Доклады Академии Наук СССР
1947. Том LVIII, № 9

МАТЕМАТИКА

Н. В. ВОЛНИНА

О ПРИВОДИМОСТИ ПОЛИНОМОВ В ИРРАЦИОНАЛЬНЫХ ПОЛЯХ

(Представлено академиком С. Н. Бернштейном 3 VIII 1947)

В некоторых вопросах, связанных с теорией Галуа, в частности, при фактическом определении группы Галуа уравнения с помощью основных модулей ([2], стр. 78—81), требуется уменье разлагать полиномы на множители в любом поле. Однако практические приемы, которые применяются обычно для разложения полиномов на неприводимые множители в поле рациональных чисел, не могут быть проведены в этом случае. Основная причина заключается в том, что каждое целое алгебраическое число может быть представлено в виде произведения целых алгебраических чисел бесконечным числом способов в силу существования алгебраических единиц.

Наиболее интересным является случай, когда поле $K(\beta)$, в котором мы хотим разложить полином на множители, является алгебраическим расширением поля K алгебраических чисел. Достаточно рассмотреть случай поля, образованного одним корнем алгебраического уравнения, в силу теоремы о примитивных элементах алгебраических расширений (см. [2], стр. 71—72). Пусть нужно разложить полином

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_n \tag{1}$$

на неприводимые множители в поле $K(\beta)$, где β удовлетворяет неприводимому в поле K уравнению

$$g(y) = (y - \beta_1)\,(y - \beta_2) \ldots (y - \beta_m) = 0 \tag{2}$$

степени m. Пусть коэффициенты $a_1, a_2, \ldots, a_n$ также лежат в поле $K(\beta)$. Следовательно,

$$f(x) = x^n + a_1(\beta)\,x^{n-1} + \ldots + a_n(\beta) = f(x, \beta).$$

Считаем, что $f(x, \beta)$ не имеет кратных корней, от которых легко было бы избавиться, найдя общий делитель полинома и его производной.

Построим норму полинома $f(x, \beta)$, которая определяется следующим образом:

$$N(f(x, \beta)) = f(x, \beta_1) \cdot f(x, \beta_2) \ldots f(x, \beta_m) = F(x). \tag{3}$$

Коэффициенты полинома $F(x)$, очевидно, рациональны.

Легко убедиться, что если $F(x)$ неприводим в поле K, то $f(x, \beta)$ неприводим в поле $K(\beta)$. Покажем, что, пользуясь нормой, можно всегда разложить полином с коэффициентами из поля $K(\beta)$ на непри-

водимые множители в том же поле. Если $N(f(x, \beta))$ не является неприводимым полиномом в поле K, то возможны два случая:

1. $N(f(x, \beta))$ разлагается в произведение взаимно простых множителей в поле K. Пусть

$$N(f(x, \beta)) = H(x)R(x), \tag{4}$$

где $H(x)$ и $R(x)$ — взаимно простые рациональные полиномы. Тогда $f(x, \beta)$ не может одновременно быть делителем обоих полиномов $H(x)$ и $R(x)$, в силу чего один из общих наибольших делителей пар $f(x, \beta)$, $H(x)$ и $f(x, \beta)$, $R(x)$ должен отличаться от $f(x, \beta)$. С другой стороны, ни один из них не может быть равен единице, так как из взаимной простоты полиномов $f(x, \beta)$ и $H(x)$ мы, в силу неприводимости уравнения (2), заключили бы о взаимной простоте каждой пары

$$f(x, \beta_i), \quad H(x) \qquad (i = 1, 2, \ldots, m),$$

в силу чего были бы взаимно просты полиномы

$$N(f(x, \beta)), \quad H(x),$$

что невозможно в силу (4). Таким образом, $f(x, \beta)$ будет иметь истинным делителем один из общих наибольших делителей

$$(f(x, \beta), H(x)), \quad (f(x, \beta), R(x))$$

и потому разложится на множители.

Продолжая процесс, мы после конечного числа шагов придем к случаю

2. $N(f(x, \beta))$ есть степень неприводимого в поле K полинома $H(x)$:

$$N(f(x, \beta)) = [H(x)]^k. \tag{5}$$

В этом случае мы должны воспользоваться способом, который М. Бауэр [1] применил к доказательству одной теоремы Такаги.

Пусть

$$f(x) = \prod_{\nu=1}^{n} (x - \alpha_\nu), \quad g(y) = \prod_{\mu=1}^{m} (y - \beta_\mu) \tag{6}$$

неприводимые в поле K полиномы, любые два корня которых мы соответственно обозначим через α и β. Пусть полином $\varphi(x, y)$ выбран в поле K так, чтобы $\varphi(\alpha_\nu, \beta_\mu) = \gamma_{\mu\nu}$ были отличны друг от друга. Проще всего взять в качестве $\varphi(x, y)$ линейный полином. Пусть величины $\gamma_{\mu\nu}$ являются корнями рационального полинома $S(z)$, который пусть разлагается в поле K на неприводимые множители

$$S(z) = s_1(z)s_2(z) \ldots s_e(z) \tag{7}$$

степеней $k_1, k_2, \ldots, k_e$.

Рассмотрим общие наибольшие делители

$$f_i(x, \beta) = (s_i(\varphi(x, \beta)), f(x)) \quad (i = 1, 2, \ldots, e). \tag{8}$$

Каждый из полиномов

$$f_i(x, \beta_\mu) \quad (\mu = 1, 2, \ldots, m)$$

имеет одну и ту же степень, которую мы обозначим через n_i. Норма

$$N(f_i(x, \beta)) = f_i(x, \beta_1) f_i(x, \beta_2) \ldots f_i(x, \beta_m), \tag{9}$$

с одной стороны, является полиномом степени mn_i. С другой стороны, в силу (8), степень полинома $N(f_i(x, \beta))$ равна числу таких значений $\gamma_{\mu\nu}=\varphi(\alpha_\nu, \beta_\mu)$ с фиксированным значком μ, которые являются корнями полинома $s_i(z)$. Заставляя значок μ пробегать все значения $1, 2, \ldots, m$, мы получим k_i, т. е. степень полинома $s_i(z)$. Таким образом,

$$k_i = n_i m.$$

Покажем, что полиномы $f_i(x, \beta_\mu)$ неприводимы в поле $K(\beta_\mu)$. Действительно, пусть величина α удовлетворяет в поле $K(\beta_\mu)$ неприводимому уравнению степени $v_i \leqslant n_i$.

Следовательно, величина $\gamma=\varphi(\alpha, \beta_\mu)$ удовлетворяет в поле $K(\beta_\mu)$ уравнению степени v_i, а в поле K уравнению степени mv_i. С другой стороны, величина γ удовлетворяет в поле K неприводимому уравнению $s_i(z)=0$ степени $k_i=mn_i$. Отсюда $mv_i \leqslant mn_i$, что в связи с другим полученным неравенством дает

$$n_i = v_i,$$

ч. и т. д.

Очевидно, что в поле $K(\beta)$ полином $f(x)$ разлагается на неприводимые множители следующим образом:

$$f(x)=f_1(x, \beta)f_2(x, \beta)\ldots f_e(x, \beta). \qquad (10$$

В самом деле, каждый корень полинома $f(x)$, например α_i, дает корень $\varphi(\alpha_i, \beta_\mu)$ полинома $S(z)$, который должен быть корнем какого-нибудь из полиномов $s_i(z)$. В этом случае α_i в силу (8) должен быть корнем полинома $f_i(x, \beta_\mu)$. С другой стороны, полиномы $f_i(x, \beta_\mu)$ $(i=1, 2, \ldots, e)$ не могут иметь общих корней, так как тогда б

$$s_i(z) \quad (i=1, 2, \ldots, e)$$

имели бы общие корни, а это противоречит способу выбора полинома $\varphi(x, y)$.

Из доказанного следует, что для отыскания неприводимых в поле $K(\beta)$ множителей полинома $f(x, \beta)$ мы можем поступать следующим образом. Определим неприводимый в поле K полином $g(y)$, которому удовлетворяет величина β. Затем построим полином $\varphi(\alpha, \beta)$ от корней полиномов $f(x)$ и $g(y)$. Далее, найдем полином $S(z)$, корнями которого служат все величины $\varphi(\alpha_\nu, \beta_\mu)$, и разложим его на неприводимые в поле K множители:

$$S(z)=s_1(z)\ldots s_e(z).$$

Тогда общие наибольшие делители $f_i(x, \beta)$ полиномов $f(x)$ и $s_i(\varphi(x, \beta))$ будут неприводимыми множителями в поле $K(\beta)$:

$$f(x)=f_1(x, \beta)f_2(x, \beta)\ldots f_e(x, \beta).$$

Для разложения полинома $f(x, \beta)$ с коэффициентами из поля $K(\beta)$ мы должны предварительно привести задачу к случаю 2, а затем поступить указанным образом с полиномом $H(x)$ (см. формулу (5)). Тогда произведение некоторых из неприводимых в поле $K(\beta)$ множителей полинома $H(x)$ составит заданный полином $f(x, \beta)$.

Поступило
3 VIII 1947

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] M. Bauer, J. reine u. angew. Math., **163**, 249 (1930). [2] Н. Чеботарев. Основы теории Галуа, ч. 1, 1934.