ՀԱՅԿԱԿԱՆ ՍՍՀ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԿԱԴԵՄԻԱՅԻ ԶԵԿՈՒՅՑՆԵՐ
ДОКЛАДЫ АКАДЕМИИ НАУК АРМЯНСКОЙ ССР

LXXXI 1985 2

УДК 512.62

МАТЕМАТИКА

М. К. Кюрегян

Разложение полиномов и синтез неприводимых полиномов над конечными полями

(Представлено чл.-корр. АН Армянской ССР Р. Р. Варшамовым 3/II 1985)

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

В настоящей работе приводятся некоторые результаты относительно возможности построения неприводимых полиномов; если полином неприводим над полем $GF(q)$, то какой вид имеет его разложение над полем $GF(q^m)$.

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

Пусть $f(x)=\sum_{u=0}^{n} a_u x^u$—неприводимый над полем $GF(q)$ полином степени n. Известно, что все корни полинома $f(x)$ принадлежат полю $GF(q^k)$, где $n \setminus k$ и $GF(q^n)$—минимальное поле, содержащее все корни полинома $f(x)$.

Кроме того, если α—корень полинома $f(x)$ в расширении поля $GF(q)$, то α, α^q, ..., $\alpha^{q^{n-1}}$ образуют совокупность всех корней $f(x)$ ([2]).

Пусть β—любой элемент расширения $GF(q)$. Полином $g(x)$, наименьшей степени над полем $GF(q)$, такой, что $g(\beta)=0$, называется минимальным полиномом или минимальной функцией для β. Ясно, что минимальная функция $g(x)$ для любого элемента β является неприводимым многочленом над полем $GF(q)$ ([1]).

Элементы поля, минимальные многочлены которых равны, называются сопряженными. Значит, элементы α, α^q, ..., $\alpha^{q^{n-1}}$ являются сопряженными.

Будем говорить, что β является собственным элементом расширения поля $GF(q)$ степени m, если $\beta \in GF(q^m)$ и $\beta \notin GF(q^d)$, где d—любой собственный делитель m. В этом случае пишется $\deg(\beta)=m$.

Теперь приведем некоторые результаты.

Теорема 1. *Если $(m, n)=d$ и $f(x)$—неприводимый над полем $GF(q)$ полином степени n, то разложение полинома $f(x)$ над полем $GF(q^m)$ содержит d различных неприводимых над полем $GF(q^m)$ полиномов степени n/d, все коэффициенты которых принадлежат полю $GF(q^d)$ и которые имеют хотя бы один коэффициент b_u такой, что $\deg(b_u)=d$.*

Пусть дан произвольный полином $g(x)=\sum_{u=0}^{k} b_u x^u$ степени k с коэффициентами из поля $GF(q^m)$. Обозначим

$$g^{(q^l)}(x)=\sum_{u=0}^{k} b_u^{q^l} x^u.$$

Теорема 2. *Пусть $f(x)$—произвольный неприводимый над полем $GF(q)$ полином степени n, а $g(x)$—простой делитель степени n/d полинома $f(x)$ над полем $GF(q^m)$, где $(n, m)=d$. Тогда полиномы $g^{(q^l)}(x)$, где $0\leqslant l<d$, неприводимы над полем $GF(q^m)$ и $f(x)=\prod_{l=0}^{d-1} g^{(q^l)}(x)$ над полем $GF(q^m)$.*

Доказательство. В самом деле, пусть $f(x)$—неприводимый над полем $GF(q)$ полином степени n. Тогда согласно теореме 1, если $(m, n)=d$, то разложение полинома $f(x)$ над полем $GF(q^m)$ содержит d различных неприводимых над полем $GF(q^m)$ полиномов степени n/d, все коэффициенты которых принадлежат $GF(q^d)$ и которые имеют хотя бы один коэффициент b_u такой, что $\deg(b_u)=d$, т. е.

$$f(x)=\prod_{j=1}^{d} f_j(x). \tag{1}$$

Как уже отмечалось выше, поле $GF(q^n)$ содержит все корни полинома $f(x)$, и если α—произвольный корень $f(x)$, то элементы α^q, α^{q^2}, ..., $\alpha^{q^{n-1}}$ также являются его корнями и все они различные, так как $f(x)$ неприводим над полем $GF(q)$. По этой же причине, так как согласно теореме 1 $f_j(x)$—различные неприводимые над полем $GF(q^d)$ полиномы степени n/d, все корни полиномов $f_j(x)$ принадлежат $GF(q^n)$ и они различные. Вследствие того, что $f_j(x)$—различные полиномы (неприводимые) над полем $GF(q^m)$, и согласно соотношению (1) множества корней полиномов $f(x)$ и $f_j(x)$ совпадают.

Допустим, α—корень полинома $f(x)$, являющийся одновременно корнем полинома $g(x)$. Общность доказательства теоремы не нарушится, если предположить, что $f_1(x)=g(x)$. Ясно, что α, α^{q^d}, $\alpha^{q^{2d}}$, ..., $\alpha^{q^{\left(\frac{n}{d}-1\right)d}}$ являются корнями полинома $f_1(x)$. Теперь нетрудно убедиться в том, что α, α^q, ..., $\alpha^{q^{d-1}}$ корни различных многочленов, входящих в разложение $f(x)$. Так как их количество равно d, то в разложении (1) каждый полином $f_j(x)$ имеет корень из множества α, α^q, ..., $\alpha^{q^{d-1}}$.

Допустим, α^{q^l}, где $0\leqslant l<d$, является корнем многочлена $f_{l+1}(x)$ и покажем, что α^{q^l} является корнем полинома $g^{(q^l)}(x)$. Действительно,

$$g^{(q^l)}(\alpha^{q^l})=\sum_{u=0}^{\frac{n}{d}} b_u^{q^l}(\alpha^{q^l})^u.$$

Отсюда в силу тождества Галуа имеем

$$g^{(q^l)}(\alpha^{q^l})=\left(\sum_{u=0}^{\frac{n}{d}} b_u\alpha^u\right)^{q^l}=(g(\alpha))^{q^l}=0.$$

Но, так как $f_{l+1}(x)$ является минимальным полиномом α^{q^l}, то $f_{l+1}(x)\setminus g^{(q^l)}(x)$. Учитывая, что $st(f_{l+1}(x))=st(g^{(q^l)}(x))$, и нормированность $f_{l+1}(x)$ и $g^{(q^l)}(x)$, получим $f_{l+1}(x)=g^{(q^l)}(x)$. Значит, $g^{(q^l)}(x)$—неприводимый над полем $GF(q^m)$ полином, и этот полином делит $f(x)$ над полем $GF(q^m)$. Тем самым теорема полностью доказана.

Теорема 3. *Пусть $g(x)$—произвольный неприводимый над полем $GF(q^m)$ полином степени n, все коэффициенты которого принадлежат полю $GF(q^d)$, где $d\setminus m$, и который имеет хотя бы один коэффициент* $\deg(a_u)=d$. *Тогда полиномы вида $g^{(q^l)}(x)$, где $1\leqslant i<d$, неприводимы над полем $GF(q^m)$.*

Доказательство. Ясно, что $g(x)$ неприводим над полем $GF(q^d)$. Допустим, что полином $g(x)$ принадлежит показателю e и α является произвольным корнем $g(x)$ в некотором расширении поля $GF(q^d)$. Тогда e является порядком α. Как известно, $e\setminus q^{dn}-1$ и $e\nmid q^k-1$, если $k<dn$ (1). Используя этот факт, докажем, что существует неприводимый над полем $GF(q)$ полином $f(x)$ степени dn, который делится на $g(x)$ над полем $GF(q^d)$. Действительно, согласно теореме Дедекинда полином $x^{q^{dn}-1}-1$ имеет над полем $GF(q)$ следующее разложение:

$$x^{q^{dn}-1}-1=\prod_{v\setminus dn} J_v(x),$$

где $J_v(x)$—произведение всевозможных неприводимых над полем $GF(q)$ полиномов степени v (1). Следовательно, так как $e\setminus q^{dn}-1$, то получим

$$\prod_{v\setminus dn} J_v(\alpha)=\alpha^{q^{dn}-1}-1=0. \qquad (2)$$

Если одновременно с формулой (2) учесть также сепарабельность $x^{q^{dn}-1}-1$ над полем $GF(q)$ (2), то станет ясно, что существует единственный неприводимый над полем $GF(q)$ полином $f(x)$ такой, что $f(\alpha)=0$, следовательно, $g(x)\setminus f(x)$ над полем $GF(q^d)$. Покажем, что $st(f(x))=dn$. Действительно, если предположить, что $st(f(x))=k<dn$, то, так как $f(\alpha)=0$, $e\setminus q^k-1$, что невозможно. Теперь, используя теорему 2, получим, что полиномы $g^{(q^i)}(x)$ неприводимы над полем $GF(q^d)$.

Теорема 4. *Пусть $g(x)$—произвольный неприводимый над полем $GF(q^m)$ полином степени n, все коэффициенты которого принадлежат $GF(q^d)$ и который имеет хотя бы один коэффициент a_u такой, что* $\deg(a_u)=d$, *где $d\setminus m$. Тогда полином вида $f(x)=\prod_{i=0}^{d-1} g^{(q^i)}(x)$ неприводим над полем $GF(q)$.*

Доказательство. Пусть полином $g(x)$ принадлежит показателю e. Как известно, количество неприводимых над полем $CF(q^m)$

полиномов степени n, принадлежащих показателю e, равно $\frac{\varphi(e)}{n}$, где $\varphi(e)$—функция Эйлера. Как доказано выше, если существует неприводимый над полем $GF(q^m)$ полином степени n, все коэффициенты которого принадлежат $GF(q^d)$, и существует хотя бы один коэффициент a_u такой, что $\deg(a_u)=d$, то если этот полином принадлежит показателю e, то существует неприводимый над полем $GF(q)$ полином степени nd. Как известно, из существования одного полинома степени nd, принадлежащего показателю e и неприводимого над полем $GF(q)$, следует существование $\frac{\varphi(e)}{dn}$ таких же полиномов.

Используя теорему 1 и учитывая, что разложения над полем $GF(q)$ полиномов $f_1(x)$ и $f_2(x)$ не могут иметь общего множителя, получим следующее: разложение над полем $GF(q^d)$ всевозможных неприводимых над полем $GF(q)$ полиномов степени nd и принадлежащих показателю e содержат ровно $\frac{d\varphi(e)}{nd}=\frac{\varphi(e)}{n}$ различных неприводимых над полем $GF(q^d)$ полиномов степени n, принадлежащих показателю e. Теперь ясно, что для любого неприводимого над полем $GF(q^m)$ полинома $g(x)$ степени n, все коэффициенты которого принадлежат $GF(q^d)$ и который имеет хотя бы один коэффициент a_u такой, что $\deg(a_u)=d$, имеется неприводимый над полем $GF(q)$ полином $f(x)$ степени nd, который делится на полином $g(x)$ над полем $GF(q^m)$. Следовательно, согласно теореме 2 получим $f(x)=\prod_{l=0}^{d-1} g^{(q^l)}(x)$, что и требовалось доказать.

Следствие 1. *Если $f(x)$—произвольный неприводимый над полем $GF(q^m)$ полином степени n, принадлежащий показателю e, все коэффициенты которого принадлежат полю $GF(q^d)$, где $d \setminus m$, и который имеет хотя бы один коэффициент $\deg(a_u)=d$, тогда $f^{(q^i)}(x)$ неприводимый над полем $GF(q^m)$ полином степени n для любого $0<i<d$, принадлежащий показателю e, а $F(x)=\prod_{i=0}^{d-1} f^{(q^i)}(x)$—неприводимый над полем $GF(q)$ и принадлежащий показателю e.*

Следствие 2. *Если $f(x)$—произвольный неприводимый над полем $GF(q^m)$ и примитивный над полем $GF(q^d)$ полином степени n, все коэффициенты которого принадлежат полю $GF(q^d)$, где $d \setminus m$, то $f^{(q^i)}(x)$, где $0<i<m$, примитивен над полем $GF(q^d)$, а $F(x)=\prod_{i=0}^{d-1} f^{(q^i)}(x)$—примитивный над полем $GF(q)$ полином степени dm.*

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

Вычислительный центр
Академии наук Армянской ССР
и Ереванского государственного университета

Մ. Կ. ՆՅՈՒՐՆՎՅԱՆ

Վերջավոր դաշտերի վրա բազմանդամների վերածելիությունը և անվերածելի բազմանդամների սինթեզը

Աշխատանքում ապացուցված են մի շարք թեորեմներ, որոնք հնարավորություն են տալիս անվերածելի բազմանդամներ կառուցել բացահայտ տեսքով՝ Գալուայի կամայական դաշտի վրա։ Բացի այդ, ստացված է Գալուայի $GF(q)$ դաշտի վրա անվերածելի բազմանդամների վերածելիության տեսքը $GF(q^m)$ դաշտի վրա։

ЛИТЕРАТУРА — ԴՐԱԿԱՆՈՒԹՅՈՒՆ

[1] *А. А. Альберт.* Кибернетический сборник. Новая серия, вып. 3, Мир, М., 1966.
[2] *Р. Р. Варшамов.* К математической теории кодов, докт. дис., ИАТ АН СССР, 1966.