ՀԱՅԿԱԿԱՆ ՍՍՀ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԿԱԴԵՄԻԱՅԻ ԶԵԿՈՒՅՑՆԵՐ
ДОКЛАДЫ АКАДЕМИИ НАУК АРМЯНСКОЙ ССР

LXXXIV 1987 4

УДК 512.62

МАТЕМАТИКА

М. К. Кюрегян

Операторные подстановки Варшамова в поле Галуа и их приложение

(Представлено чл.-корр. АН Армянской ССР Р. Р. Варшамовым 25/XI 1986)

Статья посвящена изложению некоторых результатов конструктивной теории синтеза неприводимых полиномов над полем Галуа. Идейно она тесно связана с работами Р. Р. Варшамова, и поэтому все определения и обозначения взяты из ([1]).

Пусть $GF(q)$—поле Галуа порядка $q=p^s$, $\sigma_q^l(g(x), \delta)=$ $=\sum_{u=0}^{n} a_u\left(\sum_{v=0}^{m} b_v x^{q^v}+\delta\right)^u$—оператор, областью определения которого 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 $GF(q^r)$.

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 $\alpha \overline{\in} GF(q^d)$, где d—любой собственный делитель k. В этом случае пишется $deg_q(\alpha)=k$.

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

Теорема 1. *Пусть* $(rn, q^m-1)=1$, $g(x)\neq x-1$ *примитивный над полем* $GF(q)$ *полином степени* m, $f(x)$*—неприводимый над полем* $GF(q^r)$ *полином степени* n, $\sigma_q^x(g(x), 0)\equiv R(x)(\mathrm{mod}\, f(x))$ *и* $\psi(x)=$ $=\sum_{u=0}^{n} \psi_u x^u$, *где* ψ_u*—нетривиальное решение сравнения*

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

Тогда полиномы $\psi(x)$ *и* $F(x)=(f(x))^{-1}\sigma_q^{\psi}(g(x), 0)$ *степени* n *и* $n(q^m-1)$ *соответственно неприводимы над полем* $GF(q^r)$.

Доказательство. При $n=1$ доказательство теоремы следует из ([2]). Поэтому докажем ее для $n>1$.

Согласно ([2]) полином $H(x)=x^{-1}\sigma_q^x(g(x), 0)$ неприводим над полем $GF(q)$. Так как $(rn, q^m-1)=1$, то из работы ([3]) следует, что полином $H(x)$ неприводим также и над полем $GF(q^{rn})$. Пусть α—корень $f(x)$, т. е. $f(\alpha)=0$, тогда среди коэффициентов полинома $H(x-\alpha)=h(x)=$ $=\sum_{u=0}^{q^m-1} h_u x^u$ согласно ([4]), поскольку $n>1$, найдется хотя бы один

коэффициент такой, что $\deg_{q^r}(h_u)=n(u=\overline{0, q^m-2})$. Если одновременно с этим учесть также следующую легко доказываемую формулу $h^{(v)}(x)=H(x-\alpha^{q^{rv}})=\sum_{u=0}^{q^m-1} h_u^{q^{rv}} x^u$, где h_u $(u=\overline{0, q^m-1})$—коэффициенты полинома $h(x)$, то согласно (3) полином $F(x)=\prod_{v=0}^{n-1} h^v(x)$ будет неприводимым над полем $GF(q^r)$. Поэтому

$$\prod_{u=0}^{n-1}\left(\sigma_q^x(g(x), 0)-\left(\sum_{v=0}^{m} b_v x^{q^v}\right)^{q^{ru}}\right)=\prod_{u=0}^{n-1}(x-\alpha^{q^{ru}})h^{(u)}(x)=f(x)F(x). \quad (1)$$

Покажем теперь, что $\sum_{v=0}^{m} b_v\alpha^{q^v}=\beta$ является собственным элементом поля $GF(q^{rn})$. Допустим противное, а именно предположим, что максимальная степень элемента β над полем $GF(q^r)$ равна d, т. е. $\deg_{q^r}(\beta)=d$, где d—собственный делитель n. Тогда $\prod_{u=0}^{n-1}(x-\beta^{q^{ru}})=(\psi(x))^k$ $(n=dk, k>1)$, следовательно, согласно (1) будем иметь $(\psi(\sigma_q^x(g(x), 0))^k=f(x)F(x)$. Но поскольку полиномы $f(x)$ и $F(x)$ неприводимы, то имеем $k=2$ и $n=n(q^m-1)$, что невозможно. Значит, β является собственным элементом поля $GF(q^{rn})$, что в свою очередь устанавливает неприводимость полинома $\psi(x)=\sum_{u=0}^{n-1}(x-\beta^{q^{ru}})$ над полем $GF(q^r)$.

Таким образом, в силу (1) полином $F(x)=(f(x))^{-1}\psi(\sigma_q^x(g(x), 0))$ будет неприводим над полем $GF(q^r)$.

Нетрудно убедиться, что $\psi(R(x))\equiv 0(\mathrm{mod} f(x))$ или

$$\sum_{u=0}^{n}\psi_u(R(x))^u\equiv 0(\mathrm{mod} f(x)), \quad (2)$$

где $\psi_u(u=\overline{0, n})$ являются нетривиальным решением (2) и $\sigma_q^x(g(x), 0)\equiv R(x)(\mathrm{mod} f(x))$, что и требовалось доказать.

Следствие. *Пусть* $a_l=\sum_{u=0}^{[n^{-1}(m-i)]} b_{nu+i}(i=\overline{1, n-1})$ *и пусть кроме того для некоторого* i, $a_l\neq 0$, $a_j=0(j\neq i)(j=\overline{1, n-1})$. *Тогда многочлен* $F(x)=(f(x))^{-1}f(a_i^{-1}\sigma_q^x(g(x), 0))$ *неприводим над полем* $GF(q^r)$.

В дальнейшем нам будет полезным преобразование Варшамова.

Теорема 2. *Пусть* $q^n>2$, $f(x)$—*примитивный над полем* $GF(q)$ *полином степени* n, β *и* γ—*произвольные элементы поля* $GF(q)$ *такие, что* $\beta+\gamma\neq 0$, $h(x)=f((\beta+\gamma)x+1)$, $h^*(x)=x^n h(1/x)$. *Тогда полином* $F(x)=(x-\gamma)^n f((x-\gamma)^{-1}(x^{q^n}+\beta))(h^*(x-\gamma))^{-1}$ *степени* $n(q^n-1)$ *не будет разлагаться над полем* $GF(q)$.

Доказательство. Пусть α—корень уравнения $f(x)=0$. Тогда, учитывая неприводимость полинома $f(x)$ в поле $GF(q)$, мы получим соотношение

$$f(x)=\prod_{u=0}^{n-1}(x-\alpha^{q^u}). \quad (3)$$

Заменив в (3) x на $(x-\gamma)^{-1}(x^{q^n}+\beta)$ и умножив его обе части на $(x-\gamma)^n$, получим:

$$(x-\gamma)^n f((x-\gamma)^{-1}(x^{q^n}+\beta))=\prod_{u=0}^{n-1}(x^{q^n}-\alpha^{q^u}x+\beta+\gamma\alpha^{q^u}). \qquad (4)$$

Так как $q^n>2$ и элемент α^{q^u} примитивен в поле $GF(q^n)$, то согласно теореме Диксона ([5]) каждый из полиномов $x^{q^n}-\alpha^{q^u}x+\beta+\gamma\alpha^{q^u}$ является произведением линейного множителя на неприводимый в поле $GF(q^n)$ полином степени q^n-1. Заметим, что в поле $GF(q^n)$ легко найти корень полинома $x^{q^n}-\alpha^{q^u}x+\beta+\gamma\alpha^{q^u}$. Действительно, если $\theta\in GF(q^n)$, то $\theta^{q^{n+u}}=\theta^{q^u}$ $(u=\overline{0,\ n-1})$, и поэтому $\theta^{q^u}(\alpha^{q^u}-1)=\beta+\gamma\alpha^{q^u}$ в том и только том случае, если $\theta^{q^u}=(\beta+\gamma\alpha^{q^u})(\alpha^{q^u}-1)^{-1}$. Стало быть $x^{q^n}-\alpha^{q^u}x+\beta+\gamma\alpha^{q^u}=(x-\theta^{q^u})(x^{q^n-1}+\theta^{q^u}x^{q^n-2}+\theta^{2q^u}x^{q^n-3}+\ldots+\theta^{(q^n-2)q^u}x+1-\alpha^{q^u})=(x-\theta^{q^u})Q^{(u)}(x)$, где $u=\overline{0,\ n-1}$.

Из (4) непосредственно вытекает выражение

$$(x-\gamma)^n f((x-\gamma)^{-1}(x^{q^n}+\beta))=\prod_{u=0}^{n-1}(x-\theta^{q^u})Q^{(u)}(x).$$

Как легко показать, каждый из полиномов $Q^{(u)}(x)$ имеет хотя бы один коэффициент, являющийся собственным элементом поля $GF(q^n)$, поэтому из работы ([3]) следует неприводимость полинома $\prod_{u=0}^{n-1}Q^{(u)}(x)$ над полем $GF(q)$.

Таким образом, исходя из того, что θ является собственным элементом поля $GF(q^n)$, мы получим $(x-\gamma)^n f((x-\gamma)^{-1}(x^{q^n}+\beta))=H(x)F(x)$.

Покажем теперь, что $\prod_{u=0}^{n-1}(x-\theta^{q^u})=H(x)=h^*(x-\gamma)$. Действительно, $\theta^{q^u}=(\beta+\gamma)(\alpha^{q^u}-1)^{-1}+\gamma$, и так как $(\beta+\gamma)^{-1}(\alpha^{q^u}-1)$ является корнем полинома $h(x)=f((\beta+\gamma)x+1)$, то согласно ([6]) $(\beta+\gamma)(\alpha^{q^u}-1)^{-1}$ будет корнем $h^*(x)$, а, следовательно, θ^{q^u}—корень полинома $h^*(x-\gamma)$. Теорема доказана.

Теорема 3. *Пусть $q>2$, $(n, q-1)=1$, $f(x)$—неприводимый над полем $GF(q)$ полином степени n, θ--примитивный элемент поля $GF(q)$, δ—произвольный элемент $GF(q)$, $\sigma_q^x(x-\theta, 0)\equiv R(x)(\mathrm{mod}\, f(x))$ и $\psi(x)=\sum_{u=0}^{n}\psi_u x^u$, где ψ_u—нетривиальное решение сравнения*

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

Тогда полином $\psi(x)$ степени n, а также полином $(f(x-\delta(\theta-1)^{-1}))^{-1}\sigma_q^{\psi}(x-\theta, \delta)$ степени $n(q-1)$ неприводимы в поле $GF(q)$.

Доказательство. Для $n=1$ доказательство теоремы непосредственно следует из ([5]). Поэтому докажем ее для $n>1$.

Действительно, по теореме Диксона ([5]). полином $x^q-\theta x+\delta=$

$=(x-\beta)Q(x)$, где $Q(x)=\sum_{u=0}^{q-1}\beta^{q-1-u}x^u-\theta$, $(\beta=\delta(\theta-1)^{-1})$. Так как $(n, q-1)=1$, то согласно ([3]) полином $Q(x)$ неприводим также и над полем $GF(q^n)$. Пусть α — корень $f(x)$, тогда среди коэффициентов полинома $Q(x-\alpha)=h(x)=\sum_{v=0}^{q-1}h_vx^v$ согласно ([4]), поскольку $n>1$, найдется хотя бы один коэффициент такой, что $\deg_q(h_v)=n(v=\overline{0, q-2})$. Если одновременно с этим учесть также и следующую легко доказываемую формулу $h^{(u)}(x)=Q(x-\alpha^{q^u})=\sum_{v=0}^{q-1}h_v^{q^u}x^v$, где $h_i(v=\overline{0, q-1})$ коэффициенты полинома $h(x)$, то согласно ([3]) будет вытекать неприводимость полинома $F(x)=\prod_{u=0}^{n-1}h^{(u)}(x)$ над $GF(q)$, а поэтому

$$\prod_{u=0}^{n-1}(\sigma_q^x(x-\theta, \delta)-(\alpha^q-\theta\alpha)^{\gamma^u})=\prod_{u=0}^{n-1}(x-(\alpha+\beta)^{q^u})h^{(u)}(x).$$

Дальнейшие рассуждения аналогичны доказательству теоремы 1.

Теорема 4. *Пусть* $(n, p)=1$, $f(x)$ *— неприводимый над* $GF(q)$ *полином степени* n, $x^p+\beta x+\delta$ *— произвольный неприводимый над полем* $GF(q)$ *полином,* $x^p+\beta x\equiv R(x)(\mathrm{mod}f(x))$ *и* $\psi(x)=\sum_{u=0}^{n}\psi_ux^u$, *где* ψ_u *— нетривиальное решение сравнения*

$$\sum_{u=0}^{n}\psi_u(R(x))^u\equiv C(\mathrm{mod}f(x)). \qquad (5)$$

Тогда полином $\psi(x)$ *степени* n *и полином* $\psi(x^p+\beta x+\delta)$ *степени* pn *неприводимы над полем* $GF(q)$.

Доказательство. Сначала докажем теорему для случая $n=1$. Учитывая, что $x^p+\beta x=(x+\gamma)(x^{p-1}-\gamma x^{p-2}+\ldots+(-\gamma)^{p-2}x+(-\gamma)^{p-1}+\beta)-\gamma(\beta+\gamma^{p-1})$, где $\gamma\in GF(q)$, имеем: $(R(x))^0=1$, $R(x)=-\gamma(\beta+\gamma^{p-1})$. Согласно сравнению (5) коэффициенты $\psi(x)$ будут иметь вид: $\psi_1=1$ и $\psi_0=\gamma(\beta+\gamma^{p-1})$, следовательно $\psi(x)=x+\gamma(\beta+\gamma^{p-1})$. Таким образом, $\psi(x^p+\beta x+\delta)=(x+\gamma)^p+\beta(x+\gamma)+\delta$. Однако последний полином неприводим над полем $GF(q)$ по условию теоремы.

Рассмотрим теперь случай, когда $n>1$. Так как полином $x^p+\beta x+\delta$ неприводим над полем $GF(q)$, то согласно ([3]) он неприводим также и над полем $GF(q^n)$.

Пусть α — корень $f(x)$. Тогда согласно ([4]), поскольку $n>1$, $x^p+\beta x-(\alpha^p+\beta\alpha-\delta)$ неприводим над полем $GF(q^n)$ и $\alpha^p+\beta\alpha$ является собственным элементом поля $GF(q^n)$. Следовательно, полином

$$\psi(x)=\prod_{u=0}^{n-1}(x-(\alpha^p+\beta\alpha)^{q^u}) \qquad (6)$$

неприводим над полем $GF(q)$. Заменив в соотношении (6) x на $x^p+\beta x+\delta$, получим $\psi(x^p+\beta x+\delta)=\prod_{u=0}^{n-1}(x^p+\beta x+\delta-(\alpha^p+\beta\alpha)^{q^u})$. Следова-

тельно, согласно (3) полином $\prod_{u=0}^{n-1}(x^p+\beta x+\delta-(\alpha^p+\beta\alpha)^{q^u})$ неприводим над полем $GF(q)$. В дальнейшем теорема 4 доказывается аналогично теореме 1.

Теорема 5. *Пусть* $(rn, 2)=1$, $f(x)$—*неприводимый над полем* $GF(2^r)$ *полином степени* n, $x^4+x\equiv R(x)(\mathrm{mod} f(x))$ *и* $\psi(x)=\sum_{u=0}^{n}\psi_u x^u$, *где* ψ_u—*нетривиальное решение сравнения*

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

Тогда полином $\psi(x)$ *степени* n, *а также и полином* $\psi(x^4+x+1)$ *степени* $4n$ *неприводимы над полем* $GF(2^r)$.

Теорема 5 доказывается аналогично теореме 4.

Автор считает своим приятным долгом выразить благодарность чл.-корр. АН Армянской ССР Р. Р. Варшамову за постановку задачи и полезные советы.

Вычислительный центр Академии
наук Армянской ССР и Ереванского
государственного университета

Մ. Կ. ԿՅՈՒՐԵՂՅԱՆ

Վարշամովի տեղադրման օպերատորները Գալուայի դաշտում և նրանց կիրառությունը

Գալուայի դաշտերի վրա բազմանդամների վերլուծելիության արտակարգ ինքնուրույն հետաքրքրություն ներկայացնող պրոբլեմը կարևոր դեր է կատարում ժամանակակից տեխնիկայում։ Աշխատանքում դիտարկվում են մի շարք օպերատորներ, որոնց որոշման տիրույթը՝ Գալուայի $GF(q)$ դաշտից վերցված գործակիցներով բազմանդամներ են։

Աշխատանքում ապացուցված են մի շարք թեորեմներ, որոնք հնարավորություն են տալիս անվերածելի բազմանդամներ կառուցել բացահայտ տեսքով Գալուայի կամայական դաշտի վրա։ Բացի այդ, տրվում է Գալուայի $GF(q)$ դաշտի վրա բարձր աստիճանների անվերածելի բազմանդամների կառուցման եղանակներ։

Թեորեմ. Դիցուք $q^r>2$, $f(x)$—n-րդ աստիճանի պրիմիտիվ բազմանդամ է Գալուայի $GF(q)$ դաշտի վրա, β և γ կամայական տարբեր են $GF(q)$ դաշտից, այնպես, որ $\beta+\gamma\neq 0$, $h(x)=f[(\beta+\gamma)x+1]$ $h^*(x)=x^n h(1/x)$ Այդ դեպքում

$$F(x)=(x-\gamma)^n f((x-\gamma)^{-1}(x^{q^n}+\beta))(h^*(x-\gamma))^{-1}$$

$n(q^n-1)$ -րդ աստիճանի բազմանդամն անվերածելի է $GF(q)$ դաշտի վրա:

ЛИТЕРАТУРА — ԳՐԱԿԱՆՈՒԹՅՈՒՆ

[1] *Р. Р. Варшамов*, ДАН СССР, т. 211, № 4 (1973). [2] *Р. Р. Варшамов*, ДАН АрмССР, т. 79, № 1 (1984). [3] *М. К. Кюрегян*, ДАН АрмССР, т. 81, № 2, (1985). [4] *М. К. Кюрегян*, ДАН АрмССР, т. 83, № 2 (1986). [5] *А. А. Альберт*, Кибернетический сб. Новая серия, вып. 3, Мир, М., 1966. [6] *Р. Р. Варшамов, Г. А. Гараков*, Мат. вопр. кибернетики и вычислительной техники, т. 6 (1970)