Общероссийский математический портал

В. Л. Куракин, Представление линейных рекуррентных последовательностей функцией след, *Матем. сб.*, 2002, том 193, номер 6, 123–142

DOI: <https://doi.org/10.4213/sm663>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.166.219.16

26 апреля 2023 г., 16:19:14

УДК 512.55+519.7

В. Л. Куракин

Представление линейных рекуррентных последовательностей функцией след

Исследуется возможность представления линейных рекуррентных последовательностей над коммутативными локальными кольцами и модулями над ними функцией след. Действие самой функции след выражается в терминах автоморфизмов и в терминах p -адических разложений.

Библиография: 19 названий.

Всюду далее термин кольцо означает коммутативное кольцо с единицей. Последовательность $u = (u(0), u(1), \dots)$ над кольцом R называется *линейной рекуррентной последовательностью* (ЛРП) порядка m , если существуют элементы $c_0, \dots, c_{m-1} \in R$ такие, что

$$u(i+m) = c_{m-1}u(i+m-1) + \dots + c_1u(i+1) + c_0u(i), \quad i \geq 0. \quad (1)$$

Многочлен $F(x) = x^m - c_{m-1}x^{m-1} - \dots - c_1x - c_0 \in R[x]$ называется *характеристическим многочленом* ЛРП u , а вектор $u(\overline{0, m-1}) = (u(0), \dots, u(m-1)) \in R^m$ — ее *начальным вектором*. Характеристический многочлен наименьшей степени называется *минимальным многочленом*, а его степень — рангом ЛРП u . Множество всех ЛРП над кольцом R с характеристическим многочленом $F(x)$ обозначим через $L_R(F)$.

Известно [1; теорема 8.24], что всякая ЛРП u над конечным полем $P = \text{GF}(q)$ с неприводимым характеристическим многочленом $F(x) \in P[x]$ степени m имеет представление

$$u(i) = \text{tr}_P^Q(c\theta^i), \quad i \geq 0,$$

где θ — корень многочлена $F(x)$ в его минимальном поле разложения $Q = \text{GF}(q^m)$, $c \in Q$ — однозначно определенная константа, tr_P^Q — след из поля Q в поле P , определяемый соотношением

$$\text{tr}_P^Q(a) = a + a^q + \dots + a^{q^{m-1}}, \quad a \in Q.$$

В [2], [3] показано, что представление функцией след имеют ЛРП над кольцами Гауа. Аналогичное представление найдено автором для ЛРП над конечными квазифробениусовыми модулями специального вида [4].

Представление функцией след позволяет находить произвольный знак $u(i)$ ЛРП u без рекуррентного вычисления предыдущих знаков. Это представление используется также для нахождения распределения элементов в линейных рекуррентных

последовательностях [5], [6], оценки линейной сложности линейных рекуррент и их координатных последовательностей [4], [7], построения помехоустойчивых кодов с использованием линейных рекуррент над кольцами и модулями [2], [3], [6], [8], [9]. Представление функцией след часто является первым шагом в решении той или иной прикладной задачи, связанной с линейными рекуррентами.

В настоящей статье доказывается, что если $u \in L_R(F)$ – ЛРП над локальным кольцом R и многочлен $F(x)$ представляется в виде произведения степеней многочленов, образы которых над полем вычетов кольца R являются различными неприводимыми и сепарабельными многочленами, то ЛРП u обладает представлением функцией след над некоторым расширением S кольца R . Аналогичное утверждение доказано для ЛРП над модулем ${}_R M$. Сама функция след, как и в [3], выражается в терминах автоморфизмов кольца S над R , а также в терминах p -адических разложений элементов колец R и S .

Напомним определение функции след [10], [11]. Пусть A – алгебра над кольцом R , являющаяся конечно порожденным проективным R -модулем. В силу [12; теорема 5.4.2] для любой системы образующих $a_1, \dots, a_m$ модуля ${}_R A$ существуют гомоморфизмы $\varphi_i \in \text{Hom}_R(A, R)$, $1 \leq i \leq m$, такие, что

$$\forall a \in A \quad a = \sum_{i=1}^m \varphi_i(a) a_i.$$

Набор (a_i, φ_i) называется *координатной системой* проективного модуля A . Следом из A в R называется гомоморфизм R -модулей $\text{tr}_{A/R}: A \rightarrow R$, определяемый равенством

$$\text{tr}_{A/R}(a) = \sum_{i=1}^m \varphi_i(a a_i), \quad a \in A.$$

Это определение не зависит от выбора координатной системы и обладает следующим свойством транзитивности: если B – подалгебра, содержащаяся в центре алгебры A , ${}_R B$ и ${}_B A$ – конечно порожденные проективные модули, то ${}_R A$ – конечно порожденный проективный модуль и $\text{tr}_{A/R}(a) = \text{tr}_{B/R}(\text{tr}_{A/B}(a))$, $a \in A$. В случае, когда R – поле и A – его конечное алгебраическое расширение, $\text{tr}_{A/R}$ совпадает с обычной функцией след из поля A в подполе R (см. [13]), которую мы будем обозначать tr_R^A .

Пусть R – локальное кольцо с максимальным идеалом $J = J(R)$ и полем вычетов $R/J = \overline{R}$. Многочлены $F(x), G(x) \in R[x]$ будем называть *взаимно простыми* и записывать это в виде $(F, G) = 1$, если $FU + GV = 1$ для некоторых $U(x), V(x) \in R[x]$. В силу [14; предложение III.4.2] если хотя бы один из многочленов $F(x), G(x)$ унитарен, то

$$(F, G) = 1 \Leftrightarrow (\overline{F}, \overline{G}) = 1, \quad (2)$$

где $\overline{F}(x)$ – канонический образ многочлена $F(x)$ над полем вычетов $\overline{R}$. Унитарный многочлен $F(x)$ будем называть *сепарабельным*, если многочлен $\overline{F}(x)$ не имеет кратных корней в поле разложения. Такое определение сепарабельного многочлена (и элемента) над локальным кольцом использовалось, например, в [15; часть II,

с. 129]. Ввиду [16; теорема 2.2] данное определение эквивалентно определению сепарабельного многочлена из [11], [16], согласно которому $F(x)$ сепарабелен, если $R[x]/F(x)$ – сепарабельная R -алгебра.

Для унитарного многочлена $F(x) \in R[x]$ степени m рассмотрим расширение $S = R[x]/F(x) = R[\theta]$ кольца R корнем $\theta = [x]_F$ многочлена $F(x)$. Модуль ${}_R S$ является свободным модулем ранга m с базисом $1, \theta, \dots, \theta^{m-1}$, и произвольный элемент $a \in S$ однозначно записывается в виде $a = [a(x)]_F = a(\theta)$, где $a(x) = a_0 + a_1x + \dots + a_{m-1}x^{m-1} \in R[x]$ – многочлен степени меньше m . Положим $\varphi_i(a) = a_i$, $0 \leq i \leq m-1$. Тогда (θ^i, φ_i) – координатная система свободного модуля ${}_R S$ и

$$\mathrm{tr}_{S/R}(a) = \sum_{i=0}^{m-1} \varphi_i(a\theta^i), \quad a \in S. \quad (3)$$

ПРЕДЛОЖЕНИЕ 1. Пусть R – локальное кольцо, $F(x) \in R[x]$ – унитарный многочлен степени m такой, что его образ $\overline{F}(x)$ является неприводимым многочленом над полем $\overline{R}$, $S = R[x]/F(x)$ и $\theta = [x]_F$. Тогда справедливы следующие утверждения.

(а) S – локальное кольцо с максимальным идеалом $J(S) = J(R)S$. Если $J(R)$ – ниль-идеал, то и $J(S)$ – ниль-идеал. Если $J(R)$ нильпотентен (индекса нильпотентности n), то и $J(S)$ нильпотентен (индекса нильпотентности n).

(б) Если $F(x) = x^m + c_{m-1}x^{m-1} + \dots + c_1x + c_0$, то $\mathrm{tr}_{S/R}(1) = m$ и $\mathrm{tr}_{S/R}(\theta) = -c_{m-1}$.

(в) Пусть $a \in S$ и A – матрица линейного преобразования (гомометии) $\hat{a}: S \rightarrow S$, $\hat{a}(s) = as$, $s \in S$, в базисе $1, \theta, \dots, \theta^{m-1}$ (или в любом другом базисе) модуля ${}_R S$. Тогда $\mathrm{tr}_{S/R}(a) = \mathrm{tr} A$, где $\mathrm{tr} A$ – сумма диагональных элементов матрицы A .

(г) Если $a = [a(x)]_F = a(\theta) \in S$, то $\mathrm{tr}_{S/R}(a) = \mathrm{tr} a(S(F))$, где $S(F)$ – сопровождающая матрица многочлена $F(x)$.

(д) $\overline{\mathrm{tr}_{S/R}(a)} = \mathrm{tr}_{\overline{S}/\overline{R}}(\overline{a}) = \mathrm{tr}_{\overline{R}}(\overline{a})$.

(е) Если многочлен $F(x)$ сепарабелен, то $\mathrm{tr}_{S/R}$ – эпиморфизм на R .

ДОКАЗАТЕЛЬСТВО. (а) Очевидно, $J(R)S$ – идеал в S . Если $a = [a(x)]_F \notin J(R)S$, то $\overline{a}(x) \neq 0$. Так как $\overline{F}(x)$ неприводим, то $(\overline{a}(x), \overline{F}(x)) = 1$ и ввиду (2) $a(x)u(x) + F(x)v(x) = 1$ для некоторых многочленов $u(x), v(x) \in R[x]$. Тогда элемент $u = [u(x)]_F \in S$ является обратным к элементу a в кольце S . Таким образом, множество $J(R)S$ совпадает с множеством всех необратимых элементов кольца S . Следовательно, кольцо S локально и $J(S) = J(R)S$. Остальные утверждения п. (а) следуют из доказанного.

(б) Утверждение получается непосредственным применением формулы (3).

(в) Строка с номером $i = \overline{0, m-1}$ матрицы $A = (a_{ij})$ состоит из коэффициентов разложения элемента $a\theta^i$ в базисе $1, \theta, \dots, \theta^{m-1}$. Следовательно, $\varphi_j(a\theta^i) = a_{ij}$ и

$$\mathrm{tr}_{S/R}(a) = \sum_{i=0}^{m-1} \varphi_i(a\theta^i) = \sum_{i=0}^{m-1} a_{ii} = \mathrm{tr} A.$$

(г) Так как $\text{tr}_{S/R}$ является R -линейным отображением, то достаточно доказать, что $\text{tr}_{S/R}(\theta^k) = \text{tr } S(F)^k$. Действительно, матрица линейного преобразования $\hat{\theta}$ в базисе $1, \theta, \dots, \theta^{m-1}$ есть $S(F)$. Следовательно, матрица линейного преобразования $\hat{\theta}^k$ есть $S(F)^k$, и требуемое равенство вытекает из (в).

(д) В силу (г) $\overline{\text{tr}_{S/R}(a)} = \overline{\text{tr } a(S(F))} = \text{tr } \bar{a}(S(\bar{F})) = \text{tr}_{\bar{S}/\bar{R}}(\bar{a})$. Равенство $\text{tr}_{\bar{S}/\bar{R}}(\bar{a}) = \text{tr}_{\bar{R}}(\bar{a})$ известно из [10], [11], [13].

(е) Так как $\bar{S}$ – конечное алгебраическое сепарабельное расширение поля $\bar{R}$, то ввиду [13; теорема VIII.9] $\text{tr}_{\bar{S}/\bar{R}}: \bar{S} \rightarrow \bar{R}$ – эпиморфизм. Поэтому существует элемент $a \in S$ такой, что $\text{tr}_{\bar{S}/\bar{R}}(\bar{a}) \neq 0$. В силу (д) $\overline{\text{tr}_{S/R}(a)} \neq 0$, т.е. $\text{tr}_{S/R}(a) \in R^*$. Отсюда $\text{tr}_{S/R}(Ra) = R$ и $\text{tr}_{S/R}$ – эпиморфизм. Отметим, что утверждение (е) следует также из [11; следствие III.2.3].

ТЕОРЕМА 2. Пусть R – локальное кольцо, $F(x) \in R[x]$ – унитарный сепарабельный многочлен степени m такой, что его образ $\bar{F}(x)$ неприводим над полем $\bar{R}$, $S = R[x]/F(x)$ и $\theta = [x]_F$. Тогда для любой ЛРП $u \in L_R(F)$ существует единственная константа $c \in S$ такая, что

$$u(i) = \text{tr}_{S/R}(c\theta^i), \quad i \geq 0. \quad (4)$$

Любая последовательность вида (4) принадлежит $L_R(F)$.

ДОКАЗАТЕЛЬСТВО. Если $F(x) = x^m - \sum_{j=0}^{m-1} a_j x^j$, то

$$\begin{aligned} u(i+m) &= \text{tr}_{S/R}(c\theta^{i+m}) = \text{tr}_{S/R}\left(c\theta^i \sum a_j \theta^j\right) \\ &= \sum a_j \text{tr}_{S/R}(c\theta^{i+j}) = \sum a_j u(i+j). \end{aligned}$$

Поэтому любая последовательность вида (4) принадлежит $L_R(F)$. Обратно, пусть $u \in L_R(F)$. Элемент $c \in S$ удовлетворяет условию (4) тогда и только тогда, когда

$$u(i) = \text{tr}_{S/R}(c\theta^i), \quad 0 \leq i \leq m-1. \quad (5)$$

Пусть $c = [c(x)]_F = c(\theta)$, где $c(x) = c_0 + c_1 x + \dots + c_{m-1} x^{m-1} \in R[x]$. Тогда условие (5) запишется в виде

$$u(i) = \text{tr}_{S/R}\left(\sum_{j=0}^{m-1} c_j \theta^{i+j}\right) = \sum_{j=0}^{m-1} c_j \text{tr}_{S/R}(\theta^{i+j}), \quad 0 \leq i \leq m-1,$$

или

$$(u(0), \dots, u(m-1)) = (c_0, \dots, c_{m-1})A, \quad (6)$$

где $A = (a_{ij})$ – матрица размера $m \times m$, $a_{ij} = \text{tr}_{S/R}(\theta^{i+j})$, $0 \leq i, j \leq m-1$. Ввиду [16; теорема 2.2] или [11; теорема III.4.4] матрица A обратима. Следовательно, система линейных уравнений (6) имеет единственное решение. Теорема доказана.

Отметим, что условие сепарабельности неприводимого многочлена $\bar{F}(x)$ в теореме 2 существенно. Действительно, если R – поле и $F(x)$ – неприводимый, но

не сепарабельный многочлен над R , то поле $S = R[x]/F(x)$ является несепарабельным расширением поля R и след $\text{tr}_{S/R} = \text{tr}_R^S$ есть нулевое отображение [13; § VIII.5]. Поэтому лишь нулевая последовательность из $L_R(F)$ имеет представление (4) функций след.

Ниже мы докажем, что в случае, когда R — кольцо Галуа, представление (4) совпадает с представлением функций след из [3; теорема 8]. Но вначале рассмотрим более общую ситуацию.

Напомним [14], что коммутативное локальное кольцо R называется *гензелевым*, если для всякого унитарного многочлена $F(x) \in R[x]$ и для любого разложения $\overline{F}(x)$ в произведение $\overline{F}(x) = g(x)h(x)$ унитарных взаимно простых многочленов существуют унитарные многочлены $G(x), H(x) \in R[x]$ такие, что $\overline{G}(x) = g(x)$, $\overline{H}(x) = h(x)$ и $F(x) = G(x)H(x)$. Если кольцо R гензелево и S — коммутативная R -алгебра, представляющая собой локальное кольцо и конечно порожденный R -модуль, то кольцо S гензелево [14; упражнение III.4.3]. Всякое отделимое и полное локальное кольцо является гензелевым (лемма Гензеля [14; теорема III.4.1]). В частности, гензелевыми являются *вполне примарные*¹ кольца, т.е. локальные кольца, у которых максимальный идеал является ниль-идеалом.

Пусть R — гензелево кольцо, $F(x) \in R[x]$ — унитарный сепарабельный многочлен степени m , и пусть многочлен $\overline{F}(x)$ над полем $\overline{R}$ имеет каноническое разложение $\overline{F}(x) = f_1(x) \cdots f_r(x)$, где $f_1(x), \dots, f_r(x)$ — различные унитарные неприводимые над полем $\overline{R}$ многочлены. Тогда над кольцом R имеет место разложение $F(x) = F_1(x) \cdots F_r(x)$, где $F_i(x)$ — унитарный многочлен и $\overline{F}_i(x) = f_i(x)$, $1 \leq i \leq r$. Предположим, что среди $F_i(x)$ есть многочлен степени больше 1, например $\deg F_1(x) > 1$. Рассмотрим расширение $S_1 = R[x]/F_1(x) = R[\theta_1]$ кольца R корнем $\theta_1 = [x]_{F_1}$ многочлена $F_1(x)$. Тогда кольцо S_1 гензелево. Над полем $\overline{S}_1$ многочлен $\overline{F}(x)$ имеет каноническое разложение $\overline{F}(x) = g_1(x) \cdots g_t(x)$, $t > r$, где $g_1(x), \dots, g_t(x)$ — различные унитарные неприводимые над полем $\overline{S}_1$ многочлены. Тогда над кольцом S_1 имеет место разложение $F(x) = G_1(x) \cdots G_t(x)$, где $G_i(x)$ — унитарный многочлен и $\overline{G}_i(x) = g_i(x)$, $1 \leq i \leq t$. Если среди $G_i(x)$ есть многочлен степени больше 1, например $\deg G_1(x) > 1$, то рассмотрим расширение $S_2 = S_1[x]/G_1(x) = S_1[\theta_2]$ кольца S_1 корнем $\theta_2 = [x]_{G_1}$ многочлена $G_1(x)$ и т.д. Через конечное число шагов получим расширение T кольца R , порожденное корнями многочлена $F(x)$ и являющееся гензелевым, над которым многочлен $F(x)$ разлагается на линейные множители:

$$F(x) = (x - \theta_1)(x - \theta_2) \cdots (x - \theta_m), \quad \overline{\theta}_i \neq \overline{\theta}_j \quad 1 \leq i < j \leq m. \quad (7)$$

При этом ${}_R T$ — конечно порожденный свободный модуль и в силу предложения 1 (а) $J(T) = J(R)T$. Кольцо T будем называть *кольцом разложения* сепарабельного многочлена $F(x)$ над гензелевым кольцом R . Эта конструкция хорошо известна. Например, в случае вполне примарных колец кольцо разложения рассматривалось в [15], а в случае сепарабельных алгебр над коммутативным кольцом без собственных идемпотентов — в [11], [16].

¹Этот термин взят из [15]. В книге [14] такие кольца называются примарными. Другие авторы используют оба этих термина и в ином смысле.

Так как T гензелево, то в кольце T многочлен $F(x)$ имеет в точности m корней $\theta_1, \dots, \theta_m$ и разложение (7) однозначно. Мы будем иногда говорить, что кольцо разложения T получается присоединением к кольцу R всех корней многочлена $F(x)$.

Кольцо разложения точно так же строится для многочлена $F(x) \in R[x]$, не являющегося сепарабельным, но имеющего над R разложение $F(x) = F_1(x)^{k_1} \dots F_r(x)^{k_r}$, где многочлены $F_1(x), \dots, F_r(x) \in R[x]$ унитарны и $\overline{F_1}(x), \dots, \overline{F_r}(x)$ — неприводимые над полем $\overline{R}$ сепарабельные многочлены.

Обозначим через $G = \text{Aut}(T/R)$ группу автоморфизмов кольца T над R и через T^G неподвижное подкольцо группы G . Для $\sigma \in G$ корректно определено отображение $\overline{\sigma}: \overline{T} \rightarrow \overline{T}$, $\overline{\sigma}(\overline{a}) = \overline{\sigma(a)}$, $a \in T$, причем $\overline{\sigma} \in \text{Aut}(\overline{T}/\overline{R})$. Следующая теорема и ее следствие доказываются в целом так же, как в случае полей [13] и конечных колец [17]. Для полноты изложения мы приводим доказательство.

ТЕОРЕМА 3. Пусть R — гензелево кольцо, $F(x) \in R[x]$ — унитарный сепарабельный многочлен, T — его кольцо разложения над R . Тогда поле $\overline{T}$ является расширением Галуа поля $\overline{R}$. Пусть $[\overline{T} : \overline{R}] = n$ и $\text{Aut}(\overline{T}/\overline{R}) = \{\tau_1 = 1, \tau_2, \dots, \tau_n\}$ — группа Галуа расширения $\overline{T}$ поля $\overline{R}$. Тогда группа $G = \text{Aut}(T/R)$ состоит из n автоморфизмов $\sigma_1, \dots, \sigma_n$ таких, что $\overline{\sigma}_i = \tau_i$, $1 \leq i \leq n$. Справедливы равенства $T^G = R$ и

$$\text{tr}_{T/R}(a) = \sum_{\sigma \in \text{Aut}(T/R)} \sigma(a), \quad a \in T. \quad (8)$$

ДОКАЗАТЕЛЬСТВО. Поле $\overline{T}$ является минимальным полем разложения многочлена $\overline{F}(x)$ над $\overline{R}$. Следовательно, $\overline{T}$ — расширение Галуа поля $\overline{R}$. По теореме о нормальном базисе [13; теорема VIII.20] существует элемент $w \in \overline{T}$ такой, что элементы $w = \tau_1(w), \tau_2(w), \dots, \tau_n(w)$ образуют базис пространства ${}_{\overline{R}}\overline{T}$. Пусть $g(x) \in \overline{R}[x]$ — минимальный многочлен элемента w над $\overline{R}$. Тогда $\deg g(x) \geq n$, так как $g(x)$ имеет n различных корней $\tau_1(w), \dots, \tau_n(w)$, и $\deg g(x) \leq n$, так как $[\overline{T} : \overline{R}] = n$. Следовательно, $g(x)$ — неприводимый над полем $\overline{R}$ сепарабельный многочлен степени n . Выберем произвольный унитарный многочлен $G(x) \in R[x]$ такой, что $\overline{G}(x) = g(x)$. Так как кольцо T гензелево, то многочлен $G(x)$ разлагается над T на линейные множители:

$$G(x) = (x - \xi_1)(x - \xi_2) \cdots (x - \xi_n), \quad \overline{\xi}_i = \tau_i(w), \quad 1 \leq i \leq n, \quad (9)$$

и имеет в кольце T в точности n корней $\xi_1, \dots, \xi_n$.

Так как $\overline{\xi}_1, \dots, \overline{\xi}_n$ — базис пространства ${}_{\overline{R}}\overline{T}$, кольцо R локально и ${}_RT$ — конечно порожденный свободный модуль, то в силу [14; предложение II.3.5] $\xi_1, \dots, \xi_n$ — базис свободного модуля ${}_RT$. Аналогично для любого $i = \overline{1}, \dots, \overline{n}$ элементы $1, \xi_i, \xi_i^2, \dots, \xi_i^{n-1}$ образуют базис ${}_RT$. Из последнего утверждения при $i = 1$ также следует, что $T = R[\xi_1]$ и каждый элемент $a \in T$ однозначно представляется в виде $a = [a(x)]_G = a(\xi_1)$, где $a(x) \in R[x]$ — многочлен степени меньшей n .

Непосредственно проверяется, что отображения

$$\sigma_i: T \rightarrow T, \quad \sigma_i(a(\xi_1)) = a(\xi_i), \quad 1 \leq i \leq n,$$

являются автоморфизмами кольца T над R . Любой автоморфизм из $\text{Aut}(T/R)$ переводит ξ_1 в некоторый корень ξ_i многочлена $G(x)$ и, поскольку $T = R[\xi_1]$, определяется этим однозначно. Следовательно, автоморфизмами $\sigma_1, \dots, \sigma_n$ исчерпываются все автоморфизмы кольца T над R . При этом $\overline{\sigma_i(a(\xi_1))} = \overline{a(\xi_i)} = \overline{a}(\xi_i) = \tau_i(\overline{a}(\xi_1))$, т.е. $\overline{\sigma_i} = \tau_i$, $1 \leq i \leq n$.

Равенство $T^G = R$ следует из [16; следствие 1.8 и предложение 1.9]. Докажем (8). Так как $T = R[\xi_i] \cong R[x]/G(x)$ – расширение кольца R корнем ξ_i многочлена $G(x)$, то по предложению 1(б) $\text{tr}_{T/R}(\xi_i) = -g_{n-1}$, $1 \leq i \leq n-1$, где $g_{n-1} \in R$ – коэффициент многочлена $G(x)$ в разложении $G(x) = x^n + g_{n-1}x^{n-1} + \dots + g_1x + g_0$. Следовательно, ввиду (9)

$$\text{tr}_{T/R}(\xi_i) = -g_{n-1} = \xi_1 + \dots + \xi_n = \sum_{k=1}^n \sigma_k(\xi_i) = \sum_{\sigma \in \text{Aut}(T/R)} \sigma(\xi_i)$$

для произвольного $i = \overline{1, n}$. Так как $\xi_1, \dots, \xi_n$ – базис модуля ${}_RT$ и отображение $\text{tr}_{T/R}$ линейно над R , то отсюда следует соотношение (8).

Иногда удобно выразить функцию след не через автоморфизмы кольца разложения T многочлена $F(x)$, а через гомоморфные вложения кольца $S = R[x]/F(x)$ в T .

СЛЕДСТВИЕ 4. Пусть R геззелево, $F(x) \in R[x]$ – унитарный сепарабельный многочлен степени m такой, что многочлен $\overline{F}(x)$ неприводим над полем $\overline{R}$, $S = R[x]/F(x) = R[\theta]$, где $\theta = [x]_F$, T – кольцо разложения многочлена $F(x)$ над S . Тогда существует m различных гомоморфных вложений $\eta_1, \dots, \eta_m$ кольца S в T над R и

$$\text{tr}_{S/R}(a) = \sum_{i=1}^m \eta_i(a), \quad a \in S. \quad (10)$$

ДОКАЗАТЕЛЬСТВО. Над кольцом T многочлен $F(x)$ имеет в точности m корней $\theta = \theta_1, \theta_2, \dots, \theta_m$. Непосредственно проверяется, что отображения

$$\eta_i: S \rightarrow T, \quad \eta_i(a(\theta_1)) = a(\theta_i), \quad 1 \leq i \leq m, \quad (11)$$

являются мономорфизмами кольца S в T над R (здесь $a(x) \in R[x]$ – многочлен степени меньше m). Любой мономорфизм S в T над R переводит θ_1 в некоторый корень θ_i многочлена $F(x)$ и, поскольку $S = R[\theta_1]$, определяется параметром i однозначно. Следовательно, $\eta_1, \dots, \eta_m$ – все мономорфизмы кольца S в T над R .

Докажем (10). Рассмотрим башню колец $R \subseteq S \subseteq T$ и башню полей вычетов $\overline{R} \subseteq \overline{S} \subseteq \overline{T}$. Обозначим $[\overline{T} : \overline{S}] = k$. Тогда $[\overline{S} : \overline{R}] = m$ и $[\overline{T} : \overline{R}] = mk$. В силу теоремы 3 $G = \text{Aut}(T/R)$ – группа мощности mk и $H = \text{Aut}(T/S)$ – ее подгруппа мощности k , т.е. индекса m . Пусть $\sigma_1, \dots, \sigma_m$ – представители всех левых смежных классов группы G по подгруппе H .

Пусть $a \in S$. В силу предложения 1(е) $a = \text{tr}_{T/S}(b)$ для некоторого $b \in T$. Ввиду транзитивности функции след $\text{tr}_{S/R}(a) = \text{tr}_{T/R}(b)$. Пользуясь теоремой 3, получаем:

$$\text{tr}_{S/R}(a) = \text{tr}_{T/R}(b) = \sum_{\sigma \in G} \sigma(b) = \sum_{i=1}^m \sum_{h \in H} \sigma_i h(b) = \sum_{i=1}^m \sigma_i \left(\sum_{h \in H} h(b) \right).$$

По теореме 3 внутренняя сумма есть $\text{tr}_{T/S}(b) = a$. Следовательно,

$$\text{tr}_{S/R}(a) = \sum_{i=1}^m \sigma_i(a).$$

Так как $a \in S$, то $\sigma_i(a)$ можно заменить на $\sigma'_i(a)$, где σ'_i – ограничение $\sigma_i: T \rightarrow T$ на S . Так как $\sigma'_1, \dots, \sigma'_m$ – мономорфизмы S в T над R , причем они различны, поскольку $\sigma_1, \dots, \sigma_m$ – представители различных смежных классов G по H , то $\{\sigma'_1, \dots, \sigma'_m\} = \{\eta_1, \dots, \eta_m\}$. Следовательно,

$$\text{tr}_{S/R}(a) = \sum_{i=1}^m \sigma'_i(a) = \sum_{i=1}^m \eta_i(a).$$

Напомним [3], [16], [17], что *кольцом Галуа* называется конечное коммутативное локальное кольцо R , максимальный идеал которого равен pR для некоторого простого числа p . Кольцо Галуа с точностью до изоморфизма определяется своей характеристикой p^n и числом элементов q^n , где $q = p^r$, и обозначается $\text{GR}(q^n, p^n)$. Частные случаи колец Галуа – примарные кольца вычетов $\mathbb{Z}_{p^n} = \text{GR}(p^n, p^n)$ и конечные поля $\text{GF}(q) = \text{GR}(q, p)$. Если $F(x)$ – унитарный многочлен степени m над кольцом Галуа $R = \text{GR}(q^n, p^n)$ такой, что $\overline{F}(x)$ – неприводимый многочлен над полем вычетов $\overline{R} = \text{GF}(q)$, то кольцо $S = R[x]/F(x) = R[\theta]$, где $\theta = [x]_F \in S$, является кольцом Галуа $S = \text{GR}(q^{mn}, p^n)$, называемым расширением Галуа кольца R . Функция *след из кольца Галуа S в R* определяется равенством (см. [3])

$$\text{Tr}_R^S(a) = \sum_{\sigma \in \text{Aut}(S/R)} \sigma(a), \quad a \in S. \quad (12)$$

Группа $\text{Aut}(S/R)$ в данном случае является циклической группой порядка m . Согласно [3; теорема 8] каждая ЛРП $u \in L_R(F)$ представляется в виде

$$u(i) = \text{Tr}_R^S(c\theta^i), \quad i \geq 0, \quad (13)$$

где константа $c \in S$ определена однозначно. Из теоремы 3 вытекает

СЛЕДСТВИЕ 5. Если R – кольцо Галуа и S – его расширение Галуа, то $\text{Tr}_R^S = \text{tr}_{S/R}$ и представление (4) совпадает с представлением (13).

В работе [3; теорема 7] в случае, когда R – кольцо Галуа, найдено явное описание действия автоморфизмов $\sigma \in \text{Aut}(S/R)$ и функции след $\text{Tr}_R^S(a)$ в терминах p -адического разложения элемента $a \in S$. Такое описание полезно при решении ряда прикладных задач [3], [4], [7], [9]. Мы обобщим этот результат на произвольное конечное локальное кольцо R и даже на следующий более широкий класс колец.

Пусть R – локальное кольцо с конечным полем вычетов $\overline{R} = \text{GF}(q)$ характеристики p и нильпотентным радикалом, $J(R)^n = 0$, где n – индекс нильпотентности. Так как кольцо R вполне примарно, то оно гензелево. Следовательно, множество

$$\Gamma(R) = \{a \in R : a^q = a\}$$

корней многочлена $x^q - x$ в кольце R состоит из q элементов, попарно несовместимых по модулю $J(R)$. Очевидно, $\Gamma(R)$ замкнуто относительно умножения. Назовем $\Gamma(R)$ p -адическим координатным множеством кольца R .

Рассмотрим R -модули $M_i = J(R)^i / J(R)^{i+1}$, $0 \leq i \leq n-1$, являющиеся также векторными пространствами над полем $\overline{R}$ относительно внешней операции

$$\overline{a}(c + J(R)^{i+1}) = ac + J(R)^{i+1}, \quad a \in R, \quad c \in J(R)^i.$$

Зафиксируем базисы $\{e_{i\alpha} + J(R)^{i+1} : \alpha \in A_i\}$ пространств M_i над полем $\overline{R}$, где $e_{i\alpha} \in J(R)^i$ и A_i – некоторые множества индексов, $|A_i| = \dim_{\overline{R}} M_i$. В частности, $M_0 = \overline{R}$, $|A_0| = 1$, и кольцо R конечно тогда и только тогда, когда множества $A_1, \dots, A_{n-1}$ конечны. Легко увидеть, что произвольный элемент $a \in R$ однозначно представляется в виде

$$a = \sum_{i=0}^{n-1} \sum_{\alpha \in A_i} a_{i\alpha} e_{i\alpha}, \quad a_{i\alpha} \in \Gamma(R), \quad (14)$$

где лишь конечное число элементов $a_{i\alpha}$ отлично от нуля. Представление (14) будем называть p -адическим разложением элемента a или его разложением в p -адическом координатном множестве, а элементы $a_{i\alpha}$ – p -адическими координатами элемента a . (Разложение и p -адические координаты элемента a зависят от выбора базисов пространств M_i .) Если $R = \text{GR}(q^n, p^n)$ – кольцо Галуа, то $\dim M_i = 1$, $0 \leq i \leq n-1$, и если в качестве базиса M_i взять элемент $p^i + J(R)^{i+1}$, то p -адическое разложение будет иметь вид (см. [3; утверждение 1])

$$a = \sum_{i=0}^{n-1} a_i p^i, \quad a_i \in \Gamma(R).$$

ТЕОРЕМА 6. Пусть R – локальное кольцо с конечным полем вычетов $\overline{R} = \text{GF}(q)$ и нильпотентным радикалом индекса нильпотентности $n \geq 1$, $F(x) \in R[x]$ – унитарный многочлен степени t такой, что многочлен $\overline{F}(x)$ неприводим над полем $\overline{R}$, $S = R[x]/F(x)$. Пусть $\{e_{i\alpha} + J(R)^{i+1} : \alpha \in A_i\}$ – базис пространства $J(R)^i/J(R)^{i+1}$ над полем $\overline{R}$, $0 \leq i \leq n-1$. Тогда выполняются следующие утверждения:

(а) многочлен $F(x)$ сепарабелен, и кольцо S является кольцом разложения $F(x)$ над R ;

(б) $\{e_{i\alpha} + J(S)^{i+1} : \alpha \in A_i\}$ есть базис пространства $N_i = J(S)^i/J(S)^{i+1}$ над полем $\overline{S}$, $0 \leq i \leq n-1$;

(в) для любого автоморфизма $\sigma \in \text{Aut}(S/R)$ существует единственное число $t = \overline{0, t-1}$ такое, что действие σ на произвольном элементе $a \in S$ с p -адическим разложением

$$a = \sum_{i=0}^{n-1} \sum_{\alpha \in A_i} a_{i\alpha} e_{i\alpha}, \quad a_{i\alpha} \in \Gamma(S), \quad (15)$$

задается равенством

$$\sigma(a) = \sum_{i=0}^{n-1} \sum_{\alpha \in A_i} a_{i\alpha}^{q^t} e_{i\alpha}. \quad (16)$$

Группа $\text{Aut}(S/R)$ является циклической группой порядка t и порождается автоморфизмом Фробениуса, получающимся при $t = 1$.

ДОКАЗАТЕЛЬСТВО. (а) Так как $\overline{R}$ конечно, то $\overline{F}(x)$ сепарабелен и $\overline{S}$ – минимальное поле разложения $\overline{F}(x)$ над $\overline{R}$. Так как R гензелево, то и S гензелево. Отсюда следует, что S является кольцом разложения $F(x)$ над R .

(б) По предложению 1(а) $J(S)^i = (J(R)S)^i = J(R)^i S$ и $N_i = J(R)^i S / J(S)^{i+1}$. Теперь доказательство того, что $\{e_{i\alpha} + J(S)^{i+1} : \alpha \in A_i\}$ – базис N_i над $\overline{S}$, заключается в стандартной проверке. При доказательстве линейной независимости используется, что ${}_R S$ – свободный модуль.

(в) Если $\sigma \in \text{Aut}(S/R)$, то $\overline{\sigma} \in \text{Aut}(\overline{S}/\overline{R})$ и в силу [1], [13] существует единственное число $t = \overline{0, t-1}$ такое, что $\overline{\sigma}(\overline{a}) = \overline{a}^{q^t}$, $a \in S$. Так как $\Gamma(S)$ – множество корней многочлена $x^{q^m} - x \in R[x]$ в кольце S , то $\sigma(\Gamma(S)) \subseteq \Gamma(S)$. Поэтому если $a \in \Gamma(S)$, то $\sigma(a)$ – элемент из $\Gamma(S)$, сравнимый с a^{q^t} по модулю $J(S)$. Так как $\Gamma(S)$ замкнуто относительно умножения, то $a^{q^t} \in \Gamma(S)$. В итоге

$$\sigma(a) = a^{q^t}, \quad a \in \Gamma(S).$$

Поскольку σ – автоморфизм над R и $e_{i\alpha} \in R$, то действие σ на элементе $a \in S$ с p -адическим разложением (15) задается равенством (16).

Нашей дальнейшей задачей является обобщение теоремы 2 в двух направлениях: во-первых, мы расширим класс многочленов $F(x)$, для которых любая ЛРП из $L_R(F)$ имеет представление функцией след, и, во-вторых, рассмотрим ЛРП над модулями.

Напомним, что *биномиальной последовательностью* над кольцом R с корнем $a \in R$ порядка $l \geq 0$ называется последовательность $a^{[l]}$ со знаками

$$a^{[l]}(\overline{0, l}) = (0, \dots, 0, 1), \quad a^{[l]}(i) = \binom{i}{l} a^{i-l}, \quad \text{если } i > l. \quad (17)$$

Формулу $a^{[l]}(i) = \binom{i}{l} a^{i-l}$ будем использовать при всех $i \geq 0$, считая, что $a^0 = e$ для любого $a \in R$ и что если $\binom{i}{l} = 0$, то и $\binom{i}{l} a^{i-l} = 0$ независимо от того, определена ли степень a^{i-l} . Биномиальная последовательность $a^{[l]}$ есть ЛРП над R с единственным минимальным многочленом $(x - a)^{l+1}$ (см. [7]). Ниже используется также выражение $\binom{i}{k} \text{tr}_{S/R}(c\theta^{i-k})$, где $i, k \geq 0$, которое мы полагаем равным нулю при $i - k < 0$.

ТЕОРЕМА 7. Пусть R — локальное кольцо, $F(x) \in R[x]$ — унитарный сепарабельный многочлен такой, что его образ $\overline{F}(x)$ неприводим над полем $\overline{R}$, $S = R[x]/F(x) = R[\theta]$, где $\theta = [x]_F$, и $k \geq 1$. Тогда для любой ЛРП $u \in L_R(F^k)$ существует единственный набор констант $c_0, \dots, c_{k-1} \in S$ таких, что

$$u(i) = \text{tr}_{S/R}(c_0 \theta^i) + \binom{i}{1} \text{tr}_{S/R}(c_1 \theta^{i-1}) + \dots + \binom{i}{k-1} \text{tr}_{S/R}(c_{k-1} \theta^{i-k+1}), \quad i \geq 0. \quad (18)$$

Любая последовательность вида (18) принадлежит $L_R(F^k)$.

ДОКАЗАТЕЛЬСТВО. Убедимся в том, что любая последовательность вида (18) принадлежит $L_R(F^k)$. Достаточно доказать, что для любого $n \geq 0$ последовательность $v(i) = \binom{i}{n} \text{tr}_{S/R}(c\theta^{i-n})$, $i \geq 0$, принадлежит $L_R(F^{n+1})$. Проведем индукцию по n . При $n = 0$ утверждение следует из теоремы 2. Пусть утверждение доказано для параметров меньших n .

Напомним [7], что произведением многочлена $F(x) = \sum_{s \geq 0} f_s x^s$ на последовательность v называется последовательность $w = F(x)v$ со знаками $w(i) = \sum_{s \geq 0} f_s v(i+s)$, $i \geq 0$. Относительно этой операции множество последовательностей над кольцом R образует левый $R[x]$ -модуль, и условие $v \in L_R(F^{n+1})$ равносильно тому, что $F(x)^{n+1}v = 0$. Рассмотрим последовательность $w = F(x)v$. Имеем

$$w(i) = \sum_{s \geq 0} f_s v(i+s) = \sum_{s \geq 0} f_s \binom{i+s}{n} \text{tr}_{S/R}(c\theta^{i+s-n}).$$

Так как

$$\begin{aligned} \binom{i+s}{n} &= \binom{i+s-1}{n} + \binom{i+s-1}{n-1} \\ &= \binom{i+s-2}{n} + \binom{i+s-2}{n-1} + \binom{i+s-1}{n-1} \\ &= \dots = \binom{i}{n} + \binom{i}{n-1} + \binom{i+1}{n-1} + \dots + \binom{i+s-1}{n-1}, \end{aligned}$$

то $w = w_1 + w_2$, где

$$\begin{aligned} w_1(i) &= \sum_{s \geq 0} f_s \binom{i}{n} \operatorname{tr}_{S/R}(c\theta^{i+s-n}) = \binom{i}{n} \operatorname{tr}_{S/R}\left(\sum_{s \geq 0} f_s c\theta^{i+s-n}\right) \\ &= \binom{i}{n} \operatorname{tr}_{S/R}(c\theta^{i-n}F(\theta)) = 0, \\ w_2(i) &= \sum_{s \geq 0} f_s \left[\binom{i}{n-1} + \binom{i+1}{n-1} + \cdots + \binom{i+s-1}{n-1} \right] \operatorname{tr}_{S/R}(c\theta^{i+s-n}). \end{aligned}$$

По предположению индукции $w = w_2 \in L_R(F^n)$. Следовательно, $v \in L_R(F^{n+1})$. Тем самым доказано, что любая последовательность вида (18) принадлежит $L_R(F^k)$.

Обратно, пусть $u \in L_R(F^k)$. Тогда условие (18) равносильно условию

$$u(i) = \sum_{r=0}^{k-1} \binom{i}{r} \operatorname{tr}_{S/R}(c_r \theta^{i-r}), \quad 0 \leq i \leq mk-1, \quad (19)$$

где $m = \deg F(x)$. Элемент $c_r \in S$ представим в виде $c_r = [c_r(x)]_F = c_r(\theta)$, где $c_r(x) = c_{r0} + c_{r1}x + \cdots + c_{r,m-1}x^{m-1} \in R[x]$. Тогда условие (19) запишется в виде

$$u(i) = \sum_{r=0}^{k-1} \sum_{j=0}^{m-1} \binom{i}{r} c_{rj} \operatorname{tr}_{S/R}(\theta^{i-r+j}), \quad 0 \leq i \leq mk-1,$$

или

$$(u(0), \dots, u(mk-1)) = (c_{00}, c_{01}, \dots, c_{k-1,m-1})A,$$

где A – матрица размера $mk \times mk$ над кольцом R . Для доказательства теоремы достаточно убедиться в том, что матрица A обратима. Так как R локально, то это равносильно обратимости матрицы $\bar{A}$ над полем $\bar{R}$. Доказательство последнего утверждения, очевидно, равносильно доказательству теоремы для ЛРП $\bar{u}$ над полем $\bar{R}$. Таким образом, доказательство свелось к проверке того, что любая последовательность $u \in L_R(F^k)$, где R – поле, представляется в виде (18). Поэтому далее считаем, что R – поле.

Множество последовательностей вида (18) при различных $c_0, \dots, c_{k-1} \in S$ является пространством над полем R . В силу доказанного это есть подпространство в $L_R(F^k)$. Размерность последнего пространства равна mk . Так как размерность над R пространства векторов $(c_0, \dots, c_{k-1}) \in S^k$ равна $[S : R]k = mk$, то достаточно проверить, что если $(c_0, \dots, c_{k-1})$ – ненулевой вектор, то и последовательность u , определенная в (18), ненулевая.

Пусть $c_n \neq 0$, причем $n = \overline{0, k-1}$ – наибольшее число с этим свойством. Достаточно доказать, что $F(x)^n u \neq 0$. В силу доказанного $F(x)^n u = F(x)^n v$, где $v(i) = \binom{i}{n} \operatorname{tr}_{S/R}(c_n \theta^{i-n})$, $i \geq 0$. Пусть T – минимальное поле разложения многочлена $F(x)$ над полем S и $\theta = \theta_1, \theta_2, \dots, \theta_m$ – все корни $F(x)$ в поле T . Тогда ввиду следствия 4 и соотношения (11)

$$v(i) = \binom{i}{n} \sum_{t=1}^m \eta_t(c_n \theta^{i-n}) = \binom{i}{n} \sum_{t=1}^m \eta_t(c_n) \eta_t(\theta)^{i-n} = \sum_{t=1}^m \eta_t(c_n) \binom{i}{n} \theta_t^{i-n}.$$

Биномиальная последовательность $\theta_t^{[n]}(i) = \binom{i}{n} \theta_t^{i-n}$ есть ЛРП над полем T с минимальным многочленом $(x - \theta_t)^{n+1}$. Так как $c_n \neq 0$, то $\eta_t(c_n) \neq 0$. Поэтому $\eta_t(c_n)\theta_t^{[n]}$ — ЛРП с минимальным многочленом $(x - \theta_t)^{n+1}$, $1 \leq t \leq m$. Поскольку минимальный многочлен суммы ЛРП с попарно взаимно простыми минимальными многочленами равен произведению минимальных многочленов слагаемых [7], v — ЛРП с минимальным многочленом $F(x)^{n+1}$. Следовательно, $F(x)^n v \neq 0$. Теорема доказана.

Будем говорить, что унитарный многочлен $F(x) \in R[x]$ над локальным кольцом R обладает *сепарабельным каноническим разложением* над R , если он представляется в виде

$$F(x) = F_1(x)^{k_1} \cdots F_t(x)^{k_t}, \quad (20)$$

где $F_i(x) \in R[x]$, $1 \leq i \leq t$, — унитарный сепарабельный многочлен такой, что $\overline{F}_i(x)$ неприводим над полем $\overline{R}$ и $\overline{F}_i(x) \neq \overline{F}_j(x)$ при $1 \leq i < j \leq t$. Рассмотрим кольцо $S = R[\theta_1, \dots, \theta_t]$, полученное последовательным присоединением к кольцу R по одному корню θ_i каждого из многочленов $F_i(x)$, $1 \leq i \leq t$. Кольцо S содержит подкольца $R[\theta_i] \cong R[x]/F_i(x)$, $1 \leq i \leq t$. Многочлен $F_i(x)$ имеет корень в кольце S , но может не разлагаться над S на линейные множители. Если R гезелево, будем также рассматривать кольцо разложения T многочлена $F(x)$, полученное присоединением всех корней многочленов $F_1, \dots, F_t$ к кольцу R . В башне $R \subseteq S \subseteq T$ каждое включение может быть строгим.

СЛЕДСТВИЕ 8. Пусть R — локальное кольцо, $F(x) \in R[x]$ — унитарный многочлен, имеющий над R сепарабельное каноническое разложение (20), $S = R[\theta_1, \dots, \theta_t]$ — расширение кольца R корнями $\theta_1, \dots, \theta_t$ многочленов $F_1(x), \dots, F_t(x)$ соответственно. Тогда для любой ЛРП $u \in L_R(F)$ существует единственный набор констант $c_{s0}, \dots, c_{s, k_s-1} \in R[\theta_s]$, $1 \leq s \leq t$, таких, что

$$u(i) = \sum_{s=1}^t \sum_{r=0}^{k_s-1} \binom{i}{r} \text{tr}_{R[\theta_s]/R}(c_{sr} \theta_s^{i-r}), \quad i \geq 0. \quad (21)$$

Любая последовательность вида (21) принадлежит $L_R(F)$.

ДОКАЗАТЕЛЬСТВО. Ввиду (2) многочлены $F_i(x)^{k_i}$ и $F_j(x)^{k_j}$ над кольцом R взаимно просты. Поэтому в силу [7]

$$L_R(F) = L_R(F_1^{k_1}) \dot{+} \cdots \dot{+} L_R(F_t^{k_t}).$$

Теперь следствие вытекает стандартным образом из теоремы 7.

Представление (21) и его частные случаи (4) и (18) будем называть *представлением линейной рекуррентной последовательности и функцией след*. Для ЛРП над конечным полем такое представление известно из [1], для ЛРП над кольцом Галуа представление (4) получено в [3].

ЗАМЕЧАНИЕ 1. Отметим, что представление функцией след или его однозначность не сохраняется при переходе к расширениям. Действительно, пусть выполнены условия следствия 4 и $u \in L_R(F)$. Тогда u обладает представлением функцией след $u(i) = \text{tr}_{S/R}(c\theta^i)$ над S , причем константа $c \in S$ определяется однозначно. С другой стороны, над расширением T кольца S

$$\text{tr}_{T/R}(c\theta^i) = \text{tr}_{S/R}(\text{tr}_{T/S}(c\theta^i)) = \text{tr}_{S/R}(c\theta^i \text{tr}_{T/S}(1)) = k \text{tr}_{S/R}(c\theta^i) = ku(i),$$

где $k = [\overline{T} : \overline{S}]$. В частности, если k делится на характеристику кольца R , то правая часть равна нулю. Таким образом, представление функцией след не сохраняется при переходе от кольца S к расширению T . В частности, в представлении (21) $\text{tr}_{R[\theta_s]/R}$ нельзя заменить на $\text{tr}_{S/R}$. Возвращаясь к условиям следствия 4, заметим, что по предположению 1(e) можно найти элемент $c_1 \in T$, для которого $c = \text{tr}_{T/S}(c_1)$. Тогда

$$u(i) = \text{tr}_{T/R}(c_1\theta^i), \quad i \geq 0,$$

однако константа $c_1 \in T$ здесь уже не определена однозначно.

Замечание 1 показывает, что если дана ЛРП u над кольцом R и расширение $R \subseteq T$, то правильнее говорить о существовании представления ЛРП u функцией след не над кольцом T , а над некоторым специально подобранным подкольцом S кольца T (или несколькими подкольцами, как в представлении (21)).

Рассмотрим теперь представление функцией след для ЛРП над модулями. Пусть ${}_R M$ – левый модуль над кольцом R . Напомним [7], что последовательность $u = (u(0), u(1), \dots)$ элементов M называется *линейной рекуррентной последовательностью* порядка m над модулем M , если существуют элементы $c_0, \dots, c_{m-1} \in R$ такие, что выполняется условие (1). Многочлен $F(x) = x^m - c_{m-1}x^{m-1} - \dots - c_1x - c_0 \in R[x]$ называется *характеристическим многочленом* ЛРП u . Множество всех ЛРП над M с характеристическим многочленом $F(x)$ обозначим через $L_M(F)$.

Пусть S – расширение кольца R , являющееся конечно порожденным проективным R -модулем. Рассмотрим левый S -модуль $N = S \otimes M$, где $\otimes = \otimes_R$, получающийся расширением кольца коэффициентов модуля M . Определим функцию *след* $\text{tr}_{N/M}: N \rightarrow M$ соотношением

$$\text{tr}_{N/M}(s \otimes m) = \text{tr}_{S/R}(s)m, \quad s \in S, \quad m \in M.$$

Корректность этого определения следует из билинейности над R отображения $S \times M \rightarrow M, (s, m) \mapsto \text{tr}_{S/R}(s)m$.

ТЕОРЕМА 9. Пусть ${}_R M$ – модуль над локальным кольцом R , $F(x) \in R[x]$ – унитарный сепарабельный многочлен такой, что $\overline{F}(x)$ неприводим над полем $\overline{R}$, $S = R[x]/F(x) = R[\theta]$, где $\theta = [x]_F$. Тогда для любой ЛРП $u \in L_M(F)$ существует единственная константа $c \in N = S \otimes M$ такая, что

$$u(i) = \text{tr}_{N/M}(\theta^i c), \quad i \geq 0. \quad (22)$$

Любая последовательность вида (22) принадлежит $L_M(F)$.

ДОКАЗАТЕЛЬСТВО. Пусть $(m_\alpha, \alpha \in A)$ – произвольная система образующих R -модуля M . Обозначим $\deg F(x) = m$. Для $i = \overline{0, m-1}$ представим $u(i)$ в виде $u(i) = \sum_{\alpha \in A} u_\alpha(i) m_\alpha$, где $u_\alpha(i) \in R$ и для каждого $i = \overline{0, m-1}$ лишь конечное число элементов $u_\alpha(i)$ не равно нулю. Рассмотрим последовательность $v_\alpha \in L_R(F)$ над кольцом R с начальным вектором $v_\alpha(\overline{0, m-1}) = u_\alpha(\overline{0, m-1})$, $\alpha \in A$, и положим $v = \sum_{\alpha \in A} v_\alpha m_\alpha$ (в этой сумме лишь конечное число последовательностей $v_\alpha \neq 0$). Тогда v – ЛРП из $L_M(F)$ с начальным вектором $v(\overline{0, m-1}) = u(\overline{0, m-1})$, следовательно, $v = u$, т.е. $u = \sum_{\alpha \in A} v_\alpha m_\alpha$. По теореме 2 для каждого $\alpha \in A$ существует константа $c_\alpha \in S$ такая, что

$$v_\alpha(i) = \text{tr}_{S/R}(c_\alpha \theta^i), \quad i \geq 0.$$

Так как лишь конечное число последовательностей $v_\alpha \neq 0$, то лишь конечное число элементов $c_\alpha \neq 0$. Тогда для $c = \sum_{\alpha \in A} c_\alpha \otimes m_\alpha \in N$ имеем:

$$u(i) = \sum_{\alpha \in A} v_\alpha(i) m_\alpha = \sum_{\alpha \in A} \text{tr}_{S/R}(c_\alpha \theta^i) m_\alpha = \text{tr}_{N/M}(\theta^i c), \quad i \geq 0.$$

Тем самым доказано существование представления (22). Тот факт, что любая последовательность вида (22) принадлежит $L_M(F)$, проверяется так же, как в доказательстве теоремы 2.

Докажем однозначность представления (22). Для этого достаточно доказать, что из равенства нулю последовательности u , определенной в (22), следует равенство $c = 0$. Пусть $u(i) = \text{tr}_{N/M}(\theta^i c) = 0$, $i \geq 0$. Элемент c можно записать в виде $c = \sum_{\alpha \in A} c_\alpha \otimes m_\alpha$, где $c_\alpha \in S$ и лишь конечное число элементов $c_\alpha \neq 0$. Элементы c_α представим в виде $c_\alpha = c_\alpha(\theta)$, где $c_\alpha(x) = c_{\alpha 0} + c_{\alpha 1}x + \dots + c_{\alpha, m-1}x^{m-1} \in R[x]$. Тогда

$$u(i) = \text{tr}_{S/R} \left(\sum_{\alpha \in A} \sum_{j=0}^{m-1} c_{\alpha j} \theta^{i+j} \right) m_\alpha = \sum_{j=0}^{m-1} \text{tr}_{S/R}(\theta^{i+j}) x_j = 0, \quad (23)$$

где $x_j = \sum_{\alpha \in A} c_{\alpha j} m_\alpha \in M$, $0 \leq j \leq m-1$. Как и в доказательстве теоремы 2, матрица $(\text{tr}_{S/R}(\theta^{i+j}))$, $0 \leq i, j \leq m-1$, обратима ввиду [16; теорема 2.2]. Поэтому из (23) вытекает, что $x_j = 0$, $0 \leq j \leq m-1$. Следовательно,

$$c = \sum_{\alpha \in A} c_\alpha \otimes m_\alpha = \sum_{\alpha \in A} \sum_{j=0}^{m-1} c_{\alpha j} \theta^j \otimes m_\alpha = \sum_{j=0}^{m-1} \theta^j \otimes \sum_{\alpha \in A} c_{\alpha j} m_\alpha = \sum_{j=0}^{m-1} \theta^j \otimes x_j = 0,$$

что и требовалось доказать.

ТЕОРЕМА 10. Пусть ${}_R M$ – модуль над локальным кольцом R , $F(x) \in R[x]$ – унитарный многочлен, имеющий над кольцом R сепарабельное каноническое разложение (20), $S_j = R[x]/F_j(x) = R[\theta_j]$, где $\theta_j = [x]_{F_j}$, $1 \leq j \leq t$. Тогда

для любой ЛРП $u \in L_M(F)$ существует единственный набор констант $c_{jr} \in N_j = S_j \otimes_R M$, $1 \leq j \leq t$, $0 \leq r < k_j$, такой, что

$$u(i) = \sum_{j=1}^t \sum_{r=0}^{k_j-1} \binom{i}{r} \operatorname{tr}_{N_j/M}(\theta_j^{i-r} c_{jr}), \quad i \geq 0. \quad (24)$$

Любая последовательность вида (24) принадлежит $L_R(F)$.

Доказательство аналогично доказательству теоремы 9 со ссылками на теорему 7 и следствие 8 вместо теоремы 2.

ЗАМЕЧАНИЕ 2. Поскольку не каждый унитарный многочлен над локальным кольцом R обладает сепарабельным каноническим разложением, существование представления функцией след доказано не для произвольной ЛРП над локальным кольцом R и модулем ${}_R M$.

С другой стороны, пусть кольцо R вполне примарно. Если $F(x)$ и $G(x)$ — два многочлена над R такие, что $\overline{F}(x) = \overline{G}(x)$, то все коэффициенты многочлена $\Delta(x) = F(x) - G(x)$ нильпотентны. Тогда $\Delta(x)^n = 0$ для некоторого n , откуда легко вытекает, что $F(x)$ делит $G(x)^n$. Как следствие получаем, что если кольцо R вполне примарно и имеет совершенное поле вычетов, то любой унитарный многочлен $F(x) \in R[x]$ делит многочлен $H(x) \in R[x]$, имеющий сепарабельное каноническое разложение над R . Тогда произвольная ЛРП $u \in L_M(F)$ принадлежит $L_M(H)$ и обладает представлением функцией след.

ПРИМЕР 1. Пусть $R = \mathbb{Z}_4$, $F(x) = x^2 + 1$, $S = R[x]/F(x) = R[\theta]$. По предложению 1(a) $\operatorname{tr}_{S/R}(1) = 2$ и $\operatorname{tr}_{S/R}(\theta) = 0$, поэтому $\operatorname{tr}_{S/R}(S) = 2R$. Отсюда следует, что в ЛРП-семействе $L_R(F)$ лишь последовательности из $2L_R(F)$ представляются функцией след над кольцом S . Причина заключается в том, что многочлен $F(x)$ не сепарабелен и не имеет сепарабельного канонического разложения над R . С другой стороны, $F(x)$ делит $(x-1)^4$, поэтому $L_R(F) \subseteq L_R((x-1)^4)$ и по теореме 7 любая ЛРП $u \in L_R(F)$ имеет представление функцией след. В данном случае это — представление над самим кольцом R и оно имеет вид

$$u(i) = c_0 + \binom{i}{1} c_1 + \binom{i}{2} c_2 + \binom{i}{3} c_3, \quad i \geq 0, \quad \text{где } c_i \in R.$$

ЗАМЕЧАНИЕ 3. Пусть $R = R_1 \dot{+} \dots \dot{+} R_t$ — прямая сумма колец. Тогда любой R -модуль M представляется в виде прямой суммы R -модулей $M = M_1 \dot{+} \dots \dot{+} M_t$, где M_i является модулем над кольцом R_i , $1 \leq i \leq t$. Соответственно любой многочлен $F(x)$ над кольцом R и любая ЛРП u над модулем M (в частном случае — над кольцом R) однозначно представляются в виде $F(x) = F_1(x) + \dots + F_t(x)$ и $u = u_1 + \dots + u_t$, где $F_i(x)$ — многочлен над кольцом R_i , u_i — последовательность над модулем M_i , $1 \leq i \leq t$. При этом $u \in L_M(F)$ тогда и только тогда, когда $u_i \in L_{M_i}(F_i)$, $1 \leq i \leq t$. Если каждая ЛРП u_i представляется функцией след, то и ЛРП u имеет представление функцией след, равное сумме этих представлений.

В частности, так как произвольное (коммутативное) артиново кольцо представляется в виде прямой суммы локальных [18], то любая ЛРП над артиновым кольцом R или модулем ${}_R M$ обладает представлением функцией след.

В примере 1 представление ЛРП u функцией след совпадает с ее *биномиальным представлением*, т.е. представлением в виде линейной комбинации биномиальных последовательностей. В оставшейся части работы мы сравним эти два представления. Вначале приведем пример, показывающий различия между ними (эти различия могут показаться несущественными). При этом оказывается важным, какое именно расширение исходного кольца R рассматривается.

ПРИМЕР 2. Пусть $R = \mathbb{Q}$ – поле рациональных чисел и $F(x) = x^3 - 2$. Обозначим через $\theta = \sqrt[3]{2}$, θ_2, θ_3 комплексные корни многочлена $F(x)$. Рассмотрим расширение $S = \mathbb{Q}(\theta)$ и минимальное поле разложения $T = \mathbb{Q}(\theta, \theta_1, \theta_2)$ многочлена $F(x)$ над полем $\mathbb{Q}$. По теореме 2 любая ЛРП $u \in L_{\mathbb{Q}}(F)$ имеет представление $u(i) = \text{tr}_{S/\mathbb{Q}}(c\theta^i)$ функцией след над полем S , где константа $c \in S$ определена однозначно. Над полем T ЛРП u не имеет однозначного представления функцией след, хотя справедливы соотношения

$$u(i) = \frac{1}{2} \text{tr}_{T/\mathbb{Q}}(c\theta^i), \quad u(i) = \text{tr}_{T/\mathbb{Q}}(c_1\theta^i),$$

где константа $c_1 \in T$ определена неоднозначно. С другой стороны, ЛРП u имеет биномиальное представление над полем T :

$$u(i) = c_1\theta^i + c_2\theta_2^i + c_3\theta_3^i,$$

где константы $c_1, c_2, c_3 \in T$ определены однозначно, но не имеет биномиального представления над полем S , за исключением случая $u = 0$ (причина в том, что S не содержит всех корней многочлена $F(x)$). Таким образом, ЛРП u имеет представление функцией след над S , но не над T , и имеет биномиальное представление над T , но не над S .

Следующее предложение описывает связь между представлением функцией след и биномиальным представлением. Из него, в частности, следует, что в условиях примера 2 представление ЛРП u функцией след над S совпадает с биномиальным представлением над T , если функцию $\text{tr}_{S/\mathbb{Q}}$ выразить через вложения S в T над $\mathbb{Q}$.

ПРЕДЛОЖЕНИЕ 11. В условиях следствия 8 пусть кольцо R гензелево и T – кольцо разложения многочлена $F(x)$ над S . Тогда представление (21) ЛРП $u \in L_R(F)$ функцией след над кольцом S (точнее, над подкольцами кольца S) является биномиальным представлением ЛРП u над кольцом T .

ДОКАЗАТЕЛЬСТВО. Ввиду следствия 4

$$\text{tr}_{R[\theta_s]/R}(a) = \sum_{j=1}^{m_s} \eta_{sj}(a), \quad a \in R[\theta_s], \quad 1 \leq s \leq t,$$

где $\eta_{sj}: R[\theta_s] \rightarrow T$, $1 \leq j \leq m_s$, – мономорфизмы. (Отметим, что ввиду (11) элементы $\eta_{s1}(\theta_s), \dots, \eta_{sm_s}(\theta_s)$ являются всеми корнями многочлена $F_s(x)$ в кольце T .) Следовательно, соотношение (21) имеет вид

$$u(i) = \sum_{s=1}^t \sum_{r=0}^{k_s-1} \sum_{j=1}^{m_s} \binom{i}{r} \eta_{sj}(c_{sr}) \eta_{sj}(\theta_s)^{i-r}, \quad i \geq 0.$$

В правой части получили линейную комбинацию биномиальных последовательностей с корнями $\eta_{sj}(\theta_s)$ и коэффициентами $\eta_{sj}(c_{sr})$ из кольца T .

В связи с предложением 11 интересно выяснить, как выглядит представление функцией след непосредственно над кольцом S , без перехода к кольцу разложения T и представления функции след автоморфизмами. Покажем это на примере 2.

ПРИМЕР 2 (ПРОДОЛЖЕНИЕ). Элемент c поля $S = \mathbb{Q}(\theta)$ представим в виде $c = c_0 + c_1\theta + c_2\theta^2$. Пусть $\varphi_r(c) = c_r$ – проекции S на R , введенные в (3). В силу предложения 1(a) $\text{tr}_{S/\mathbb{Q}}(1) = 3$ и $\text{tr}(\theta) = \text{tr}(\theta^2) = 0$. Учитывая, что $\theta^3 = 2$, получаем:

$$\text{tr}_{S/\mathbb{Q}}(c\theta^i) = \text{tr}_{S/\mathbb{Q}}(c_0\theta^i + c_1\theta^{i+1} + c_2\theta^{i+2}) = 2^k \cdot \begin{cases} 3c_0, & i = 3k, \\ 6c_2, & i = 3k + 1, \\ 6c_1, & i = 3k + 2. \end{cases}$$

Таким образом, в данном случае след “чередует” коэффициенты $3c_0, 6c_2, 6c_1 \in \mathbb{Q}$ и умножает результат на 2 через каждые три такта. Элемент $c \in \mathbb{Q}(\theta)$, для которого $u(i) = \text{tr}_{S/\mathbb{Q}}(c\theta^i)$, выражается через начальный вектор ЛРП u следующим образом:

$$c = \frac{1}{6}(2u(0) + u(2)\theta + u(1)\theta^2).$$

ЗАМЕЧАНИЕ 4. Пусть R – гёизелево кольцо, $F(x) \in R[x]$ – сепарабельный многочлен такой, что многочлен $\overline{F}(x)$ неприводим над полем вычетов $\overline{R}$, $\theta_1, \dots, \theta_m$ – все корни $F(x)$ в кольце разложения T . Согласно [7], [19] произвольная ЛРП $u \in L_R(F)$ имеет над T биномиальное представление

$$u(i) = c_1\theta_1^i + \dots + c_m\theta_m^i, \quad i \geq 0, \quad (25)$$

где $c_r \in T$, $1 \leq r \leq m$. Если коэффициенты c_r пробегает кольцо T , то последовательности (25) пробегает семейство $L_T(F)$. Для последовательностей из подсемейства $L_R(F)$ коэффициенты c_r в представлении (25) не будут независимыми. Ввиду теоремы 2 и следствия 4

$$u(i) = \text{tr}_{S/R}(c\theta_1^i) = \sum_{r=1}^m \eta_r(c)\theta_r^i, \quad i \geq 0,$$

где $S = R[\theta_1] \subseteq T$, $c \in S$ и $\eta_1, \dots, \eta_m$ – все вложения S в T над R . Таким образом, один коэффициент (например, c_1 , если η_1 – тождественное вложение) пробегает

кольцо S (но не все кольцо T), а остальные сопряжены с ним посредством вложений кольца S в T над R . Это показывает, что представление функцией след уточняет вид коэффициентов биномиального представления.

Одной из открытых задач является обобщение полученных результатов на полилинейные рекуррентные последовательности (см. [7]) над кольцами и модулями. Другой задачей является изучение возможности представления функцией след линейных рекуррент над нелокальными кольцами с использованием понятий сепарабельных алгебр и сепарабельных многочленов [11], [16].

Список литературы

1. Лидл Р., Нидеррайтер Г. Конечные поля. Т. 2. М.: Мир, 1988.
2. Нечаев А. А. Функция "след" в кольце Галуа и помехоустойчивые коды // V Всесоюз. симпозиум по теории колец, алгебр и модулей. Тезисы сообщений. Новосибирск, 1982. С. 97.
3. Нечаев А. А. Код Кердока в циклической форме // Дискрет. матем. 1989. Т. 1. № 4. С. 123–139.
4. Нечаев А. А., Кузьмин А. С., Куракин В. Л. Структурные, аналитические и статистические свойства линейных и полилинейных рекуррент // Труды по дискретной математике. Т. 3. М.: Изд-во ТВП, 2000. С. 155–194.
5. Камловский О. В., Кузьмин А. С. Распределение элементов на циклах линейных рекуррентных последовательностей над кольцами Галуа // УМН. 1998. Т. 53. № 2. С. 149–150.
6. Kurakin V., Kuzmin A., Nechaev A. Codes and linear recurrences over Galois rings and QF -modules of the characteristic 4 // Proceedings of the Sixth International workshop on algebraic and combinatorial coding theory (ACCT-VI). Pskov, Russia, September 6–12, 1998. Moskva: MTNTI, 1998. P. 166–171.
7. Kurakin V. L., Kuzmin A. S., Mikhalev A. V., Nechaev A. A. Linear recurring sequences over rings and modules // J. Math. Sci. (New York). 1995. V. 76. № 6. P. 2793–2915.
8. Hammons A. R., Kumar P. V., Calderbank A. R., Sloane N. J. A., Sole P. The $\mathbb{Z}_4$ -linearity of Kerdock, Preparata, Goethals, and related codes // IEEE Trans. Inform. Theory. 1994. V. 40. № 2. P. 301–319.
9. Nechaev A. A., Kuzmin A. S. Trace-function on a Galois ring in coding theory // Lecture Notes in Comput. Sci. 1997. V. 1255. P. 277–290.
10. Борович А. З., Толасов Б. А. Введение в теорию Галуа колец. Орджоникидзе: Северо-Осетинский государственный университет им. К. Л. Хетагурова, 1984.
11. DeMeyer F., Ingraham E. Separable algebras over commutative rings. Berlin: Springer-Verlag, 1971. (Lecture Notes in Math. V. 181.)
12. Каш Ф. Модули и кольца. М.: Мир, 1981.
13. Ленг С. Алгебра. М.: Мир, 1968.
14. Бурбаки Н. Коммутативная алгебра. М.: Мир, 1971.
15. Snapper E. Completely primary rings. I, II, III, IV // Ann. of Math. (2). 1950. V. 52. № 3. P. 666–693; 1951. V. 53. № 1. P. 125–142; 1951. V. 53. № 2. P. 207–234; 1952. V. 55. № 1. P. 46–64.
16. Janusz G. J. Separable algebras over commutative ring // Trans. Amer. Math. Soc. 1966. V. 122. P. 461–479.
17. McDonald B. R. Finite rings with identity. New York: Marcel Dekker, 1974.
18. Атья М., Макдональд И. Введение в коммутативную алгебру. М.: Мир, 1972.

19. *Куракин В. Л.* Биномиальное представление линейных рекуррентных последовательностей // *Фундам. и прикл. матем.* 1995. Т. 1. № 2. С. 553–556.

Москва

Поступила в редакцию
02.10.2001