



# Math-Net.Ru

Общероссийский математический портал

В. Л. Куракин, Полиномиальные преобразования линейных рекуррентных последовательностей над конечными коммутативными кольцами, *Дискрет. матем.*, 2000, том 12, выпуск 3, 3–36

DOI: 10.4213/dm342

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: 18.97.14.85

20 марта 2025 г., 16:40:56



УДК 519.7

## Полиномиальные преобразования линейных рекуррентных последовательностей над конечными коммутативными кольцами

© 2000 г. В. Л. Куракин

Пусть  $u$  — линейная рекуррентная последовательность (ЛРП) над конечным коммутативным локальным кольцом  $R$  с единицей и  $\Phi(x) \in R[x]$ . В работе найден характеристический многочлен  $H(x)$  и получена верхняя оценка ранга (линейной сложности) над кольцом  $R$  для последовательности  $v = \Phi(u)$ . В случае, когда  $\bar{u}$  — ЛРП максимального периода над полем вычетов  $\bar{R} = R/J(R) = \text{GF}(q)$  кольца  $R$  и  $\deg \Phi(x) \leq q - 1$ , доказано, что эта оценка достигается и  $H(x)$  является минимальным многочленом ЛРП  $v$ . Аналогичные результаты получены для последовательности  $v = \Phi(u_1, \dots, u_k)$ , получающейся полиномиальным преобразованием нескольких линейных рекуррент  $u_1, \dots, u_k$  над кольцом  $R$ .

### 1. Введение

Пусть  $R$  — коммутативное кольцо с единицей,  $u$  — линейная рекуррентная последовательность (ЛРП) над кольцом  $R$  с характеристическим многочленом  $F(x) \in R[x]$  степени  $m$ . Последовательность

$$v(i) = \Phi(u(i), \dots, u(i + s - 1)), \quad i \geq 0,$$

где  $\Phi(x_1, \dots, x_s) \in R[x_1, \dots, x_s]$ ,  $s \geq 1$ , будем называть полиномиальным преобразованием последовательности  $u$ . Последовательность  $v$  является линейной рекуррентой над кольцом  $R$ . Рангом (или линейной сложностью) ЛРП  $v$  будем называть степень ее минимального многочлена, то есть характеристического многочлена наименьшей степени. Наша цель — описать характеристический многочлен ЛРП  $v$  возможно меньшей степени и оценить ранг ЛРП  $v$ , а в некоторых случаях — найти минимальный многочлен и точное значение ранга ЛРП  $v$ .

Для линейных рекуррент над полем (в большинстве случаев конечным) эта задача широко исследовалась в [11–19, 22, 24]. При этом использовались результаты о произведении линейных рекуррент над полем (см. [25], а также [23, 8]) и аппарат биномиального представления последовательностей над полем, частным случаем которого является представление линейных рекуррент над конечным полем функцией след.

Если  $P = \text{GF}(q)$ ,  $u$  — ЛРП над  $P$  с неприводимым характеристическим многочленом степени  $m$ ,  $\Phi(x) = \sum_{d \geq 0} \varphi_d x^d \in R[x]$  и  $D = \{d \geq 0 : \varphi_d \neq 0\}$ , то в указанных

работах доказана, в частности, оценка

$$\text{rank } \Phi(u) \leq \sum_{d \in D} \binom{m+d-1}{d}, \quad (1)$$

где через  $\Phi(u)$  обозначается последовательность со знаками  $\nu(i) = \Phi(u(i))$ ,  $i \geq 0$ . Если  $q = p$  — простое число,  $u$  — ЛРП максимального периода над полем  $P$ ,  $\deg \Phi \leq p-1$ , то эта оценка достигается и неравенство обращается в равенство. Если  $q = p^l$ , где  $p$  простое,  $l \geq 1$ , то справедлива более точная оценка

$$\text{rank } \Phi(u) \leq \sum_{d \in D} \binom{m + \nu_0(d) - 1}{\nu_0(d)} \cdots \binom{m + \nu_{l-1}(d) - 1}{\nu_{l-1}(d)}, \quad (2)$$

где  $\nu_0(d), \nu_1(d), \dots$  —  $p$ -ичные разряды числа  $d$ . Если  $u$  — ЛРП максимального периода и  $\deg \Phi \leq q-1$ , то неравенство (2) обращается в равенство.

Нашей целью является получение аналогичных результатов для линейных рекуррент над конечным коммутативным кольцом  $R$  с единицей. Стандартными рассуждениями задача сводится к случаю локального кольца  $R$ , и основные результаты статьи получены в этом предположении. Ряд результатов сохраняется также для некоторых классов бесконечных колец, об этом говорится в замечаниях в конце разделов.

Перечислим основные результаты работы. Чтобы не перегружать введение, мы не формулируем результаты в том общем виде, в котором они доказываются ниже, а ограничиваемся наиболее интересными частными случаями.

Произведение последовательностей над произвольным коммутативным кольцом с единицей рассматривалось в [20, 21], где доказано, что

$$\text{rank } uv \leq \text{rank } u \text{ rank } v.$$

Используя этот результат, легко выводится оценка (см. следствие 1)

$$\text{rank } \Phi(u) \leq \sum_{d \in D} m^d.$$

Однако, эта оценка менее точная, чем (1), и не является ее аналогом ни по формулировке, ни по методам доказательства.

Оценка, аналогичная (1), доказывается нами в разделе 4 для ЛРП  $u$  над конечным коммутативным локальным кольцом  $R$  (см. теорему 2). В частности, если характеристический многочлен ЛРП  $u$  над кольцом  $R$  сепарабелен, то вид полученной оценки совпадает с (1) (см. формулу (16)). Используемые в доказательстве свойства многочленов над кольцом  $R$  и результаты о биномиальном представлении линейных рекуррент над  $R$  излагаются предварительно в разделе 3.

Доказанные в разделе 4 оценки являются простыми и легко вычислимыми, однако, они не достаточно точные и не являются достижимыми для класса всех конечных коммутативных колец с единицей. Основные результаты работы получаются в разделах 5 и 6. В предположении, что характеристический многочлен ЛРП  $u$  над кольцом  $R$  сепарабелен, доказывается более точная оценка ранга ЛРП  $\Phi(u)$  (см. теорему 5 и следствие 4). Если образ  $\bar{u}$  ЛРП  $u$  над полем вычетов  $\bar{R} = R/J(R) = \text{GF}(q)$  кольца  $R$  является линейной рекуррентой максимального периода и  $\deg \Phi(x) \leq q-1$ ,

то эта оценка достигается. В последнем случае описан минимальный многочлен и найдено точное значение ранга ЛРП  $\Phi(u)$  (теорема 7). При условии, что  $R$  — кольцо главных идеалов, в частности, кольцо Гауа или примарное кольцо вычетов  $Z_{p^n}$ , описывается аннулятор последовательности  $\Phi(u)$  (следствие 8). Указанная оценка является достаточно громоздкой и здесь не приводится. Она учитывает порядки коэффициентов многочлена  $\Phi(x)$  в группе  $(R, +)$ . Если  $R = \text{GF}(q)$ , то эта оценка превращается в (2).

Аналогичные результаты получены для полиномиальных преобразований нескольких последовательностей, то есть для последовательности

$$v = \Phi(u_1, \dots, u_K),$$

где  $u_1, \dots, u_K$  — линейные рекурренты,  $\Phi(x_1, \dots, x_K)$  — многочлен над кольцом  $R$ . Так, в случае, когда характеристические многочлены  $F_1(x), \dots, F_K(x)$  последовательностей  $u_1, \dots, u_K$  сепарабельны и имеют степени  $m_1, \dots, m_K$  соответственно, в теореме 4 доказывается оценка

$$\text{rank } \Phi(u_1, \dots, u_K) \leq \sum_{(d_1, \dots, d_K) \in D} \binom{m_1 + d_1 - 1}{d_1} \dots \binom{m_K + d_K - 1}{d_K},$$

где  $D$  — множество векторов  $(d_1, \dots, d_K) \in \mathbf{N}_0^K$  таких, что в запись многочлена  $\Phi$  входит с ненулевым коэффициентом моном  $x_1^{d_1} \dots x_K^{d_K}$ . Однако, эта оценка не является достижимой, в частности, не учитывает свойств кольца  $R$ . В разделе 5 получена более точная, но и более громоздкая, оценка (теорема 6 и следствие 5), а в разделе 6 доказывается, что если  $\bar{u}_1, \dots, \bar{u}_K$  — ЛРП максимального периода над полем  $\bar{R}$ , числа  $m_1, \dots, m_K$  попарно взаимно просты и степень многочлена  $\Phi(x_1, \dots, x_K)$  по переменной  $x_k$  меньше  $M_k = \min\{q, m_k, (q-2)m_k/(q-1) + 1\}$ ,  $k = 1, \dots, K$ , то оценка достигается (теорема 8). В последнем случае описан минимальный многочлен и найдено точное значение ранга ЛРП  $\Phi(u_1, \dots, u_K)$ . Отметим, что если  $R = \text{GF}(q)$  — конечное поле, то эта оценка также справедлива и обобщает результат работы [22] на более широкий класс многочленов  $\Phi(x_1, \dots, x_K)$ , не свободных от квадратов переменных.

Полиномиальные преобразования линейных рекуррент над кольцом  $R = Z_{p^2}$  исследовались автором в [7]. Результаты данной работы обобщают и расширяют результаты [7]. Для тех утверждений данной работы, которые являются аналогами соответствующих утверждений из [7], в ряде случаев найдены более простые доказательства.

## 2. Верхние оценки ранга

В этом разделе будут получены верхние оценки рангов полиномиальных преобразований линейных рекуррентных последовательностей над произвольным коммутативным кольцом с единицей.

Всюду далее термин кольцо означает коммутативное кольцо с единицей. Множество последовательностей над кольцом  $R$  обозначим  $R^\infty$ . Произведением многочлена

$$F(x) = \sum_{s \geq 0} c_s x^s \in R[x]$$

на последовательность  $u \in R^\infty$  называется последовательность  $v = F(x)u \in R^\infty$  со знаками

$$v(i) = \sum_{s \geq 0} c_s u(i + s), \quad i \geq 0.$$

Относительно этой операции абелева группа  $(R^\infty, +)$  образует левый модуль над кольцом  $R[x]$  (см. [4], глава 25, теорема 1, или [9, 19]). Если  $F(x)u = 0$ , то будем говорить, что многочлен  $F(x)$  аннулирует последовательность  $u$ . Идеал

$$\text{Ann}(u) = \{F(x) \in R[x] : F(x)u = 0\}$$

кольца  $R[x]$  называется аннулятором последовательности  $u$ . Если последовательность  $u$  аннулируется некоторым унитарным многочленом  $F(x)$ , то она называется линейной рекуррентной последовательностью (ЛРП) над кольцом  $R$ , а унитарный многочлен  $F(x)$  — ее характеристическим многочленом. Множество всех ЛРП над  $R$  с характеристическим многочленом  $F(x)$  будем обозначать  $L_R(F)$ . Характеристический многочлен ЛРП  $u$  наименьшей степени называется ее минимальным многочленом, а степень минимального многочлена называется рангом  $\text{rank}_R u = \text{rank } u$  ЛРП  $u$ . Минимальный многочлен ЛРП над полем определен однозначно, в общем случае минимальный многочлен ЛРП над кольцом определен неоднозначно.

Напомним, что сопровождающей матрицей для унитарного многочлена

$$F(x) = x^m + c_{m-1}x^{m-1} + \dots + c_1x + c_0 \in R[x]$$

называется матрица

$$S = S(F) = \begin{pmatrix} 0 & 0 & \dots & 0 & -c_0 \\ e & 0 & \dots & 0 & -c_1 \\ 0 & e & \dots & 0 & -c_2 \\ & & \dots & & \\ 0 & 0 & \dots & e & -c_{m-1} \end{pmatrix}.$$

Характеристический многочлен этой матрицы равен  $F(x)$ . Пусть

$$S(F)^{\otimes d} = S(F) \otimes \dots \otimes S(F),$$

где тензорное произведение матриц берется  $d \geq 1$  раз, и  $S(F)^{\otimes 0} = (e)$ , где  $(e)$  — единичная матрица размера  $1 \times 1$ . Тогда  $S(F)^{\otimes d}$  — матрица размера  $m^d \times m^d$ ,  $d \geq 0$ . Результаты этого раздела основаны на следующей теореме из [20].

**Теорема 1** ([20]). *Если  $u, v$  — ЛРП над кольцом  $R$  с характеристическими многочленами  $F(x), G(x) \in R[x]$  степеней  $m, n \geq 1$ , то характеристический многочлен матрицы  $S(F) \otimes S(G)$  является характеристическим многочленом ЛРП  $uv$ , и  $\text{rank } uv \leq mn$ .*

**Предложение 1.** *Пусть  $u$  — ЛРП над кольцом  $R$  с характеристическим многочленом  $F(x) \in R[x]$  степени  $m \geq 1$ ,  $\Phi(x_1, \dots, x_s) \in R[x_1, \dots, x_s]$ ,*

$$v(i) = \Phi(u(i), \dots, u(i + s - 1)), \quad i \geq 0,$$

*$D$  — множество чисел  $d \geq 0$  таких, что в запись многочлена  $\Phi$  входит с ненулевым коэффициентом моном степени  $d$ ,  $F_d(x)$  — характеристический многочлен матрицы  $S(F)^{\otimes d}$ .*

Тогда многочлен

$$H(x) = \prod_{d \in D} F_d(x)$$

является характеристическим многочленом ЛРП  $v$ , и

$$\text{rank } v \leq \Phi^*(m), \quad (3)$$

где

$$\Phi^*(x) = \sum_{d \in D} x^d \in Z[x].$$

*Доказательство.* Многочлен  $\Phi$  можно записать в виде

$$\Phi = \sum_{d \in D} \Phi_d,$$

где  $\Phi_d(x_1, \dots, x_s)$  — форма степени  $d$ . Пусть

$$v_d(i) = \Phi_d(u(i), \dots, u(i + s - 1)), \quad i \geq 0.$$

Тогда

$$v = \sum_{d \in D} v_d.$$

По теореме 1 многочлен  $F_d(x)$  является характеристическим многочленом ЛРП  $v_d$ ,  $d \geq 2$ ; при  $d = 0$  и  $d = 1$  это утверждение, очевидно, также выполнено. Следовательно, многочлен  $H(x)$  является характеристическим многочленом ЛРП  $v$ . Так как  $\deg F_d(x) = m^d$ ,  $d \geq 0$ , то отсюда вытекает оценка (3).

**Следствие 1.** Пусть  $u$  — ЛРП над кольцом  $R$  с характеристическим многочленом  $F(x) \in R[x]$  степени  $m$ ,  $\Phi(x) \in R[x]$ . Тогда

$$\text{rank } \Phi(u) \leq \Phi^*(m),$$

где  $\Phi^*(x)$  — многочлен над кольцом целых чисел, полученный из  $\Phi(x)$  заменой всех ненулевых коэффициентов на 1.

Аналогично доказывается следующий результат о полиномиальных преобразованиях нескольких последовательностей.

**Предложение 2.** Пусть  $u_1, \dots, u_K$  — линейные рекурренты над кольцом  $R$  с характеристическими многочленами  $F_1(x), \dots, F_K(x) \in R[x]$ , соответственно, степеней  $m_1, \dots, m_K \geq 1$ ,  $\Phi(x_{1,1}, \dots, x_{1,s_1}, \dots, x_{K,1}, \dots, x_{K,s_K})$  — многочлен над кольцом  $R$ , где  $s_1, \dots, s_K \geq 0$ ,

$$v(i) = \Phi(u_1(i), \dots, u_1(i + s_1 - 1), \dots, u_K(i), \dots, u_K(i + s_K - 1)), \quad i \geq 0,$$

$D$  — множество векторов  $(d_1, \dots, d_K) \in \mathbb{N}_0^K$  таких, что в запись многочлена  $\Phi$  входит с ненулевым коэффициентом моном, сумма степеней которого по переменным  $x_{k,1}, \dots, x_{k,s_k}$  равна  $d_k$ ,  $k = 1, \dots, K$ ,  $F_{(d_1, \dots, d_K)}(x)$  — характеристический многочлен матрицы  $S(F_1)^{\otimes d_1} \otimes \dots \otimes S(F_K)^{\otimes d_K}$ .

Тогда многочлен

$$H(x) = \prod_{(d_1, \dots, d_K) \in D} F_{(d_1, \dots, d_K)}(x)$$

является характеристическим многочленом ЛРП  $v$ , и

$$\text{rank } v \leq \Phi^*(m_1, \dots, m_K), \quad (4)$$

где

$$\Phi^*(x_1, \dots, x_K) = \sum_{(d_1, \dots, d_K) \in D} x_1^{d_1} \dots x_K^{d_K} \in Z[x_1, \dots, x_K].$$

**Следствие 2.** Пусть в условиях предложения 2  $s_1 = \dots = s_K = 1$ , то есть  $v = \Phi(u_1, \dots, u_K)$ . Тогда

$$\text{rank } \Phi(u_1, \dots, u_K) \leq \Phi^*(m_1, \dots, m_K),$$

где  $\Phi^*(x_1, \dots, x_K)$  — многочлен над кольцом целых чисел, полученный из  $\Phi(x_1, \dots, x_K)$  заменой всех ненулевых коэффициентов на 1.

Оценки (3) и (4) универсальны: они верны для линейных рекуррент с любыми характеристическими многочленами над произвольным кольцом  $R$ . Однако для линейных рекуррент над конечными кольцами (на самом деле и для более широкого класса колец, см. замечания 1, 2 и 4) можно доказать более точные оценки. Это делается в следующих разделах.

Пусть кольцо  $R$  представляется в виде прямой суммы идеалов

$$R = R_1 \dot{+} \dots \dot{+} R_t,$$

и соответственно единица кольца  $R$  представляется в виде

$$e = e_1 + \dots + e_t, \quad e_j \in R_j, \quad j = 1, \dots, t.$$

Тогда  $R_j = e_j R$  — кольцо с единицей  $e_j$ ,  $j = 1, \dots, t$ , и каждый многочлен  $F(x) \in R[x]$  и каждая последовательность  $u \in R^\infty$  однозначно представляются в виде

$$\begin{aligned} F(x) &= F_1(x) + \dots + F_t(x), & F_j(x) &= e_j F(x) \in R_j[x], \\ u &= u_1 + \dots + u_t, & u_j &= e_j u \in R_j^\infty, \quad j = 1, \dots, t. \end{aligned}$$

При этом, если многочлен  $F(x)$  унитарен и является характеристическим многочленом ЛРП  $u$ , то каждый из многочленов  $F_j(x)$  унитарен в кольце  $R_j[x]$  и является характеристическим многочленом ЛРП  $u_j$  при  $j = 1, \dots, t$ . Обратно, если  $F_j(x) \in R_j[x]$  — характеристический многочлен ЛРП  $u_j$  при  $j = 1, \dots, t$ , то многочлен

$$F(x) = \sum_{j=1}^t x^{m-m_j} F_j(x), \quad m = \max\{m_1, \dots, m_t\}, \quad m_j = \deg F_j(x), \quad j = 1, \dots, t.$$

является характеристическим многочленом ЛРП  $u$ . При этом

$$\text{rank}_R u = \max\{\text{rank}_{R_1} u_1, \dots, \text{rank}_{R_t} u_t\}.$$

Таким образом, задача нахождения характеристического многочлена и ранга ЛРП  $u$  над кольцом  $R$  сводится к задаче нахождения характеристических многочленов и рангов последовательностей  $u_j$  над кольцом  $R_j$  при  $j = 1, \dots, t$ .

Поскольку, согласно [1, 5], каждое конечное (каждое артиново) кольцо  $R$  однозначно, с точностью до перестановки слагаемых, представляется в виде прямой суммы локальных конечных (артиновых) колец, то в дальнейшем мы будем предполагать, что кольцо  $R$  локально.

### 3. Необходимые сведения о конечных локальных кольцах и линейных рекуррентах

Всюду далее, если не оговорено противное,  $R$  — конечное локальное кольцо. Пусть  $J(R)$  — максимальный идеал кольца  $R$ , совпадающий с его радикалом Джекобсона,  $\bar{R} = R/J(R) = \text{GF}(q)$  — поле вычетов кольца  $R$ ,  $n = \text{ind } J(R)$  — индекс нильпотентности идеала  $J(R)$ , то есть наименьшее число  $n \geq 0$  такое, что  $J(R)^n = 0$ . Обозначим через  $\bar{a}$  образ элемента  $a \in R$  при действии естественного эпиморфизма  $R \rightarrow \bar{R}$ . Аналогично определяются образы  $\bar{F}(x)$ ,  $\bar{u}$  многочлена  $F(x) \in R[x]$  и последовательности  $u \in R^\infty$ .

Многочлены  $F(x), G(x) \in R[x]$  будем называть взаимно простыми (над кольцом  $R$ ) и писать

$$(F(x), G(x)) = e,$$

если

$$U(x)F(x) + V(x)G(x) = e$$

для некоторых  $U(x), V(x) \in R[x]$ .

**Предложение 3.** Если  $F(x), G_0(x), H_0(x)$  — унитарные многочлены над кольцом  $R$  такие, что  $\bar{F}(x) = \bar{G}_0(x)\bar{H}_0(x)$ ,  $(\bar{G}_0(x), \bar{H}_0(x)) = \bar{e}$ , то существует единственная пара унитарных многочленов  $G(x), H(x) \in R[x]$  таких, что

$$F(x) = G(x)H(x), \quad \bar{G}(x) = \bar{G}_0(x), \quad \bar{H}(x) = \bar{H}_0(x)$$

(лемма Гензеля);

$$(\bar{F}(x), \bar{G}(x)) = \bar{e} \Leftrightarrow (F(x), G(x)) = e.$$

Доказательство первого утверждения см. в [2, стр. 275], или в [5, стр. 323]. Второе утверждение доказано в [9, стр. 209].

Унитарный многочлен  $F(x) \in R[x]$  называется примарным, если  $\bar{F}(x) = \bar{G}(x)^k$ , где  $\bar{G}(x) \in \bar{R}[x]$  — неприводимый над полем  $\bar{R}$  многочлен,  $k \geq 1$ .

**Следствие 3.** Любой унитарный многочлен  $F(x) \in R[x]$  однозначно, с точностью до перестановки сомножителей, представляется в виде произведения примарных попарно взаимно простых многочленов:

$$F(x) = F_1(x) \dots F_T(x), \quad \bar{F}_t(x) = \bar{G}_t(x)^{a_t}, \quad a_t \geq 1, \quad t = 1, \dots, T, \quad (5)$$

где многочлен  $G_t(x) \in R[x]$  унитарен и  $\bar{G}_t(x)$  неприводим над полем  $\bar{R}$ .



Разложение (5) будем называть примарным каноническим разложением многочлена  $F(x)$ . При условии (5) положим

$$a(F) = a(\bar{F}) = \max\{a_1, \dots, a_T\}. \quad (6)$$

Многочлен  $F(x)$  будем называть сепарабельным, если многочлен  $\bar{F}(x)$  над полем  $\bar{R}$  сепарабелен, то есть не имеет кратных корней в поле разложения. Поскольку конечное поле  $\bar{R}$  является совершенным [3], это равносильно тому, что многочлен  $\bar{F}(x)$  не имеет кратных множителей в каноническом разложении над полем  $\bar{R}$ , то есть условию  $a(F) = 1$ .

Радикалом  $\text{rad } f(x)$  ненулевого многочлена  $f(x)$  над конечным (или совершенным) полем называется унитарный многочлен, равный произведению всех неприводимых многочленов, входящих в каноническое разложение многочлена  $f(x)$ . Радикал многочлена над конечным полем является сепарабельным многочленом и вычисляется по формуле  $\text{rad } f(x) = f(x)/(f(x), f'(x))$ .

**Определение 1.** Радикалом  $\text{rad } F(x)$  унитарного многочлена  $F(x)$  над кольцом  $R$  будем называть сам многочлен  $F(x)$ , если  $F(x)$  сепарабелен, или произвольный унитарный многочлен  $G(x) \in R[x]$  такой, что  $\bar{G}(x) = \text{rad } \bar{F}(x)$ , если  $F(x)$  не сепарабелен.

Радикал  $G(x) = \text{rad } F(x)$  многочлена  $F(x)$  над кольцом  $R$  является сепарабельным многочленом, удовлетворяющим условию  $\bar{G}(x) \mid \bar{F}(x)$ , однако не всегда  $G(x) \mid F(x)$ . В связи с этим полезным оказывается следующий результат.

**Предложение 4.** Пусть  $F(x), G(x) \in R[x]$ ,  $\bar{G}(x) \mid \bar{F}(x)$ . Тогда  $G(x) \mid F(x)^n$ , где  $n = \text{ind } J(R)$ .

В частности,  $\text{rad } F(x) \mid F(x)^n$  и  $F(x) \mid (\text{rad } F)^{na(F)}$ .

*Доказательство.* Пусть  $\bar{F}(x) = \bar{G}(x)\bar{Q}(x)$ . Тогда

$$F(x) = G(x)Q(x) + \Delta(x),$$

где  $\Delta(x) \in J(R)[x]$ ,  $\Delta(x)^n = 0$ . Следовательно,

$$F^n = (GQ + \Delta)^n = \sum_{i=0}^n \binom{n}{i} (GQ)^i \Delta^{n-i} = \sum_{i=1}^n \binom{n}{i} (GQ)^i \Delta^{n-i},$$

откуда получаем, что  $G(x) \mid F(x)^n$ . Последние два соотношения теперь следуют из того, что  $(\text{rad } F) = \text{rad } \bar{F} \mid \bar{F}$  и  $\bar{F} \mid (\text{rad } \bar{F})^{a(F)}$ .

Унитарный многочлен  $F(x) \in R[x]$  называется абсолютно неприводимым или многочленом Галуа, если  $\bar{F}(x)$  — неприводимый многочлен над полем  $\bar{R}$ . Пусть  $F(x)$  — многочлен Галуа степени  $m$  над  $R$ . Тогда факторкольцо  $S = R[x]/F(x)$  является локальным конечным кольцом. Можно считать, что  $R \subseteq S$ . Тогда  $S$  называется расширением Галуа степени  $m$  кольца  $R$ . Кольцо  $S$ , полученное конечным числом таких расширений, также будем называть расширением Галуа кольца  $R$ , а его степень  $m$  считать равной степени  $[\bar{S} : \bar{R}]$  расширения поля  $\bar{S} = S/J(S)$  над  $\bar{R}$ . Кольцо  $S$  является свободным  $R$ -модулем ранга  $m$ , в частности,  $|S| = |R|^m$ . Справедливы соотношения  $J(S) = J(R)S$ ,  $\text{ind } J(S) = \text{ind } J(R)$ ,  $\bar{S} = \text{GF}(q^m)$ .

Пусть  $F(x) \in R[x]$  — унитарный многочлен с каноническим разложением (5),  $G(x) = \text{rad } F(x)$ ,  $S$  — расширение Галуа кольца  $R$  степени  $[\text{deg } G_1, \dots, \text{deg } G_T]$ . Тогда

многочлены  $\bar{G}_1(x), \dots, \bar{G}_T(x)$  и, следовательно, многочлен  $\bar{G}(x) = \bar{G}_1(x) \dots \bar{G}_T(x)$ , раскладываются на линейные множители над полем  $\bar{S}$ . Так как многочлен  $G(x)$  сепарабелен, по лемме Гензеля он однозначно раскладывается в произведение линейных множителей над  $S$ :

$$G(x) = (x - \vartheta_1) \dots (x - \vartheta_m), \quad \vartheta_1, \dots, \vartheta_m \in S, \quad m = \deg G(x). \quad (7)$$

Напомним, что биномиальной последовательностью над кольцом  $S$  порядка  $l \geq 0$  с корнем  $\vartheta \in S$  называется последовательность  $\vartheta^{[l]} \in S^\infty$ , определяемая соотношениями

$$(\vartheta^{[l]}(0), \dots, \vartheta^{[l]}(l)) = (0, \dots, 0, e), \quad \vartheta^{[l]}(i) = \binom{i}{l} \vartheta^{i-l}, \quad i > l. \quad (8)$$

Мы кратко пишем  $\vartheta^{[l]}(i) = \binom{i}{l} \vartheta^{i-l}$  при всех  $i \geq 0$ , полагая, что если  $\binom{i}{l} = 0$ , то и  $\binom{i}{l} \vartheta^{i-l} = 0$  независимо от того, определена ли степень  $\vartheta^{i-l}$ . Последовательность  $\vartheta^{[l]}$  имеет минимальный многочлен  $(x - \vartheta)^{l+1}$  и является импульсной последовательностью семейства  $L_S((x - \vartheta)^{l+1})$  (см. [19]).

**Предложение 5.** Пусть  $F(x) \in R[x]$  — унитарный многочлен,  $a = a(F)$ ,  $G(x) = \text{rad } F(x)$ ,  $m = \deg G(x)$  и над некоторым расширением Галуа  $S$  кольца  $R$  выполняется соотношение (7). Тогда произвольная ЛРП  $u \in L_R(F)$  представляется в виде

$$u = \sum_{r=1}^m \sum_{l=0}^{an-1} c_{rl} \vartheta_r^{[l]}, \quad (9)$$

то есть

$$u(i) = \sum_{r=1}^m \sum_{l=0}^{an-1} c_{rl} \binom{i}{l} \vartheta_r^{i-l}, \quad i \geq 0,$$

где коэффициенты  $c_{rl} \in S$  определены однозначно,  $n = \text{ind } J(R)$ .

Если многочлен  $F(x)$  сепарабелен, то  $G(x) = F(x)$  и произвольная ЛРП  $u \in L_R(F)$  представляется в виде

$$u = \sum_{r=1}^m c_r \vartheta_r^{[0]}, \quad (10)$$

то есть

$$u(i) = \sum_{r=1}^m c_r \vartheta_r^i, \quad i \geq 0,$$

где коэффициенты  $c_r \in S$  определены однозначно.

**Доказательство.** В силу (7) и предложения 4

$$F(x) \mid G(x)^{an} = (x - \vartheta_1)^{an} \dots (x - \vartheta_m)^{an}.$$

Поэтому

$$u \in L_R(F) \subseteq L_S(F) \subseteq L_S((x - \vartheta_1)^{an} \dots (x - \vartheta_m)^{an}).$$

Так как элементы  $\bar{\vartheta}_1, \dots, \bar{\vartheta}_m$  в (7) попарно различны, ввиду предложения 3 многочлены  $(x - \vartheta_1)^{an}, \dots, (x - \vartheta_m)^{an}$  попарно взаимно просты. Следовательно, в силу предложения 6(a) из [9]

$$L_S((x - \vartheta_1)^{an} \dots (x - \vartheta_m)^{an}) = L_S((x - \vartheta_1)^{an}) \dot{+} \dots \dot{+} L_S((x - \vartheta_m)^{an}).$$

Биномиальные последовательности  $\vartheta^{[0]}, \dots, \vartheta^{[an-1]}$  принадлежат  $L_S((x - \vartheta)^{an})$  и, как следует непосредственно из (8), образуют базис этого семейства как модуля над  $S$ . Отсюда вытекает существование и единственность представления (9) ЛРП  $u$ .

Если  $F(x)$  сепарабелен, то  $G(x) = F(x)$  и

$$u \in L_R(F) \subseteq L_S(F) = L_S(x - \vartheta_1) \dot{+} \dots \dot{+} L_S(x - \vartheta_m).$$

Отсюда вытекает существование и единственность представления (10).

Соотношения (9), (10) будем называть биномиальным представлением ЛРП  $u$ .

В дальнейшем нам потребуется следующая лемма.

**Лемма 1.** Пусть  $\vartheta_1, \dots, \vartheta_k \in R$ ,  $l_1, \dots, l_k \geq 0$ ,  $i_1, \dots, i_k \geq 0$ ,  $k \geq 1$ . Тогда последовательность

$$z(i) = \vartheta_1^{[l_1]}(i + i_1) \dots \vartheta_k^{[l_k]}(i + i_k), \quad i \geq 0,$$

аннулируется многочленом  $(x - \vartheta_1 \dots \vartheta_k)^{l_1 + \dots + l_k + 1}$ .

*Доказательство.* Будем считать, что  $\vartheta^{[l]} = 0$  при  $l < 0$ . Нетрудно видеть, что

$$\begin{aligned} ((x - \vartheta_1 \dots \vartheta_k)z)(i) &= z(i + 1) - \vartheta_1 \dots \vartheta_k z(i) \\ &= \prod_{s=1}^k \binom{i + i_s + 1}{l_s} \vartheta_s^{i + i_s + 1 - l_s} - \vartheta_1 \dots \vartheta_k \prod_{s=1}^k \binom{i + i_s}{l_s} \vartheta_s^{i + i_s - l_s} \\ &= \prod_{s=1}^k \left( \binom{i + i_s}{l_s} + \binom{i + i_s}{l_s - 1} \right) \vartheta_s^{i + i_s + 1 - l_s} - \prod_{s=1}^k \binom{i + i_s}{l_s} \vartheta_s^{i + i_s + 1 - l_s} \\ &= \sum_A \binom{i + i_1}{l_1 - \alpha_1} \dots \binom{i + i_k}{l_k - \alpha_k} \vartheta_1^{i + i_1 + 1 - l_1} \dots \vartheta_k^{i + i_k + 1 - l_k} \\ &= \sum_A \vartheta_1^{1 - \alpha_1} \dots \vartheta_k^{1 - \alpha_k} \vartheta_1^{[l_1 - \alpha_1]}(i + i_1) \dots \vartheta_k^{[l_k - \alpha_k]}(i + i_k), \end{aligned}$$

где суммирование в двух последних суммах проводится по множеству

$$A = \{\alpha_1, \dots, \alpha_k \in \{0, 1\} : (\alpha_1, \dots, \alpha_k) \neq (0, \dots, 0)\}.$$

Таким образом, последовательность  $(x - \vartheta_1 \dots \vartheta_k)z$  есть линейная комбинация последовательностей

$$\vartheta_1^{[t_1]}(i + i_1) \dots \vartheta_k^{[t_k]}(i + i_k)$$

таких, что

$$t_1 + \dots + t_k = l_1 - \alpha_1 + \dots + l_k - \alpha_k \leq l_1 + \dots + l_k - 1,$$

где  $t_1, \dots, t_k \in \mathbb{Z}$ . Индукцией по  $l$  доказывается, что последовательность  $(x - \vartheta_1 \dots \vartheta_k)^l z$  есть линейная комбинация последовательностей

$$\vartheta_1^{[t_1]}(i + i_1) \dots \vartheta_k^{[t_k]}(i + i_k), \quad t_1 + \dots + t_k \leq l_1 + \dots + l_k - l, \quad t_1, \dots, t_k \in \mathbb{Z}.$$

При  $l = l_1 + \dots + l_k + 1$  получим, что  $t_1 + \dots + t_k \leq -1$ , поэтому

$$\vartheta_1^{[t_1]}(i + i_1) \dots \vartheta_k^{[t_k]}(i + i_k) = 0$$

при всех наборах  $t_1, \dots, t_k$  и, следовательно,  $(x - \vartheta_1 \dots \vartheta_k)^l z = 0$ .

#### 4. Верхние оценки ранга

Пусть  $u$  — ЛРП над конечным локальным кольцом  $R$  с характеристическим многочленом  $F(x) \in R[x]$ , имеющим примарное каноническое разложение (5). Пусть

$$a = a(F), \quad G(x) = \text{rad } F(x), \quad m = \deg G(x),$$

и  $S$  — расширение Галуа кольца  $R$ , над которым многочлен  $G(x)$  имеет разложение (7) на линейные множители.

При  $d \geq 0$  пусть

$$G^{(d)}(x) = \prod (x - \vartheta_{i_1} \dots \vartheta_{i_d}), \quad (11)$$

где произведение берется по всем различным элементам

$$\vartheta_{i_1} \dots \vartheta_{i_d}, \quad 1 \leq i_1 \leq \dots \leq i_d \leq m,$$

кольца  $S$ . В частности,

$$G^{(0)}(x) = x - e, \quad G^{(1)}(x) = G(x).$$

Так как многочлен  $G^{(d)}(x)$  не изменится при произвольной перестановке элементов  $\vartheta_1, \dots, \vartheta_m$ , коэффициенты многочлена  $G^{(d)}(x)$  являются симметрическими функциями элементов  $\vartheta_1, \dots, \vartheta_m$ . По основной теореме о симметрических многочленах коэффициенты многочлена  $G^{(d)}(x)$  полиномиально выражаются через элементарные симметрические многочлены от  $\vartheta_1, \dots, \vartheta_m$ , то есть, ввиду (7), через коэффициенты многочлена  $G(x)$ . Следовательно,  $G^{(d)}(x) \in R[x]$ . Многочлен  $G^{(d)}(x)$  также можно записать в виде

$$G^{(d)}(x) = \prod (x - \vartheta_1^{j_1} \dots \vartheta_m^{j_m}), \quad (12)$$

где произведение берется по всем различным элементам

$$\vartheta_1^{j_1} \dots \vartheta_m^{j_m}, \quad j_1 + \dots + j_m = d, \quad j_1, \dots, j_m \geq 0,$$

кольца  $S$ . Степень многочлена  $G^{(d)}(x)$  не превосходит числа решений уравнения  $j_1 + \dots + j_m = d$  в целых неотрицательных числах  $j_1, \dots, j_m$ . Следовательно,

$$\deg G^{(d)}(x) \leq \binom{m + d - 1}{d}, \quad d \geq 0. \quad (13)$$

**Предложение 6.** Для фиксированных  $i_1, \dots, i_d \geq 0$ ,  $d \geq 1$  пусть

$$w(i) = u(i + i_1) \dots u(i + i_d), \quad i \geq 0.$$

Тогда многочлен  $G^{(d)}(x)^{(an-1)d+1}$  является характеристическим многочленом ЛРП  $w, u$

$$\text{rank } w \leq \binom{m+d-1}{d} ((an-1)d+1).$$

Если многочлен  $F(x)$  сепарабелен, то  $G(x) = F(x)$ ,  $m = \deg F(x)$ , многочлен  $G^{(d)}(x)$  является характеристическим многочленом ЛРП  $w, u$

$$\text{rank } w \leq \binom{m+d-1}{d}.$$

*Доказательство.* По предложению 5 ЛРП  $u$  имеет биномиальное представление (9). Тогда

$$\begin{aligned} w(i) &= u(i+i_1) \dots u(i+i_d) = \prod_{j=1}^d \left( \sum_{r=1}^m \sum_{l=0}^{an-1} c_{rl} \vartheta_r^{[l]}(i+i_j) \right) \\ &= \sum_{A(m,d)} c_{r_1, l_1} \dots c_{r_d, l_d} \vartheta_{r_1}^{[l_1]}(i+i_1) \dots \vartheta_{r_d}^{[l_d]}(i+i_d), \quad i \geq 0, \end{aligned} \quad (14)$$

где суммирование в последней сумме проводится по множеству

$$A(m, d) = \{(r_j, l_j) : 1 \leq r_j \leq m, 0 \leq l_j \leq an-1, j = 1, \dots, d\}.$$

По лемме 1 последовательность

$$z(i) = \vartheta_{r_1}^{[l_1]}(i+i_1) \dots \vartheta_{r_d}^{[l_d]}(i+i_d), \quad i \geq 0,$$

аннулируется многочленом  $(x - \vartheta_{r_1} \dots \vartheta_{r_d})^{l_1 + \dots + l_d + 1}$ . Так как  $0 \leq l_j \leq an-1$  при  $j = 1, \dots, d$ , то

$$l_1 + \dots + l_d + 1 \leq (an-1)d + 1,$$

и указанный многочлен делит  $G^{(d)}(x)^{(an-1)d+1}$  в силу определения (11). Поэтому последовательность  $z$  аннулируется многочленом  $G^{(d)}(x)^{(an-1)d+1}$ . Теперь из (14) следует, что и ЛРП  $w$  аннулируется многочленом  $G^{(d)}(x)^{(an-1)d+1}$ . Оценка ранга ЛРП  $w$  следует из (13).

Если многочлен  $F(x)$  сепарабелен, то ЛРП  $u$  имеет биномиальное представление (10) и

$$\begin{aligned} w(i) &= u(i+i_1) \dots u(i+i_d) = \prod_{j=1}^d \left( \sum_{r=1}^m c_r \vartheta_r^{i+i_j} \right) \\ &= \sum_{1 \leq r_1, \dots, r_d \leq m} c_{r_1} \dots c_{r_d} \vartheta_{r_1}^{i_1} \dots \vartheta_{r_d}^{i_d} (\vartheta_{r_1} \dots \vartheta_{r_d})^i, \quad i \geq 0. \end{aligned}$$

Так как каждая последовательность  $(\vartheta_{r_1} \dots \vartheta_{r_d})^i$ ,  $i \geq 0$ , аннулируется многочленом  $G^{(d)}(x)$ , то и последовательность  $w$  аннулируется многочленом  $G^{(d)}(x)$ .

**Теорема 2.** Пусть  $u$  — ЛРП над кольцом  $R$  с характеристическим многочленом  $F(x) \in R[x]$  степени  $m \geq 1$ ,  $n = \text{ind } J(R)$ ,  $a = a(F)$ ,  $G(x) = \text{rad } F(x)$ ,  $m = \deg G(x)$ ,  $\Phi(x_1, \dots, x_s) \in R[x_1, \dots, x_s]$ ,  $r = \deg \Phi$ ,

$$v(i) = \Phi(u(i), \dots, u(i+s-1)), \quad i \geq 0,$$

$D$  — множество чисел  $d \geq 0$  таких, что в запись многочлена  $\Phi$  входит с ненулевым коэффициентом моном степени  $d$ . Тогда многочлен

$$H(x) = \prod_{d \in D} G^{(d)}(x)^{(an-1)d+1}$$

является характеристическим многочленом ЛРП  $v$ , и

$$\text{rank } v \leq \sum_{d \in D} \binom{m+d-1}{d} ((an-1)d+1) \leq \binom{m+r}{r} ((an-1)r+1). \quad (15)$$

Если многочлен  $F(x)$  сепарабелен, то  $G(x) = F(x)$ ,  $m = \deg F(x)$ , многочлен

$$H_1(x) = \prod_{d \in D} G^{(d)}(x)$$

является характеристическим многочленом ЛРП  $v$ , и

$$\text{rank } v \leq \sum_{d \in D} \binom{m+d-1}{d} \leq \binom{m+r}{r}. \quad (16)$$

*Доказательство.* Последовательность  $v$  есть линейная комбинация последовательностей

$$w(i) = u(i+i_1) \dots u(i+i_d), \quad 0 \leq i_1, \dots, i_d \leq s-1, \quad d \in D,$$

с некоторыми коэффициентами, равными коэффициентам многочлена  $\Phi$  (при  $d=0$  получаем последовательность-константу  $\Phi(0, \dots, 0)$ ). Ввиду предложения 6 последовательность  $w$  аннулируется многочленом  $G^{(d)}(x)^{(an-1)d+1}$  (или  $G^{(d)}(x)$ , если  $F(x)$  сепарабелен). Следовательно, последовательность  $v$  аннулируется многочленом  $H(x)$  (многочленом  $H_1(x)$ , если  $F(x)$  сепарабелен). Оценки ранга следуют из (13) и соотношения (см., например, [10])

$$\sum_{d=0}^r \binom{m+d-1}{d} = \binom{m+r}{r}. \quad (17)$$

Отметим, что если многочлен  $F(x)$  сепарабелен, то оценка (16) является более точной, чем (3), поскольку  $\binom{m+d-1}{d} \leq m^d$ . Если многочлен  $F(x)$  не сепарабелен, то более точной может оказаться как оценка (3), так и оценка (15). Например, если  $\Phi(x) = x^d$  и в разложении (7)  $a_1 = \dots = a_T = a$ , то  $\deg F(x) = am$ , и правые части оценок (3), (15) имеют вид

$$(am)^d, \quad \binom{m+d-1}{d} ((an-1)d+1).$$

Какая из оценок лучше, зависит от параметров  $a$ ,  $m$ ,  $n$  и  $d$ .

Рассмотрим теперь полиномиальные преобразования нескольких последовательностей. Пусть  $F_1(x), \dots, F_K(x)$  — унитарные многочлены над кольцом  $R$ , имеющие примарные канонические разложения

$$\begin{aligned} F_k(x) &= F_{k,1}(x) \dots F_{k,T_k}(x), \\ \bar{F}_{kt}(x) &= \bar{G}_{kt}(x)^{a_{kt}}, \quad a_{kt} \geq 1, \quad t = 1, \dots, T_k, \quad k = 1, \dots, K. \end{aligned} \quad (18)$$

Введем обозначения

$$G_k(x) = \text{rad } F_k(x), \quad G(x) = \text{rad } G_1(x) \dots G_K(x) = \text{rad } F_1(x) \dots F_K(x), \quad m = \deg G(x).$$

Многочлен  $G(x)$  является сепарабельным. Пусть  $S$  — расширение Галуа кольца  $R$ , над которым многочлен  $G(x)$  раскладывается (однозначно) на линейные множители. Пусть это разложение имеет вид (7), и  $G^{(d)}(x)$  — многочлен, определенный в (11).

**Теорема 3.** Пусть  $u_1, \dots, u_K$  — линейные рекурренты над кольцом  $R$  с характеристическими многочленами  $F_1(x), \dots, F_K(x) \in R[x]$ ,

$$\Phi(x_{1,1}, \dots, x_{1,s_1}, \dots, x_{K,1}, \dots, x_{K,s_K})$$

— многочлен над кольцом  $R$ ,  $s_1, \dots, s_K \geq 0$ ,  $r = \deg \Phi$ ,

$$v(i) = \Phi(u_1(i), \dots, u_1(i + s_1 - 1), \dots, u_K(i), \dots, u_K(i + s_K - 1)), \quad i \geq 0,$$

$D$  — множество чисел  $d \geq 0$  таких, что в запись многочлена  $\Phi$  входит с ненулевым коэффициентом моном степени  $d$ .

Тогда многочлен

$$H(x) = \prod_{d \in D} G^{(d)}(x)^{(an-1)d+1},$$

где  $a = \max\{a(F_1), \dots, a(F_K)\}$ ,  $n = \text{ind } J(R)$ , является характеристическим многочленом ЛРП  $v$ , и

$$\text{rank } v \leq \sum_{d \in D} \binom{m+d-1}{d} ((an-1)d+1) \leq \binom{m+r}{r} ((an-1)r+1). \quad (19)$$

Если многочлены  $F_1(x), \dots, F_K(x)$  сепарабельны и попарно взаимно просты, то

$$G(x) = F_1(x) \dots F_K(x), \quad m = \deg F_1 + \dots + \deg F_K,$$

многочлен

$$H_1(x) = \prod_{d \in D} G^{(d)}(x)$$

является характеристическим многочленом ЛРП  $v$ , и

$$\text{rank } v \leq \sum_{d \in D} \binom{m+d-1}{d} \leq \binom{m+r}{r}. \quad (20)$$

**Доказательство.** Последовательность  $v$  есть линейная комбинация последовательностей

$$w(i) = u_{k_1}(i + i_1) \dots u_{k_d}(i + i_d), \quad i \geq 0,$$

где  $d \in D$ ,  $1 \leq k_1, \dots, k_d \leq K$ ,  $i_1, \dots, i_d \geq 0$ , с некоторыми коэффициентами, равными коэффициентам многочлена  $\Phi$ . Так как  $\bar{F}_k(x) \mid \bar{G}_k(x)^a$  и  $\bar{G}_k(x) \mid \bar{G}(x)$ , по предложению 4  $F_k(x) \mid G(x)^{an}$ ,  $k = 1, \dots, K$ . Из доказательства предложения 5 следует, что ЛРП  $u_k$  представляется в виде

$$u_k = \sum_{r=1}^m \sum_{l=0}^{an-1} c_{krl} \vartheta_r^{[l]}, \quad c_{krl} \in S, \quad k = 1, \dots, K. \quad (21)$$

Так же, как в предложении 6, доказываем, что ЛРП  $w$  аннулируется многочленом  $G^{(d)}(x)^{(an-1)d+1}$ . Отсюда вытекает, что последовательность  $v$  аннулируется многочленом  $H(x)$ .

Случай, когда многочлены  $F_1(x), \dots, F_K(x)$  сепарабельны и попарно взаимно просты, рассматривается аналогично.

Докажем еще одну, как правило более точную, верхнюю оценку ранга ЛРП  $v$ . Над кольцом  $S$  многочлены  $G_k(x)$  однозначно представляются в виде

$$G_k(x) = (x - \vartheta_{k,1}) \dots (x - \vartheta_{k,m_k}), \quad m_k = \deg G_k(x), \quad k = 1, \dots, K.$$

При  $d_1, \dots, d_K \geq 0$  введем обозначение

$$G^{(d_1, \dots, d_K)}(x) = \prod (x - \vartheta_{1,i_{11}} \dots \vartheta_{1,i_{1d_1}} \dots \vartheta_{K,i_{K1}} \dots \vartheta_{K,i_{Kd_K}}), \quad (22)$$

где произведение берется по всем различным элементам

$$\vartheta_{1,i_{11}} \dots \vartheta_{1,i_{1d_1}} \dots \vartheta_{K,i_{K1}} \dots \vartheta_{K,i_{Kd_K}}, \quad i_{kr} \geq 0, \quad r = 1, \dots, d_k, \quad k = 1, \dots, K, \quad (23)$$

кольца  $S$ . Многочлен  $G^{(d_1, \dots, d_K)}(x)$  можно также записать в виде

$$G^{(d_1, \dots, d_K)}(x) = \prod \left( x - \vartheta_{1,1}^{j_{1,1}} \dots \vartheta_{1,m_1}^{j_{1,m_1}} \dots \vartheta_{K,1}^{j_{K,1}} \dots \vartheta_{K,m_K}^{j_{K,m_K}} \right), \quad (24)$$

где произведение берется по всем различным элементам

$$\vartheta_{1,1}^{j_{1,1}} \dots \vartheta_{1,m_1}^{j_{1,m_1}} \dots \vartheta_{K,1}^{j_{K,1}} \dots \vartheta_{K,m_K}^{j_{K,m_K}}, \quad (25)$$

$$j_{k,1} + \dots + j_{k,m_k} = d_k, \quad j_{k,r} \geq 0, \quad r = 1, \dots, m_k, \quad k = 1, \dots, K,$$

кольца  $S$ . Аналогично (13) отсюда следует, что

$$\deg G^{(d_1, \dots, d_K)}(x) \leq \binom{m_1 + d_1 - 1}{d_1} \dots \binom{m_K + d_K - 1}{d_K}, \quad d_1, \dots, d_K \geq 0. \quad (26)$$

Доказательство того, что  $G^{(d_1, \dots, d_K)}(x) \in R[x]$ , основывается на следующем утверждении.

**Предложение 7.** Пусть  $f(x_{1,1}, \dots, x_{1,m_1}, \dots, x_{K,1}, \dots, x_{K,m_K})$  — многочлен над коммутативным кольцом  $R$  с единицей, не меняющийся при произвольной перестановке переменных внутри каждого из векторов  $(x_{k,1}, \dots, x_{k,m_k})$ ,  $k = 1, \dots, K$ .

Тогда  $f$  полиномиально выражается через элементарные симметрические многочлены

$$\sigma_i(x_{k,1}, \dots, x_{k,m_k}), \quad i = 1, \dots, m_k, \quad k = 1, \dots, K.$$

*Доказательство.* Проведем индукцию по  $K$ . При  $K = 1$  утверждение совпадает с основной теоремой о симметрических многочленах. Проведем шаг индукции. Пусть

$$f = f(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_K),$$

где  $\mathbf{x}_k = (x_{k,1}, \dots, x_{k,m_k})$ ,  $k = 1, \dots, K$ . Рассмотрим кольцо  $S = R[\mathbf{x}_2, \dots, \mathbf{x}_K]$ . Тогда  $f \in S[\mathbf{x}_1]$  — симметрический многочлен. По основной теореме о симметрических многочленах существует единственный многочлен  $a(\mathbf{x}_1) \in S[\mathbf{x}_1]$  такой, что

$$f(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_K) = a(\sigma_1(\mathbf{x}_1), \dots, \sigma_{m_1}(\mathbf{x}_1)).$$



Записывая  $a(\mathbf{x}_1)$  как многочлен  $A(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_K)$  над кольцом  $R$ , получим, что

$$f(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_K) = A(\sigma_1(\mathbf{x}_1), \dots, \sigma_{m_1}(\mathbf{x}_1), \mathbf{x}_2, \dots, \mathbf{x}_K).$$

Из последнего равенства следует, что многочлен  $A(\sigma_1(\mathbf{x}_1), \dots, \sigma_{m_1}(\mathbf{x}_1), \mathbf{x}_2, \dots, \mathbf{x}_K)$  не меняется при перестановке переменных внутри каждого из векторов  $\mathbf{x}_2, \dots, \mathbf{x}_K$ . Докажем, что и многочлен  $A(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_K)$  обладает этим свойством. Действительно, в противном случае существуют перестановки  $\mathbf{x}'_2, \dots, \mathbf{x}'_K$  переменных такие, что

$$A(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_K)$$

и

$$A'(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_K) = A(\mathbf{x}_1, \mathbf{x}'_2, \dots, \mathbf{x}'_K)$$

— различные многочлены. Рассмотрим их как многочлены  $a(\mathbf{x}_1)$  и  $a'(\mathbf{x}_1)$  над кольцом  $S$ . Тогда  $a(\mathbf{x}_1) \neq a'(\mathbf{x}_1)$ , но

$$a(\sigma_1(\mathbf{x}_1), \dots, \sigma_{m_1}(\mathbf{x}_1)) = a'(\sigma_1(\mathbf{x}_1), \dots, \sigma_{m_1}(\mathbf{x}_1)),$$

что противоречит утверждению о единственности в основной теореме о симметрических многочленах.

Рассмотрим кольцо  $Q = R[\mathbf{x}_1]$ . Тогда  $A$  есть многочлен над кольцом  $Q$  от переменных  $\mathbf{x}_2, \dots, \mathbf{x}_K$ . По доказанному этот многочлен удовлетворяет предположению индукции. Поэтому существует многочлен  $b(\mathbf{x}_2, \dots, \mathbf{x}_K)$  над кольцом  $Q$  такой, что

$$A(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_K) = b(\sigma_1(\mathbf{x}_2), \dots, \sigma_{m_2}(\mathbf{x}_2), \dots, \sigma_K(\mathbf{x}_K), \dots, \sigma_{m_K}(\mathbf{x}_K)).$$

Записывая  $b(\mathbf{x}_2, \dots, \mathbf{x}_K)$  как многочлен  $B(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_K)$  над кольцом  $R$ , получим, что

$$A(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_K) = B(\mathbf{x}_1, \sigma_1(\mathbf{x}_2), \dots, \sigma_{m_2}(\mathbf{x}_2), \dots, \sigma_K(\mathbf{x}_K), \dots, \sigma_{m_K}(\mathbf{x}_K)).$$

Следовательно,

$$\begin{aligned} f(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_K) &= A(\sigma_1(\mathbf{x}_1), \dots, \sigma_{m_1}(\mathbf{x}_1), \mathbf{x}_2, \dots, \mathbf{x}_K) \\ &= B(\sigma_1(\mathbf{x}_1), \dots, \sigma_{m_1}(\mathbf{x}_1), \sigma_1(\mathbf{x}_2), \dots, \sigma_{m_2}(\mathbf{x}_2), \dots, \sigma_K(\mathbf{x}_K), \dots, \sigma_{m_K}(\mathbf{x}_K)). \end{aligned}$$

Теперь заметим, что для любого  $k = 1, \dots, K$  многочлен  $G^{(d_1, \dots, d_K)}(x)$  не изменится при произвольной перестановке набора элементов  $\vartheta_{k,1}, \dots, \vartheta_{k,m_k}$ . В силу предложения 7 коэффициенты многочлена  $G^{(d_1, \dots, d_K)}(x)$  полиномиально выражаются через элементарные симметрические многочлены от  $K$  указанных наборов элементов, то есть через коэффициенты многочленов  $G_1(x), \dots, G_K(x)$ . Следовательно,  $G^{(d_1, \dots, d_K)}(x) \in R[x]$ .

**Предложение 8.** Пусть  $u_k \in L_R(F_k)$ ,  $a_k = a(F_k)$ ,  $d_k \geq 0$ ,  $k = 1, \dots, K$ . Тогда многочлен  $G^{(d_1, \dots, d_K)}(x)^A$ , где

$$A = \sum_{k=1}^K ((a_k n - 1)d_k + 1),$$

является характеристическим многочленом последовательности

$$w(i) = u_1(i + i_{1,1}) \dots u_1(i + i_{1,d_1}) \dots u_K(i + i_{K,1}) \dots u_K(i + i_{K,d_K}), \quad i \geq 0,$$

$u$

$$\text{rank } w \leq \binom{m_1 + d_1 - 1}{d_1} \cdots \binom{m_K + d_K - 1}{d_K} \sum_{k=1}^K ((a_k n - 1)d_k + 1).$$

Если многочлены  $F_1(x), \dots, F_K(x)$  сепарабельны, то многочлен  $G^{(d_1, \dots, d_K)}(x)$  является характеристическим многочленом последовательности  $w, u$

$$\text{rank } w \leq \binom{m_1 + d_1 - 1}{d_1} \cdots \binom{m_K + d_K - 1}{d_K}.$$

**Доказательство.** По предложению 5 ЛРП  $u_k$  имеет биномиальное представление

$$u_k = \sum_{r=1}^{m_k} \sum_{l=0}^{a_k n - 1} c_{krl} \vartheta_{kr}^{[l]}, \quad c_{krl} \in S, \quad k = 1, \dots, K. \quad (27)$$

Тогда ЛРП  $w$  есть линейная комбинация последовательностей вида

$$\vartheta_{1,r_{11}}^{[l_{11}]}(i + i_{11}) \cdots \vartheta_{1,r_{1d_1}}^{[l_{1d_1}]}(i + i_{1d_1}) \cdots \vartheta_{K,r_{K1}}^{[l_{K1}]}(i + i_{K1}) \cdots \vartheta_{K,r_{Kd_K}}^{[l_{Kd_K}]}(i + i_{Kd_K}).$$

Здесь  $l_{kt} \leq a_k n - 1$  при  $1 \leq t \leq d_k, 1 \leq k \leq K$ , поэтому  $\sum_{k,t} l_{kt} \leq A - 1$ . По лемме 1 такая последовательность аннулируется многочленом

$$(x - \vartheta_{1,r_{11}} \cdots \vartheta_{1,r_{1d_1}} \cdots \vartheta_{K,r_{K1}} \cdots \vartheta_{K,r_{Kd_K}})^A,$$

а значит, и многочленом  $G^{(d_1, \dots, d_K)}(x)^A$ . Следовательно, ЛРП  $w$  аннулируется многочленом  $G^{(d_1, \dots, d_K)}(x)^A$ .

Если многочлены  $F_1(x), \dots, F_K(x)$  сепарабельны, то по предложению 5

$$u_k = \sum_{r=1}^{m_k} c_{kr} \vartheta_{kr}^{[0]}, \quad c_{kr} \in S, \quad k = 1, \dots, K. \quad (28)$$

Тогда ЛРП  $w$  есть линейная комбинация последовательностей вида

$$\vartheta_{1,r_{11}}^{[0]}(i + i_{11}) \cdots \vartheta_{1,r_{1d_1}}^{[0]}(i + i_{1d_1}) \cdots \vartheta_{K,r_{K1}}^{[0]}(i + i_{K1}) \cdots \vartheta_{K,r_{Kd_K}}^{[0]}(i + i_{Kd_K}).$$

По лемме 1 такая последовательность аннулируется многочленом

$$(x - \vartheta_{1,r_{11}} \cdots \vartheta_{1,r_{1d_1}} \cdots \vartheta_{K,r_{K1}} \cdots \vartheta_{K,r_{Kd_K}}),$$

а значит, и многочленом  $G^{(d_1, \dots, d_K)}(x)$ . Следовательно, ЛРП  $w$  аннулируется многочленом  $G^{(d_1, \dots, d_K)}(x)$ .

Указанные в формулировке оценки рангов вытекают из (26).

**Теорема 4.** Пусть  $u_1, \dots, u_K$  — линейные рекурренты над кольцом  $R$  с характеристическими многочленами  $F_1(x), \dots, F_K(x) \in R[x]$ ,  $a_k = a(F_k)$ ,  $n = \text{ind } J(R)$ ,

$$\Phi(x_{1,1}, \dots, x_{1,s_1}, \dots, x_{K,1}, \dots, x_{K,s_K})$$

— многочлен над кольцом  $R$ ,  $s_1, \dots, s_K \geq 0$ ,

$$v(i) = \Phi(u_1(i), \dots, u_1(i + s_1 - 1), \dots, u_K(i), \dots, u_K(i + s_K - 1)), \quad i \geq 0,$$

$D$  — множество векторов  $(d_1, \dots, d_K) \in \mathbb{N}_0^K$  таких, что в запись многочлена  $\Phi$  входит с ненулевым коэффициентом моном, сумма степеней которого по переменным  $x_{k,1}, \dots, x_{k,s_k}$  равна  $d_k$ ,  $k = 1, \dots, K$ .

Тогда многочлен

$$H(x) = \prod_{(d_1, \dots, d_K) \in D} G^{(d_1, \dots, d_K)}(x)^{\sum_{k=1}^K ((a_k n - 1)d_k + 1)}$$

является характеристическим многочленом ЛРП  $v$ , и

$$\text{rank } v \leq \sum_{(d_1, \dots, d_K) \in D} \binom{m_1 + d_1 - 1}{d_1} \dots \binom{m_K + d_K - 1}{d_K} \sum_{k=1}^K ((a_k n - 1)d_k + 1). \quad (29)$$

Если многочлены  $F_1(x), \dots, F_K(x)$  сепарабельны, то многочлен

$$H_1(x) = \prod_{(d_1, \dots, d_K) \in D} G^{(d_1, \dots, d_K)}(x)$$

является характеристическим многочленом ЛРП  $v$ , и

$$\text{rank } v \leq \sum_{(d_1, \dots, d_K) \in D} \binom{m_1 + d_1 - 1}{d_1} \dots \binom{m_K + d_K - 1}{d_K}. \quad (30)$$

Теорема вытекает из предложения 8.

Отметим, что если многочлены  $F_1(x), \dots, F_K(x)$  сепарабельны и попарно взаимно просты, то оценка (30) сильнее оценки (20). Действительно, достаточно заметить, что в этом случае  $m = m_1 + \dots + m_K$  и справедливо тождество

$$\sum_{d_1 + \dots + d_K = d} \binom{m_1 + d_1 - 1}{d_1} \dots \binom{m_K + d_K - 1}{d_K} = \binom{m + d - 1}{d}.$$

Для его доказательства достаточно приравнять коэффициенты при  $x^d$  в равенстве

$$(1-x)^{-m_1} \dots (1-x)^{-m_K} = (1-x)^{-m}.$$

Кроме того, оценка (30) сильнее оценки (4), поскольку

$$\binom{m_k + d_k - 1}{d_k} \leq m_k^{d_k}, \quad k = 1, \dots, K.$$

Однако, в общем случае из оценок (4), (19), (29) любая может оказаться более сильной. Например, если

$$F_1(x) = \dots = F_K(x) = G(x)^a, \quad \Phi(x_1, \dots, x_k) = x_1 \dots x_k,$$

то

$$\deg G(x) = m = m_1 = \dots = m_K, \quad \deg F(x) = am$$

и правые части оценок (4), (19) и (29) имеют вид

$$(am)^K, \quad \binom{m + K - 1}{K} ((an - 1)K + 1), \quad m^K$$

соответственно. Какая из оценок более точная, зависит от параметров  $a, m, n, K$ .

**Замечание 1.** Результаты разделов 3 и 4 верны и для некоторых бесконечных колец. Так, все результаты сохраняются, если  $R$  — локальное кольцо с нильпотентным радикалом и конечным полем вычетов. Примером такого кольца является  $R = P[x_1, x_2, \dots]/I$ , где  $P$  — конечное поле,  $I$  — идеал, порожденный всеми мономами степени  $n$ .

Результаты разделов 3 и 4 сохраняются также в случае, когда  $R$  — локальное кольцо с нильпотентным радикалом и совершенным полем вычетов. Единственное отличие заключается в том, что расширение Галуа  $S$  кольца  $R$ , над которым многочлен  $G(x) = \text{rad } F(x)$  имеет разложение (7) на линейные множители, не обязательно имеет степень  $[\text{deg } G_1, \dots, \text{deg } G_T]$ , как сказано выше в случае конечного поля вычетов  $\bar{R}$ .

Если  $R$  — локальное кольцо с нильпотентным радикалом и произвольным полем вычетов, то результаты разделов 3 и 4 сохраняются при условии, что неприводимые над полем  $\bar{R}$  многочлены  $\bar{G}_t(x)$  и  $\bar{G}_{kt}(x)$  в разложениях (5) и (18) сепарабельны, то есть не имеют кратных корней в поле разложения. В частности, полностью сохраняются результаты, сформулированные для случаев, когда многочлены  $F(x)$  и  $F_1(x), \dots, F_K(x)$  сепарабельны. Для перечисленных выше классов колец формулировки и доказательства остаются без изменений. Отметим также, что ввиду свойств, перечисленных в конце разделе 2, полученные результаты переносятся и на прямые суммы таких колец.

Если же  $R$  — локальное кольцо с нильпотентным радикалом и не совершенным полем вычетов, и хотя бы один из многочленов  $\bar{G}_t(x)$  (или  $\bar{G}_{kt}(x)$ ) в разложении (5) (или (18)) не сепарабелен, то требуется по-другому определять уже понятие радикала  $\text{rad } \bar{F}(x) = \bar{G}(x)$  многочлена  $\bar{F}(x)$  над полем  $\bar{R}$  и изменять определение многочлена  $G^{(d)}(x)$ . Здесь мы не исследуем этот случай.

## 5. Уточнение верхних оценок ранга

Пусть  $R$  — конечное локальное кольцо. В этом разделе при условии, что характеристический многочлен  $F(x)$  ЛРП  $u$  сепарабелен, мы приведем более точную оценку ранга ЛРП  $v = \Phi(u)$ . Аналогично при условии, что многочлены  $F_1(x), \dots, F_K(x)$  сепарабельны,  $u_k \in L_R(F_k)$ ,  $k = 1, \dots, K$ , мы укажем более точную оценку ранга ЛРП  $v = \Phi(u_1, \dots, u_K)$ . В следующем разделе будут даны достаточные условия, при которых эти оценки достигаются.

Пусть  $F(x) \in R[x]$  — унитарный сепарабельный многочлен степени  $m \geq 1$ ,  $S$  — расширение Галуа кольца  $R$ , над которым многочлен  $F(x)$  (однозначно) раскладывается на линейные множители:

$$F(x) = (x - \vartheta_1) \dots (x - \vartheta_m), \quad \vartheta_1, \dots, \vartheta_m \in S. \quad (31)$$

Пусть  $\bar{R} = \text{GF}(q)$ ,  $q = p^l$ ,  $p$  — простое число. Наша ближайшая цель — определить многочлены  $F^{(d, \epsilon)}(x)$ , аналогичные многочленам  $G^{(d)}(x)$  из (11), но имеющие несколько меньшие степени (за счет чего получается более точная оценка ранга). Напомним, что если  $F(x)$  сепарабелен, то, в обозначениях раздела 4,  $F(x) = G(x)$  и  $G^{(d)}(x) = F^{(d)}(x)$ . Предварительно введем ряд обозначений.

Пусть целое неотрицательное число  $d$  имеет  $p$ -ичное разложение

$$d = \sum_{r \geq 0} \nu_r(d) p^r, \quad 0 \leq \nu_r(d) \leq p - 1, \quad r \geq 0.$$

Величину

$$w_p(d) = \sum_{r \geq 0} \nu_r(d)$$

назовем  $p$ -ичным весом числа  $d$ . Сумму  $d = d_1 + \dots + d_m$ ,  $d_j \geq 0$ , будем называть  $p$ -разложением и записывать в виде

$$d = d_1 + \dots + d_m,$$

если  $\nu_r(d_1) + \dots + \nu_r(d_m) = \nu_r(d)$  при всех  $r \geq 0$ , то есть, если при сложении чисел  $d_1, \dots, d_m$  в  $p$ -ичной системе счисления не возникает переносов. Это условие равносильно тому, что

$$w_p(d_1) + \dots + w_p(d_m) = w_p(d)$$

(см. лемму 2(д) в [6]).

В общем случае, когда сумма  $d = d_1 + \dots + d_m$  не обязательно является  $p$ -разложением,

$$w_p(d_1) + \dots + w_p(d_m) = w_p(d) + (p-1)\varepsilon$$

для некоторого  $\varepsilon \geq 0$  (см. лемму 2(в, г) в [6]). Легко видеть, что  $\varepsilon$  — число переносов, возникающих при сложении чисел  $d_1, \dots, d_m$  в  $p$ -ичной системе счисления.

При  $d \geq 0$ ,  $\varepsilon \geq 0$  определим многочлен

$$F^{(d, \varepsilon)}(x) = \prod \left( x - \vartheta_1^{j_1} \dots \vartheta_m^{j_m} \right), \quad (32)$$

где произведение берется по всем различным элементам

$$\vartheta_1^{j_1} \dots \vartheta_m^{j_m}, \quad (j_1, \dots, j_m) \in J_p(d, m, \varepsilon),$$

кольца  $S$ , а множество  $J_p(d, m, \varepsilon)$  определяется следующим образом:

$$J_p(d, m, \varepsilon) = \{(j_1, \dots, j_m) : j_1, \dots, j_m \geq 0, j_1 + \dots + j_m = d, \\ (w_p(j_1) + \dots + w_p(j_m) - w_p(d))/(p-1) \leq \varepsilon\}. \quad (33)$$

Таким образом, множество  $J_p(d, m, \varepsilon)$  состоит из всех векторов  $(j_1, \dots, j_m) \in \mathbf{N}_0^m$  таких, что  $j_1 + \dots + j_m = d$  и при вычислении последней суммы в  $p$ -ичной системе счисления возникает не более  $\varepsilon$  переносов. Положим

$$F^{(d, \varepsilon)}(x) = e, \quad \varepsilon < 0.$$

Так как элементы  $\vartheta_1, \dots, \vartheta_m$  входят в определение (32) симметрично, то так же, как для многочлена  $G^{(d)}(x)$ , показывается, что  $F^{(d, \varepsilon)}(x) \in R[x]$ .

Пусть  $F^{(d)}(x) = G^{(d)}(x)$  — многочлен, определенный в (11). Следующие соотношения вытекают из определений многочленов  $F^{(d, \varepsilon)}(x)$  и  $F^{(d)}(x)$ :

$$F^{(0, \varepsilon)}(x) = x - e, \quad F^{(1, \varepsilon)}(x) = F(x), \quad \varepsilon \geq 0, \quad (34)$$

$$F^{(d, \varepsilon)}(x) = F^{(d)}(x), \quad 0 \leq d \leq p-1, \quad \varepsilon \geq 0, \quad (35)$$

$$F^{(d, \varepsilon)}(x) \mid F^{(d, \varepsilon+1)}(x), \quad F^{(d, \varepsilon)}(x) \mid F^{(d)}(x), \quad d \geq 0, \quad \varepsilon \in \mathbf{Z}. \quad (36)$$

Наряду с последним условием заметим, что  $F^{(d, \varepsilon)}(x) = F^{(d)}(x)$  при достаточно больших  $\varepsilon$ . Действительно, из условия  $j_1 + \dots + j_m = d$  следует, что

$$(w_p(j_1) + \dots + w_p(j_m) - w_p(d))/(p-1) \leq (d - w_p(d))/(p-1).$$

Поэтому при  $\varepsilon \geq (d - w_p(d))/(p - 1)$  последнее условие в (33) лишнее, и согласно (32) и (12)  $F^{(d,\varepsilon)}(x) = F^{(d)}(x)$ .

Степень многочлена  $F^{(d,\varepsilon)}(x)$  не превосходит мощности множества  $J_p(d, m, \varepsilon)$ . В частности, при  $\varepsilon = 0$  степень многочлена  $F^{(d,0)}(x)$  не превосходит числа наборов  $(j_1, \dots, j_m)$  таких, что  $j_1 + \dots + j_m = d$ , то есть

$$\nu_r(j_1) + \dots + \nu_r(j_m) = \nu_r(d), \quad r \geq 0.$$

Отсюда получаем формулу

$$\deg F^{(d,0)}(x) \leq \binom{m + \nu_0(d) - 1}{\nu_0(d)} \binom{m + \nu_1(d) - 1}{\nu_1(d)} \dots, \quad d \geq 0. \quad (37)$$

Отметим, что многочлен  $\bar{F}^{(d,0)}(x)$  над полем  $\bar{R} = \text{GF}(q)$  в случае, когда  $\bar{F}(x)$  — многочлен максимального периода, рассматривался, например, в [19].

Для  $a \in R$  пусть

$$\begin{aligned} \lambda(a) &= \max\{i \in \mathbf{N}_0 : p^i a \neq 0\}, \quad a \neq 0, \\ \lambda(0) &= -1. \end{aligned}$$

Отметим, что для любого  $a \in R$  справедливо равенство

$$\lambda(a) = \min\{i \in \mathbf{N}_0 : p^i a = 0\} - 1.$$

Если  $e$  — единица кольца  $R$ , то  $p\bar{e} = \bar{0}$ , следовательно,  $pe \in J(R)$  и  $p^n e = 0$ . Поэтому  $\lambda(a) < n = \text{ind } J(R)$ . Более того,  $\text{char } R = p^k$  для некоторого  $k = 1, \dots, n$ , и тогда  $\lambda(a) < k$  для любого  $a \in R$ .

**Предложение 9.** Пусть  $u$  — ЛРП над конечным локальным кольцом  $R$  с сепарабельным характеристическим многочленом  $F(x)$  степени  $m \geq 1$ ,  $a \in R$ ,  $d \geq 0$ .

Тогда многочлен  $F^{(d,\lambda(a))}(x)$  является характеристическим многочленом ЛРП  $au^d$ , и  $\text{rank } au^d \leq |J_p(d, m, \lambda(a))|$ .

*Доказательство.* Если  $a = 0$ , то  $\lambda(a) = -1$  и  $F^{(d,-1)}(x) = e$  — минимальный многочлен ЛРП  $au^d = 0$ . Если  $a \neq 0$ ,  $d = 0$ , то  $\lambda(a) \geq 0$  и  $F^{(0,\lambda(a))}(x) = x - e$  — минимальный многочлен ЛРП  $au^d = a$ .

Пусть  $a \neq 0$ ,  $d > 0$ . В силу (31) и предложения 5 ЛРП  $u$  имеет биномиальное представление (10). Тогда

$$au(i)^d = a \left( \sum_{r=1}^m c_r \vartheta_r^i \right)^d = a \sum_{j_1 + \dots + j_m = d} \frac{d!}{j_1! \dots j_m!} c_1^{j_1} \dots c_m^{j_m} \left( \vartheta_1^{j_1} \dots \vartheta_m^{j_m} \right)^i. \quad (38)$$

В силу леммы 6.39 из [8] максимальная степень числа  $p$ , на которую делится полиномиальный коэффициент  $d!/(j_1! \dots j_m!)$ , равна

$$(w_p(j_1) + \dots + w_p(j_m) - w_p(d))/(p - 1).$$

Поэтому при  $(w_p(j_1) + \dots + w_p(j_m) - w_p(d))/(p - 1) > \lambda(a)$  коэффициент в сумме (38) при биномиальной последовательности  $(\vartheta_1^{j_1} \dots \vartheta_m^{j_m})^i$  равен 0. Следовательно, с учетом (33), сумму (38) можно записать в виде

$$au(i)^d = a \sum_{(j_1, \dots, j_m) \in J_p(d, m, \lambda(a))} \frac{d!}{j_1! \dots j_m!} c_1^{j_1} \dots c_m^{j_m} (\vartheta_1^{j_1} \dots \vartheta_m^{j_m})^i, \quad i \geq 0. \quad (39)$$

В силу определения (32) каждая биномиальная последовательность в сумме (39) аннулируется многочленом  $F^{(d, \lambda^{(a)})}(x)$ . Следовательно, и ЛРП  $au^d$  аннулируется многочленом  $F^{(d, \lambda^{(a)})}(x)$ .

**Теорема 5.** Пусть  $u$  — ЛРП над конечным локальным кольцом  $R$  с сепарабельным характеристическим многочленом  $F(x)$  степени  $m \geq 1$ ,

$$\Phi(x) = \sum_{d \geq 0} \varphi_d x^d \in R[x].$$

Тогда многочлен

$$F^{(\Phi)}(x) = \prod_{d \geq 0} F^{(d, \lambda(\varphi_d))}(x)$$

является характеристическим многочленом ЛРП  $v = \Phi(u)$  и

$$\text{rank } \Phi(u) \leq \sum_{d \geq 0} |J_p(d, m, \lambda(\varphi_d))|. \quad (40)$$

*Доказательство.* Так как

$$v = \sum_{d \geq 0} \varphi_d u^d,$$

теорема следует из предложения 9 и определения многочлена  $F^{(\Phi)}(x)$ .

Для получения числовой оценки ранга ЛРП  $\Phi(u)$  требуется найти  $|J_p(d, m, \varepsilon)|$ . Для этого введем понятие производного множества. Предшественником бесконечного целочисленного вектора

$$(\nu_0, \nu_1, \dots), \quad \nu_j \geq 0, \quad j \geq 0, \quad (41)$$

лишь конечное число координат которого отлично от нуля, назовем произвольный вектор  $(\nu'_0, \nu'_1, \dots)$  такой, что для некоторого  $i \geq 1$  выполняются соотношения

$$\nu_i \geq 1, \quad \nu'_i = \nu_i - 1, \quad \nu'_{i-1} = \nu_{i-1} + p, \quad \nu'_j = \nu_j, \quad j \in \mathbf{N}_0 \setminus \{i-1, i\}.$$

Если  $M$  — множество, состоящее из некоторых векторов вида (41), то множество, состоящее из всех предшественников векторов из  $M$ , обозначим  $M'$ . В частности, если множество  $M$  состоит из таких векторов (41), что  $\nu_j = 0$  при  $j \geq 1$ , то у этих векторов нет предшественников и  $M' = \emptyset$ . Положим

$$M^{(0)} = M, \quad M^{(e+1)} = (M^{(e)})', \quad e \geq 1.$$

Легко видеть, что для любого  $M$  существует  $e \geq 0$  такое, что  $M^{(e)} = \emptyset$ .

При  $d \geq 0$  введем обозначение

$$M(d) = \{(\nu_0(d), \nu_1(d), \dots)\}.$$

Тогда множество  $M(d)^{(e)}$  состоит из всех векторов вида (41) с  $\nu_0 + \nu_1 p + \dots = d$ , для которых при вычислении последней суммы в  $p$ -ичной системе счисления возникает

$e$  переносов. Это доказывается индукцией по  $e \geq 0$  с использованием определения производного множества. Следовательно,

$$J_p(d, m, \varepsilon) = \{(j_1, \dots, j_m) : j_1, \dots, j_m \geq 0, \\ (\nu_0(j_1) + \dots + \nu_0(j_m), \nu_1(j_1) + \dots + \nu_1(j_m), \dots) \in M(d)^{(e)}, 0 \leq e \leq \varepsilon\}. \quad (42)$$

Для каждого целочисленного вектора  $(\nu_0, \nu_1, \dots)$  число векторов  $(j_1, \dots, j_m)$  таких, что  $j_1, \dots, j_m \geq 0$  и

$$\begin{aligned} \nu_0(j_1) + \dots + \nu_0(j_m) &= \nu_0, \\ \nu_1(j_1) + \dots + \nu_1(j_m) &= \nu_1, \\ &\dots \end{aligned}$$

равно

$$\left\{ \begin{matrix} m \\ \nu_0 \end{matrix} \right\}_p \left\{ \begin{matrix} m \\ \nu_1 \end{matrix} \right\}_p \dots,$$

где  $\left\{ \begin{matrix} m \\ k \end{matrix} \right\}_p$  — число решений в целых числах уравнения

$$y_1 + \dots + y_m = k, \quad 0 \leq y_1, \dots, y_m \leq p - 1,$$

то есть число размещений  $k$  одинаковых предметов по  $m$  различным ячейкам при условии, что в каждую ячейку попадает не более  $p - 1$  предметов.

Множество  $M(d)^{(e)}$  либо пусто (при достаточно больших  $e$ ), либо состоит из векторов, вес (то есть сумма компонент) которых равен  $w_p(d) + (p - 1)e$ . В частности, множества  $M(d)^{(e)}$ ,  $e \geq 0$ , попарно не пересекаются. Теперь из (42) следует, что при  $d \geq 0$ ,  $\varepsilon \in \mathbf{Z}$

$$|J_p(d, m, \varepsilon)| = \sum_{\varepsilon=0}^{\varepsilon} \sum_{(\nu_0, \nu_1, \dots) \in M(d)^{(e)}} \left\{ \begin{matrix} m \\ \nu_0 \end{matrix} \right\}_p \left\{ \begin{matrix} m \\ \nu_1 \end{matrix} \right\}_p \dots \quad (43)$$

(при  $\varepsilon < 0$  сумма по пустому множеству индексов полагается равной 0). Так как в каждом векторе из  $M(d)^{(e)}$  лишь конечное число координат отлично от нуля, произведение в (43) является конечным.

Согласно [10],

$$\left\{ \begin{matrix} m \\ k \end{matrix} \right\}_p = \sum_{j \geq 0} (-1)^j \binom{m}{j} \binom{m + k - pj - 1}{m - 1}, \quad k \geq 0. \quad (44)$$

Справедливы неравенства

$$\binom{m}{k} \leq \left\{ \begin{matrix} m \\ k \end{matrix} \right\}_p \leq \binom{m + k - 1}{k},$$

поскольку в левой части находится число размещений  $k$  одинаковых предметов по  $m$  различным ячейкам при условии, что в каждую ячейку попадает не более одного предмета, а в правой части — число размещений  $k$  предметов по  $m$  ячейкам без ограничений на число предметов в ячейках. Заметим также, что

$$\begin{aligned} \left\{ \begin{matrix} m \\ k \end{matrix} \right\}_p &= \binom{m + k - 1}{k}, & k = 0, 1, \dots, p - 1, \\ \left\{ \begin{matrix} m \\ k \end{matrix} \right\}_2 &= \binom{m}{k}, & p = 2, \quad k \geq 0. \end{aligned}$$



С учетом формулы (43) оценку (40) можно записать следующим образом.

**Следствие 4.** В условиях теоремы 5

$$\text{rang } \Phi(u) \leq \sum_{d \geq 0} \sum_{e=0}^{\lambda(\varphi_d)} \sum_{(\nu_0, \nu_1, \dots) \in M(d)(\varepsilon)} \left\{ \begin{matrix} m \\ \nu_0 \end{matrix} \right\}_p \left\{ \begin{matrix} m \\ \nu_1 \end{matrix} \right\}_p \dots \quad (45)$$

Отметим, что входящие в сумму (45) производные множества  $M(d)(\varepsilon)$  легко строятся по множеству  $M(d) = \{(\nu_0(d), \nu_1(d), \dots)\}$ .

Рассмотрим теперь случай нескольких последовательностей. Пусть

$$F_1(x), \dots, F_K(x)$$

— сепарабельные многочлены над кольцом  $R$  степеней  $m_1, \dots, m_K$  соответственно,  $S$  — расширение Галуа кольца  $R$ , над которым многочлены  $F_1(x), \dots, F_K(x)$  (однозначно) раскладывается на линейные множители:

$$F_k(x) = (x - \vartheta_{k,1}) \dots (x - \vartheta_{k,m_k}), \quad \vartheta_{k,1}, \dots, \vartheta_{k,m_k} \in S, \quad k = 1, \dots, K. \quad (46)$$

При  $d_1, \dots, d_K \geq 0$ ,  $\varepsilon \geq 0$  пусть

$$F^{(d_1, \dots, d_K, \varepsilon)}(x) = \prod (x - \vartheta_{1,1}^{j_{1,1}} \dots \vartheta_{1,m_1}^{j_{1,m_1}} \dots \vartheta_{K,1}^{j_{K,1}} \dots \vartheta_{K,m_K}^{j_{K,m_K}}), \quad (47)$$

где произведение берется по всем различным элементам

$$\vartheta_{1,1}^{j_{1,1}} \dots \vartheta_{1,m_1}^{j_{1,m_1}} \dots \vartheta_{K,1}^{j_{K,1}} \dots \vartheta_{K,m_K}^{j_{K,m_K}}$$

кольца  $S$  таким, что

$$(j_{1,1}, \dots, j_{1,m_1}, \dots, j_{K,1}, \dots, j_{K,m_K}) \in J_p(\mathbf{d}, \mathbf{m}, \varepsilon),$$

и

$$\begin{aligned} J_p(\mathbf{d}, \mathbf{m}, \varepsilon) &= J_p(d_1, \dots, d_K, m_1, \dots, m_K, \varepsilon) \\ &= \{(j_{1,1}, \dots, j_{1,m_1}, \dots, j_{K,1}, \dots, j_{K,m_K}) : j_{k,r} \geq 0, \\ &\quad j_{k,1} + \dots + j_{k,m_k} = d_k, \quad r = 1, \dots, m_k, \quad k = 1, \dots, K, \\ &\quad \sum_{k=1}^K (w_p(j_{k,1}) + \dots + w_p(j_{k,m_k}) - w_p(d_k)) / (p-1) \leq \varepsilon\}. \end{aligned} \quad (48)$$

Таким образом,  $J_p(\mathbf{d}, \mathbf{m}, \varepsilon)$  есть множество векторов  $(j_{1,1}, \dots, j_{K,m_K})$  с целыми неотрицательными координатами такими, что  $j_{k,1} + \dots + j_{k,m_k} = d_k$  при  $k = 1, \dots, K$ , и общее число переносов, возникающих при вычислении этих  $K$  сумм в  $p$ -ичной системе счисления, не превосходит  $\varepsilon$ . Так как для каждого  $k = 1, \dots, K$  элементы  $\{\vartheta_{k,1}, \dots, \vartheta_{k,m_k}\}$  входят в определение (47) симметрично, то так же, как для многочленов  $G^{(d_1, \dots, d_K)}(x)$  в разделе 4, доказывается, что  $F^{(d_1, \dots, d_K, \varepsilon)}(x) \in R[x]$ . При  $\varepsilon < 0$  положим

$$F^{(d_1, \dots, d_K, \varepsilon)}(x) = e.$$

Справедливы соотношения

$$F^{(d_1, \dots, d_K, \varepsilon)}(x) = F^{(d_1, \dots, d_K)}(x), \quad 0 \leq d_1, \dots, d_K \leq p-1, \quad \varepsilon \geq 0, \quad (49)$$

и

$$\begin{aligned} F^{(d_1, \dots, d_K, \varepsilon)}(x) &| F^{(d_1, \dots, d_K, \varepsilon+1)}(x), \\ F^{(d_1, \dots, d_K, \varepsilon)}(x) &| F^{(d_1, \dots, d_K)}(x), \quad d_1, \dots, d_K \geq 0, \quad \varepsilon \in \mathbf{Z}. \end{aligned} \quad (50)$$

При достаточно больших  $\varepsilon$ , зависящих от  $p, d_1, \dots, d_K$ , выполняется равенство

$$F^{(d_1, \dots, d_K, \varepsilon)}(x) = F^{(d_1, \dots, d_K)}(x).$$

Степень многочлена  $F^{(d_1, \dots, d_K, \varepsilon)}(x)$  при  $\varepsilon \geq 0$  не превосходит мощности множества  $J_p(\mathbf{d}, \mathbf{m}, \varepsilon)$ . В частности, при  $\varepsilon = 0$  степень многочлена  $F^{(d_1, \dots, d_K, 0)}(x)$  не превосходит числа наборов

$$(j_{1,1}, \dots, j_{1,m_1}, \dots, j_{K,1}, \dots, j_{K,m_K})$$

таких, что

$$j_{k,1} + \dots + j_{k,m_k} = d_k, \quad k = 1, \dots, K,$$

и, аналогично (37), удовлетворяет неравенству

$$\deg F^{(d_1, \dots, d_K, 0)}(x) \leq \prod_{k=1}^K \binom{m_k + \nu_0(d_k) - 1}{\nu_0(d_k)} \binom{m_k + \nu_1(d_k) - 1}{\nu_1(d_k)} \dots \quad (51)$$

**Предложение 10.** Пусть  $u_1, \dots, u_K$  — линейные рекурренты над конечным локальным кольцом  $R$  с сепарабельными характеристическими многочленами  $F_1(x), \dots, F_K(x) \in R[x]$  степеней  $m_1, \dots, m_K \geq 1$  соответственно,  $a \in R, d_1, \dots, d_K$  неотрицательны.

Тогда многочлен  $F^{(d_1, \dots, d_K, \lambda(a))}(x)$  является характеристическим многочленом ЛРП  $w = au_1^{d_1} \dots u_K^{d_K}$  и  $\text{rank } w \leq |J_p(\mathbf{d}, \mathbf{m}, \lambda(a))|$ .

*Доказательство.* В силу (46) и предложения 5 последовательности  $u_1, \dots, u_K$  представляются в виде

$$u_k(i) = \sum_{r=1}^{m_k} c_{kr} \vartheta_{kr}^i, \quad i \geq 0, \quad c_{kr} \in S, \quad k = 1, \dots, K. \quad (52)$$

Тогда

$$\begin{aligned} w(i) &= a \left( \sum_{r=1}^{m_1} c_{1,r} \vartheta_{1,r}^i \right)^{d_1} \dots \left( \sum_{r=1}^{m_K} c_{K,r} \vartheta_{K,r}^i \right)^{d_K} \\ &= a \sum_{j_{k,1} + \dots + j_{k,m_k} = d_k} \frac{d_1!}{j_{1,1}! \dots j_{1,m_1}!} \dots \frac{d_K!}{j_{K,1}! \dots j_{K,m_K}!} \\ &\quad \times c_{1,1}^{j_{1,1}} \dots c_{1,m_1}^{j_{1,m_1}} \dots c_{K,1}^{j_{K,1}} \dots c_{K,m_K}^{j_{K,m_K}} (\vartheta_{1,1}^{j_{1,1}} \dots \vartheta_{1,m_1}^{j_{1,m_1}} \dots \vartheta_{K,1}^{j_{K,1}} \dots \vartheta_{K,m_K}^{j_{K,m_K}})^i, \end{aligned} \quad (53)$$

где суммирование в последней сумме проводится по

$$j_{k,1}, \dots, j_{k,m_k} \geq 0, \quad 1 \leq k \leq K.$$

В силу леммы 6.39 из [8] максимальная степень числа  $p$ , на которую делится произведение полиномиальных коэффициентов в сумме (53), равна

$$E = \sum_{k=1}^K (w_p(j_{k,1}) + \dots + w_p(j_{k,m_k}) - w_p(d_k)) / (p - 1).$$

Поэтому при  $E > \lambda(a)$  соответствующее слагаемое в сумме (53) равно 0. Следовательно, с учетом (48),

$$w(i) = a \sum_{(j_{1,1}, \dots, j_{K, m_K}) \in J_p(\mathbf{d}, \mathbf{m}, \lambda(a))} \frac{d_1!}{j_{1,1}! \dots j_{1, m_1}!} \dots \frac{d_K!}{j_{K,1}! \dots j_{K, m_K}!} \times c_{1,1}^{j_{1,1}} \dots c_{1, m_1}^{j_{1, m_1}} \dots c_{K,1}^{j_{K,1}} \dots c_{K, m_K}^{j_{K, m_K}} (\vartheta_{1,1}^{j_{1,1}} \dots \vartheta_{1, m_1}^{j_{1, m_1}} \dots \vartheta_{K,1}^{j_{K,1}} \dots \vartheta_{K, m_K}^{j_{K, m_K}})^i. \quad (54)$$

В силу определения (47) каждая биномиальная последовательность в сумме (54) аннулируется многочленом  $F^{(d_1, \dots, d_K, \lambda(a))}(x)$ . Следовательно, и последовательность  $w$  аннулируется этим многочленом.

Для многочлена

$$\Phi(x_1, \dots, x_K) = \sum_{d_1, \dots, d_K \geq 0} \varphi_{d_1 \dots d_K} x_1^{d_1} \dots x_K^{d_K}$$

над кольцом  $R$  положим

$$F^{(\Phi)}(x) = \prod_{d_1, \dots, d_K \geq 0} F^{(d_1, \dots, d_K, \lambda(\varphi_{d_1 \dots d_K}))}(x). \quad (55)$$

**Теорема 6.** Пусть  $u_1, \dots, u_K$  — линейные рекурренты над конечным локальным кольцом  $R$  с сепарабельными характеристическими многочленами  $F_1(x), \dots, F_K(x) \in R[x]$  степеней  $m_1, \dots, m_K \geq 1$  соответственно,

$$\Phi(x_1, \dots, x_K) \in R[x_1, \dots, x_K].$$

Тогда многочлен  $F^{(\Phi)}(x)$  является характеристическим многочленом ЛРП  $v = \Phi(u_1, \dots, u_K)$ , и

$$\text{rank } \Phi(u_1, \dots, u_K) \leq \sum_{d_1, \dots, d_K \geq 0} |J_p(\mathbf{d}, \mathbf{m}, \lambda(\varphi_{d_1 \dots d_K}))|. \quad (56)$$

Теорема следует из предложения 10.

Получим числовую оценку ранга ЛРП  $\Phi(u_1, \dots, u_K)$ . В силу (33), (48)

$$J_p(\mathbf{d}, \mathbf{m}, \varepsilon) = \{(j_{1,1}, \dots, j_{1, m_1}, \dots, j_{K,1}, \dots, j_{K, m_K}) : (j_{k,1}, \dots, j_{k, m_k}) \in J_p(d_k, m_k, e_k), e_k \geq 0, k = 1, \dots, K, e_1 + \dots + e_K \leq \varepsilon\}.$$

Используя (42), получим, что

$$\begin{aligned} J_p(\mathbf{d}, \mathbf{m}, \varepsilon) &= \{(j_{1,1}, \dots, j_{1, m_1}, \dots, j_{K,1}, \dots, j_{K, m_K}) : \\ &\quad (\nu_0(j_{k,1}) + \dots + \nu_0(j_{k, m_k}), \nu_1(j_{k,1}) + \dots + \nu_1(j_{k, m_k}), \dots) \in M(d_k)^{(e_k)}, \\ &\quad j_{k,r} \geq 0, \quad e_k \geq 0, \quad r = 1, \dots, m_k, \quad k = 1, \dots, K, \quad e_1 + \dots + e_K \leq \varepsilon\} \\ &= \bigcup_{\substack{e_1, \dots, e_K \geq 0 \\ e_1 + \dots + e_K \leq \varepsilon}} \{(j_{1,1}, \dots, j_{1, m_1}, \dots, j_{K,1}, \dots, j_{K, m_K}) : j_{k,r} \geq 0, \quad r = 1, \dots, m_k, \\ &\quad (\nu_0(j_{k,1}) + \dots + \nu_0(j_{k, m_k}), \nu_1(j_{k,1}) + \dots + \nu_1(j_{k, m_k}), \dots) \in M(d_k)^{(e_k)}, \\ &\quad k = 1, \dots, K\}, \end{aligned}$$

причем в последнем соотношении объединяемые множества попарно не пересекаются, поскольку множества  $M(d)^{(e)}$ ,  $e \geq 0$ , попарно не пересекаются. Следовательно, при  $d_1, \dots, d_K \geq 0$ ,  $\varepsilon \geq 0$  аналогично (43) получаем равенство

$$|J_p(\mathbf{d}, \mathbf{m}, \varepsilon)| = \sum_{\substack{e_1, \dots, e_K \geq 0 \\ e_1 + \dots + e_K \leq \varepsilon}} \sum_{\substack{(\nu_{k0}, \nu_{k1}, \dots) \in M(d_k)^{(e_k)} \\ k=1, \dots, K}} \prod_{k=1}^K \left\{ \begin{matrix} m_k \\ \nu_{k0} \end{matrix} \right\}_p \left\{ \begin{matrix} m_k \\ \nu_{k1} \end{matrix} \right\}_p \dots$$

Поскольку в каждом векторе из  $M(d_k)^{(e_k)}$  лишь конечное число координат отлично от нуля, последнее произведение является конечным.

**Следствие 5.** В условиях теоремы 6

$$\begin{aligned} & \text{rang } \Phi(u_1, \dots, u_K) \\ & \leq \sum_{d_1, \dots, d_K \geq 0} \sum_{\substack{e_1 + \dots + e_K \leq \lambda(\varphi_{d_1 \dots d_K}) \\ e_1, \dots, e_K \geq 0}} \sum_{\substack{(\nu_{k0}, \nu_{k1}, \dots) \in M(d_k)^{(e_k)} \\ k=1, \dots, K}} \prod_{k=1}^K \left\{ \begin{matrix} m_k \\ \nu_{k0} \end{matrix} \right\}_p \left\{ \begin{matrix} m_k \\ \nu_{k1} \end{matrix} \right\}_p \dots \end{aligned} \quad (57)$$

Напомним, что величины  $\left\{ \begin{matrix} m \\ k \end{matrix} \right\}_p$  в этой оценке вычисляются по формуле (44).

**Замечание 2.** Формулировки и доказательства результатов этого параграфа сохраняются и в случае, когда  $R$  — локальное кольцо с нильпотентным радикалом, поле вычетов которого имеет характеристику  $p > 0$ .

## 6. Минимальный многочлен и точное значение ранга

В этом параграфе будет доказано, что при дополнительных условиях на последовательности  $u$ ,  $u_1, \dots, u_K$  и многочлен  $\Phi$  многочлены  $F^{(\Phi)}(x)$ , определенные в теоремах 5 и 6, являются минимальными многочленами последовательностей  $\Phi(u)$  и  $\Phi(u_1, \dots, u_K)$ , и верхние оценки рангов, полученные в следствиях 4 и 5, обращаются в равенства.

Пусть  $R$  — конечное локальное кольцо с полем вычетов  $\bar{R} = \text{GF}(q)$ ,  $F(x) \in R[x]$  — многочлен Галуа степени  $m$ ,  $S$  — расширение Галуа кольца  $R$  степени  $m$ . Над кольцом  $S$  многочлен  $F(x)$  представляется в виде (31), причем, если обозначить  $\vartheta = \vartheta_1$ , то элементы  $\vartheta_2, \dots, \vartheta_m$  можно занумеровать так, что

$$\bar{\vartheta}_r = \bar{\vartheta}^{q^{r-1}}, \quad r = 1, \dots, m.$$

Напомним, что неприводимый многочлен  $\bar{F}(x)$  над полем  $\bar{R}$  называется многочленом максимального периода или примитивным многочленом, если его корень  $\bar{\vartheta}$  является примитивным элементом поля  $\bar{S} = \text{GF}(q^m)$ , то есть  $\text{ord } \bar{\vartheta} = q^m - 1$ .

**Предложение 11.** Пусть  $F(x) \in R[x]$  — многочлен Галуа степени  $m \geq 1$  такой, что  $\bar{F}(x)$  — многочлен максимального периода над полем  $\bar{R}$ . Тогда выполняются следующие утверждения.

При  $d \doteq 0, 1, \dots, q-1$  справедливы равенства

$$F^{(d)}(x) = \prod_{\substack{j_1 + \dots + j_m = d \\ j_1, \dots, j_m \geq 0}} (x - \vartheta_1^{j_1} \dots \vartheta_m^{j_m}), \quad \deg F^{(d)}(x) = \binom{m+d-1}{d}. \quad (58)$$

Многочлены  $F^{(1)}(x), \dots, F^{(q-1)}(x)$  сепарабельны и попарно взаимно просты.

Если  $m \geq 2$ , то многочлены  $F^{(0)}(x) = x - e, F^{(1)}(x), \dots, F^{(q-1)}(x)$  попарно взаимно просты.

*Доказательство.* Так как  $\bar{F}(x)$  — многочлен максимального периода, элементы

$$\bar{\vartheta}_1^{j_1} \dots \bar{\vartheta}_m^{j_m} = \bar{\vartheta}^{j_1 + qj_2 + \dots + q^{m-1}j_m} \quad (59)$$

при  $0 \leq j_1, \dots, j_m \leq q-1, (j_1, \dots, j_m) \neq (0, \dots, 0)$  попарно различны, при этом

$$\bar{\vartheta}_1^0 \dots \bar{\vartheta}_m^0 = \bar{e} = \bar{\vartheta}_1^{q-1} \dots \bar{\vartheta}_m^{q-1}.$$

Теперь первое утверждение вытекает из определения (12). Второе и третье утверждения вытекают из того, что элементы (59) попарно различны.

Следующее утверждение доказано в [9].

**Предложение 12.** Пусть ЛРП  $u_1, \dots, u_s$  над кольцом  $R$  имеют попарно взаимно простые характеристические многочлены,  $u = u_1 + \dots + u_s$ . Тогда произведение минимальных многочленов ЛРП  $u_1, \dots, u_s$  является минимальным многочленом ЛРП  $u$  и  $\text{rank } u = \text{rank } u_1 + \dots + \text{rank } u_s$ .

**Предложение 13.** Пусть  $F(x) \in R[x]$  — многочлен Галуа степени  $m \geq 1$  такой, что  $\bar{F}(x)$  — многочлен максимального периода над полем  $\bar{R}$ ,  $u \in L_R(F)$ ,  $\bar{u} \neq 0$ ,  $a \in R$ ,  $0 \leq d \leq q-1$ . Тогда многочлен  $F^{(d, \lambda(a))}(x)$  является минимальным многочленом ЛРП  $au^d$  и  $\text{rank } au^d = |J_p(d, m, \lambda(a))|$ .

*Доказательство.* Поскольку выполняются условия предложения 9, можно использовать соотношение (39). Как следует из доказательства предложения 9, для каждого слагаемого суммы (39) выполняется условие  $ad!/(j_1! \dots j_m!) \neq 0$ . Так как  $\bar{u} \neq 0$ , в биномиальном представлении (10)  $\bar{c}_r \neq 0, r = 1, \dots, m$ , откуда,  $\bar{c}_1^{j_1} \dots \bar{c}_m^{j_m} \neq 0$ . Следовательно, в сумме (39) коэффициент при каждой биномиальной последовательности  $(\vartheta_1^{j_1} \dots \vartheta_m^{j_m})^i$  не равен 0.

Таким образом, соотношение (39) есть представление ЛРП  $au^d$  в виде суммы последовательностей с минимальными многочленами

$$x - \vartheta_1^{j_1} \dots \vartheta_m^{j_m}, \quad (j_1, \dots, j_m) \in J_p(d, m, \lambda(a)).$$

Из доказательства предложения 11 и условия  $d \leq q-1$  следует, что элементы  $\bar{\vartheta}_1^{j_1} \dots \bar{\vartheta}_m^{j_m}$  поля  $\bar{S}$  такие, что  $(j_1, \dots, j_m) \in J_p(d, m, \lambda(a))$ , попарно различны. Следовательно, ввиду второго утверждения предложения 3, указанные минимальные многочлены попарно взаимно просты. Теперь из (39) и предложения 12 получаем, что  $F^{(d, \lambda(a))}(x)$  — минимальный многочлен ЛРП  $au^d$  и  $\text{rank } au^d = |J_p(d, m, \lambda(a))|$ .

**Теорема 7.** Пусть  $R$  — конечное локальное кольцо,  $F(x) \in R[x]$  — многочлен Галуа степени  $m \geq 1$  такой, что  $\bar{F}(x)$  — многочлен максимального периода над полем  $\bar{R}$ ,  $u \in L_R(F)$ ,  $\bar{u} \neq 0$ ,  $\Phi(x) \in R[x]$  — многочлен степени не выше  $q-1$  и либо  $m \geq 2$ , либо  $m = 1$ ,  $\Phi(0) = 0$ .

Тогда многочлен

$$F^{(\Phi)}(x) = \prod_{d \geq 0} F^{(d, \lambda(\varphi_d))}(x)$$

из теоремы 5 является минимальным многочленом ЛРП  $v = \Phi(u)$  и оценки (40), (45) обращаются в равенства.

*Доказательство.* Пусть

$$\Phi(x) = \sum_{d=0}^{q-1} \varphi_d x^d.$$

Тогда

$$v = \sum_{d=0}^{q-1} \varphi_d u^d.$$

По предложению 13 многочлен  $F^{(d, \lambda(\varphi_d))}(x)$  является минимальным многочленом ЛРП  $\varphi_d u^d$ ,  $d = 0, 1, \dots, q-1$ . Ввиду (36)  $F^{(d, \lambda(\varphi_d))}(x) \mid F^{(d)}(x)$ . Если  $m \geq 2$ , то из третьего утверждения в 11 следует, что многочлены  $F^{(d, \lambda(\varphi_d))}(x)$ ,  $d = 0, 1, \dots, q-1$ , попарно взаимно просты. Если же  $m = 1$ , то по условию  $\varphi_0 = 0$ , откуда,  $\lambda(\varphi_0) = -1$  и  $F^{(0, \lambda(\varphi_0))}(x) = e$ . В этом случае, в силу второго утверждения предложения 11, многочлены  $F^{(d, \lambda(\varphi_d))}(x)$ ,  $d = 0, 1, \dots, q-1$ , также попарно взаимно просты. Из предложения 12 теперь следует, что произведение минимальных многочленов последовательностей  $\varphi_d u^d$ ,  $d = 0, 1, \dots, q-1$ , то есть многочлен  $F^{(\Phi)}(x)$ , является минимальным многочленом ЛРП  $v$ .

Вычисление ранга ЛРП  $v = \Phi(u)$  с помощью формулы (45) сопряжено с построением производных множеств  $M(d)^{(e)}$ ,  $e \geq 0$ . Укажем оценки ранга ЛРП  $v$ , которые являются более простыми и не требуют построения производных множеств.

**Следствие 6.** В условиях теоремы 7 пусть  $D = \{d \geq 0: \varphi_d \neq 0\}$ . Тогда

$$\sum_{d \in D} \binom{m + \nu_0(d) - 1}{\nu_0(d)} \binom{m + \nu_1(d) - 1}{\nu_1(d)} \dots \leq \text{rank } v \leq \sum_{d \in D} \binom{m + d - 1}{d}. \quad (60)$$

*Доказательство.* Если  $d \in D$ , то  $\lambda(\varphi_d) \geq 0$  и ввиду (36)  $F^{(d,0)}(x) \mid F^{(d, \lambda(\varphi_d))}(x)$ . Следовательно,

$$\prod_{d \in D} F^{(d,0)}(x) \mid F^{(\Phi)}(x).$$

Поэтому

$$\text{rank } v = \deg F^{(\Phi)}(x) \geq \sum_{d \in D} \deg F^{(d,0)}(x).$$

Так как элементы (59) попарно различны, неравенство (37) обращается в равенство. Отсюда получаем нижнюю оценку в (60). Верхняя оценка совпадает с оценкой (16), доказанной в теореме 2.

**Следствие 7.** Если в условиях теоремы 7  $\deg \Phi \leq p - 1$ , то

$$F^{(\Phi)}(x) = \prod_{d \in D} F^{(d)}(x), \quad \text{rank } v = \sum_{d \in D} \binom{m + d - 1}{d},$$

то есть для ранга достигается оценка (16).

Утверждения следствия вытекают из формул (35), (58).

**Следствие 8.** Пусть в условиях теоремы 7  $R$  — кольцо главных идеалов с радикалом  $J(R) = \pi R$  индекса нильпотентности  $n$ . Тогда

$$\text{Ann}(v) = (F^{(\Phi)}(x), \pi F^{(\pi\Phi)}(x), \dots, \pi^{n-1} F^{(\pi^{n-1}\Phi)}(x)).$$

*Доказательство.* По теореме 7 многочлен  $F^{(\pi^t\Phi)}(x)$  является минимальным многочленом последовательности  $\pi^t v$ ,  $t = 0, 1, \dots, n - 1$ . Другими словами,  $F^{(\pi^t\Phi)}(x)$  — многочлен наименьшей степени среди унитарных многочленов  $G(x) \in R[x]$  таких, что  $\pi^t G(x) \in \text{Ann}(v)$ . Из утверждения 13 в [9] следует, что идеал  $\text{Ann}(v)$  порождается многочленами

$$\pi^t F^{(\pi^t\Phi)}(x), \quad t = 0, 1, \dots, n - 1,$$

что и требовалось доказать.

Теорема 7 и ее следствия справедливы, в частности, если  $R = \text{GR}(q^n, p^n)$  — кольцо Галуа из  $q^n$  элементов характеристики  $p^n$ . Отметим, что в этом случае

$$\lambda(a) = n - \|a\| - 1,$$

где

$$\|a\| = \max\{r \in \{0, \dots, n\} : a \in p^r R\}$$

— норма элемента  $a \in R$  (см. [19, 9]).

Рассмотрим теперь полиномиальные преобразования нескольких последовательностей. Пусть  $F_1(x), \dots, F_K(x)$  — многочлены Галуа над  $R$  степеней  $m_1, \dots, m_K$  соответственно. Над расширением Галуа  $S$  кольца  $R$  степени  $[m_1, \dots, m_K]$  многочлены  $F_1(x), \dots, F_K(x)$  представляются в виде (46), причем если положить  $\vartheta_k = \vartheta_{k,1}$ , то корни многочлена  $F_k(x)$  можно занумеровать так, что

$$\bar{\vartheta}_{k,r} = \bar{\vartheta}_k^{q^{r-1}}, \quad r = 1, \dots, m_k, \quad k = 1, \dots, K. \quad (61)$$

Положим

$$M_k = \min \left\{ q, m_k, \frac{q-2}{q-1} m_k + 1 \right\}, \quad k = 1, \dots, K.$$

**Предложение 14.** Пусть  $F_1(x), \dots, F_K(x)$  — многочлены Галуа над кольцом  $R$  степеней  $m_1, \dots, m_K \geq 1$  соответственно такие, что  $\bar{F}_1(x), \dots, \bar{F}_K(x)$  — многочлены максимального периода над полем  $\bar{R}$ , числа  $m_1, \dots, m_K$  попарно взаимно просты и  $0 \leq d_k < M_k$ ,  $k = 1, \dots, K$ .

Тогда

$$F^{(d_1, \dots, d_K)}(x) = \prod (x - \vartheta_{1,1}^{j_{1,1}} \dots \vartheta_{1,m_1}^{j_{1,m_1}} \dots \vartheta_{K,1}^{j_{K,1}} \dots \vartheta_{K,m_K}^{j_{K,m_K}}),$$

где произведение берется по множеству

$$\{j_{k,1}, \dots, j_{k,m_k} : j_{k,1} + \dots + j_{k,m_k} = d_k, j_{k,r} \geq 0, 1 \leq r \leq m_k, 1 \leq k \leq K\},$$

и

$$\deg F^{(d_1, \dots, d_K)}(x) = \binom{m_1 + d_1 - 1}{d_1} \dots \binom{m_K + d_K - 1}{d_K}. \quad (62)$$

Многочлены

$$F^{(d_1, \dots, d_K)}(x), \quad 0 \leq d_k < M_k, \quad k = 1, \dots, K,$$

сепарабельны и попарно взаимно просты.

*Доказательство.* Ввиду определения (24) перечисленные утверждения являются следствием того, что элементы

$$\bar{\vartheta}_{1,1}^{j_{1,1}} \dots \bar{\vartheta}_{1,m_1}^{j_{1,m_1}} \dots \bar{\vartheta}_{K,1}^{j_{K,1}} \dots \bar{\vartheta}_{K,m_K}^{j_{K,m_K}} \quad (63)$$

такие, что

$$j_{k,1} + \dots + j_{k,m_k} = d_k, \quad j_{k,r} \geq 0, \quad r = 1, \dots, m_k, \quad 0 \leq d_k < M_k, \quad k = 1, \dots, K,$$

попарно различны. Докажем это. Ввиду (61)

$$\begin{aligned} \bar{\vartheta}_{1,1}^{j_{1,1}} \dots \bar{\vartheta}_{1,m_1}^{j_{1,m_1}} \dots \bar{\vartheta}_{K,1}^{j_{K,1}} \dots \bar{\vartheta}_{K,m_K}^{j_{K,m_K}} \\ = \bar{\vartheta}_1^{j_{1,1} + qj_{1,2} + \dots + q^{m_1-1}j_{1,m_1}} \dots \bar{\vartheta}_K^{j_{K,1} + qj_{K,2} + \dots + q^{m_K-1}j_{K,m_K}}. \end{aligned}$$

Введем обозначения

$$b_k = j_{k,1} + qj_{k,2} + \dots + q^{m_k-1}j_{k,m_k}, \quad k = 1, \dots, K.$$

Тогда множество элементов (63) запишется следующим образом:

$$\bar{\vartheta}_1^{b_1} \dots \bar{\vartheta}_K^{b_K}, \quad b_k = 0, 1, \dots, q^{m_k} - 1, \quad 0 \leq w_q(b_k) < M_k, \quad k = 1, \dots, K.$$

Предположим, что два таких элемента совпадают:

$$\begin{aligned} \bar{\vartheta}_1^{b_1} \dots \bar{\vartheta}_K^{b_K} = \bar{\vartheta}_1^{b'_1} \dots \bar{\vartheta}_K^{b'_K}, \\ b_k, b'_k = 0, 1, \dots, q^{m_k} - 1, \quad 0 \leq w_q(b_k), w_q(b'_k) < M_k, \quad k = 1, \dots, K. \end{aligned} \quad (64)$$

Так как  $\vartheta_k$  — корень многочлена Галуа  $F_k(x)$  степени  $m_k$ , то  $\bar{\vartheta}_k \in \text{GF}(q^{m_k})$ ,  $k = 1, \dots, K$ . Поскольку числа  $m_1, \dots, m_K$  попарно взаимно просты, из равенства (64) следует, что

$$\bar{\vartheta}_k^{b_k - b'_k} \in \bar{R} = \text{GF}(q), \quad k = 1, \dots, K.$$

Так как  $\bar{F}_k(x)$  — многочлен максимального периода, то  $\bar{\vartheta}_k$  — примитивный элемент поля  $\text{GF}(q^{m_k})$ ,  $k = 1, \dots, K$ . В силу следующей леммы  $b_k = b'_k$ ,  $k = 1, \dots, K$ , что завершает доказательство предложения 14.

**Лемма 2.** Если  $\vartheta$  — примитивный элемент поля  $\text{GF}(q^m)$  и  $\vartheta^{a-b} \in \text{GF}(q)$ , где

$$a, b \in \{0, 1, \dots, q^m - 1\}, \quad 0 \leq w_q(a), w_q(b) < \min \left\{ m, \frac{q-2}{q-1} m + 1 \right\},$$

то  $a = b$ .



Доказательство получается из доказательства леммы 1 из [7] заменой  $p$  на  $q$ .

**Предложение 15.** Пусть в условиях предложения 14

$$u_k \in L_R(F_k), \quad \bar{u}_k \neq 0, \quad k = 1, \dots, K, \quad a \in R, \quad 0 \leq d \leq q - 1.$$

Тогда многочлен  $F^{(d_1, \dots, d_K, \lambda(a))}(x)$  является минимальным многочленом ЛРП  $w = au_1^{d_1} \dots u_K^{d_K}$  и  $\text{rank } w = |J_p(\mathbf{d}, \mathbf{m}, \lambda(a))|$ .

*Доказательство.* Так как выполнены условия предложения 10, справедливо соотношение (54). Поскольку  $\bar{u}_k \neq 0$ , в биномиальном представлении (52)  $\bar{c}_{kr} \neq 0$ ,  $r = 1, \dots, m_k$ ,  $k = 1, \dots, K$ . Тогда из доказательства предложения 10 следует, что коэффициент при каждой биномиальной последовательности в сумме (54) не равен нулю. Поэтому минимальный многочлен последовательности, являющейся слагаемым в (54), равен

$$x - v_{1,1}^{j_{1,1}} \dots v_{1,m_1}^{j_{1,m_1}} \dots v_{K,1}^{j_{K,1}} \dots v_{K,m_K}^{j_{K,m_K}}.$$

Как показано выше, все элементы (63) попарно различны. Следовательно, ввиду второго утверждения предложения 3, указанные минимальные многочлены попарно взаимно просты. Теперь из (54) и предложения 12 получаем, что  $F^{(d_1, \dots, d_K, \lambda(a))}(x)$  — минимальный многочлен ЛРП  $w$ , и  $\text{rank } w = |J_p(\mathbf{d}, \mathbf{m}, \lambda(a))|$ .

**Теорема 8.** Пусть  $R$  — конечное локальное кольцо,  $F_1(x), \dots, F_K(x)$  — многочлены Галуа над  $R$  степеней  $m_1, \dots, m_K \geq 1$  такие, что  $\bar{F}_1(x), \dots, \bar{F}_K(x)$  — многочлены максимального периода над полем  $\bar{R}$ ,  $u_k \in L_R(F_k)$ ,  $\bar{u}_k \neq 0$ ,  $k = 1, \dots, K$ ,  $\Phi(x_1, \dots, x_K)$  — многочлен над кольцом  $R$ . Предположим, что числа  $m_1, \dots, m_K$  попарно взаимно просты и степень многочлена  $\Phi$  по переменной  $x_k$  меньше  $M_k$ ,  $k = 1, \dots, K$ .

Тогда многочлен  $F^{(\Phi)}(x)$ , определенный в (55), является минимальным многочленом ЛРП  $v = \Phi(u_1, \dots, u_K)$  и оценки (56), (57) обращаются в равенство.

*Доказательство.* По условию многочлен  $\Phi$  представляется в виде

$$\Phi(x_1, \dots, x_K) = \sum_{0 \leq d_k < M_k, k=1, \dots, K} \varphi_{d_1 \dots d_K} x_1^{d_1} \dots x_K^{d_K}.$$

Тогда

$$v = \sum_{0 \leq d_k < M_k, k=1, \dots, K} \varphi_{d_1 \dots d_K} u_1^{d_1} \dots u_K^{d_K}.$$

По предложению 15 многочлен  $F^{(d_1, \dots, d_K, \lambda(\varphi_{d_1 \dots d_K}))}(x)$  является минимальным многочленом ЛРП  $\varphi_{d_1 \dots d_K} u_1^{d_1} \dots u_K^{d_K}$  при  $0 \leq d_k < M_k$ ,  $k = 1, \dots, K$ . Из (50) и предложения 14 следует, что указанные многочлены попарно взаимно просты. Согласно предложению 12 произведение этих многочленов, то есть многочлен  $F^{(\Phi)}(x)$ , является минимальным многочленом ЛРП  $v$ .

**Следствие 9.** В условиях теоремы 8 пусть

$$D = \{(d_1, \dots, d_K) \in \mathbf{N}_0^K : \varphi_{d_1 \dots d_K} \neq 0\}.$$

Тогда

$$\sum_{(d_1, \dots, d_K) \in D} \prod_{k=1}^K \binom{m_k + \nu_0(d_k) - 1}{\nu_0(d_k)} \binom{m_k + \nu_1(d_k) - 1}{\nu_1(d_k)} \dots \leq \text{rank } v$$

$$\leq \sum_{(d_1, \dots, d_K) \in D} \prod_{k=1}^K \binom{m_k + d_k - 1}{d_k}.$$

*Доказательство.* Ввиду (50)

$$\prod_{(d_1, \dots, d_K) \in D} F^{(d_1, \dots, d_K, 0)}(x) \mid F^{(\Phi)}(x), \quad F^{(\Phi)}(x) \mid \prod_{(d_1, \dots, d_K) \in D} F^{(d_1, \dots, d_K)}(x).$$

При этом справедливо равенство (62), а так как элементы (63) попарно различны, то и неравенство (51) обращается в равенство. Отсюда следуют требуемые оценки (отметим, что верхняя оценка уже была доказана ранее, см. (30)).

**Следствие 10.** *Если в условиях теоремы 8 степень многочлена  $\Phi$  по каждой переменной не превосходит  $p - 1$ , то*

$$F^{(\Phi)}(x) = \prod_{(d_1, \dots, d_K) \in D} F^{(d_1, \dots, d_K)}(x),$$

$$\text{rank } v = \sum_{(d_1, \dots, d_K) \in D} \binom{m_1 + d_1 - 1}{d_1} \dots \binom{m_K + d_K - 1}{d_K},$$

то есть для ранга достигается оценка (30).

Эти утверждения следуют из теоремы 8 и соотношений (49), (62).

**Следствие 11.** *Пусть в условиях теоремы 8  $R$  — кольцо главных идеалов с радикалом  $J(R) = \pi R$  индекса нильпотентности  $n$ . Тогда*

$$\text{Ann}(v) = (F^{(\Phi)}(x), \pi F^{(\pi\Phi)}(x), \dots, \pi^{n-1} F^{(\pi^{n-1}\Phi)}(x)).$$

Доказательство повторяет доказательство следствия 8.

**Замечание 3.** Для последовательностей над конечным полем в случае, когда многочлен  $\Phi(x_1, \dots, x_K)$  свободен от квадратов, утверждение следствия 10 доказано в [22]. Если многочлен  $\Phi$  свободен от квадратов, то для него выполняются условия теоремы 8 (при  $m_k \geq 2, k = 1, \dots, K$ ). Поэтому теорема 8 и следствие 10 обобщают результат статьи [22] не только на последовательности над кольцом  $R$ , но и на более широкий класс многочленов  $\Phi$ . Отметим, однако, что в случае, когда многочлен  $\Phi$  свободен от квадратов, результат следствия 10 доказан в [14, 15, 16, 22] при значительно более общих условиях на последовательности  $u_1, \dots, u_K$  над конечным полем. Таким образом, по сравнению с указанными статьями, в теореме 8 (если ее рассматривать в случае, когда  $R$  — конечное поле) рассматриваются многочлены  $\Phi$  более общего вида, но на последовательности  $u_1, \dots, u_K$  накладываются более сильные ограничения.

**Замечание 4.** Результаты этого параграфа сохраняются в случае, когда  $R$  — локальное кольцо с нильпотентным радикалом и конечным полем вычетов. Пример бесконечного кольца такого вида приведен в замечании 1.

## Список литературы

1. Атья М., Макдональд И., *Введение в коммутативную алгебру*. Мир, Москва, 1972.
2. Бурбаки Н., *Коммутативная алгебра*. Мир, Москва, 1971.
3. Ван дер Варден Б. Л., *Алгебра*. Наука, Москва, 1979.
4. Глухов М. М., Елизаров В. П., Нечаев А. А., *Алгебра*. Часть II. Москва, 1991.
5. Зарисский О., Самюэль П., *Коммутативная алгебра*. ИЛ, Москва, 1963.
6. Куракин В. Л., Представления над кольцом  $\mathbb{Z}_p^n$  линейной рекуррентной последовательности максимального периода над полем  $\text{GF}(p)$ . *Дискретная математика* (1992) 4, № 4, 96–116.
7. Куракин В. Л., Полиномиальные преобразования линейных рекуррентных последовательностей над кольцом  $\mathbb{Z}_p^2$ . *Дискретная математика* (1999) 11, № 2, 40–65.
8. Лидл Р., Нидеррайтер Г., *Конечные поля*. т. 1, 2. Мир, Москва, 1988.
9. Нечаев А. А., Линейные рекуррентные последовательности над коммутативными кольцами. *Дискретная математика* (1991) 3, № 4, 107–121.
10. Сачков В. Н., *Введение в комбинаторные методы дискретной математики*. Наука, Москва, 1982.
11. Bernasconi J., Günter C. G., Analysis of a nonlinear feedforward logic for binary sequence generators. *Lect. Notes Comput. Sci.* (1986) 219, 161–166.
12. Brynielsson L., On the linear complexity of combined shift register sequences. *Lect. Notes Comput. Sci.* (1986) 219, 156–160.
13. Chan A. H., Goresky M., Klapper A., On the linear complexity of feedback registers. *IEEE Trans. Inform. Theory*, (1990) 36, № 3, 640–644.
14. Golić S. D., On the linear complexity of functions of periodic  $\text{GF}(q)$  sequences. *IEEE Trans. Inform. Theory* (1989) 35, № 1, 69–75.
15. Herlestam T., On the complexity of functions of linear shift register sequences. *Int. Symp. Inform. Theory*, Les Arc, France, 1982.
16. Herlestam T., On functions of linear shift register sequences. *Lect. Notes Comput. Sci.* (1986) 219 (1986), 119–129.
17. Key E. L., An analysis of the structure and complexity of nonlinear binary sequence generators. *IEEE Trans. Inform. Theory* (1976) 22, № 6, 732–736.
18. Klapper A., The vulnerability of geometric sequences based on fields of odd characteristic. *J. Cryptology*, (1994) 7, 33–51.
19. Kurakin V. L., Kuzmin A. S., Mikhalev A. V., Nechaev A. A., Linear recurring sequences over rings and modules. *J. Math. Sci.* (1995) 76, № 6, 2793–2915.
20. Lu P., Song G., Feasible calculation of the generator for combined LFSR sequences. *Lect. Notes Comput. Sci.* (1991) 508, 86–95.
21. Lu P., Song G., Zhou J., Tensor product with application to linear recurring sequences. *J. Math. Res. Exposition* (1992) 12, № 4, 551–558.
22. Rueppel R. A., Staffelbach O. J., Products of linear recurring sequences with maximum complexity. *IEEE Trans. Inform. Theory* (1987) 33, № 1, 126–131.
23. Selmer E. S., *Linear Recurrence Relations Over Finite Fields*. Univ. Bergen, Bergen, 1966.
24. Vajda I., Nemetz T., Substitution of characters in  $q$ -ary  $m$ -sequences. *Lect. Notes Comput. Sci.* (1991) 508, 96–105.
25. Zierler N., Mills W. H., Products of linear recurring sequences. *J. Algebra* (1973) 27, № 1, 147–157.