Доклады Академии наук СССР
1973. Том 211, № 4

УДК 512.44

МАТЕМАТИКА

Р. Р. ВАРШАМОВ

ОПЕРАТОРНЫЕ ПОДСТАНОВКИ В ПОЛЕ ГАЛУА И ИХ ПРИЛОЖЕНИЕ

(Представлено академиком Б. Н. Петровым 29 V 1972)

Заметка посвящена в основном изложению некоторых результатов конструктивной теории синтеза неприводимых полиномов над полем Галуа.

Пусть $GF(q)$ — поле Галуа порядка $q = p^s$. Введем в рассмотрение класс операторов $\sigma_q^f(g(x), \delta) = \sum_{u=0}^{n} a_u \left(\sum_{v=0}^{m} b_v x^{q^v} + \delta \right)^u$, областью определения которых являются полиномы $g(x) = \sum_{v=0}^{m} b_v x^v$ и $f(x) = \sum_{u=0}^{n} a_u x^u$ с коэффициентами $b_v \in GF(q)$ и $a_u \in GF(q^r)$, $r \geqslant 1$, соответственно, δ — произвольный элемент $GF(q^r)$.

Теорема 1. *Пусть $g(x) \neq x - 1$ и $f(x)$ — два неприводимых полинома степени m и n соответственно, удовлетворяющих условию $(rn, T) = 1$, где T — показатель* $g(x)$, $r(x) \equiv g(x)^{-1} (\mathrm{mod}\, x^{nr} - 1)$, $R(x) = \sigma_q^x(r(x), 0)$ и $\psi(x) = \sum_{u=0}^{n} \psi_u x^u$, где ψ_u — нетривиальное решение** сравнения*

$$\sum_{u=0}^{n} \psi_u R(x^u) \equiv 0 \ (\mathrm{mod}\, f(x + \delta)).$$

Тогда полином

$$\psi(x)^{-1} \sigma_q^f(g(x), \delta),$$

является произведением $T^{-1}(q^m - 1)$ различных неприводимых в поле $GF(q^r)$ делителей степени nT.

Теорема 1 имеет ряд приложений. Рассмотрим некоторые из них.

Следствие 1. *Для того чтобы выражение $\psi(x)^{-1}\sigma_q^{(f)}(g(x), \delta)$ не разлагалось в поле $GF(q^r)$, необходимо и достаточно, чтобы $g(x)$ был примитивным полиномом над полем $GF(q)$.*

Как тривиальный частный случай следствия 1, при $f(x) = x$ и $\delta = 0$ автоматически вытекает известная теорема Уре ([1], теорема 10) и Глисона — Марша [2] или же при $f(x) = x$ и $g(x) = x - \theta$, где θ — первообразный элемент поля $GF(q)$, теорема Диксона ([2], теорема 24).

Следствие 2. *Пусть $g(x) = x^m - x^k + 1$ — примитивный трехчлен над полем $GF(q)$, $r = (m - k)N^{-1}$ — целое и $(r, q^m - 1)$.*

Тогда выражение $f(x)^{-1}\sigma_q^{(f)}(g(x), 0)$ является неразложимым полиномом над полем $GF(q^r)$, при всякой неприводимой в $GF(q^r)$ функции $f(x)$, степень n которой удовлетворяет условиям $n|N$ и $(n, q^m - 1) = 1$.

Следствие 3. *Пусть $g(x) = x^m + x^k - 1$ — примитивный трехчлен над полем $GF(q)$ и r — любой, взаимно простой с $q^m - 1$, делитель (m, k).*

* Т. е. минимальное натуральное число с условием $x^T \equiv 1 \ (\mathrm{mod}\, g(x))$.

** В условиях теоремы 1 это сравнение всегда имеет решение.

Тогда выражение $f(x)^{-1}\sigma_q^{(f)}(g(x), 0)$ *является неразложимым полиномом над полем* $GF(q^r)$, *при всякой неприводимой в* $GF(q^r)$ *функции* $f(x)$, *степень* n *которой удовлетворяет условиям* $n \mid mr^{-1}$ *и* $(n, q^m - 1) = 1$.

В близком отношении к теореме 1 стоит также и следующая

Теорема 2. *Пусть* $q > 2$, $(n, q-1) = 1$, $f(x)$ *— неприводимый в* $GF(q^r)$ *полином степени* n, θ *— первообразный элемент поля* $GF(q^r)$ *и* δ *— произвольный элемент* $GF(q^r)$.

Тогда полином

$$\psi(x)^{-1}\sigma_q^{(f)}(x - \theta, \delta)$$

степени $n(q-1)$ *неприводим в поле* $GF(q^r)$.

Этот результат является прямым обобщением указанной выше теоремы Диксона ([2]).

В дальнейшем нам понадобятся следующие две леммы.

Лемма 1. *В поле* $GF(q)$ *полином* $\sigma_q(r(x)) = \sigma_q^{(x)}(r(x), 0)$ *делит без остатка выражение* $\sigma_q(g(x))$, *тогда и только тогда, когда* $r(x)$ *является делителем* $g(x)$.

Лемма 2. *В любом поле характеристики* p, *функция* $\sigma_{p^t}(g(x))$ *является сепарабельной при всяких натуральном* t *и полиноме* $g(x)$, *свободный член которого* $b_0 \neq 0$.

Инъективное преобразование σ: $f(x) \to \sigma_p^{(f)}(x-1, \delta) = f(x^p - x + \delta)$, где δ — произвольный элемент $GF(q)$, будем называть p-отображением полинома $f(x)$. Обозначим через $J_n^{(u)}(x)$, $J_n^{(0)}(x) = 1$, $J_n^{(t(n))}(x) = J_n(x)$, произведение u различных нормированных * неприводимых в поле $GF(q)$ полиномов степени n, общее количество которых $t(n) = n^{-1}\sum_{u \mid n} \mu(u) q^{u^{-1}n}$, где $\mu(u)$ — функция Мёбиуса. Пусть дан произвольно полином $f(x)$ степени n неприводимый в поле $GF(q)$.

Теорема 3. *Выражение* $f(x^p - x + \delta)$ *либо неприводимо в поле* $GF(q)$, *либо разлагается на произведение* p *неприводимых множителей степени* n; *причем вероятность того, что функция* $f(x^p - x + \delta)$ *может оказаться неприводимой, равна* **

$$P(n) = \frac{p-1}{p}\left(\sum_{u \mid n,\ p \times u} \mu(u) q^{u^{-1}n}\right)\left(\sum_{u \mid n} \mu(u) q^{u^{-1}n}\right)^{-1} = \frac{p-1}{p}\bar{t}(n)\, t(n)^{-1}.$$

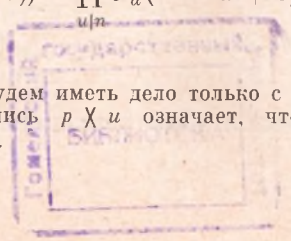
Доказательство. Для доказательства теоремы, очевидно, достаточно показать, что

$$J_n(x^p - x + \delta) = J_n^{(\Delta(n))}(x)\, J_{np}^{(\bar{\Delta}(n))}(x), \tag{1}$$

где $\Delta(n) = p\left(t(n) - \frac{p-1}{p}\bar{t}(n)\right)$, $\bar{\Delta}(n) = \frac{p-1}{p}\bar{t}(n)$.

Пусть $n = Np^\theta$, $\theta \geqslant 0$, $p \nmid N$. Предположим, что для любого k — собственного делителя n и $k = up^{\theta+1}$, где $u \mid N$, $u \neq N$, выполняется условие (1).

Тогда, рассматривая p-отображение выражения $x^{q^n} - x = \prod_{u \mid n} J_u(x)$ (т. е. $\sigma_p^{(f)}((x^{s^n} - 1)(x-1)) = \prod_{u \mid n} J_u(x^p - x + \delta)$) и принимая во внимание,



* В дальнейшем мы будем иметь дело только с нормированными полиномами.

** Здесь и далее запись $p \nmid u$ означает, что u не делится на p, т. е. $\neg \exists k((k > 1) \& (pk = u))$.

что $\Delta(u) = t(u)(p \nmid u)u\Delta(up) + \bar{\Delta}(u) = t(up)$, получим

$$\sigma_p((x^{sn}-1)(x-1)) =$$
$$= J_n(x^p - x + \delta) J_n^{(\overline{\Delta}(np^{-1}))}(x) \prod_{u|N,\, u\neq N} J_{up^{\theta+1}}^{(\overline{\Delta}(up^{\theta}))}(x) \prod_{u|n,\, u\neq n} J_u(x), \qquad (2)$$

считая $\bar{\Delta}(np^{-1}) = 0$, $p \nmid n$.

И кроме того, учитывая, что, в силу леммы 2, выражение $\sigma_p((x^{sn}-1)(x-1))$ сепарабельно, получим

$$J_{kp^{-1}}(x^p - x + \delta) J_k(x^p - x + \delta) = J_{kp^{-1}}^{(\overline{\Delta}(kp^{-1}))}(x) J_k(x) J_{kp}^{(\Delta(k))}(x). \qquad (3)$$

Опираясь на (3), можно показать, что

$$\left(J_n(x^p - x + \delta), \prod_{u|N,\, u\neq N} J_{up^{\theta+1}}(x)\right) = 1. \qquad (4)$$

Но согласно лемме 1, $x^{q^n} - x \,|\, \sigma_p((x^{sn}-1)(x-1))$ и $\sigma_p((x^{sn}-1)\cdot(x-1)) \,|\, x^{q^{np}} - x$, а это совместно с (2) и (4) даст формулу (1). Нетрудно понять, что этим фактически завершается доказательство теоремы 3.

Теорема 4. *Для того чтобы полином $f(x^p - x + \delta)$ был неприводим, необходимо и достаточно, чтобы выполнялось условие*

$$\sum_{u=0}^{s-1} (n\delta + \pi)^{p^u} \neq 0,$$

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

Доказательство. Пусть ζ — корень уравнения $f(x) = 0$. Но тогда $\zeta, \zeta^q, \ldots, \zeta^{q^{n-1}}$ суть все корни $f(x)$ и, поскольку $-\pi = \sum_{u=0}^{n-1} \zeta^{q^u}$, то

$$f(x) \,\Big|\, \Lambda\left(x, \sum_{u=0}^{s-1} \pi^{p^u}\right), \qquad (5)$$

где $\Lambda(x\xi) = \sigma_p\left(\sum_{u=0}^{ns-1} x^u, \xi\right)$.

Между тем,

$$\Lambda\left(x^p - x + \delta, \sum_{u=0}^{s-1} \pi^{p^u}\right) = \sigma_q(x^n - 1, \omega), \qquad (6)$$

где $\omega = n\sum_{u=0}^{s-1} \delta^{p^u} + \sum_{u=0}^{s-1} \pi^{p^u}$.

Но $\sigma_q((x^n-1)(x-1)) = (\sigma_q(x^n-1)^{q-1} - 1)\sigma_q(x^n-1)$ и $\sigma_q((x^n-1)\cdot(x-1)) \,|\, x^{q^{np}} - x$. Поэтому $\sigma_q(x^n-1)^{q-1} - 1 \,|\, x^{q^{np}} - x$, в то время как $(\sigma_q(x-1)^{q-1} - 1, x^{q^n} - 1) = 1$. Следовательно, для того чтобы полином $f(x^p - x + \delta)$ был неприводим в силу (5), (6), теоремы 3 и, учитывая, что $\sigma_p((x^{sn}-1)(x-1)) \,|\, \sigma_q((x^n-1)(x-1))$, достаточно, чтобы выражение $\sigma_q(x^n - 1, \omega)$ являлось делителем $\sigma_q(x^n-1)^{q-1} - 1$. А для этого необходимо и достаточно, чтобы $\omega = 0$, т. е. $\sum_{u=0}^{s-1} (n\delta + \pi)^{p^u}$. Что и требовалось показать.

Теорема 4 является существенным усилением известного результата ([2], теорема 23).

Кроме того, опираясь на теоремы 3 и 4, можно получить важный в приложении * результат:

$$N_{n,p}(a_1 = 0) = \frac{1}{np}\left(p \sum_{u|n,\, p\nmid u} \mu(u)\, p^{u^{-1}n} - \sum_{u|n} \mu(u)\, p^{u^{-1}n}\right),$$
$$N_{n,p}(a_1 \neq 0) = -\frac{1}{np} \sum_{u|n} \mu(u)\, p^{u^{-1}n}, \tag{7}$$

где $N_{n,\,p}(a_{u_i} = \delta_i,\ i = 1, \ldots, t)$ — общее число всевозможных нормированных неприводимых в поле $GF(p)$ полиномов $f(x) = \sum_{u=0}^{n} a_u x^u$ степени n, коэффициенты a_{u_i}, $0 \leqslant u_i < n$, которых принимают соответственно заранее заданные значения $\delta_i \in GF(q)$.

Большая роль в изучении этих функций, связанная с получением их оценок, принадлежит А. Вейлю. Однако не существует, по-видимому, конечных формул, позволяющих вычислить значения функций $N_{n,\,p}(\cdot)$ (кроме тривиального случая $t = 0$, т. е. формулы Дедекинда). Причем получение таких формул, как уже отмечалось выше, представляет интерес также и в связи с возможностью использования их косвенно в решении задачи синтеза неприводимых полиномов методом «проб и ошибок».

Т е о р е м а 5. *Пусть t — натуральное число, $n \geqslant t$ и δ — произвольный элемент поля $GF(2)$.*

Тогда

$$\sum_{i=0}^{t-1} 2^i \left(2^{n-t} - \sum_{km=n-i} kN_{k,2}(M(m,\ t-j) = \delta(j),\ j = 0,\ \ldots,\ i)\right) = 0, \tag{8}$$

где

$$M(m, u) = \sum_{\alpha_1 + 2\alpha_2 + \cdots + u\alpha_u} \frac{m! \prod_{i=1}^{u} a_i^{\alpha_i}}{(m - \alpha_1 - \cdots - \alpha_u)!\, \alpha_1! \cdots \alpha_u!}, \quad \delta(j) = \begin{cases} \delta, & \text{если } j = 0, \\ 0, & \text{если } j > 0. \end{cases}$$

Опираясь на соотношение (8) и используя некоторые вспомогательные средства, можно сравнительно легко получать соответствующие выражения для различных значений функций $N_{n,\,2}(\cdot)$. Так, например, полагая в формуле (8) $t = 1$ и используя формулу обращения Дедекинда — Лиувилля, получим соотношение (7) или же при $t = 2$, $2 \nmid n$ будем иметь

$$N_{n,2}(a_1 = \delta_1,\ a_2 = \delta_2) = \frac{1}{n} \sum_{su=n} \mu(u)\left(2^{(s-1)/2} + (-1)^{(s^2-1)/8 + \delta_1(n-1)/2 + \delta_2}\right) 2^{(s-3)/2},$$

и т. д.

Вычислительный центр
Академии наук АрмССР и
Ереванского государственного университета
Ереван

Поступило
22 V 1972

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] O. O r e, Trans. Am. Math. Soc., 36, 243 (1934). [2] A. A. A l b e r t, Fundamental Concepts of Higher Algebra, Chikago, 1956.

* Имеется в виду синтез неприводимых полиномов методом «проб и ошибок».