

УДК 512.62

МАТЕМАТИКА

М. К. Кюреган

**Некоторые вопросы конструктивной теории приводимости
 полиномов над конечными полями**

(Представлено чл.-корр. АН Армянской ССР Р. Р. Варшамовым 20/III 1986)

Проблема синтеза неприводимых над полем Галуа полиномов заданной степени в явном виде является наиболее важной и трудной проблемой современной алгебры. Фундаментальные результаты конструктивной теории приводимости полиномов над конечными полями в основном принадлежат Р. Р. Варшамову (1-3) и др. Данная статья является продолжением этих работ.

Пусть $GF(q)$ — поле Галуа порядка $q = p^s$, p — простое число, s — натуральное. Обозначим и в дальнейшем будем понимать $f(x) = \sum_{u=0}^n a_u x^u$ произвольный нормированный неприводимый над полем $GF(q)$ полином степени n .

Опираясь на полученные в (4) результаты, докажем следующий факт.

Теорема 1. Пусть $g(x) = \sum_{v=0}^k g_v x^v$ — неприводимый над полем $GF(q^{dn})$ полином степени k , где $g_v \in GF(q^d)$ ($n, d = 1, d \geq 1, f(\alpha) = 0$). Тогда полином $f(g(x))$ степени kn не будет разлагаться в поле $GF(q^d)$.

Доказательство. Согласно (4) полином $f(x)$ неприводим над полем $GF(q^d)$, следовательно, над полем $GF(q^{dn})$ имеем: $f(x) = \prod_{u=0}^{n-1} (x - \alpha^{q^{du}})$ и после замены x через $g(x)$ получим $f(g(x)) = \prod_{u=0}^{n-1} (g(x) - \alpha^{q^{du}})$. Согласно (4) $f(g(x))$ неприводим над полем $GF(q^d)$.

Теорема доказана.

Теорема 2. Пусть $\delta, \delta_1 \in GF(q)$, $\delta \neq 0$ и $x^{\frac{p^s n - 1}{p - 1}} \equiv 1 \pmod{f(x - \delta_1)}$ (α). Тогда полином

$$x^n f\left(\frac{x^p - \delta_1 x - \delta}{x}\right) \quad (1)$$

степени pn неприводим над полем $GF(q)$ в том и только в том случае, если имеет место соотношение

$$\sum_{u=0}^{sn-1} \delta p^u x^{\frac{p^{ns} - p}{p-1} u + 1} \not\equiv 0 \pmod{f(x - \delta_1)} \quad (2)$$

и полином (1) разлагается на произведение p неприводимых множителей степени n тогда и только тогда, когда условие (б) не имеет места.

Доказательство. Учитывая неприводимость полинома $f(x)$ над полем $GF(q)$, имеем над полем $GF(q^n)$ соотношение

$$f(x) = \prod_{u=0}^{n-1} (x - \alpha^{q^u}). \quad (2)$$

Заменив в соотношении (2) x на $\frac{x^p - \delta_1 x - \delta}{x}$ и умножив обе части (2) на x^n , получим

$$x^n f\left(\frac{x^p - \delta_1 x - \delta}{x}\right) = \prod_{u=0}^{n-1} (x^p - (\delta_1 + \alpha)^{q^u} x - \delta). \quad (3)$$

Согласно работе (5) при выполнении условий $(\delta_1 + \alpha)^{\frac{p^{sn}-1}{p-1}} = 1$ и

$$\begin{aligned} \frac{\delta}{\delta_1 + \alpha} + \frac{\delta^p}{(\delta_1 + \alpha)^{1+p}} + \frac{\delta^{p^2}}{(\delta_1 + \alpha)^{1+p+p^2}} + \dots + \frac{\delta^{p^{sn-1}}}{(\delta_1 + \alpha)^{1+p+\dots+p^{sn-1}}} = \\ = \sum_{u=0}^{ns-1} \delta^{p^u} (\delta_1 + \alpha)^{\frac{p^{ns-pu+1}}{p-1}} \neq 0 \end{aligned}$$

полином $x^p - (\delta_1 + \alpha)x - \delta$ неприводим над полем $GF(q^n)$, тогда из (4) следует неприводимость полинома (1) над полем $GF(q)$. Из этого следует, что если выполнены условия (а) и (б), то полином (1) неприводим над полем $GF(q)$.

Полином $x^p - (\delta_1 + \alpha)x - \delta$, для которого $(\delta_1 + \alpha)^{\frac{p^{sn}-1}{p-1}} = 1$, согласно (5) разлагается на p линейных множителей, т. е. имеем соотношение

$$x^p - (\delta_1 + \alpha)x - \delta = \prod_{v=1}^p (x - \beta_v)$$

тогда и только тогда, когда

$$\sum_{u=0}^{ns-1} \delta^{p^u} (\delta_1 + \alpha)^{\frac{p^{ns-pu+1}}{p-1}} = 0.$$

Легко убедиться, что

$$x^p - (\delta_1 + \alpha)x - \delta = \prod_{v=1}^p (x - \beta_v^{q^u}). \quad (4)$$

Учитывая соотношения (3) и (4), получим

$$x^n f\left(\frac{x^p - \delta_1 x - \delta}{x}\right) = \prod_{v=1}^p \prod_{u=0}^{n-1} (x - \beta_v^{q^u}).$$

Отсюда следует, что полином (1) разлагается на p сомножителей тогда и только тогда, когда выполнены условия (а) и (б), т. е. теорема доказана. Доказанный результат является существенным усилением работы (6).

Рассмотрим случай, когда $\delta = 1$ и $q = 2^s$. Условие (а) автомати-

чески выполняется, т. е. всегда верно равенство $x^{2^n-1} = 1 \pmod{f(x+\delta_1)}$.

Упростим условие (б). Ясно, что

$$\sum_{u=0}^{sn-1} (\delta_1 + \alpha)^{2^{sn}-2^{u+1}} = (\delta_1 + \alpha)^{2^{sn}} \left(\sum_{u=0}^{sn-1} \left(\frac{1}{\delta_1 + \alpha} \right)^{2^{u+1}} \right) =$$

$$= (\delta_1 + \alpha) \left[\left(\sum_{u=0}^{s-1} \left(\sum_{v=0}^{n-1} \left(\frac{1}{\delta_1 + \alpha} \right)^{2^{sv}} \right)^{2^u} \right)^2 \right]$$

$$\text{и } f(x+\delta_1) = \sum_{u=0}^n a_u (x+\delta_1)^u = \sum_{u=0}^n b_u x^u.$$

Отсюда согласно теореме Виетта

$$\sum_{u=0}^{s-1} \left(\sum_{v=0}^{n-1} \left(\frac{1}{\delta_1 + \alpha} \right)^{2^{sv}} \right)^{2^u} = \sum_{u=0}^{s-1} ((b_1 b_0^{-1})^{-1})^{2^u}.$$

Для этого случая из теоремы 2 получим

Следствие. Пусть $\delta_1 \in GF(2^s)$, тогда полином $x^n f\left(\frac{x^2 + \delta_1 x + 1}{x}\right)$ неприводим над полем $GF(2^s)$ тогда и только тогда, когда

$$\sum_{u=0}^{s-1} [b_1 b_0^{-1}]^{2^u} = 1 \quad (б_1)$$

и разлагается на произведение двух двойственных неприводимых над полем $GF(2^s)$ полиномов степени n тогда и только тогда, когда условие (б₁) не имеет места.

Теорема 3. Пусть $\delta, \delta_1 \in GF(q)$ и $\delta_1^{\frac{q-1}{p-1}} = 1$. Тогда полином

$$f(x^p - \delta_1 x - \delta) \quad (5)$$

степени pn неприводим над полем $GF(q)$, если

$$\sum_{u=0}^{sn-1} \delta_1^{\frac{p^{sn}-p^{u+1}}{p-1}} x^{p^u} \not\equiv 0 \pmod{f(x-\delta)}, \quad (6)$$

и разлагается на произведение p неприводимых множителей степени n тогда и только тогда, когда не имеет места условие (6).

Доказательство. В формуле (2) заменим x на $x^p - \delta_1 x - \delta$, получим $f(x^p - \delta_1 x - \delta) = \prod_{u=0}^{n-1} (x^p - \delta_1 x - (\delta + \alpha)^{q^u})$. Согласно работе (5)

при выполнении условий $\delta_1^{\frac{p^{sn}-1}{p-1}} = 1$ и

$$\frac{\delta + \alpha}{\delta_1} + \frac{(\delta + \alpha)^p}{\delta_1^{1+p}} + \frac{(\delta + \alpha)^{p^2}}{\delta_1^{1+p+p^2}} + \dots + \frac{(\delta + \alpha)^{p^{sn-1}}}{\delta_1^{1+p+p^2+\dots+p^{sn-1}}} \neq 0$$

или, что то же самое,

$$\delta_1^{\frac{p^n-1}{p-1}} = 1 \text{ и } \sum_{u=0}^{sn-1} (\delta + \alpha)^{p^u} \delta_1^{\frac{p^{sn}-p^{u+1}}{p-1}} \neq 0$$

полином $x^p - \delta_1 x - (\delta + \alpha)$ неприводим над полем $GF(q^n)$, а из теоремы 1 следует неприводимость полинома $f(x^p - \delta_1 x - \delta)$ над полем $GF(q)$.

Из этого следует, что если выполнено условие (6), то полином (5) неприводим над полем $GF(q)$.

Полином $x^p - \delta_1 x - (\delta + \alpha)$, для которого $\delta_1^{p^{s-1}} = 1$, согласно (5) разлагается на p линейных множителей, т. е. имеем: $x^p - \delta_1 x - (\delta + \alpha) = \prod_{v=1}^p (x - \beta_v)$ тогда и только тогда, когда

$$\sum_{u=0}^{sn-1} (\delta + \alpha)^{p^u} \delta_1^{\frac{p^{sn-p^u+1}}{p-1}} = 0.$$

Отсюда следует $f(x^p - \delta_1 x - \delta) = \prod_{v=1}^p \prod_{u=0}^{n-1} (x - \beta_v^{q^u})$.

Значит, полином (5) разлагается на p сомножителей тогда и только тогда, когда не выполнены условия (6), что и требовалось доказать.

Теорема 3 является существенным усилением результатов (2, 7, 8).

Следствие. Если $\delta_1, \delta \in GF(2^s)$, то полином $f(x^2 - \delta_1 x - \delta)$ степени $2n$ неприводим над полем $GF(2^s)$, если

$$\sum_{u=0}^{s-1} \left(\frac{n\delta - \pi}{\delta_1^2} \right)^{2^u} \neq 0, \quad (7)$$

где π — коэффициент при неизвестном x^{n-1} полинома $f(x)$ и разлагается на произведение двух неприводимых множителей степени n , если не выполнено условие (7).

Теорема 4. Пусть $\delta, \delta_1 \in GF(q)$ и $\delta_1 \neq 0$. Тогда полином степени pn

$$f(x^p - \delta_1^{p-1} x - \delta) \quad (8)$$

неприводим над полем $GF(q)$ тогда и только тогда, когда

$$\sum_{u=0}^{s-1} \left(\frac{n\delta - \pi}{\delta_1^p} \right)^{p^u} \neq 0, \quad (9)$$

где π — коэффициент при неизвестном x^{n-1} полинома $f(x)$.

Доказательство. В формуле (2) заменим x на $x^p - \delta_1 x - \delta$, получим $f(x^p - \delta_1^{p-1} x - \delta) = \prod_{u=0}^{n-1} (x^p - \delta_1^{p-1} x - (\delta + \alpha)^{q^u})$. Согласно работе (5) для неприводимости полинома $x^p - \delta_1^{p-1} x - (\delta + \alpha)$ над полем $GF(q^n)$ необходимо и достаточно, чтобы выполнялось условие

$$\frac{\delta + \alpha}{\delta_1^p} + \left(\frac{\delta + \alpha}{\delta_1^p} \right)^p + \left(\frac{\delta + \alpha}{\delta_1^p} \right)^{p^2} + \dots + \left(\frac{\delta + \alpha}{\delta_1^p} \right)^{p^{ns-1}} \neq 0 \text{ или } \sum_{u=0}^{s-1} \left(\frac{n\delta - \pi}{\delta_1^p} \right)^{p^u} \neq 0.$$

Теперь из теоремы 1 следует неприводимость полинома (8) над полем $GF(q)$. Отсюда получаем, что соотношение (9) является необходимым и достаточным условием неприводимости полинома (8) над полем $GF(q)$. Теорема доказана.

Опираясь на полученные результаты и используя работу (4), можно будет доказать следующий факт.

Теорема 5. Пусть $\delta, \delta_1, \delta_2, \delta_3 \in GF(2^s)$ и $\delta_1, \delta_2 \neq 0$. Тогда для того чтобы полином

$$f(x^4 + (z_1^2 + z_4)x^2 + z_1z_4x + z_2^2 + z_3z_4 + z_2)$$

был неприводим над полем $GF(2^v)$, необходимо и достаточно, чтобы выполнялось условие

$$\sum_{v=0}^{s-1} \left(\frac{\pi + n^2}{z_1^2} \right)^{2^v} = 1 \quad \text{и} \quad \sum_{v=0}^{s-1} n z_1^{2^v} z_2^{-2^v+1} = 1,$$

где π — коэффициент при неизвестном x^{n-1} полинома $f(x)$.

Теорема 5 является существенным усилением результата (9) и более конструктивна.

Автор считает своим приятным долгом выразить благодарность Р. Р. Варшамову за полезные советы в процессе работы над статьей.

Вычислительный центр Академия наук Армянской ССР и
Ереванского государственного университета

Մ. Կ. ԿՅՈՒՐԵՂՅԱՆ

Վերջավոր դաշտերի բազմանդամների վերածելիության
կոնստրուկտիվ տեսության մի փանի հարցեր

Գալուայի դաշտերի վրա բազմանդամների վերածելիության արտակարգ ինքնուրույն հետաքրքրություն ներկայացնող պրոբլեմը կարևոր դեր է կատարում ժամանակակից տեսնիկայում:

Աշխատանքում հետազոտվում են մի քանի ձևափոխություններ, որոնց համար որպես որոշման աիրույթ հանդիսանում է Գալուայի $GF(q)$ դաշտից վերցված գործակիցներով բազմանդամների օղակը: Ապացուցվում են մի շարք թևորեմներ, որոնք հնարավորություն են տալիս անվերածելի բազմանդամներ կառուցել բացահայտ տեսքով Գալուայի $GF(q)$ կամայական դաշտի վրա:

Ստացված արդյունքներից, որպես մասնավոր դեպքեր, ստացվում են մի քանի հայտնի թևորեմներ:

ЛИТЕРАТУРА — ԳՐԱԿԱՆՈՒԹՅՈՒՆ

- ¹ P. P. Varshamov, Studia Scientiarum Mathematicarum Hungarica, 5—19, 1973.
² P. P. Варшамов, ДАН СССР, т. 211, №4 (1973). ³ P. P. Варшамов, ДАН СССР, т. 275, №5 (1984). ⁴ М. К. Кюрелян, ДАН АрмССР, т. 81, № 2 (1985). ⁵ S. Schwarz, Matematichko-fizikalny casopis sav, m. 10, №2, 68—80 (1960). ⁶ P. P. Варшамов, Г. А. Гараков, Мат. попр. кибернетики и вычислительной техники, т. 6, 1970. ⁷ A. A. Albert, Fundamental concepts of higher algebra. Univ. of Chicago Press, 1956.
⁸ Agou Simon, J. of Number Theory, 9, №2, 229—239 (1977). ⁹ Agou Simon, J. of Number Theory, 10 L, 64—69 (1978).