ՀԱՅԿԱԿԱՆ ՍՍՀ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԿԱԴԵՄԻԱՅԻ ԶԵԿՈՒՅՑՆԵՐ
ДОКЛАДЫ АКАДЕМИИ НАУК АРМЯНСКОЙ ССР

LXXXIV 1987 2

УДК 512.62

МАТЕМАТИКА

М. К. Кюрегян

Квадратичные преобразования и синтез неприводимых полиномов над конечными полями

(Представлено чл.-корр. АН Армянской ССР Р. Р. Варшамовым 27/VIII 1986)

Как известно, для всякого простого p и натурального числа s существует с точностью до изоморфизма единственное поле Галуа F_q порядка $q=p^s$.

Проблема синтеза неприводимых над полем Галуа F_q полиномов заданной степени в явном виде является одной из важных и трудных проблем современной алгебры. Основа теории неприводимости заложена в работах Е. Артина, Л. Диксона, О. Оре, А. Альберта, Р. Р. Варшамова и др. Отметим, что наибольший вклад в решение данной проблемы внес Р. Р. Варшамов, получивший ряд фундаментальных результатов в области синтеза неприводимых полиномов. В частности, он рассмотрел общий подход к построению неприводимых над основным полем F_q полиномов заданной степени в явном виде. Настоящая работа, посвященная построению неприводимых над полем F_q полиномов, возникла на основе идей, изложенных в работе [1]. В ней предлагается конструктивный метод построения неприводимых полиномов, сложность которого меньше ранее известных методов. Помимо этого впервые проводится метод построения неприводимых самодвойственных полиномов над конечным полем нечетной характеристики.

В работе рассматриваются только нормированные полиномы, т. е. полиномы, старший коэффициент которых равен единице.

Теорема 1. *Пусть* $q>2$, $f(x)=\sum_{u=0}^{n} a_u x^u$ *произвольный неприводимый над полем* F_q *полином степени* n *и* σ*—порядок эл.* $\delta=(-1)^n a_0 \neq 1$, *где* a_0*—свободный член полинома* $f(x)$, $t>1$*—такое целое число, что все его простые делители* p_i *являются также делителями числа* $\sigma=\prod_{i=0}^{r} p_i^{\alpha_i}\cdot N$, *и* $(p_i, N)=1$, $p_i^{\alpha_i+1}\nmid q-1$. *Положим также, что* $t\not\equiv 0 \pmod 4$, *если* $q^n\equiv -1 \pmod 4$. *Тогда* $f_t(x)=\sum_{u=0}^{n} a_u x^{ut}$ *неприводимый над полем* F_q *полином степени* nt *и принадлежит показателю* et, *где* e*—показатель полинома* $f(x)$.

Доказательство. Пусть α—произвольный корень полинома в некотором расширении поля F_q, тогда α, α^q, α^{q^2}, ..., $\alpha^{q^{n-1}}$ образуют совокупность всех корней $f(x)$, которые имеют порядок e. По теореме Виетта

$$\alpha^{\frac{q^n-1}{q-1}} = (-1)^n a_0 = \delta, \qquad (1)$$

поэтому $e \nmid \frac{q^n-1}{q-1}$, значит, $q^n-1 = ekM$, где $k = p_1^{\beta_1} p_2^{\beta_2} \cdot \ldots \cdot p_r^{\beta_r}$,

$k_1 = p_1^{\gamma_1} p_2^{\gamma_2} \ldots \cdot p_r^{\gamma_r}$, $\gamma_i \leqslant \beta_i (i = \overline{1, r})$, $k_1 \setminus s$, $(p_i, M) = 1$, $s = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r} N$, $(p_i, N) = 1$, $p^{\alpha i+1} \nmid q-1$. С другой стороны, согласно (1) $\delta^{\frac{q-1}{k_1}} = \alpha^{e\frac{k}{k_1} M} = 1$, но это равенство невозможно, так как $s \nmid \frac{q-1}{k_1}$. Таким образом, $q^n-1 = eM$, где $(M, p_i) = 1$. Отсюда, согласно работе (2), если t удовлетворяет условиям теоремы, то полином $f_t(x)$ степени nt неприводим над полем F_q и принадлежит показателю et. Теорема доказана.

Следствие 1. *Пусть* $q > 2$, $f(x) = \sum_{u=0}^{n} a_u x^u$ *— произвольный неприводимый над полем* F_q *полином степени* n, $\delta = (-1)^n a_0$ *является примитивным элементом поля* F_q, $t > 1$ *— такое целое число, что все его простые делители являются также делителями числа* $q-1$. *Положим также, что* $t \not\equiv 0 \pmod 4$, *если* $q^n \equiv -1 \pmod 4$.

Тогда $f_t(x) = \sum_{u=0}^{n} a_u x^{ut}$ *неприводимый над полем* F_q *полином степени* nt *и принадлежит показателю* et, *где* e *— показатель полинома* $f(x)$.

Лемма 1. *Пусть* $q > 2$ *— нечетное число,* $f(x)$ *— произвольный неприводимый над полем* F_q *полином степени* n, a_0 *— свободный член полинома* $f(x)$, s *— порядок элемента* $\delta = (-1)^n a_0 \neq 1$, k *— простое число. Тогда корень* α *полинома* $f(x)$ *не может быть представлен в виде* k*-ой степени ни одного из элементов поля* F_{q^n}, *если* $s = k^m N$, $(k, N) = 1$, *но* $k^{m+1} \nmid q-1$.

Доказательство. Из доказательства теоремы 1 следует, что $q^n - 1 = eM$, где e — показатель полинома $f(x)$ и $k \setminus e$, $(k, M) = 1$. Пусть β — некоторый примитивный элемент поля F_{q^n}, тогда, как известно, $\alpha = \beta^v$, так что $e = \frac{q^n-1}{(v, q^n-1)} = \frac{eM}{(v, eM)}$, а это значит, что $k \nmid v$. С другой стороны, если $\alpha = \theta^k$, где $\theta \in F_{q^n}$, то $\alpha = (\beta^r)^k = \beta^{rk}$, где $\theta = \beta^r$, следовательно $\beta^{rk-v} = 1$. Отсюда вытекает, что $rk = (q^n-1)u + v$, а это невозможно, так как $k \nmid v$. Лемма доказана.

Элемент $\alpha \in F_q$ будем называть квадратом, если можно указать такой элемент $\beta \in F_q$, что $\alpha = \beta^2$, и неквадратом в противном случае.

Следствие 2. *Пусть* $q > 2$ *— нечетное число,* $f(x)$ *— произвольный неприводимый над полем* F_q *полином степени* n, a_0 *— свободный член полинома* $f(x)$, s *— порядок эл.* $\delta = (-1)^n a_0 \neq 1$, *тогда корень* α *полинома* $f(x)$ *не является квадратом поля* F_{q^n}, *если* $s = 2^m N$, $2 \nmid N$, *но* $2^{m+1} \nmid q-1$.

Лемма 2. *Пусть* $f(x)$ *произвольный неприводимый над полем* F_q *полином степени* n, $g(x) - \alpha h(x) = \sum_{v=0}^{n_1} g_v x^v - \alpha \left(\sum_{u=0}^{n_2} h_u x^u \right)$ *неприво-*

димый над полем F_{q^n} полином, где g_v, h_u принадлежат F_q и $f(\alpha)=0$.

Тогда полином $(h(x))^n f\left(\frac{g(x)}{h(x)}\right)$ не будет разлагаться в поле F_q.

Доказательство. Учитывая неприводимость полинома $f(x)$ над полем F_q, имеем над полем F_{q^n} соотношение

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

Заменив в соотношении (2) x на $\frac{g(x)}{h(x)}$ и умножив обе части (2) на $(h(x))^n$, получим:

$$(h(x))^n f\left(\frac{g(x)}{h(x)}\right)=\prod_{u=0}^{n-1}(g(x)-\alpha^{q^u}h(x)).$$

Согласно ([3]) $(h(x))^n f\left(\frac{g(x)}{h(x)}\right)$ неприводим над полем F_q. Лемма доказана.

Теорема 2. *Пусть $q>2$ нечетное число, $f(x)$—произвольный неприводимый над полем F_q полином степени n, и a, b, c, d—произвольные элементы поля F_q, такие что $c\neq 0$. Тогда полином*

$$F(x)=(cx+d)^n f\left(\frac{x^2+ax+b}{cx+d}\right)$$

не будет разлагаться над полем F_q, если $d^2-dca+c^2b=\delta^2\neq 0$ является квадратом в поле F_q, а среди элементов $(-1)^n f\left(\frac{ac-2d+2\delta}{c^2}\right)\neq 0$ и $(-1)^n f\left(\frac{ac-2d-2\delta}{c^2}\right)\neq 0$ лишь один не является квадратом в поле F_q.

Доказательство. Пусть α—корень $f(x)$, т. е. $f(\alpha)=0$. Тогда, заменив в формуле (2) x на $\frac{x^2+ax+b}{cx+d}$ и умножив обе части (2) на $(cx+d)^n$, получим

$$(cx+d)^n f\left(\frac{x^2+ax+b}{cx+d}\right)=\prod_{u=0}^{n-1}(x^2-(c\alpha^{q^u}-a)x+b-d\alpha^{q^u}).$$

Дискриминант многочлена $x^2-(c\alpha-a)x+b-d\alpha$ согласно теореме Суона ([4]) определяется формулой $D(x^2-(c\alpha-a)x+b-d\alpha)=(c\alpha-a)^2-4(b-d\alpha)=c^2\alpha^2+2(2d-ca)\alpha+a^2-4b$.

Учитывая, что $d^2-dca+c^2b=\delta^2$ является квадратом в поле F_q, имеем $c^2x^2+2(2d-ca)x+a^2-4b=c^2\left(x-\frac{ac-2d+2\delta}{c^2}\right)\left(x-\frac{ac-2d-2\delta}{c^2}\right)$.

Учитывая, что q^n степень нечетного простого числа, по теореме Штикельбергера ([4]) квадратный многочлен неприводим над полем F_{q^n}, если его дискриминант есть неквадрат в F_{q^n}. Легко понять, что если $f(x)$ неприводим над F_q, то полиномы $f\left(x+\frac{ac-2d+2\delta}{c^2}\right)$ и

$f\left(x+\frac{ac-2d-2\delta}{c^2}\right)$ со свободными членами $f\left(\frac{ac-2d+2\varepsilon}{c^2}\right)$ и $f\left(\frac{ac-2d-2\delta}{c^2}\right)$ и с корнями $\alpha-\frac{ac-2d+2\delta}{c^2}$ и $\alpha-\frac{ac-2d-2\delta}{c^2}$ соответственно будут также неприводимы над полем F_q. Учитывая, что из $(-1)^n f\left(\frac{ac-2d+2\delta}{c^2}\right)\neq 0$ и $(-1)^n f\left(\frac{ac-2d-2\delta}{c^2}\right)\neq 0$ лишь один не является квадратом в поле F_q, нетрудно убедиться, что согласно следствию 2 лишь один из элементов $\alpha-\frac{ac-2d+2\delta}{c^2}$ и $\alpha-\frac{ac-2d-2\delta}{c^2}$ не является квадратом в поле F_{q^n}, что в свою очередь устанавливает неприводимость полинома $x^2-(c\alpha-a)x+b-d\alpha$ над полем F_{q^n}. Теперь из леммы 2 следует неприводимость полинома $(cx+d)^n f\left(\frac{x^2+ax+b}{cx+d}\right)$ над полем F_q. Теорема доказана.

Рассмотрим случай, когда $b=1$, $c=1$, $d=0$ и, следовательно, $a^2-dca+c^2b=1$.

Тогда полином $F(x)=x^n f\left(\frac{x^2+ax+1}{x}\right)$ степени $2n>0$ при любой функции $f(x)$ является самодвойственным полиномом (см. [1]). Действительно, $F^*(x)=x^{2n}F\left(\frac{1}{x}\right)=x^{2n}\frac{1}{x^n}f\left|\frac{\frac{1}{x^2}+a\frac{1}{x}+1}{\frac{1}{x}}\right|=x^n f\left(\frac{x^2+ax+1}{x}\right)=$

$=F(x)$.

Для этого случая из теоремы 2 получим следующее следствие.

Следствие 3. *Пусть $q>2$—нечетное число, $f(x)$—произвольный неприводимый над полем F_q полином степени n, a—произвольный элемент поля F_q, тогда самодвойственный полином $F(x)=x^n f\left(\frac{x^2+ax+1}{x}\right)$ неприводим над полем F_q, если из элементов $(-1)^n f(a+2)\neq 0$ и $(-1)^n f(a-2)\neq 0$ лишь один не является квадратом в поле F_q.*

Теорема 3. *Пусть $q>2$—нечетное число, $f(x)$—произвольный неприводимый над полем F_q полином степени n, δ и γ—произвольные элементы поля F_q. Тогда полином $F(x)=f(x^2+\delta x+\gamma)$ не будет разлагаться над полем F_q, если $(-1)^n f\left(\frac{4\gamma-\delta^2}{4}\right)$ не является квадратом в поле F_q.*

Доказательство. Пусть α—корень $f(x)$. Заменив в формуле (2) x на $x^2+\delta x+\gamma$, получим

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

Дискриминант многочлена $x^2+\delta x+\gamma-\alpha$ согласно ([4]) определяется формулой $D(x^2+\delta x+\gamma-\alpha)=\delta^2-4\gamma+4\alpha=4\left(\alpha-\frac{4\gamma-\delta^2}{4}\right)$.

Легко понять, что если $f(x)$ неприводим над F_q, то $f\left(x+\frac{4\gamma-\delta^2}{4}\right)$ со свободным членом $f\left(\frac{4\gamma-\delta^2}{4}\right)$ и корнем $\alpha-\frac{4\gamma-\delta^2}{4}$ будет неприводим над полем F_q. Учитывая, что $(-1)^n f\left(\frac{4\gamma-\delta^2}{4}\right)$ не является квадратом в поле F_q, нетрудно убедиться, что согласно следствию 2 $\alpha-\frac{4\gamma-\delta^2}{4}$ будет неквадратом в поле F_{q^n}, что в свою очередь устанавливает неприводимость полинома $x^2+\delta x+\gamma-\alpha$ над полем F_{q^n}. Теперь из работы ([3]) следует неприводимость полинома $f(x^2+\delta x+\gamma)$ над полем F_q.

Теорема доказана

Автор считает своим приятным долгом выразить благодарность чл.-корр. АН Армянской ССР Р. Р. Варшамову за полезные советы в процессе работы над статьей.

Вычислительный центр Академии наук
Армянской ССР и Ереванского государственного университета

Մ. Կ. ԿՅՈՒՐԵՂՅԱՆ

Վերջավոր դաշտերի վրա բառակուսային ձևափոխություններ և անվերածելի բազմանդամների սինթեզը

Աշխատանքում ապացուցված են մի շարք թեորեմներ, որոնք հնարավորություն են տալիս անվերածելի բազմանդամներ կառուցել բացահայտ տեսքով Գալուայի կամայական դաշտի վրա։

Թեորեմ 1. Ենթադրենք $q>2$ կենտ թիվ է, $f(x)$-ը n-րդ աստիճանի անվերածելի բազմանդամ է F_q Գալուայի դաշտի վրա, իսկ a, b, c, d կամայական տարրեր են Գալուայի F_q դաշտից այնպես, որ $c\neq 0$. Այդ դեպքում $F(x)=(cx+d)^n f\left(\frac{x^2+ax+b}{cx+d}\right)$ բազմանդամը անվերածելի է F_q դաշտի վրա, եթե $d^2-dca+c^2b=\delta^2\neq 0$ այսինքն քառակուսային տարր է F_q դաշտում, իսկ

$$(-1)^n f\left(\frac{ac-2d+2\delta}{c^2}\right)\neq 0 \text{ և } (-1)^n f\left(\frac{ac-2d-2\delta}{c^2}\right)\neq 0$$

տարրերից ելնշտ միայն մեկն է հանդիսանում ոչ քառակուսային տարր F_q դաշտում:

Թեորեմ 2. Ենթադրենք $q>2$ կենտ թիվ է, $f(x)$-ը n-րդ աստիճանի անվերածելի բազմանդամ է F_q Գալուայի դաշտի վրա, իսկ δ և γ—կամայական տարրեր են F_q դաշտից: Այդ դեպքում $F(x)=f(x^2+\delta x+\gamma)$ բազմանդամը անվերածելի է F_q դաշտի վրա, եթե $(-1)^n\left(\frac{4\gamma-\delta^2}{4}\right)$ հանդիսանում է ոչ քառակուսային տարր F_q դաշտում:

ЛИТЕРАТУРА — ԳՐԱԿԱՆՈՒԹՅՈՒՆ

[1] *Р. Р. Варшамов*, К математической теории кодов. Докт. дис., ИАТ АН СССР. 1966. [2] *А. А. Альберт*, Кибернетический сборник. Новая серия, Мир, М., 1966. [3] *М. К. Кюрегян*, ДАН АрмССР, т. 81, № 2 (1985). [4] *Э. Берлекэмп*, Алгебраическая теория кодирования, Мир, М., 1971.