ПОМИ ПРЕПРИНТ — 09/2002

КРИТЕРИЙ НЕРАЗРЕШИМОСТИ В РАДИКАЛАХ НЕПРИВОДИМОГО УРАВНЕНИЯ ПРОСТОЙ СТЕПЕНИ

Б. Б. Лурье

Российская Академия Наук
Математический институт
им. В. А. Стеклова
Санкт-Петербургское отделение
РОССИЯ, 191011, С.-Петербург
наб. р.Фонтанки, 27

3 июня 2002

ABSTRACT

A sufficient condition under which an irreducible equation of prime degree is unsolvable in radicals is obtained. This condition is that the discriminant of an equation cannot be expressed as the sum of two squares in the ground field. For an equation of degree 5 this condition implies that the Galois group is $\mathfrak{S}_5$.

1. Напомним вначале хорошо известные факты из классической теории Галуа (см. [1]–[5]).

Пусть $f(x)$ – многочлен простой нечетной степени p над полем k, и пусть L – поле разложения многочлена f. Мы можем считать L сепарабельным расширением поля k (расширением первого рода), поскольку многочлен простой степени, дающий несепарабельное расширение, является двучленным, и дальнейшее рассмотрение бессодержательно. Неприводимость многочлена f означает, что группа Галуа G расширения L/k транзитивна на множестве корней f. Когда степень f – простое число, группа галуа G содержит "длинный цикл", т.е. при надлежащей нумерации корней некоторый автоморфизм $\sigma \in G$ переводит корни многочлена $(x_1, x_2, \dots, x_p)$ в $(x_2, x_3, \dots, x_p, x_1)$ соответственно.

Предположим теперь, что G – разрешимая подгруппа симметрической группы $\mathfrak{S}_p$. Тогда G является подгруппой т.н. "полной метациклической" группы H, также разрешимой и определенной с точностью до изоморфизма. Именно, при некоторой нумерации корней группа H порождается "длинным циклом" σ и циклом τ длины $p-1$, причем $\tau^{-1}\sigma\tau = \sigma^j$, где j – первообразный индекс по модулю p, т.е. $p-1$ – наименьший натуральный показатель, для которого $j^{p-1} \equiv 1 (\operatorname{mod} p)$. Заметим, что H – голоморф группы порядка p.

Дискриминант D уравнения $f(x) = 0$ принадлежит полю k и выражается в виде некоторого определителя матрицы порядка $2p-1$, составленной из коэффициентов многочлена. Группа Галуа G уравнения содержится в знакопеременной группе $\mathfrak{A}_p$ в том и только том случае, когда дискриминант уравнения D является квадратом в поле k.

2. Перейдем к изложению основного результата данной работы.

Пусть G – разрешимая группа Галуа неприводимого уравнения $f(x) = 0$ простой степени p над полем k, характеристика которого не равна 2, и пусть G *не содержится в знакопеременной группе* $\mathfrak{A}_p$. Обозначим G_0 пересечение G и $\mathfrak{A}_p$. Тогда G_0 – нормальная подгруппа в G индекса 2, и отвечающее ей подполе K_0 в поле разложения L многочлена f является квадратичным расширением поля k, полученным присоединением квадратичного корня из дискриминанта D.

Таким образом, квадратичное расширение K_0/k погружается в поле L с группой Галуа G над K. При этом автоморфизм $\sigma \in G$, ограниченный на поле K_0, является тождественным, когда σ – четная подстановка корней многочлена f, и переводит $\sqrt{D}$ в $-\sqrt{D}$, когда σ – нечетная подстановка. Иначе говоря, L является решением задачи погружения $(K_0/k, G, \varphi)$, где φ – указанный выше морфизм G на группу Галуа квадратичного расширения K_0/k (см. [6]).

Возникшая задача погружения является довольно простой и хорошо изученной. Силовская 2-подгруппа группы G является циклической порядка q, где q – максимальная степень числа 2, делящая $p-1$. А сама группа G, как подгруппа полной метациклической группы, представляется как полупрямое расширение нормальной подгруппы нечетного порядка посредством циклической 2-группы. Поэтому задача погружения $(K_0/k, G, \varphi)$ эквивалентна задаче с 2-группами $(K_0/k, G_2, \varphi)$, где G_2 – циклическая 2-группа, порядок которой делит $p-1$. (Впрочем, для наших целей вполне достаточно и того, что из разрешимости задачи $(K_0/k, G, \varphi)$ следует разрешимость задачи погружения $(K_0/k, G_2, \varphi)$.)

При $p \equiv -1 (\operatorname{mod} 4)$ группа G_2 имеет порядок 2, и поэтому задача погружения $(K_0/k, G_2, \varphi)$ бессодержательна. Но при $p \equiv 1 (\operatorname{mod} 4)$ ядро задачи погружения $\operatorname{Ker} \varphi$

не единичное, и разрешимость такой задачи не гарантируется при произвольных поле k и дискриминанте D.

Итак, нами доказана основная теорема.

Основная теорема. *Пусть f – многочлен простой степени $p \equiv 1 (\mathrm{mod}\, 4)$ над полем k, характеристика которого не равна 2, и пусть его группа Галуа G разрешима и содержит нечетную подстановку корней. Тогда является разрешимой задача погружения квадратичного расширения $k(\sqrt{D})$ в поле с циклической группой порядка q, где q – максимальная степень 2, делящая $p-1$.*

3. Выведем интересное следствие из доказанной теоремы. Сопутствующей (см. [6]) для нашей задачи погружения $(K_0/k, G_2, \varphi)$ является задача погружения квадратичного расширения $K_0 = k(\sqrt{D}))$ в поле с циклической группой порядка 4 (при $p \equiv 1(\mathrm{mod}\, 4)$. Соответственно, и эта задача погружения должна иметь решение.

Условие погружаемости квадратичного расширения $k(\sqrt{D})$ в расширение с циклической группой порядка 4 легко вычисляется и хорошо известно (см. [6]). Оно состоит в том, что D является суммой двух квадратов из поля k (т.е. $D = u^2 + v^2$, где $u, v \in k$). Заметим также, что когда группа Галуа многочлена f содержится в знакопеременной группе $\mathfrak{A}_p$, дискриминант D сам является квадратом в поле k, а значит, и суммой двух квадратов. Таким образом, мы получили следующий критерий неразрешимости уравнения степени $p \equiv 1(\mathrm{mod}\, 4)$ в радикалах.

Критерий неразрешимости. *Для того, чтобы неприводимое уравнение $f(x) = 0$ простой степени $p \equiv 1(\mathrm{mod}\, 4)$ над полем k было неразрешимо в радикалах, достаточно, чтобы его дискриминант не представлялся в виде суммы двух квадратов из k.*

(Заметим, что в этой формулировке говорить о характеристике поля k излишне, поскольку произведение сумм корней $\prod\limits_{i<j}(x_i+x_j)$ принадлежит k, и D является квадратом в случае характеристики 2.)

Для $p = 5$ этот результат может быть уточнен. Симметрическая группа $\mathfrak{S}_5$ имеет единственную собственную транзитивную подгруппу, не содержащуюся в знакопеременной группе, а именно полную метациклическую (порядка 20). Тем самым, для уравнений пятой степени имеет место следующий результат.

Теорема. *Для того, чтобы неприводимое уравнение пятой степени над полем k имело симметрическую группу Галуа, достаточно, чтобы его дискриминант не был суммой двух квадратов.*

Это дает возможность без труда строить примеры многочленов с симметрической группой Галуа.

Пример. Уравнение $x^5 - x + 1 = 0$ неприводимо. Его дискриминант равен

$$4^4(-1)^5 + 5^5 \cdot 1^4 = 2869 = 19 \cdot 151.$$

Значит, данное уравнение над $\mathbb{Q}$ имеет симметрическую группу (факт хорошо известный и ранее, но его доказательство было весьма громоздким).

Литература

1. F. Klein, *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade.* Leipzig, 1884. Перевод: Ф. Клейн, Лекции об икосаэдре и решениии уравнений пятой степени, М., 1989) .
2. Б. Л. Ван-дер-Варден, *Современная алгебра. Часть первая.* М., 1934.

3. Н. Г. Чеботарев, *Основы теории Галуа. Часть первая.* М.-Л. 1934.
4. Н. Г. Чеботарев, *Теория Галуа.* М., 1936.
5. М. М. Постников, *Теория Галуа.* М., 1963.
6. В. В. Ишханов, Б. Б. Лурье, Д. К. Фаддеев, *Задача погружения в теории Галуа.* М., 1990 Перевод: V. V. Ishkhanov, B. B. Lur'e, D. K. Faddeev, The Embedding Problem in Galois Theory, AMS, 1997) .