УДК 512.623.3

РАДИКАЛЬНЫЕ ФОРМЫ НАД ПОЛЕМ И ТЕОРИЯ ГАЛУА

© 2001 г. Р. С. Адамова

Воронежский государственный университет

В работе вводится понятие радикальной формы над полем и дается еще одна точка зрения на результаты теории Галуа разрешимости уравнений в радикалах. Все поля предполагаются лежащими в поле комплексных чисел, и основным полем считается поле рациональных чисел.

Определение 1. Радикалом n–ой степени над полем P называется выражение $\sqrt[n]{a}$, где $n \in \boldsymbol{N}$, $n > 1$, $a \in P$. Значением этого радикала называется всякое комплексное число z такое, что $z^n = a$. Символ $\sqrt[n]{\ }$ называют знаком этого радикала.

Радикал $\sqrt[n]{a}$ имеет единственное значение, если $a = 0$, и имеет n значений, если $a \neq 0$. Очевидно, все значения этого радикала составляют множество всех корней в поле $\boldsymbol{C}$ многочлена $x^n - a$. Этот факт обобщается следующим образом.

Определение 2. Радикальной формой над полем P назовем математическое выражение F, содержащее конечное число элементов поля P, знаков операций сложения, вычитания, умножения, деления, возведения в степень и знаков радикалов. Радикальную форму F назовем простой, если все входящие в нее знаки радикалов имеют показателями простые числа.

Определение 3. Значением радикальной формы F назовем всякое комплексное число w, которое получается выполнением операций, указанных в F, над значениями радикалов, получающихся в этом процессе.

Радикальные формы над полем P называются эквивалентными, если совпадают множества их значений.

Очевидно, что формы $\sqrt[mn]{a}$ и $\sqrt[m]{\sqrt[n]{a}}$ эквивалентны, поэтому всякая радикальная форма эквивалентна некоторой простой.

Теорема 1. Множество всех значений радикальной формы F над полем P совпадает с множеством всех корней в поле $\boldsymbol{C}$ некоторого многочлена f над полем P.

Доказательство. Выберем какую-либо последовательность действий при вычислении значений формы F и выпишем знаки всех радикалов, последовательно встречающихся на этом пути (включая и повторяющиеся):

$$\sqrt[m]{\ }, \ \sqrt[n]{\ }, \ \ldots \ \sqrt[p]{\ }, \ \sqrt[s]{\ }, \ \sqrt[t]{\ }. \qquad (1)$$

Для первого из них подкоренным выражением является элемент поля P, для следующих подкоренным выражением может быть как элемент поля P, так и радикальная форма над полем P, содержащая предшествующие знаки радикалов. Рассмотрим один из возможных наборов значений радикалов, отраженных знаками в последовательности (1):

$$\mu, \ \nu, \ \ldots, \ \rho, \ \sigma, \ \tau, \qquad (2)$$

и пусть w — значение формы F при этом наборе. Выполним последовательность следующих операций.

1. Последнее число в этом наборе, согласно его построению, запишем в виде: $\tau = \sqrt[t]{u}$, где $u \in S = P(\mu,\nu,\ldots,\rho,\sigma)$. Очевидно, что

$$w = f(\tau), \ f \in S[x]. \qquad (3)$$

Наряду с $\tau = \sqrt[t]{u}$ рассмотрим все другие значения этого радикала. Получим числа $\tau_1 = \tau, \tau_2, \tau_3, \ldots, \tau_t$. Соответственно им мы будем иметь значения радикальной формы F : $w_1 = w, w_2, w_3, \ldots, w_t$. Для каждого из них запишем представление вида (3):

$$w_1 = w = f(\tau) = f(\tau_1),$$
$$w_2 = f(\tau_2), \ w_3 = f(\tau_3), \ \ldots, \ w_t = f(\tau_t). \qquad (4)$$

Многочлен $f^*(x) = (x - w_1)(x - w_2)(x - w_3)\ldots(x - w_t)$ является многочленом над полем S. Действительно, коэффициенты этого многочлена не изменяются при перестановках чисел $w_1, w_2, w_3, \ldots, w_t$, поэтому, будучи выраженными че-

рез $\tau_1 = \tau, \tau_2, \tau_3, ..., \tau_t$ по формулам (4), не изменяются при перестановках и этих чисел. Тогда, согласно основной теореме о симметрических многочленах, они представляются как многочлены над полем S от чисел $\delta_1, \delta_2, \delta_3, ..., \delta_t$ — значений элементарных симметрических многочленов от $\tau_1 = \tau, \tau_2, \tau_3, ..., \tau_t$. Но $\delta_1, \delta_2, \delta_3, ..., \delta_t$ — это все корни в поле комплексных чисел многочлена $x^t - u$, следовательно, $\delta_1 = \delta_2 = \delta_3 = ... = \delta_{t-1} = 0$, $\delta_t = (-1)^t u$, так что $f^* \in S[x]$. Заметим, что проведенные рассуждения доказывают справедливость теоремы при длине последовательности (1), равной 1.

2. В последовательности (2) рассмотрим предпоследнее число — σ. Отметим, что

$$\sigma = \sqrt[s]{v}, \quad v \in P(\mu, \nu, ..., \rho). \tag{5}$$

Заменяя в последовательности (2) число s на другие значения того же радикала, мы будем получать из нее новые последовательности такого же вида. Выполняя для каждой из них построение пункта 1, будем вместо многочлена $f^* = f_1^*$ получать многочлены над полем S, которые обозначим $f_2^*, f_3^*, ..., f_s^*$. Многочлен $f^{**} = \prod_{i=1}^{i=s} f_i^*$ является многочленом над полем $P(\mu, \nu, ..., \rho)$. Множество его корней — это множество значений формы F при фиксированных последовательностью (2) значений всех радикалов кроме двух последних. Тем самым, теорема доказана при длине последовательности (1), равной 2.

3. Продолжая построение аналогичным образом, мы подойдем к началу последовательности (2) и получим требуемый результат. ■

Теперь будем рассматривать те значения радикальной формы F над полем P, которые вычислены при условии:

одинаковым радикалам придаются одинаковые значения. (6)

Относительно множества таких значений формы справедливо утверждение, аналогичное предыдущей теореме 1.

Теорема 2. Множество всех значений радикальной формы F над полем P, вычисленных при условии (6), совпадает с множеством всех корней в поле $\boldsymbol{C}$ некоторого многочлена φ над полем P.

Доказательство этой теоремы проведем аналогично доказательству предыдущей теоремы с небольшими изменениями. Так же как и там выпишем последовательность (1), но последовательность (2) выберем так, чтобы она удовлетворяла условию (6):

$$\mu, \nu, ..., \rho, \sigma, \tau. \tag{7}$$

1. *а*) Если $\tau = \sqrt[t]{u}$ и это число не встречается ранее в последовательности (7), то проводим те же построения и получаем многочлен $f^*(x) = (x - w_1)(x - w_2)(x - w_3) ... (x - w_t)$ над полем $S = P(\mu, \nu, ..., \rho, \sigma)$.

б) Если $\tau = \sqrt[t]{u}$ встречается ранее в последовательности (7), то заметим, что в этом случае, $\tau \in S = P(\mu, \nu, ..., \rho, \sigma)$, поэтому $w \in S = P(\mu, \nu, ..., \rho, \sigma)$, и положим $f^*(x) = (x - w)$.

2. *а*) Если $\sigma = \sqrt[s]{v}$ не встречается прежде в последовательности (7), то радикалу $\sqrt[s]{v}$ придаем последовательно все его значения. Получаем соответствующие им последовательности типа (7). Перемножая получаемые при этом многочлены $f^* = f_1^*, f_2^*, f_3^*, ... f_S^*$, строим многочлен f^{**} над полем $P(\mu, \nu, ..., \rho)$. Множество корней этого многочлена в поле $\boldsymbol{C}$ совпадает с множеством значений формы F при фиксированных последовательностью (7) значений всех радикалов кроме двух последних и при значениях этих последних, определяемых значениями предыдущих и условием (6).

б) Если число $\sigma = \sqrt[s]{v}$ встречается ранее в последовательности (7), то $\sigma \in P(\mu, \nu, ..., \rho)$, поэтому $P(\mu, \nu, ..., \rho, \sigma) = P(\mu, \nu, ..., \rho)$ и построенный в пункте 1 многочлен f^* будет многочленом и над полем $P(\mu, \nu, ..., \rho)$. Положим $f^{**} = f^*$. Роль построенного многочлена f^{**} та же, что отмечена выше в пункте 2.*а* у многочлена, обозначенного таким же образом.

Продолжая процесс, мы подойдем к началу последовательности (7) и в результате будет построен требуемый многочлен φ над полем P. ■

Как известно, классическое понятие разрешимости уравнения в радикалах над полем $\boldsymbol{Q}$ равносильно тому, что всякий его корень в отдельности является значением той или другой радикальной формы над $\boldsymbol{Q}$, вычисленным с условием (6). Введем понятие сильной разрешимости в радикалах и докажем его эквивалентность классическому понятию.

Определение. Уравнение с рациональными коэффициентами

$$a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n = 0$$

назовем сильно разрешимым в радикалах над полем $\boldsymbol{Q}$, если существует простая радикальная форма над этим полем, множество значений которой, вычисленных при условии (6), совпадает с множеством его корней.

Уравнение $x^2 + px + q = 0$, $p,q \in \boldsymbol{Q}$, очевидно, сильно разрешимо в радикалах над полем $\boldsymbol{Q}$. Уравнение $x^3 + px + q = 0$, $p,q \in \boldsymbol{Q}$ также сильно разрешимо в радикалах над полем $\boldsymbol{Q}$. Соответствующая форма F получается преобразованием формулы Кардано и имеет вид (если $p \neq 0$ или $q \neq 0$):

$$F = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} - \frac{p}{3\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}}.$$

Легко построить форму и для уравнения $x^4 + px^2 + qx + r = 0$ над полем $\boldsymbol{Q}$. Из сказанного следует, что всякое уравнение над полем $\boldsymbol{Q}$ степени 2, 3 и 4 сильно разрешимо в радикалах над полем $\boldsymbol{Q}$. Более того, поскольку приведенные формы дают описание множества корней и для уравнений над полем $\boldsymbol{C}$, то сильно разрешимыми в радикалах над полем $\boldsymbol{Q}$ будут и уравнения $f(x) = 0$, где многочлен $f(x)$ получается как композиция многочленов степени $n < 5$.

Теорема 3. Уравнение с рациональными коэффициентами

$$a_0\, x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n = 0 \qquad (8)$$

тогда и только тогда сильно разрешимо в радикалах над полем $\boldsymbol{Q}$, когда его группа Галуа разрешима.

Доказательство. Необходимость условия не нуждается в доказательстве, поскольку сильная разрешимость уравнения влечет его разрешимость в классическом смысле, которая эквивалентна разрешимости группы Галуа уравнения.

Пусть теперь группа Галуа уравнения (8) разрешима. Тогда имеем классическую разрешимость этого уравнения, то есть *каждый корень уравнения* (8) *является значением той или другой простой радикальной формы над полем* $\boldsymbol{Q}$, *вычисленной с условием* (6). Докажем существование простой радикальной формы, множество значений которой, вычисленных при условии (6), совпадает с множеством корней уравнения (8). Пусть α — один из корней этого уравнения и F — радикальная форма над полем $\boldsymbol{Q}$, значением которой (при условии (6)) он является. Выпишем знаки всех радикалов, последовательно встречающихся при вычислении ее значений, включая и повторяющиеся, а затем последовательность значений этих радикалов (именно тех, которые дали значение α):

$$\sqrt[m]{\ },\sqrt[n]{\ },\ldots\sqrt[p]{\ },\sqrt[s]{\ },\sqrt[t]{\ } \qquad (9)$$

$$\mu,\nu,\ldots,\rho,\sigma,\tau. \qquad (10)$$

1. Рассмотрим последнее число в последовательности (10):

$$\tau = \sqrt[t]{\omega}\ ,\ \text{где}\ \ \omega \in Q(\mu,\nu,\ldots,\rho,\sigma).$$

а) Если $\omega \in Q(\mu,\nu,\ldots,\rho,\sigma)$, то многочлен $x^t - \omega$ неприводим над полем $Q(\mu,\nu,\ldots,\rho,\sigma)$ [3]. Поэтому для любого другого значения τ_1 того же радикала существует изоморфизм $f : Q(\mu,\nu,\ldots,\rho,\sigma,\tau) \to f : Q(\mu,\nu,\ldots,\rho,\sigma,\tau_1)$, тождественный на поле $Q(\mu,\nu,\ldots,\rho,\sigma)$ и переводящий τ в τ_1. При таком изоморфизме полей коэффициенты уравнения (8) не изменяются и потому корень α преобразуется в другой его корень α_1. В то же время и значение α формы F изменится на α_1. Следовательно, в случае $\tau \notin Q(\mu,\nu,\ldots,\rho,\sigma)$ любое другое значение радикала $\sqrt[t]{\omega}$ при сохранении значений всех предшествующих придает форме F значение, которое также является корнем уравнения (8).

б) Если $\tau \in Q(\mu,\nu,\ldots,\rho,\sigma)$, то его можно представить в виде значения многочлена над полем $\boldsymbol{Q}$ от $\mu,\nu,\ldots,\rho,\sigma$. Произведя в таком представлении замену чисел $\mu,\nu,\ldots,\rho,\sigma$ на те радикальные формы, значениями которых они явились, получим новую форму над полем $\boldsymbol{Q}$. Она также имеет число α одним из своих значений. Для нее проведем аналогичные построения, пока не получим ситуацию пункта *а*).

2. Рассмотрим предпоследнее число в последовательности (10):

$$\sigma = \sqrt[s]{\nu},\ \ \nu \in Q(\mu,\nu,\ldots,\rho).$$

а) Если $\sigma \notin Q(\mu,\nu,\ldots,\rho,\sigma)$, то как и выше получим, что, заменяя число σ на любое другое значение этого радикала, мы при любых соответствующих значениях следующего будем получать значения формы, являющиеся корнями уравнения (8).

б) Если $\tau \in Q(\mu,\nu,\ldots,\rho,\sigma)$, то поступаем аналогично пункту 1 *б*).

3. Продолжая процесс, дойдем до начала последовательности (8) и построим форму F^* над полем $\boldsymbol{Q}$, все значения которой — корни уравнения (8). Возможно, это будут не все корни уравнения. Тогда по корню β, не вошедшему в это множество, аналогично построим форму G^*. Объединение их значений описывается формой:

$$H = \frac{k + \sqrt{k^2}}{2k} F^* + \frac{k - \sqrt{k^2}}{2k} G^*,$$

где k — натуральное число, не участвующее в вычислении значений форм F^* и G^*.

4. После достаточного числа таких процедур получим форму над полем $\boldsymbol{Q}$, множество значений которой, вычисленных при условии (6), совпадает с множеством корней уравнения (8). ■

СПИСОК ЛИТЕРАТУРЫ

1. Ван дер Варден Б. Л. Алгебра. — М.: Наука, 1979. — 623 с.

2. Постников М. М. Введение в теорию алгебраических чисел. — М.: Наука, 1982. — 239 с.

3. Постников М. М. Теория Галуа. — М.: Физматгиз, 1963. — 218 с.