ГЛАВА

ТЕОРИЯ ГАЛУА И ТФКП

1. Алгебраические функции и теория Галуа

В этом параграфе излагаются классические факты, относяшиеся к теории алгебраических функций одной комплексной переменной, подчеркивается связь этих фактов с теорией Галуа.

Определение. Росток $y_a(x)$ аналитической функции в точке a сферы Римана $\overline{\mathbb{C}}$ называется *ростком алгебраической функции*, если он удовлетворяет некоторому уравнению

$$P(x,y) = p_0(x)y_a^n + p_1(x)y_a^{n-1} + \cdots + p_n(x) = 0, \tag{1}$$

в котором $p_i(x)$ — полиномы.

Уравнение (1) можно считать неприводимым. Действительно, если $P(x,y) = P_1(x,y)P_2(x,y) = 0$, то либо $P_1(x, y_a(x)) \equiv 0$, либо $P_2(x, y_a(x)) \equiv 0$. Обозначим через $D(x)$ дискриминант уравнения (1). Полином $D(x)$ и старший коэффициент $p_0(x)$ имеют конечные множества корней. Обозначим эти конечные множества, соответственно, через O_1 и O_2, а их объединение, к которому добавлена бесконечно удаленая точка, через O. Перечислим свойства ростка алгебраической функции.

Утверждение 1. *1. При подходе к точкам из конечного множества O функция $y(x)$ растет не быстрее чем степеным образом, т.е. для всякой точки $o \in O$ существуют вещественные константры c и α такие, что всякое значение $y(b)$многозначной аналитической функции в точке b, где b — достаточно близкая точка к точке o удовлетворяет неравенству $|y(b)| \le cr^\alpha$, где r — расстояние от точки b до точки o.*

2. Росток $y_a(x)$ аналитически продолжается вдоль любой вещественной кривой $\gamma(t)$, $\gamma(0) = a$, не пересекающей множество O при $t > 0$.

3. Многозначная аналитическая функция, определенная ростком $y_a(x)$, в каждой точке имеет не более чем n различных значений.

Доказательство. 1. Каждый корень y алгебраического уравнения

$$p_0y^n + p_1y^{n-1} + \cdots + p_n = 0, \tag{*}$$

с комплексными коэффициентами p_i и ненулевым старшим коэффициентом $p_0 \neq 0$, для которого $|y| > 1$, хотя бы для одного k, $k = 1, \ldots, n$, удовлетворяет неравенству $|y|^k \le |p_k/p_0|/n$. Действительно, если ни одно из этих неравенств не выполнено, то число $|p_0y^n|$ будет больше числа $|p_1y^{n-1} + \cdots + p_n|$

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

и равенство (*) не может выполняться. Каждая из рациональных функций $p_k(x)/p_0(x)$ при подходе к особым точкам растет степенным образом, откуда и вытекает нужное утверждение.

2. Если $x \notin O$ и точка (x, y) удовлетворяет уравнению (1) $P(x, y) = 0$, то в точке (x, y) частная производная $\dfrac{\partial P}{\partial y}$ не обращается в нуль. Действительно, в точке x, для которой уравнения $P(x, y) = 0$ и $\dfrac{\partial P}{\partial y}(x, y) = 0$ совместны и старший коэффициент $p_0(x)$ не обращается в нуль, дискриминант $D(x)$ равен нулю. Поэтому для всякого решения уравнения $P(x, y) = 0$, лежащего над точкой $x \notin O$ выполнено условие теоремы о неявной функции. Всякую ветку $y(x)$ решения этого уравнения можно аналитичести продолжать до тех пор, пока точка x не попадает в множество O. Действительно, согласно пункту 1 в дополнении к любой окрестности множества O все значения многозначной функции $y(x)$ ограничены и поэтому ни одна из ветвей этой функции не уходит в бесконечность.

3. Аналитическое продолжение ростка $y_a(x)$ удовлетворяет уравнению (1). Алгебраическое уравнение (1) при фиксированном значении x имеет не более n решений, откуда вытекает нужное утверждение.

Покажем, что всякая многозначная аналитическая функция на сфере Римана, удовлетворяющая условиям утверждения 1, является алгебраической.

Утверждение 2. *Если для ростка $y_a(x)$ существует конечное множество O такое, что росток y_a и множество O удовлетворяют условиям утверждения 1, то найдется полином $P(x, y)$ такой, что $P(x, y_a(x)) \equiv 0$.*

Доказательство. Пусть $y_{1,a}(x), \ldots, y_{n,a}(x)$ — все ростки многозначной аналитической функции, порожденной ростком y_a над точкой x, $x \notin O$. Обозначим через $\sigma_1 = y_{1,a} + \cdots + y_{n,a}$, $\sigma_2 = \sum_{i<j} y_{i,a}y_{j,a}$, ..., $\sigma_n = y_{1,a} \ldots y_{n,a}$ основные симметрические функции от этих ростков. Покажем, что σ_i — ростки рациональных функций. Действительно,

1) росток σ_i аналитически продолжается вдоль любой кривой, не пересекающей конечное множество O, т.к. ростки $y_{i,a}$ по условию обладают этим свойством;

2) σ_i — ростки однозначных функций, аналитических в дополнении к множеству O; т.к. перестановка листов многозначной аналитической функции не меняет значения симметрической функции от этих листов;

3) функции σ_iпри подходе к точкам множества O растут не быстрее, чем степенным образом, т.к. по условию ростки $y_{i,a}$ обладают этим свойством;

4) функции σ_i рациональны, т.к. аналитическая функция вне конечного множества точек на сфере Римана, которая при подходе к этим точкам растет не более, чем степенным образом, является рациональной.

Теперь утверждение 2 доказано, т.к. росток $y_a(x)$ удовлетворяет алгебраическому уравнению

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

коэффициенты которого $\sigma_i(x)$ — рациональные функции. Умножая это уравнение на общий делитель знаменателей этих рациональных функций, получим искомое полиномиальное уравнение для ростка $y_a(x)$.

Доказательство утверждения 2 содержит чисто алгебраическое рассуждение. Выделим его отдельно. Пусть K — коммутативная алгебра без делителей нуля, на которой действует группа автоморфизмов π, и K_0 — подалгебра инвариантов, т.е. подалгебра в алгебре K, состоящая из всех элементов, остающихся неподвижными при действии всех элементов из группы π. Пусть y — элемент алгебры K, и Γ - его стационарная подгруппа (т.е. подгруппа группы π, состоящая из всех преобразований этой группы, оставляющих y неподвижным).

Утверждение 3. *Элемент y алгебры K удовлетворяет полиномиальному уравнению с коэффициентами из алгебры инвариантов K_0, если и только если его стационарная подгруппа Γ имеет конечный индекс в группе π.*

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

$$(**) \qquad p_0 y^n + \cdots + p_n = 0$$

с коэффициентами p_i из алгебры инвариантов K_0. Тогда всякий автоморфизм алгебры K, оставляющий на месте элементы алгебры K_0, переводит элемент y в один из корней уравнения $(**)$, а этих корней не более чем n, поэтому индекс в группе π стационарной подгруппы Γ элемента y не превосходит n.

2. Пусть стационарная подгруппа Γ элемента y имеет индекс n в группе π. Тогда орбита элемента y относительно действия группы π содержит n элементов. Обозначим через $y_1, \ldots, y_n$ элементы этой орбиты. Пусть $\sigma_1 = y_1 + \cdots + y_n$, $\sigma_2 = \sum_{i<j} y_i y_j$, ..., $\sigma_n = y_1 \ldots y_n$ — 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_0. Осталось заметить, что элемент y удовлетворяет алгебраическому уравнению

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

Чтобы из утверждения 3 вывести утверждение 2, достаточно рассмотреть алгебру $K(a, O)$ ростков аналитических функций в точке $a \notin O$, которые аналитически продолжаются вдоль любой вещественной кривой, не пересекающей множество O и продолжение которых растут не быстрее чем степенным образом при подходе к точкам из множества O. Обозначим через $K_0(a, O)$ подалгебру алгебры $K(a, O)$, состоящую из ростков однозначных функций $\overline{\mathbb{C}} \setminus O$. Мы используем следующий аналитический факт: все функции из подалгебры $K_0(a, O)$ рациональны. По модулю этого аналитического факта утверждение 2 полностью сводится к утверждению 3. Действительно, на алгебре $K(a, O)$ действует фундаментальная группа π области $\overline{\mathbb{C}} \setminus O$ с алгеброй инвариантов $K_0(a, O)$. Это действие каждому ростку $y_a \in K(a, O)$ и петле $\gamma \in \pi$ сопоставляет росток $\gamma(y_a)$, получающийся при продолжении ростка y_a вдоль кривой γ. Описанное действие группы π является автоморфизмом алгебры $K(a, O)$, поскольку аналитическое продолжение сохраняет арифметические операции (например, для операции сложения это означает, что сумма аналитических продолжений двух ростков равняется аналитическому продолжению их суммы).

Утверждение 4. *Ростки аналитических функций в точке $a \in \overline{\mathbb{C}}$, являющиеся ростками алгебраических функций, образуют кольцо. Если росток y_a принадлежит этому кольцу и значение этого ростка в точке a не равно нулю, то росток y_a^{-1} тоже принадлежит этому кольу.*

Доказательство. Пусть ростки y_a и z_a вместе с конечными множествами O_1 и O_2 удовлетворяют условиям утверждения 1, тогда ростки $y_a + z_a$ и $y_a z_a$ тоже удовлетворяют условиям утверждения 1 для конечного множества $O = O_1 \cup O_2$. Далее, если росток y_a удовлетворяет полиномиальному уравнению (1), то росток $z_a = y_a^{-1}$ удовлетворяет уравнению

$$p_0(x) + p_1(x)z_a + \cdots + p_n(x)z_a^n = 0.$$

Фиксируем росток y_a алгебраической функции и рассмотрим всевозможные ростки z, являющиеся рациональной функцией от ростка y_a с коэффициентами из поля рациональной функции от x. Всевозможные такие ростки z_a образуют поле. Обозначим через O множество особых точек ростка y_a, через π фундаментальную группу дополнения сферы Римана до множества O,состоящую из петель, имеющих начало и конец в точке a, и через Γ подгруппу π, состоящую из петель, продолжение вдоль которых не меняет ростка y_a. Ясно, что росток z_a, являющийся рациональной функцией от ростка y_a, обладает следующими свойствами:

1) росток z_a мероморфно продолжается вдоль любой кривой $\gamma(t)$, $\gamma(0) = a$, не пересекающей множество O, $\gamma(y) \notin O$ при $t > 0$;

2) продолжение вдоль кривых из группы Γ не меняет значения ростка z_a.

Оказывается, что условия 1) и 2) являются не только необходимыми, но и достаточными условиями представимости алгебраического ростка z_a в виде рациональной функции от алгебраического ростка y_a. Именно, справедлива следующая

Теорема 1. *Пусть алгебраический росток z_a удовлетворяет приведенным выше свойствам 1)–2). Тогда росток z_a предствим в виде рациональной функции от ростка y_a, коэффициенты которой являются растиональными функциями от x.*

Эту теорему обычно формулируют в другом эквивалентним виде: *всякая мероморфная функция на римановой поверхности алгебраической функции $y(x)$ явлуается рациональной функцией от x и y.* Доказательство сформулированной теоремы является чисто алгебраическим, причем соответствующе алгебраическое рассуждение играет центральную роль в теории Галуа. Ниже мы приведем это алгебраическое рассуждение и покажем, как из него вытекает приведенная выше теорема.

Пусть K — поле, на котором действует конечная группа автоморфизмов π, и K_0 — поле инвариантов, т.е. подполе в поле K, состоящее из всех элементов, остающихся неподвижными при дей ствии группы π. Пусть y и z — элементы поля K, и Γ_1, Γ_2 — их стационарные подгруппы (т.е. подгруппы группы Γ, состоящей из всех преобразований этой группы, оставляющих неподвижными, соответственно, y и z).

Теорема 2. *Элемент z принадлежит полю $K_0(y)$, являющемуся расширением поля инвариантов при помощи элемента y, если и только если стационарная подгруппа Γ_2 точки z содержит в стационарную подгруппу Γ_1 элемента y.*

Доказательство. Очевидно, что стационарная подгруппа каждого элемента поля $K_0(y)$ содержит группу Γ_1. Надо доказать обратное утверждение. Пусть $\Gamma_2 \supseteq \Gamma_1$. Обозначим через S множество правых классов смежности группы π по подгруппе Γ_1. Пусть множество S содержит n элементов. Занумеруем элементы $s_1, \dots, s_n$ этого множества, присвоив классу еденичного 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 Обозначм эти образы через y_i и z_i, соответственно. Ясно, что все элементы $y_1, \dots, y_n$различны (иначе стационарная группа элемента $y = y_1$ будет больше чем Γ_1), в то время как некоторые из элементов $z_1, \dots, z_n$ могут совпадать. Для всякого целого неотрицательного k элемент $a_k = z_1 y_1^k + \dots + z_n y_1^k$ будет инвариантен относительно действия группы π и, следовательно, будет принадлежать полю K_0. Для $k = 1, \dots, n-1$ имеем

$$
(2) \qquad \begin{array}{ccccccc}
z_1 & + & \dots & + & z_n & = & a_0; \\
z_1 y_1 & + & \dots & + & z_n y_n & = & a_1; \\
\vdots & & \ddots & & \vdots & & \vdots \\
z_1 y_1^{n-1} & + & \dots & + & z_n y_n^{n-1} & = & a_n.
\end{array}
$$

Рассмотрим (2) как систему н линейных уравнений с неизвестными $z_1, \dots, z_n$.

Определитель W этой системы отличен от нуля, т.к. является определителем Вандермонда различных элементов $y_1, \dots, y_n$. Решая систему (2) по правилу Крамера, получим $z = z_1 = \dfrac{W(a)}{W}$, где

$$
W(a) = \begin{vmatrix}
a_0 & 1 & \dots & 1 \\
\vdots & \vdots & \ddots & \vdots \\
a_n & y_2^{n-1} & \dots & y_n^{n-1}
\end{vmatrix},
$$

или $z = \dfrac{W(a)W}{W^2}$

Покажем, что найденное представление для элемента z и дает его выражение в виде рациональной функции элемента $y = y_1$. Обозначим через $\sigma_1 = y_1 + \dots + y_n$, ... , $\sigma_n = y_1 \dots y_n$ основные симметрические функции от $y_1, \dots y_n$ и через $\tilde{\sigma}_1 = y_2 + \dots + y_n$ ... $\tilde{\sigma}_{n-1} = y_2 \dots y_n$ основные симметрические функции от элементов $y_2, \dots, y_n$. Элементы $\sigma_1, \dots, \sigma_n$ из поля K инвариантны при действии группы π и принадлежат, следовательно, полю инвариантов K_0. Покажем, что все элементы $\tilde{\sigma}_1, \dots, \tilde{\sigma}_{n-1}$ принадлежат расширению поля K_0 элементом $y = y_1$. Действительно, очевидны следующие соотношения:

$$
\begin{aligned}
&\sigma_1 = y_1 + \tilde{\sigma}_1, \\
&\sigma_k = y_1 \tilde{\sigma}_{k-1} + \tilde{\sigma}_k \quad \text{при } n > k > 0, \\
&\sigma_n = y_1 \tilde{\sigma}_{n-1}.
\end{aligned}
$$

Эти соотношения можно рассматривать как линейную треугольную систему уравнений для нахождения $\tilde{\sigma}_i$ через σ_i и y_1. Определитель этой системы равен единице. Решая ее, убеждаемся, что элементы $\tilde{\sigma}_i$ лежат в поле $K_0(y)$. Вернемся к нашему представлению $z = \dfrac{W(a)W}{W^2}$. Элемент W^2 не меняется при перестановках $y_1, \ldots, y_n$ и поэтому лежит в поле K_0 Элемент W_aW не меняется при перестановках элементов $y_2, \ldots, y_n$. Поэтому он полиномиально выражается через эленемты $\tilde{\sigma}_1, \ldots \tilde{\sigma}_{n-1}$ и, следовательно, лежит в поле $K_0(y_1)$. Теорема 2 доказана.

Чтобы из теоремы 2 вывести теорему 1, достаточно рассмотреть поле $M(a, O)$ ростков мероморфных функций в точке $a \notin O$, которые мероморфно продолжаются вдоль любой вещественной кривой, не пересекающей множество O и которые растут не быстрее чем степенным образом при подходе к точкам из множества O. Обозначим через $M_0(a, O)$ подполе поля $M(a, O)$, состоящее из ростков мероморфных однозначных функций в $\overline{\mathbb{C}} \setminus O$. Мы используем следующий аналитический факт: все функции из подполя $M_0(a, O)$ рациональны. По модулю этого аналитического факта теорема 1 полностью сводится к теореме 2. Действительно, на поле $M(a, O)$ действует фундаментальная группа π области $\overline{\mathbb{C}} \setminus O$ с полем инвариантов $M_0(a, O)$. Это действие каждому ростку $y_a \in M(a, O)$ и петле $\gamma \in \pi$ сопоставляет росток $\gamma(y_a)$, получающийся при мероморфном продолжении ростка y_a вдоль кривой γ. Описанное действие группы π является автоморфизмом поля $M(a, O)$, посколько мероморфное продолжение сохраняет арифметические операции.