ОБ ОДНОМ КЛАССЕ МНОГОЧЛЕНОВ НАД КОНЕЧНЫМ ТЕЛОМ

ШТЕФАН ШВАРЦ, Братислава

Пусть

$$f(x) = x^n + a_1 x^{n-1} + \dots + a_n$$

есть многочлен степени n над конечным телом $GF(p^s)$, где p — простое число, а $s \geqq 1$.

Обозначим $p^s = q$ и построим следующие выражения:

$$\begin{aligned} x^0 &\equiv c_{00} + c_{01}x + \dots + c_{0,n-1}x^{n-1}, \\ x^q &\equiv c_{10} + c_{11}x + \dots + c_{1,n-1}x^{n-1}, \\ x^{2q} &\equiv c_{20} + c_{21}x + \dots + c_{2,n-1}x^{n-1}, \qquad (\operatorname{mod} f(x)) \qquad (1) \\ &\vdots \\ x^{(n-1)q} &\equiv c_{n-1,0} + c_{n-1,1}x + \dots + c_{n-1,n-1}x^{n-1}. \end{aligned}$$

Элементы $c_{i,k}$ — многочлены от коэффициентов многочлена $f(x)$. Очевидно, будет $c_{00} = 1$, $c_{01} = c_{02} = \dots = c_{0,n-1} = 0$.

Обозначим матрицу коэффициентов (c_{ik}) символом $\mathbf{C}$, а единичную матрицу порядка n — символом $\mathbf{E}$.

Пусть σ_i означает число различных неприводимых множителей многочлена $f(x)$ степени i $(1 \leqq i \leqq n)$ над телом $GF(q)$. В частности: σ_1 означает число различных корней уравнения $f(x) = 0$ в теле $GF(q)$. Очевидно, имеет место $\sum_{i=1}^{n} i\sigma_i \leqq n$. Если $f(x)$ не имеет кратных множителей, то будет точно $\sum_{i=1}^{n} i\sigma_i = n$.

В работе [5] я доказал следующую теорему: Пусть h_t означает ранг матрицы $\mathbf{C}^t - \mathbf{E}$. Тогда числа $\sigma_1, \sigma_2, \dots, \sigma_n$ однозначно определяются системой линейных уравнений:

$$\begin{aligned} (1,1)\,\sigma_1 + (1,2)\,\sigma_2 + \dots + (1,n)\,\sigma_n &= n - h_1, \\ (2,1)\,\sigma_1 + (2,2)\,\sigma_2 + \dots + (2,n)\,\sigma_n &= n - h_2, \\ (3,1)\,\sigma_1 + (3,2)\,\sigma_2 + \dots + (3,n)\,\sigma_n &= n - h_3, \qquad (2) \\ &\vdots \\ (n,1)\,\sigma_1 + (n,2)\,\sigma_2 + \dots + (n,n)\,\sigma_n &= n - h_n, \end{aligned}$$

где (i, j) — общий наибольший делитель чисел i, j.

Цель работы — показать, что соотношения (2) особенно удобны для исследования многочленов типа

$$f(x) = x^{p^m} - ax - b, \quad a, b \in GF(p^s), \qquad (3)$$

где m/s.

Результаты, которые мы получим, приводят нас с единой точки зрения к некоторым известным результатам, полученным в литературе самыми разнообразными способами. Кроме того, мы получим несколько новых теорем, которые — поскольку мне известно из литературы — не были до сих пор опубликованы.

Замечание. Ясно, что при использовании формул (2) важно знать явные выражения для матриц $\mathbf{C}, \mathbf{C}^2, \dots, \mathbf{C}^n$. При вычислении матриц $\mathbf{C}^t$, $t > 1$, можно вместо последовательного возведения матриц в степень поступать и следующим образом. Рассмотрим соотношения

$$x^{kq} \equiv c_{k,0}^{(1)} + c_{k,1}^{(1)}x + \dots + c_{k,n-1}^{(1)}x^{n-1} \qquad (\operatorname{mod} f(x)) \qquad (4)$$

$(k = 0, 1, \dots, n-1)$, где в целях единства обозначений в дальнейшем мы положили $c_{k,i}^{(1)} = c_{k,i}$. Возведя соотношение (4) в q-ю степень, мы получим

$$x^{kq^2} \equiv c_{k,0}^{(1)} + c_{k,1}^{(1)}x^q + \dots + c_{k,n-1}^{(1)}x^{q(n-1)} \qquad (\operatorname{mod} f(x)).$$

Если сюда подставить выражения для $x^q, x^{2q}, \dots, x^{(n-1)q}$ из соотношений (1), то получим соотношения вида

$$x^{kq^2} \equiv c_{k,0}^{(2)} + c_{k,1}^{(2)}x + \dots + c_{k,n-1}^{(2)}x^{n-1} \qquad (\operatorname{mod} f(x)).$$

Ясно, что матрица $(c_{k,i}^{(2)})$ тождественна с матрицей $\mathbf{C}^2$.

Аналогично: Если $x^0, x^{q^l}, x^{2q^l}, \dots, x^{(n-1)q^l}$ выразить $(\operatorname{mod} f(x))$ в виде

$$x^{kq^l} \equiv c_{k,0}^{(l)} + c_{k,1}^{(l)}x + \dots + c_{k,n-1}^{(l)}x^{n-1} \qquad (\operatorname{mod} f(x)) \qquad (4a)$$

$(k = 0, 1, \dots, n-1)$, то матрица коэффициентов $(c_{k,i}^{(l)})$ будет в точности равна матрице $\mathbf{C}^l$. Этим замечанием мы воспользуемся позднее в разделе Б.

Рассмотрим многочлен (3)

$$f(x) = x^{p^m} - ax - b$$

и положим $p^m = r$. Из соотношения m/s следует, что существует целое число l такое, что $ml = s$. Итак, $q = p^s = r^l$.

Без ограничения общности можно в дальнейшем предполагать, что $a \neq 0$. Действительно, в случае $a = 0$ будет

$$f(x) = x^{p^m} - b = x^{p^m} - b^{p^s} = (x - b^{p^{s-m}})^{p^m}$$

Итак, мы непосредственно видим, что $f(x)$ является p^m-й степенью линейного многочлена.

Из соотношения

$$x^r \equiv ax + b \qquad (\operatorname{mod} f(x))$$

мы получаем последовательным возведением в степень

$$x^{r^2} \equiv a^r x^r + b^r \equiv a^{1+r} x + a^r b + b^r,$$
$$x^{r^3} \equiv a^{r+r^2} x^r + a^{r^2} b^r + b^{r^2} \equiv a^{1+r+r^2} x + a^{r^2+r} b + a^{r^2} b^r + b^{r^2}, \quad (\operatorname{mod} f(x))$$
$$\vdots$$
$$x^{r^l} \equiv a^{1+r+\ldots+r^{l-1}} x + \beta,$$

где

$$\beta = a^{r^{l-1}+r^{l-2}+\ldots+r} b + a^{r^{l-1}+r^{l-2}+\ldots+r^2} b^r + a^{r^{l-1}+r^{l-2}+\ldots+r^3} b^{r^2} + \ldots + a^{r^{l-1}} b^{r^{l-2}} + b^{r^{l-1}} =$$
$$= a^{\frac{q-r}{r-1}} b + a^{\frac{q-r^2}{r-1}} b^r + a^{\frac{q-r^3}{r-1}} b^{r^2} + \ldots + a^{\frac{q-r^{l-1}}{r-1}} b^{r^{l-2}} + b^{r^{l-1}} =$$
$$= a^{\frac{q-1}{r-1}} \left\{ \frac{b}{a} + \frac{b^r}{a^{1+r}} + \frac{b^{r^2}}{a^{1+r+r^2}} + \ldots + \frac{b^{r^{l-1}}}{a^{1+r+r^2+\ldots+r^{l-1}}} \right\}.$$

Если положить

$$\alpha = a^{1+r+r^2+\ldots+r^{l-1}} = a^{\frac{q-1}{r-1}},$$

получим в конце концов

$$x^q \equiv \alpha x + \beta \qquad (\operatorname{mod} f(x)).$$

Соотношения (1) имеют в нашем случае вид

$$\begin{aligned} x^0 &\equiv 1 \\ x^q &\equiv \beta + \alpha x \\ x^{2q} &\equiv \beta^2 + 2\alpha\beta x + \alpha^2 x \qquad (\operatorname{mod} f(x)) \\ &\vdots \\ x^{(r-1)q} &\equiv \beta^{r-1} + (r-1)\alpha\beta^{r-2} x + \ldots + \alpha^{r-1} x^{r-1}, \end{aligned}$$

и для матрицы $\mathbf{C}$ мы получаем выражение

$$\mathbf{C} = \begin{bmatrix} 1, & 0, & 0, & \ldots & 0 \\ \beta, & \alpha, & 0, & \ldots & 0 \\ \beta^2, & 2\alpha\beta, & \alpha^2, & \ldots & 0 \\ \vdots & & & & \\ \beta^{r-1}, & (r-1)\alpha\beta^{r-2}, & \ldots & \ldots & \alpha^{r-1} \end{bmatrix}$$

Так как непосредственное вычисление рангов матриц $\mathbf{C}^t - \mathbf{E}$ $(1 \leq t \leq r)$ затруднительно, выгодно (хотя бы в некоторых случаях) воспользоваться специальными приемами. (Смотри также подстрочное замечание[1].)

В дальнейшем мы будем различать три случая.

Случай А

Пусть $\alpha \neq 1$. Покажем, что в этом случае многочлен $f(x)$ обладает линейным множителем, т. е. уравнение

$$x^r - ax - b = 0 \qquad (5)$$

имеет корень $x_0 \in GF(p^s)$.

Для того, чтобы x_0 было корнем уравнения (5), должно быть

$$x_0^r = ax_0 + b,$$

а значит и

$$x_0^q = \alpha x_0 + \beta.$$

Так как x_0 — элемент тела $GF(p^s)$, должно иметь место $x_0 = x_0^q$. Из равенства $x_0 = \alpha x_0 + \beta$ следует $x_0 = \dfrac{\beta}{1-\alpha}$. Мы доказали: если уравнение (5) имеет корень, лежащий в теле $GF(p^s)$, то им может быть лишь элемент $x_0 = \dfrac{\beta}{1-\alpha} \in GF(p^s)$.

В том, что x_0 является действительно корнем уравнения (5), нужно убедиться подстановкой. Заметим прежде всего, что

$$\alpha^r = a^{r(1+r+\ldots+r^{l-1})} = a^{r+r^2+\ldots+r^l} = a^{r+r^2+\ldots+r^{l-1}+1} = \alpha.$$

Далее дудет

$$\beta^r = a^{r^l+\ldots+r^2} b^r + a^{r^l+\ldots+r^3} b^{r^2} + \ldots + a^{r^l} b^{r^{l-1}} + b^{r^l}.$$

Так как $a^{r^l} = a$, $b^{r^l} = b$, далее получим

$$\beta^r = a[a^{r^{l-1}+\ldots+r^2} b^r + a^{r^{l-1}+\ldots+r^3} b^{r^2} + \ldots + b^{r^{l-1}}] + b = a[\beta - a^{r^{l-1}+\ldots+r} b] +$$
$$+ b = a\beta - a^{\frac{r^l-1}{r-1}} b + b = a\beta - \alpha b + b.$$

Итак, имеет место

$$f(x_0) = \left(\frac{\beta}{1-\alpha}\right)^r - a\frac{\beta}{1-\alpha} - b = \frac{\beta^r}{1-\alpha} - a\frac{\beta}{1-\alpha} - b =$$
$$= \frac{a\beta - \alpha b + b}{1-\alpha} - \frac{a\beta}{1-\alpha} - b = 0.$$

Этим мы доказали, что x_0 является действительно нулем многочлена $f(x)$.

Многочлен $f(x)$ можно, следовательно, записать в виде

$$f(x) = f(x) - f(x_0) = (x^r - ax - b) - (x_0^r - ax_0 - b) =$$
$$= (x - x_0)^r - a(x - x_0).$$

Неприводимые множители многочлена $f(x)$ и многочлена

$$\varphi(y) = y^r - ay$$

находятся во взаимно однозначном соответствии, то есть из каждого неприводимого множителя многочлена $\varphi(y)$ можно получить неприводимый множитель многочлена $f(x)$ при помощи подстановки $y = x - x_0$ и наоборот. Поэтому мы можем ограничиться исследованием разложимости многочлена $\varphi(y)$ над телом $GF(p^s)$.

Из соотношения

$$y^r \equiv ay \qquad (\text{mod } \varphi(y))$$

получаются последовательным возведением в степень сравнения

$$\begin{aligned} y^{r^2} &\equiv a^{1+r}y, \\ y^{r^3} &\equiv a^{1+r+r^2}y, \qquad (mod\ \varphi(y)) \\ &\vdots \\ y^q &\equiv \alpha y. \end{aligned}$$

Соотношения (1) имеют для многочлена $\varphi(y)$ следующий вид:

$$\begin{aligned} y^0 &\equiv 1, \\ y^q &\equiv \alpha y, \\ y^{2q} &\equiv \alpha^2 y^2, \qquad (\text{mod } \varphi(y)) \\ &\vdots \\ y^{(r-1)q} &\equiv \alpha^{r-1} y^{r-1}. \end{aligned}$$

Соответствующей матрицей $\mathbf{C}_1$ является диагональная матрица

$$\mathbf{C}_1 = \text{diag}[1, \alpha, \alpha^2, \ldots, \alpha^{r-1}].$$

Далее имеем

$$\mathbf{C}_1^t = \text{diag}\,[1, \alpha^t, \alpha^{2t}, \ldots, \alpha^{(r-1)t}],$$

$$\mathbf{C}_1^t - \mathbf{E} = \text{diag}[0, \alpha^t - 1, \alpha^{2t} - 1, \ldots, \alpha^{(r-1)t} - 1].$$

Предположим в дальнейшем, что $\alpha = a^{\frac{q-1}{r-1}}$ принадлежит показателю $e > 1$. (Это может случиться только для $r > 2$.) Очевидно $e/r - 1$. Если $d_t = (e, t)$, то все элементы

$$\alpha^t, \alpha^{2t}, \ldots, \alpha^{\left(\frac{e}{d_t}-1\right)t}$$

будут $\neq 1$, но $\alpha^{\frac{e}{d_t}t} = 1$. В диагональной матрице $\mathbf{C}_1^t - \mathbf{E}$ первый элемент диагонали равен нулю, затем следует группа элементов

$$\alpha^t - 1, \alpha^{2t} - 1, \ldots, \alpha^{\left(\frac{e}{d_t}-1\right)t} - 1, 0,$$

которая повторяется в точности $\frac{r-1}{e} \cdot d_t$ раз. Итак,

$$\mathbf{C}_1^t - \mathbf{E} = \text{diag}[0|\alpha^t - 1, \ldots, \alpha^{\left(\frac{e}{d_t}-1\right)t} - 1, 0| \ldots |\alpha^t - 1, \ldots, \alpha^{\left(\frac{e}{d_t}-1\right)t} - 1, 0|].$$

Если в матрице $\mathbf{C}_1^t - \mathbf{E}$ выпустить строки и столбцы, содержащие нули в главной диагонали, то получится матрица порядка $r - 1 - \frac{r-1}{e} d_t$, определитель которой имеет вид

$$[(\alpha^t - 1)(\alpha^{2t} - 1) \ldots (\alpha^{\left(\frac{e}{d_t}-1\right)t} - 1)]^{\frac{r-1}{e}d_t},$$

следовательно, наверное, не равен нулю. Поэтому ранг матрицы $\mathbf{C}_1^t - \mathbf{E}$ будет равен по меньшей мере $h_t = r - 1 - \frac{r-1}{e}(e, t)$. Однако, ранг написанной матрицы равен в точности числу h_t, ибо каждый ее минор высшего порядка содержит хотя бы одну нулевую строку и равняется, следовательно, нулю.

Подставим теперь в систему уравнений (2) $h_t = r - 1 - \frac{r-1}{e}(e, t)$. Тогда мы получим следующую систему линейных уравнений:

$$(t, 1)\,\sigma_1 + (t, 2)\,\sigma_2 + \ldots + (t, e)\,\sigma_e + \ldots + (t, r)\,\sigma_r = 1 + \frac{r-1}{e}(t, e),$$

где $1 \leq t \leq r$.

С первого взгляда видно, что решение этой системы имеет вид

$$\sigma_i = \begin{cases} 1 & \text{для } i = 1, \\ \dfrac{r-1}{e} & \text{для } i = e, \\ 0 & \text{для } i \neq 1, i \neq e. \end{cases}$$

Ввиду того, что (как мы уже заметили выше) неприводимые множители многочленов $f(x)$ и $\varphi(y)$ находятся во взаимно однозначном соответствии, мы доказали следующую теорему 1:

Теорема 1. *Пусть*

$$f(x) = x^{p^n} - ax - b, \qquad a, b \in GF(p),$$

есть многочлен над телом $GF(p)$ и пусть m/s. Положим $q = p^s$, $r = p^n$. Пусть $\alpha = a^{\frac{q-1}{r-1}} \neq 1$ принадлежит показателю $e > 1$. Тогда многочлен $f(x)$ можно разложить над телом $GF(q)$ на произведение одного линейного множителя и $\frac{q-1}{e}$ различных неприводимых множителей степеней e.

Поскольку я мог установить, эта общая теорема не была в литературе доказана. Известны, однако, некоторые теоремы, являющиеся ее прямыми следствиями.

Положим в теореме 1 $m = s$; тогда $\frac{q-1}{r-1} = 1$ и мы получаем следующую теорему:

Следствие 1. *Пусть дан многочлен*

$$f(x) = x^q - ax - b, \qquad a, b \in GF(q).$$

Пусть a принадлежит показателю $e > 1$. Тогда многочлен $f(x)$ над телом $GF(q)$ можно разложить на произведение одного линейного множителя и $\frac{q-1}{e}$ неприводимых множителей степеней e.

Следствие 1 приводится в работе О. Оре [4] (стр. 265).

Положим в теореме 1 $m = 1$; тогда мы получим следующий результат (см. О. Оре [4], стр. 266):

Следствие 2. *Пусть дан многочлен*

$$f(x) = x^p - ax - b, \qquad a, b \in GF(p^s).$$

Пусть элемент $a^{\frac{p^s-1}{p-1}}$ принадлежит показателю $e > 1$. Тогда $f(x)$ над телом $GF(p^s)$ будет произведением одного линейного многожителя и $\frac{p-1}{e}$ различных неприводимых множителей степеней e.

Если в теореме 1 принять в качестве a примитивный элемент тела $GF(p^s)$, т. е. $e = r - 1$, то получим следующую теорему:

Следствие 3. *Пусть дан многочлен*

$$f(x) = x^{p^m} - ax - b, \qquad a, b \in GF(p^s),$$

где m/s и $p^m > 2$. Пусть a — примитивный элемент тела $GF(p^s)$. Тогда $f(x)$ над телом $GF(p^s)$ можно разложить на произведение одного линейного и одного неприводимого множителя степени $p^m - 1$.

Это — обобщение одной более ранней теоремы Диксона, сделанное Альбертом (см. А. Альберт [1], стр. 141).

Случай Б

Предположим теперь, что при прежних обозначениях мы имеем $\alpha = a^{\frac{q-1}{r-1}} = 1$ и $\beta \neq 0$.

Соотношения (1) имеют вид

$$\begin{aligned} x^0 &\equiv 1, \\ x^q &\equiv \beta + x, \\ x^{2q} &\equiv \beta^2 + 2\beta x + x^2, \qquad\qquad (\mathrm{mod}\ f(x)) \\ &\vdots \\ x^{(r-1)q} &\equiv \beta^{r-1} + (r-1)\beta^{r-2}x + \ldots + x^{r-1}. \end{aligned}$$

Матрица $\mathbf{C}$ имеет вид

$$\mathbf{C} = \begin{bmatrix} 1 & 0 & 0 & \ldots & 0 \\ \beta & 1 & 0 & \ldots & 0 \\ \beta^2 & 2\beta & 1 & \ldots & 0 \\ \vdots \\ \beta^{r-1}, & (r-1)\beta^{r-2}, & \ldots & \ldots & 1 \end{bmatrix}.$$

Все элементы главной диагонали равны 1, а все элементы вправо от главной диагонали — нули.

Рассмотрим матрицу $\mathbf{C} - \mathbf{E}$. Все элементы первой строки равны нулю. дсементы дальнейших строк — просто коэффициенты при $x^0, x^1, \ldots, x^{r-1}$ следующих многочленов переменного x:

$$\begin{aligned} \psi_1(x) &= (\beta + x) - x, \\ \psi_2(x) &= (\beta + x)^2 - x^2, \\ &\vdots \\ \psi_{r-1}(x) &= (\beta + x)^{r-1} - x^{r-1}. \end{aligned}$$

Аналогично можно описать строки матрицы $\mathbf{C}^t - \mathbf{E}$, $t > 1$, на основании замечания, помещенного в начале работы.

Для нахождения элементов матрицы $\mathbf{C}^t$ выразим

$$x^0,\ x^{q^t},\ x^{2q^t}, \ldots x^{(r-1)q^t}\ (\mathrm{mod}\ f(x)) \text{ в виде (4а).}$$

Из соотношения

$$x^q \equiv x + \beta \qquad (\mathrm{mod}\ f(x))$$

следует для $k = 1, 2, \ldots, r-1$

$$x^{kq} \equiv (x + \beta)^k \qquad (\mathrm{mod}\ f(x))$$

и, следовательно,

$$x^{kq^2} \equiv [(x+\beta)^q]^k \equiv [x^q + \beta]^k \equiv (x + 2\beta)^k \quad (\mathrm{mod}\ f(x)).$$

Повторным возведением в степень q получим

$$x^{kq^3} \equiv [(x + 2\beta)^q]^k = [x^q + 2\beta]^k \equiv (x + 3\beta)^k \quad (\mathrm{mod}\ f(x)).$$

В общем случае будет для $t \geqq 1$

$$x^{kq^t} \equiv (x + t\beta)^k \qquad (\mathrm{mod}\ f(x)).$$

Следовательно, матрица $\mathbf{C}^t - \mathbf{E}$ имеет такой вид: В первой строке все элементы равны нулю. Элементы остальных строк — коэффициенты при возрастающих степенях x следующих многочленов:

$$\begin{aligned} \psi(1, t; x) &= (\beta t + x) - x, \\ \psi(2, t; x) &= (\beta t + x)^2 - x^2, \\ \psi(3, t; x) &= (\beta t + x)^3 - x^3, \\ &\vdots \\ \psi(r-1, t; x) &= (\beta t + x)^{r-1} - x^{r-1}. \end{aligned}$$

Притом мы положили $\psi(k, 1; x) = \psi_k(x)$.[1]
Матрица $\mathbf{C}^t - \mathbf{E}$ имеет такой вид:

$$\mathbf{C}^t - \mathbf{E} = \begin{bmatrix} 0 & 0 & \dots & 0 \\ \beta t & 0 & \dots & 0 \\ \beta^2 t^2 & 2\beta t & \dots & 0 \\ \vdots & \vdots & & \\ \beta^{r-1} t^{r-1}, & (r-1)(\beta t)^{r-2}, & \dots & 0 \end{bmatrix}$$

а) Для тех t, которые делятся на p, ранг этой матрицы равен $h_t = 0$.

б) Допустим поэтому в дальнейшем, что $p \nmid t$. По виду матрицы можно заключить, что многочлены $\psi(j, t; x)$ являются для $(j, p) = 1$ линейно независимыми друг от друга. Действительно, степень многочлена $\psi(j, t; x) = j\beta t x^{j-1} + \dots$ равна в точности $j-1$ и для возрастающих j, $p \nmid j$, степени этих многочленов постоянно возрастают.

Покажем, что каждый из многочленов

$$\psi(p, t; x),\ \psi(2p, t; x),\ \psi(3p, t; x),\ \dots,\ \psi(r-p, t; x)$$

$\left(\text{в общем числе } \frac{r}{p} - 1 = p^{m-1} - 1\right)$ является линейно зависимым от многочленов $\psi(j, t; x)$, где $p \nmid j$. Этим самым будет доказано, что ранг h_t матрицы $\mathbf{C}^t - \mathbf{E}$ равен $r - p^{m-1} = p^m - p^{m-1}$.

Для многочлена $\psi(p, t; x) = (\beta t + x)^p - x^p = (\beta t)^p$ наше утверждение справедливо, так как $\psi(p, t, x)$ является кратным многочлена $\psi(1, t; x)$. Рассмотрим теперь следующее тождество, справедливое для любого натурального числа k (и любого βt):

$$[(x + \beta t)^p - (\beta t)^{p-1}(x + \beta t)]^k = [x^p - (\beta t)^{p-1} x]^k.$$

Возведением в степень получим

$$\sum_{l=0}^{k} (-1)^l \binom{k}{l} (\beta t)^{(p-1)l} (x + \beta t)^{p(k-l)+l} = \sum_{l=0}^{k} (-1)^l \binom{k}{l} (\beta t)^{(p-1)l} x^{p(k-l)+l}.$$

[1] Аналогичное представление матрицы $\mathbf{C}^t - \mathbf{E}$ возможно и в случае $\alpha \neq 1$, т. е. в случае, разобранном в разделе А. Можно доказать, что матрица $\mathbf{C}^t - \mathbf{E}$ имеет тогда следующий вид: В первой строке все элементы равны нулю. Элементы остальных строк — коэффициенты при возрастающих степенях многочленов $(\beta_t + \alpha^t x) - x$, $(\beta_t + \alpha^t x)^2 - x^2$, $(\beta_t + \alpha^t x)^3 - x^3$, ..., $(\beta_t + \alpha^t x)^{r-1} - x^{r-1}$, где $\beta_t = \beta(1 + \alpha + \dots \alpha^{t-1})$. Среди этих $r-1$ многочленов имеется в точности $r - 1 - \frac{r-1}{e}(e, t)$ линейно независимых. Так как доказательство этого последнего утверждения занимает довольно много времени, мы воспользовались в разделе А приемом, при котором мы привели многочлен $f(x)$ подстановкой $y = x - x_0$ к виду более простого многочлена $\varphi(x)$. Такой прием в случае Б невозможен, хотя бы уже потому, что в случае $\alpha = 1$ — как мы еще увидим — многочлен $f(x)$ вообще не должен иметь линейный множитель над $GF(q)$.

Следовательно,

$$\sum_{l=0}^{k} (-1)^l \binom{k}{l} (\beta t)^{(p-1)l} \psi[p(k-l) + l, t; x] = 0.$$

Последнее соотношение можно записать в следующем явном виде:

$$\psi(kp, t; x) - \binom{k}{1}(\beta t)^{p-1} \psi[p(k-1) + 1, t; x] + \binom{k}{2}(\beta t)^{2(p-1)} \psi[p(k-2) + 2, t; x] + \dots + (-1)^k (\beta t)^{k(p-1)} \psi[k, t; x] = 0.$$

Отсюда непосредственно видно, что $\psi(kp, t; x)$, для любого целого k, является линейной комбинацией многочленов $\psi(l, t; x)$, где $l < kp$. Наше утверждение вытекает отсюда индукцией.

Подставим теперь выражения для h_t в систему уравнений (2). Для $1 \leqq t \leqq r = p^m$ получим:

$$(t, 1)\sigma_1 + (t, 2)\sigma_2 + \dots + (t, p)\sigma_p + \dots + (t, r)\sigma_r = \begin{cases} r & \text{для } p/t, \\ p^{m-1} & \text{для } p \nmid t. \end{cases}$$

Решение этой системы имеет вид $\sigma_p = p^{m-1}$, $\sigma_i = 0$ для $i \neq p$. Итак, наш многочлен можно разложить на p^{m-1} неприводимых многочленов степеней p.

Мы доказали:

Теорема 2. *Пусть дан многочлен*

$$f(x) = x^{p^m} - ax - b, \qquad a, b \in GF(p^s),$$

где m/s. *Положим* $q = p^s$, $r = p^m$, $s = ml$. *Пусть имеет место*

а) $a^{\frac{q-1}{r-1}} = 1$,

б) $\beta = \frac{b}{a} + \frac{b^r}{a^{1+r}} + \dots + \frac{b^{r^{l-1}}}{a^{1+r+\dots+r^{l-1}}} \neq 0.$

Тогда многочлен $f(x)$ можно разложить на произведение p^{m-1} неприводимых множителей, причем степень каждого из них равна p.[2])

Случай В

Пусть теперь $a^{\frac{q-1}{r-1}} = 1$ и $\beta = 0$. Тогда матрица $\mathbf{C}^t - \mathbf{E}$ будет для любого t нулевой матрицей. Значит $h_t = 0$. Система (2) имеет вид

$$(t, 1)\sigma_1 + (t, 2)\sigma_2 + \dots + (t, r)\sigma_r = r.$$

Решения этой системы получим в виде $\sigma_1 = r$, $\sigma_2 = \sigma_3 = \dots = \sigma_r = 0$. Многочлен $f(x)$ распадается над телом $GF(p^s)$ на произведение линейных факторов. Мы получили:

[2] Ввиду условия а) в этом случае можно записать β в том виде, как приводится в тексте.

Теорема 3. *Пусть дан многочлен*

$$f(x) = x^{p^m} - ax - b, \qquad a, b \in GF(p^s),$$

где m/s. Обозначим $r = p^m$, $q = p^s$. Пусть

а) $a^{\frac{q-1}{r-1}} = 1$,

б) $\frac{b}{a} + \frac{b^r}{a^{1+r}} + \ldots + \frac{b^{r^{l-1}}}{a^{1+r+\ldots+r^{l-1}}} = 0$.

Тогда многочлен $f(x)$ является над телом $GF(p^s)$ произведением p^m линейных множителей.

Насколько мне удалось установить, теоремы 2 и 3 являются новыми. Однако, из них вытекает несколько известных следствий.

Если положить $m = 1$, т. е. $r = p$, $l = s$, получаем:

Следствие 4. *Многочлен*

$$f(x) = x^p - ax - b, \qquad a, b \in GF(p^s),$$

для которого $a^{\frac{p^s-1}{p-1}} = 1$, является разложимым тогда и только тогда, если имеет место

$$\frac{b}{a} + \frac{b^p}{a^{1+p}} + \frac{b^{p^2}}{a^{1+p+p^2}} + \ldots + \frac{b^{p^s}}{a^{1+p+p^2+\ldots+p^{s-1}}} = 0. \tag{6}$$

При выполнении этого условия $f(x)$ является над телом $GF(p^s)$ произведением одних лишь линейных множителей.

Для $a = 1$ этот результат доказан в книге Л. Э. Диксон [2], стр. 29.

Если вместо a написать $a = a_1^{p-1}$, $a_1 \in GF(p^s)$, то усовие $a^{\frac{p^s-1}{p-1}} = 1$ выполняется автоматически. Подставив значение a в соотношение (6), мы получим после преобразований:

Следствие 5. *Многочлен*

$$x^p - a_1^{p-1}x - b, \qquad a_1, b \in GF(p^s)$$

является над телом $GF(p^s)$ разложимым тогда и только тогда, если

$$\frac{b}{a_1^p} + \left(\frac{b}{a_1^p}\right)^p + \left(\frac{b}{a_1^p}\right)^{p^2} + \ldots + \left(\frac{b}{a_1^p}\right)^{p^{s-1}} = 0.$$

Эта теорема приводится без доказательства в работе О. Оре [4], стр. 265.

Положив $a = 1$, мы получаем из теорем 2 и 3:

Следствие 6. *Пусть дан многочлен*

$$f(x) = x^{p^m} - x - b, \qquad b \in GF(p^s).$$

Пусть $s = m \,.\, l$. Положим $p^m = r$. Тогда многочлен $f(x)$ будет над телом $GF(p^s)$

а) *или произведением p^{m-1} неприводимых множителей степени p,*

б) *или произведением p^m линейных множителей. Второй случай наступает тогда и только тогда, если*

$$b + b^r + b^{r^2} + \ldots + b^{r^{l-1}} = 0.$$

В случае $m = 1$, т. е. $r = p$, $l = s$, это известный результат, имеющий большое значение в общей теории циклических тел (см. напр. А. А. Альберт [1], стр. 140). Доказательство случая $1 < m < s$ я в литературе не нашел.

Если в следствии 6 положить $m = s$, т. е. $l = 1$, то получим следующий известный результат (см. напр. Л. Э. Диксон [3], стр. 248, и О. Оре [4], стр. 265):

Следствие 7. *Многочлен*

$$f(x) = x^{p^s} - x - b, \qquad b \in GF(p^s),$$

а) *или является над телом $GF(p^s)$ произведением p^{s-1} неприводимых множителей степени p,*

б) *или его можно разложить на произведение p^s линейных множителей. Второй случай наступает тогда и только тогда, если $b = 0$.*

ЛИТЕРАТУРА

[1] Albert A. A., *Fundamental concepts of higher Algebra*. Univ. of Chicago Press, 1956.

[2] Dickson L. E., *Linear groups with an exposition of the Galois field theory*, Teubner, Leipzig 1901.

[3] Dickson L. E., *History of the Theory of Numbers*, Vol. I, New York (reprinted) 1934.

[4] Ore O., Contributions to the theory of finite fields, Trans. Amer. Math. Soc. 36 (1934), 243–274.

[5] Schwarz Š., On the reducibility of polynomials over a finite field, Quart. J. Math. (Oxford) (2), 7 (1956), 110–124.

Поступило 5. 1. 1960.

Katedra matematiky Slovenskej vysokej školy technickej v Bratislave

ON A CLASS OF POLYNOMIALS OVER A FINITE FIELD

By ŠTEFAN SCHWARZ, Bratislava

Summary

Let $f(x) = x^{p^m} - ax - b$ be a polynomial over the finite field $GF(p^s)$, where p is a prime, $s \geqq 1$. Suppose further that m/s.

By means of a previous general result of the author (see [5]) a complete discussion of all possible cases concerning the reducibility of $f(x)$ over $GF(p^s)$ is given.

Denote $r = p^m$, $l = \frac{s}{m}$ and

$$\alpha = a^{\frac{q-1}{r-1}},$$

$$\beta = a^{\frac{q-1}{r-1}} \left\{ \frac{b}{a} + \frac{b^r}{a^{1+r}} + \frac{b^{r^2}}{a^{1+r+r^2}} + \dots + \frac{b^{r^{l-1}}}{a^{1+r+r^2+\dots+r^{l-1}}} \right\}.$$

We then have:

1. If α belongs to the exponent $e > 1$, $f(x)$ is a product of one linear factor and of $\frac{r-1}{e}$ different irreducible factors of degree e.

2. If $\alpha = 1$, $\beta \neq 0$, $f(x)$ is a product of p^{m-1} different irreducible polynomials of degree p.

3. If $\alpha = 1$, $\beta = 0$, $f(x)$ is a product of p^m linear factors.

This general statement implies a great number of special results; some of them can be found in the bibliography.