

МАТЕМАТИКА

УДК 512.62

М. К. Кюрегян

Об одном методе построения неприводимых полиномов над полями Галуа

(Представлено чл.-корр. АН Армянской ССР Р. Р. Варшамовым 24/XII 1985)

Как известно, для любого простого p и натурального s существует, и с точностью до изоморфизма, единственное поле Галуа $GF(q)$ порядка $q = p^s$. Для того чтобы построить поле $GF(q^k)$, достаточно иметь полином степени k , неприводимый в $GF(q)$.

Имеется ряд основополагающих работ, вскрывающих элементарную структуру полей Галуа. Особенно полная теория содержится в монографии Альберта ⁽¹⁾. Единственная проблема, оставленная без внимания структурными теориями и являющаяся одновременно наиболее важной и трудной в современной алгебре, — это проблема синтеза неприводимых над полем $GF(q)$ полиномов заданной степени в явном виде.

Фундаментальные результаты конструктивной теории приводимости полиномов над конечными полями в основном принадлежат Р. Р. Варшамову ^{((2-4) и др.)}.

В работе рассматриваются возможности построения в явном виде неприводимых полиномов над конечными полями Галуа.

Будем говорить, что степень элемента α над полем $GF(q)$ равна k или же α является собственным элементом поля $GF(q^k)$, если $\alpha \in GF(q^k)$ и $\alpha \notin GF(q^v)$, где v — любой собственный делитель k . В этом случае пишется $\deg_q(\alpha) = k$.

Лемма 1. Пусть n и k — два произвольных натуральных числа, удовлетворяющих условию $(n, k) = 1$, $f(x)$ — неприводимый над полем $GF(q)$ полином степени n , α и β — произвольные элементы поля $GF(q^k)$. Тогда полином $g(x) = f(\alpha x + \beta)$ не будет разлагаться в поле $GF(q^k)$.

Доказательство. Согласно ⁽⁵⁾ полином $f(x)$ неприводим над полем $GF(q^k)$. Пусть θ — корень $f(x)$, т. е. $f(\theta) = 0$. Тогда ясно, что $\gamma = \alpha^{-1}(\theta - \beta)$ будет корнем $g(x)$. Учитывая, что $\theta^{q^{ki}} \neq \theta^{q^{kj}}$, где $i \neq j$ ($0 \leq i, j \leq n-1$), нетрудно убедиться, что и $\gamma^{q^{ki}} \neq \gamma^{q^{kj}}$. Стало быть, имеет место разложение $f(\alpha x + \beta) = \alpha^n \prod_{u=0}^{n-1} (x - \gamma^{q^{uk}})$ над полем $GF(q^k)$, что, в свою очередь, устанавливает неприводимость полинома $g(x)$ в поле $GF(q^k)$. Лемма 1 доказана.

Лемма 2. Пусть $n > 1$ и k — произвольные натуральные числа, $(n, k) = 1$, $f(x)$ — неприводимый над полем $GF(q)$ полином степени n ,

α и β — произвольные элементы поля $GF(q^k)$, удовлетворяющие условиям: $\deg_q(\alpha) = k^1$, $\deg_q(\beta) = k^2$, $\deg_q(\alpha^{-1}\beta) = k^3$ и $\varepsilon_1 + \varepsilon_2 + \varepsilon_3 > 0$, где $\varepsilon_i = 0$ или 1 ($i = \overline{1, 3}$). Тогда среди коэффициентов полинома $g(x) = f(\alpha x + \beta)$ найдется хотя бы один коэффициент g_u такой, что $\deg_q(g_u) = k$ ($u = \overline{1, n}$).

Доказательство. Допустим противное, а именно, предположим, что максимальная степень над полем $GF(q)$ среди коэффициентов полинома $g(x)$ равна $v < k$, где v собственный делитель k . Тогда элемент $\gamma = \alpha^{-1}(\theta - \beta)$, где $f(\theta) = 0$, являясь корнем неприводимого в поле $GF(q^v)$ полинома $g(x)$ степени n , будет собственным элементом поля $GF(q^{nv})$.

Рассмотрим отдельно четыре возможных случая.

1. Пусть $\deg_q(\alpha) = k$ и $\deg_q(\beta) = 1$. Поскольку $\deg_q(\theta) = n$, $\alpha = \gamma^{-1}(\theta - \beta) \in GF(q^{nv})$ и $(n, k) = 1$, то $\alpha \in GF(q^{nv}) \cap GF(q^k) = GF(q^v)$ и, следовательно, будем иметь $\deg_q(\alpha) < k$, что противоречиво.

2. Если же $\deg_q(\beta) = k$ и $\deg_q(\alpha) = 1$, то ввиду $\beta = \theta - \gamma\alpha \in GF(q^{nv})$ получим $\beta \in GF(q^{nv}) \cap GF(q^k) = GF(q^v)$, так как $(n, k) = 1$ и $\deg_q(\beta) < k$, что также противоречиво.

3. Пусть теперь $\deg_q(\alpha) = \deg_q(\beta) = k$ и $\alpha^{-1}\beta \in GF(q)$. Имеем $\gamma = \alpha^{-1}\theta - \alpha^{-1}\beta$, откуда $\alpha = \theta(\gamma - \alpha^{-1}\beta)^{-1} \in GF(q^{nv})$, т. е. $GF(q^{nv}) \cap GF(q^k) = GF(q^v)$ и, следовательно, $\deg_q(\alpha) < k$, что невозможно. И, наконец,

4. Пусть $\deg_q(\alpha) = \deg_q(\beta) = \deg_q(\alpha^{-1}\beta) = k$. Находим $\gamma = \alpha_1\theta + \alpha_2$, где $\alpha_1 = \alpha^{-1}$ и $\alpha_2 = -\alpha^{-1}\beta$ собственные элементы поля $GF(q^k)$. Если нам удастся показать, что выражение $\alpha_1\theta + \alpha_2$ является собственным элементом поля $GF(q^{kn})$, то тем самым мы достигнем нашей цели. Однако для этого достаточно будет доказать, что ни один из элементов группы Галуа поля $GF(q^{kn})$ над полем $GF(q)$ не может оставлять элемент $\alpha_1\theta + \alpha_2$ неподвижным.

Пусть $GF(q^{kn})$, $GF(q^k)$ и $GF(q^n)$ — расширения Галуа над полем $GF(q)$ с группами Галуа G , G_1 и G_2 соответственно. Как известно, если $(n, k) = 1$, т. е. $GF(q^n) \cap GF(q^k) = GF(q)$, то группа Галуа G есть прямое произведение циклических групп Галуа G_1 и G_2 , поэтому элемент группы Галуа G будет представляться парой автоморфизмов (σ, τ) , где $\sigma \in G_1$ и $\tau \in G_2$ ⁽⁸⁾.

Итак, если предположить, что элемент $\gamma = \alpha_1\theta + \alpha_2$ — несобственный, то $\alpha_1^{\sigma}\theta^{\tau} + \alpha_2^{\sigma} = \alpha_1\theta + \alpha_2$. Отсюда находим $\theta^{\tau} = \frac{\alpha_2 - \alpha_2^{\sigma}}{\alpha_1^{\sigma}} 1 + \frac{\alpha_1}{\alpha_1^{\sigma}} \theta$.

Обозначив $\frac{\alpha_2 - \alpha_2^{\sigma}}{\alpha_1^{\sigma}} = a_1$ и $\frac{\alpha_1}{\alpha_1^{\sigma}} = a_2$, получим $\theta^{\tau} = a_1 1 + a_2 \theta$ и элемент θ^{τ} будет линейно выражаться через 1 и θ . Но поля $GF(q^k)$ и $GF(q^n)$ линейно разделены на $GF(q)$. Поэтому из линейной зависимости $\theta^{\tau} = a_1 + a_2\theta$ с коэффициентами a_1, a_2 из $GF(q^k)$ вытекает линейная зависимость $\theta^{\tau} = b_1 \cdot 1 + c_1\theta$ с коэффициентами b_1, c_1 из $GF(q)$ ⁽⁷⁾. Отсюда имеем $b_1 + c_1\theta = a_1 + a_2\theta$, а это значит, что $b_1 = a_1$, $c_1 = a_2$, ибо иначе $(c_1 - b_1) \cdot 1 + (a_2 - c_1)\theta = 0$, т. е. 1 и θ линейно-зависимы с коэффициентами из поля $GF(q^k)$.

Стало быть, 1 и θ линейно-зависимы с коэффициентами из

$GF(q)$, что невозможно, так как θ собственный элемент для $GF(q^n)$. Далее, учитывая, что $x_1^2\theta^2 + \alpha_2^2 = \alpha_1^2\theta^2 + \alpha_2^2 = \alpha_1\theta + \alpha_2$, получим $\theta^2 = \frac{\alpha_1}{\alpha_1^2}\theta + \frac{\alpha_2 - \alpha_2^2}{\alpha_1^2}$.

С другой стороны, $\theta^2 = (b_1 + c_1\theta)^2 = b_2 + c_1^2\theta$, где $b_2 = b_1 + c_1b_1$, поэтому $\frac{\alpha_1}{\alpha_1^2} = c_1^2$. Аналогично $\theta^i = \frac{\alpha_1}{\alpha_1^i}\theta + \frac{\alpha_2 - \alpha_2^i}{\alpha_1^i}$ и $\theta^i = b_i + c_1^i\theta$, где $b_i = b_{i-1} + c_1^{i-1}b_{i-1}$, откуда $\frac{\alpha_1}{\alpha_1^i} = c_1^i$. Следовательно, если t_1 порядок элемента σ , т. е. $\sigma^{t_1} = 1$, то $c_1^{t_1} = 1$ и, значит, порядок c_1 делит порядок σ . Имеем $\theta^i = c_1^i\theta + b_i$, где c_1 и $b_i \in GF(q)$. Поэтому, если t_2 — порядок τ , т. е. $\tau^{t_2} = 1$, то $\theta = \theta^{\tau^{t_2}} = c_1^{t_2}\theta + b_i$ и $c_1^{t_2} = 1$, $b_i = 0$. Стало быть порядок c_1 делит порядок элемента τ . Но порядки элементов σ и τ взаимно-просты, так как $t_1 \nmid k$, $t_2 \nmid n$ и $(n, k) = 1$, а поэтому $c_1 = 1$, что невыполнимо, так как $\alpha_1^2 \neq \alpha_1$. Этим устанавливается, что элемент $\alpha_1\theta + \alpha_2$ собственный для поля $GF(q^{kn})$ и тем самым лемма 2 доказана полностью.

Опираясь на полученные результаты и используя работу (5), можно доказать следующий факт.

Теорема. Пусть n и k ($k = mt$) — произвольные натуральные числа, $(n, k) = 1$, $f(x)$ — неприводимый над полем $GF(q)$ полином степени n , α и β — произвольные элементы поля $GF(q^k)$, удовлетворяющие условиям леммы $2f(\alpha x + \beta) = g(x) = \sum_{u=0}^n g_u x^u$, и пусть, кроме того, среди коэффициентов полинома $g(x)$ существует, по крайней мере, один коэффициент g_u ($u < n$) такой, что $\deg_q(g_u^{-1}g_u) = k$. Тогда для любого целого числа i ($0 \leq i < ms$) полином степени tn

$$F(x) = \prod_{u=0}^{t-1} g^{(smu+i)}(x),$$

где $g^{(a)}(x) = \sum_{u=0}^n g_u^{p^a} x^u$, будет неприводимым над полем $GF(q^m)$.

Для иллюстрации рассмотрим следующий пример. Пусть $q = 2$, $f(x) = x^3 + x + 1$, $k = 3$ и $t = 3$. Пусть, кроме того, даны два элемента поля $GF(2^3)$, $\alpha = 1$ и β , где β — корень неприводимого в $GF(2)$ полинома $x^3 + x + 1$, т. е. $\beta^3 + \beta + 1 = 0$. Тогда, полагая $g(x) = f(x + \beta) = x^3 + x + \beta^3 + \beta + 1$ и $i = 0$, согласно теореме будем иметь $F(x) = (x^3 + x + \beta^3)(x^3 + x + \beta^3)(x^3 + x + \beta^3)$, где $\beta^{10} = \beta^3$ и $\beta^{20} = \beta^6$, и после раскрытия скобок и приведения подобных членов окончательно получим неприводимый над полем $GF(2)$ полином $F(x) = x^6 + x^5 + x^3 + x^2 + 1$.

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

Вычислительный центр Академии наук Армянской ССР
и Ереванского государственного университета

Գալուայի դաշտերի վրա շրջավոր բազմանդամների կառուցման
մի մեթոդի մասին

Գալուայի դաշտերի վրա բազմանդամների շրջավորության արտակարգ
ինքնուրույն հետաքրքրությունն ներկայացնող պրոբլեմը կարևոր դեր է կա-
տարում ժամանակակից տեխնիկայում: Հոդվածում հետազոտվում է $\alpha x + \beta$
զծային ձևափոխությունը, որտեղ α և β վերցված են Գալուայի $GF(q^k)$
դաշտից: Այս գծային ձևափոխությունը թույլ է տալիս կառուցել բացահայտ
տեսքով շրջավոր բազմանդամները՝ Գալուայի կամայական դաշտի վրա:

Այսինքն ապացուցվում է հետևյալը:

Թեորեմ. Դիցուք n և k -ն կամայական փոխադարձաբար պարզ
թվեր են, այսինքն $(n, k) = 1$, $f(x)$ շրջավոր n -րդ աստիճանի բազմանդամ
է Գալուայի $GF(x)$ դաշտի վրա, իսկ α և β կամայական տարրեր են Գա-
լուայի $GF(q^k)$ դաշտից: Եթե α և β տարրերից մեկը սեփական է $GF(q^k)$
դաշտի համար, ապա ցանկացած $i (0 \leq i < ms)$ բնական թվի համար tn -րդ
($k = tm$) աստիճանի բազմանդամը $F_i(x) = \prod_{u=0}^{t-1} g^{(smu+i)}(x)$, որտեղ $g(x) =$
 $= f(\alpha x + \beta) = \sum_{u=0}^n g_u x^u$ և $g^{(a)}(x) = \sum_{u=0}^n g^{p^a} x^u$, շրջավոր է $GF(q^m)$ դաշտի
վրա, եթե $\deg g_u g_n^{-1} = k$ ինչ-որ u -ի ($u = \overline{1, n-1}$) համար:

ЛИТЕРАТУРА — ԳՐԱԿԱՆՈՒԹՅՈՒՆ

- ¹ A. A. Albert, Fundamental concepts of higher algebra, Univ. of Chicago
Press, 1956. ² P. P. Варшамов, Studia Scleticarum Mathematicarum Hungarica, p.
5—19, 1973. ³ P. P. Варшамов, ДАН СССР, т. 211, № 4 (1973). ⁴ P. P. Варшамов,
ДАН СССР, т. 275, № 5 (1984). ⁵ М. Г. Кюрөгян, ДАН АрмССР, т. 81, № 2 (1985).
⁶ С. Ленг, Алгебра, Мир, М., 1968. ⁷ Н. Бурбаки, Алгебра. Ч. 2, Наука, М., 1965.