ՀԱՅԿԱԿԱՆ ՍՍՀ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԿԱԴԵՄԻԱՅԻ ԶԵԿՈՒՅՑՆԵՐ
ДОКЛАДЫ АКАДЕМИИ НАУК АРМЯНСКОЙ ССР

LXXIX 1984 1

УДК 512.62

МАТЕМАТИКА

Член-корреспондент АН Армянской ССР
Р. Р. Варшамов

Об одном методе построения неприводимых полиномов над конечными полями

(Представлено 5/IV 1983)

Проблемы приводимости полиномов над полями Галуа, представляющие исключительный самостоятельный интерес ([1]), играют важную роль в современной технике ([2,3]). В статье рассматриваются некоторые конструктивные методы построения неприводимых полиномов над произвольным полем Галуа F_q.

Все рассматриваемые в дальнейшем полиномы предполагаются с коэффициентами из поля F_q.

Обозначим через $L^\theta f(x)$ выражение $F(x)=\sum_{u=0}^{n} a_u(\theta(x))^{q^u-1}$, где $f(x)=\sum_{u=0}^{n} a_u x^u$, $\theta(x)=\sum_{u=0}^{m} b_u x^u$. Перепишем некоторые полезные в дальнейшем свойства оператора L^θ.

Свойство линейности. Для любых двух полиномов $f(x)$ и $g(x)$

$$L^\theta(\alpha f(x)+\beta g(x))=\alpha L^\theta f(x)+\beta L^\theta g(x)\ (\alpha,\ \beta\in F_q). \tag{1}$$

Свойство мультипликативности. Для любой функции $f(x)$ имеет место равенство

$$L^\theta f(x)=(L^\theta r(x))L^{\theta L^\theta r(x)}h(x), \tag{2}$$

где $f(x)=r(x)h(x)$.

Свойство сепорабельности. Кратность любого корня многочлена $\frac{F(x)}{(\theta(x)',F(x))}$ равна в точности q^σ, где σ—наибольшее целое, удовлетворяющее условию $f(x)=x^\sigma f_1(x)$, т. е. $a_\sigma\neq 0$ ($a_\omega=0$, $\omega<\sigma$). Используя вышеуказанные свойства оператора L^θ, можно получить следующие факты: $(L^\theta f(x),\ L^\theta g(x))=L^\theta(f(x),\ g(x))$;

$$L^{\theta L^\theta g(x)}f(x)=\frac{L^{\theta L^\theta\lambda_1(x)}(fx)}{L^{\theta L^\theta\lambda_1(x)}\lambda_2(x)}\,L^{\theta L^\theta\lambda_1(x)L^{\theta L^\theta\lambda_1(x)}f(x)}\lambda_2(x),$$

где $g(x)=\lambda_1(x)\lambda_1(x)$ и $(\lambda_2(x),\ f(x))=1$, а также:

Лемма 1. *Функция $L^{\theta L^\theta\lambda(x)+\alpha}r(x)$ делит без остатка полином $L^\theta L^\theta g(x)+a_1 f(x)$, где $r(x)\mid f(x)$, $g(x)=\lambda(x)\lambda_1(x)$, $\alpha\in F_q$, $a_1=\alpha\lambda_1(1)$ и $(\lambda_1(x),\ r(x))=1$, т. е.*

$$L^{\theta L^\theta\lambda(x)+\alpha}r(x)\mid L^\theta L^\theta g(x)+a_1 f(x). \tag{3}$$

Лемма 2. *Для любых двух полиномов* $\lambda(x)$ *и* $f(x)(f(1)\neq 0)$ *имеет место равенство*

$$L^{\theta L^{\theta}(x-1)\lambda(x)}f(x)=\prod_{a\in F_q} L^{\theta L^{\theta}\lambda(x)+a}f(x). \tag{4}$$

Из (4) вытекает соотношение

$$(\theta L^{\theta}(x-1)\lambda(x),\ L^{\theta L^{\theta}\lambda(x)+a}f(x))=1, \tag{5}$$

справедливое для любого $a\in F_q$.

Основная теорема. *Пусть* $\theta(x)=p(x)L^{p}\lambda(x)+\alpha$, *где* $p(x)$—*произвольный полином,* $\lambda(x)$ *и* $f(x)$—*полиномы с ненулевыми свободными членами,* $f(1)\neq 0$, α—*произвольный элемент поля* F_q, $K(\lambda_u, f_u)=L^{pL^{p\varepsilon(a)\lambda_u(x)}}f_u(x)$, *где* $\lambda_u(x)|\lambda(x)$, $f_u(x)|f(x)$, $\lambda_u(x)f_u(x)\neq\lambda(x)f(x)$, $\varepsilon(\alpha)=\alpha^{q-1}x-1$ *и* N—*период полинома* $S(x)=\varepsilon(\alpha)\lambda(x)f(x)$. *Тогда степень* $g(x)$—*любого непроизводимого делителя* $L^{\theta}f(x)$, *удовлетворяющего условию* $g(x)\nmid K(\lambda_u, f_u)$, *кратна* N.

Доказательство. Допустим противное, а именно, что $(m, N)\neq N$, где m степень полинома $g(x)$. Тогда $S_u(x)=(x^m-1,\ S(x))$ будет собственным делителем $S(x)$. Но $S_u(x)=a(x)(x^m-1)+b(x)S(x)$ $(S_u(x)=\varepsilon(\alpha)\lambda_u(x)f_u(x))$, а поэтому в силу (1), (2) и (3) находим

$$L^{p\varepsilon(\alpha)\lambda_u(x)}L^{pL^{p\varepsilon(\alpha)\lambda_u(x)}}f_u(x)=A(x)L^{p}(x^m-1)+B(x)L^{pL^{p\varepsilon(\alpha)\lambda(x)}}f(x). \tag{6}$$

По определению $p(x)L^{p}(x^m-1)=\sum_{u=0}^{k}p_u(x^{uq^m}-x^u)\left(p(x)=\sum_{u=0}^{k}p_ux^u\right)$, а это значит, что $x^{q^m-1}-1|p(x)L^{p}(x^m-1)$ и $g(x)|p(x)L^{p}(x^m-1)$. Согласно (5) $(p(x)L^{p\varepsilon(\alpha)\lambda(x)}, g(x))=1$, т. е. $(p(x), g(x))=1$, $g(x)|L^{p}(x^m-1)$ и ввиду (3) $(p(x)L^{p\varepsilon(\alpha)\lambda(x)}, g(x))=1$. Стало быть из (6) в силу (4) следует

$$g(x)|L^{pL^{p\varepsilon(\alpha)\lambda_u(x)}}f_u(x). \tag{7}$$

Но соотношение (7) противоречит условию теоремы. Следовательно, наше предположение оказалось неверным. Значит $(m, N)=N$, что и требовалось доказать

Прямым следствием основной теоремы являются следующие утверждения:

Теорема 1. *Пусть* $p(x)=x$. *Тогда степень полинома* $g(x)$ *совпадает с периодом* $S(x)$, *т. е.* $m=N$.

Теорема 2. *Полином* $L^{\theta}f(x)(p(x)=x)$ *разлагается на* $K=N^{-1}q^{\nu}(q^n-1)$ *различных неприводимых в поле* F_q *делителей степени* N, *где* n и ν *степени полиномов соответственно* $f(x)$ и $\lambda(x)$. *Стало быть, в частности (теорема Уре, Глисона, Карлица, Марша), для того чтобы функция* $L^{x}f(x)(p(x)=x, \lambda(x)=1, \alpha=0)$ *была неприводимой, необходимо и достаточно, чтобы полином* $f(x)$ *являлся примитивным в поле* F_q. *Или же*

Теорема 3. *Пусть* q—*простое число*,* $f(x)$ $(f(1)\neq 0)$—*примитивный полином,* $a\in F_q(a\neq 0)$ *и* $\delta=0$, 1 *или* $(1+(-1)^q)$. *Тогда полином* $L^{xL^{f}(x-1)^{\delta}+a}f(x)$ *неприводим над полем* F_q.

---

* С некоторыми незначительными ограничениями аналогичная теорема верна и для произвольного $q=p^s$.

И, наконец,

Теорема 4. *Пусть* $f(x)=\prod_{u=1}^{\sigma} f_u(x)$, *где* $f_u(x)$ $(f_u(1)\neq)$ *—примитивные над полем* F_2 *полиномы с попарно взаимно-простыми степенями* n_i, $\varepsilon=(\varepsilon_1, \ldots, \varepsilon_\sigma)$ $(0\leqslant\varepsilon_i\leqslant 1,\ i=\overline{1,\ \sigma})$

$$|\varepsilon|=\sum_{u=1}^{\sigma}\varepsilon_u,\quad f^{(\varepsilon)}(x)=\prod_{u=1}^{\sigma} f_u(x)^{\varepsilon u},\quad \theta(x)=xL^x(x-1)^\delta+\alpha$$

и $\delta=0, 1$ *или* 2. *Тогда полином*

$$F(x)=\prod_{u=0}^{[\sigma/2]}\Big(\prod_{|\varepsilon|=\sigma-2u-1} L^0 f^{(\varepsilon)}(x)\Big)^{-1}\Big(\prod_{|\varepsilon|=\sigma-2u} L^0 f^{(\varepsilon)}(x)\Big)$$

неприводим над полем F_2.

Имеет место также и следующая

Теорема 5. *Для любого натурального числа* m *полином* $\psi_m(x)$, *степени* 2^m, *определяемый рекурентным соотношением*

$$\psi_m(x)=\psi_{m-1}(x)^2+(x+\alpha)\prod_{u=0}^{m-2}\psi_u(x)^2,$$

где $\alpha\in F_2$, $\psi_0(x)=x+1+\alpha$, *неприводим над полем* F_2.

Вычислительный центр
Академии наук Армянской ССР
и Ереванского государственного университета

Հայկական ՍՍՀ ԳԱ բղթակից-անդամ Ի. Ի. ՎԱՐՇԱՄՈՎ

Վերջավոր դաշտերի վրա անվերածելի բազմանդամների կառուցման մի եղանակի մասին

Գալուայի դաշտերի վրա բազմանդամների վերածելիության արտակարգ ինքնուրույն հետաքրքրություն ներկայացնող պրոբլեմը կարևոր դեր է կատարում ժամանակակից տեխնիկայում։ Հոդվածում դիտարկվում է L^0 գծային օպերատորը, որի որոշման տիրույթը՝ Գալուայի F_q դաշտից վերցված գործակիցներով բազմանդամներն են։ Դիտարկվում են L^0 օպերատորի որոշ հատկությունները և դրանց օգնությամբ ապացուցվում են մի շարք թեորեմներ, որոնք թույլ են տալիս անվերածելի բազմանդամներ կառուցել բացահայտ տեսքով՝ Գալուայի կամայական դաշտի վրա։ Բացի այդ, վերջում տրվում է F_2 վերջավոր դաշտի վրա 2^n-րդ աստիճանի (որտեղ n-ը՝ կամայական բնական թիվ է) անվերածելի բազմանդամների կառուցման մի ռեկուրենտ եղանակ։

ЛИТЕРАТУРА—ԳՐԱԿԱՆՈՒԹՅՈՒՆ

[1] *A. A. Albert*, Fundamental concepts of Higher algebra, University of Chicago, 1956. [2] *N. Jierler*, J. Soc Induct. appl Math., v. 7 (1959). [3] *R. Pelce, P. Egreen*, A communication technique for multipath channels, Prac., v. 46 (1958).