения (7) — элементы $a_1, \ldots, a_k$ поля $K\{a_1, \ldots, a_k\}$). Теперь можно задаться вопросом о разрешимости уравнения (7) над полем $K\{a_1, \ldots, a_k\}$ в радикалах (или в k-радикалах).

Вычислим группу Галуа уравнения (7) над полем $K\{a_1, \ldots, a_k\}$. Рассмотрим еще один экземпляр $K\{x_1, \ldots, x_k\}$ поля рациональных функций от k переменных, наделенного группой автоморфизмов $S(k)$, действующей перестановками переменных $x_1, \ldots, x_k$. Поле инвариантов $K_S\{x_1, \ldots, x_k\}$ состоит из симметрических рациональных функций. По теореме о симметрических функциях, это поле изоморфно полю рациональных функций от переменных $\sigma_1 = x_1 + \cdots + x_k, \ldots, \sigma_n = x_1 \ldots x_k$. Поэтому отображение $F(a_1) = -\sigma_1, \ldots, F(a_n) = (-1)^n \sigma_n$ продолжается до изоморфизма $F : K\{a_1, \ldots, a_k\} \to K_S\{x_1, \ldots, x_k\}$. Отождествим поля $K\{a_1, \ldots, a_k\}$ и $K_S\{x_1, \ldots, x_k\}$ с помощью изоморфизма F. Из сопоставления формул Виета и формул для отображениа F видно, что при таком отождествлении переменные $x_1, \ldots, x_k$ становятся корнями уравнения (7), поле $K\{x_1, \ldots, x_k\}$ становится полем, полученным присоединением к $K\{a_1, \ldots, a_k\}$ всех корней уравнения (7), группа автоморфизмов $S(k)$ становится группой Галуа уравнения (7). Итак мы доказали следующее

Утверждение 9.8. *Группа Галуа уравнения (7) над полем $K\{a_1, \ldots, a_k\}$ изоморфна группе перестановок $S(k)$.*

Теорема 9.9. *Общее алгебраическое уравнение степени $k+1 > 4$ не решается при помощи радикалов и решения вспомогательных алгебраических уравнений степени $\leq k$.*

Доказательство. Группа $S(k+1)$ имеет следующую нормальную башню подгрупп: $\{e\} \subset A(k+1) \subset S(k+1)$, где $A(k+1)$ — знакопеременная группа. При $k+1 > 4$ группа $A(k+1)$ — простая группа. Группа $A(k+1)$

не является подгруппой группы $S(k)$, так как в группе $A(k+1)$ больше элементов, чем в группе $S(k)$. Поэтому при $k+1>4$ группа $S(k+1)$ не является k-разрешимой группой. Для завершения доказательства осталось сослаться на теорему 9.7.

В качестве следствия получаем следующую теорему.

Теорема (Абеля) 9.10. *Общее алгебраическое уравнение степени >4 не решается в радикалах.*

Замечание. Абель доказал свою теорему другим способом еще до возникновения теории Галуа. Его подход был развит Лиувиллем. Метод Лиувилля позволяет, например, доказывать, что многие элементарные интегралы не берутся в элементарных функциях (см. главу 1).

§10. Неразрешимость сложных уравнений при помощи более простых уравнений

Можно ли решить заданное сложное алгебраическое уравнение, используя в качестве допустимых операций решения других, более простых, алгебраических уравнений? Мы рассмотрели два точно поставленых вопроса такого рода: вопрос о разрешимости уравнений в радикалах (в котором более простые уравнения — это уравнения $x^n-a=0$) и вопрос о разрешимости уравнений в k-радикалах (в котором более простые уравнения — это уравнения $x^n-a=0$ и любые алгебраические уравнения степени $\le k$). В этом параграфе рассматривается общий вопрос о разрешимости сложных алгебраических уравнений при помощи более простых уравнений. В пункте 10.1 приводится постановка задачи о B-разрешимости уравнений и доказывается необходимое условие ее разрешимости. В пункте 10.2 обсуждаются классы групп, связанные с задачей B-разрешимости уравнений.

10.1. Необходимое условие разрешимости. Пусть B — некоторая совокупность алгебраических уравнений. Алгебраическое уравнение, определеное над полем K, автоматически определено и над любым большим полем K_1, $K\subset K_1$. Мы считаем, что совокупность алгебраических уравнений B вместе с каждым уравнением, определенным над полем K, содержит то же самое уравнение, рассматриваемое как уравнение, определенное над любым большим полем $K\subset K_1$.

Определение. Алгебраическое уравнение над полем K называется *разрешимым при помощи 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.

Является ли заданное алгебраическое уравнение B-разрешимым? Теория Галуа доставляет необходимое условие для B-разрешимости уравнений. В настоящем пункте мы обсудим это условие.

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

Утверждение 10.1. *Множество конечных групп $G(B)$ с каждой группой содержит все ее подгруппы.*

Доказательство. Пусть некоторое уравнение, определенное над полем K, принадлежит совокупности уравнений B. Пусть P — поле, полученное присоединением к полю K всех корней этого уравнения, G — группа Галуа поля P над полем K и $G_1 \subset G$ — подгруппа группу G. Обозначим через K_1 промежуточное поле, соответствующее подгруппе G_1. Группа Галуа рассматриваемого уравнения над полем K_1 совпадает с подгруппой G_1. По условию, совокупность уравнений B вместе со всяким уравнением, определенным над полем K, содержит то же самое уравнение над большим полем K_1.

Теорема 10.2 (необходимое условие B-разрешимости). *Если алгебраическое уравнение над полем K является B-разрешимым, то у его группы Галуа G существует нормальная башня подгрупп $G = G_0 \supset G_1 \cdots \supset G_1 = \{e\}$, каждая фактор-группа G_i/G_{i+1} относительно которой является фактор-группой 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 присоединением всех решений некоторого уравнения из совокупности B, а последнее поле K_n содержит все корни исходного алгебраического уравнения. Пусть $G = G_0 \supset \cdots \supset G_n = \{e\}$ — цепочка групп Галуа исходного уравнения над этой цепочкой полей. Покажем, что полученная цепочка подгрупп G_i удовлетворяет требованиям теоремы. Действительно, согласно теореме 7.8, группа G_{i+1} является нормальной подгруппой в группе G_i, причем, фактор-группа G_i/G_{i+1} является одновременно фактор-группой 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 $G(B)$.

10.2. Классы конечных групп. Пусть M — некоторое множество конечных групп.

Определение. *Пополнением* $\mathcal{K}(M)$ множества групп M назовем минимальный класс конечных групп, содержащий все группы из M и обладающий следующими свойствами:

1) класс $\mathcal{K}(M)$ вместе с каждой группой содержит все ее подгруппы;

2) класс $\mathcal{K}(M)$ вместе с каждой группой содержит все ее фактор-группы;

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

Доказанная выше теорема делает актуальной следующую задачу: для заданного множества M конечных групп описать его пополнение $\mathcal{K}(M)$. Напомним теорему Жордана–Гельдера. Нормальная башня $G = G_0 \supset \cdots \supset G_n = \{e\}$ группы G, называется *неуплотняемой*, если все факторгруппы G_i/G_{i+1} относительно этой башни являются простыми группами. Теорема Жордана–Гельдера утверждает, что *для всякой конечной группы G множество факторгрупп G_i/G_{i+1} относительно любой неуплотняемой нормальной башни группы G не зависит от выбора неуплотняемой башни* (и, следовательно, определено инвариантно).

Утверждение 10.3. *Группа G принадлежит классу $\mathcal{K}(M)$, если и только если каждая факторгруппа G_i/G_{i+1} относительно неуплотняемой нормальной башни группы G является факторгруппой подгруппы некоторой группы из множества M.*

Доказательство. Во-первых, по определению класса $\mathcal{K}(M)$, каждая группа G, удовлетворяющая условиям утверждения, лежит в классе $\mathcal{K}(M)$. Во-вторых, несложно проверить, что группы G, удовлетворяющие условиям утверждения, обладают свойствами 1–3 из определения пополнения множества групп M.

Следствие 10.4. *1. Пополнением множества всех конечных абелевых групп является класс всех конечных разрешимых групп.*

2. Пополнением множества групп, содержащего группу $S(k)$ и все конечные абелевы группы, является класс всех конечных k-разрешимых групп.

Замечание. Необходимые условия разрешимости алгебраических уравнений в радикалах и в k-радикалах являются частными случаями теоремы 10.2.