ЧЕБЫШЕВСКИЙ СБОРНИК
Том 18 Выпуск 2

УДК 511.3 DOI 10.22405/2226-8383-2017-18-2-54-97

О ДРОБНО-ЛИНЕЙНЫХ ПРЕОБРАЗОВАНИЯХ ФОРМ А. ТУЭ — М. Н. ДОБРОВОЛЬСКОГО — В. Д. ПОДСЫПАНИНА[1]

Н. М. Добровольский, И. Н. Балаба, И. Ю. Реброва, Н. Н. Добровольский, Е. А. Матвеева (г. Тула)

Аннотация

В работе строится алгебраическая теория полиномов Туэ. Построение теории опирается на изучение подмодулей $\mathbb{Z}[t]$-модуля $\mathbb{Z}[t]^2$. Рассматриваются подмодули, заданные одним определяющим соотношением и одним определяющим соотношением k-ого порядка. Более сложным подмодулем является подмодуль заданный одним полиномиальным соотношением. Подмодули пар Туэ j-ого порядка напрямую связаны с полиномами Туэ j-ого порядка. С помощью алгебраической теории подмодулей пар Туэ j-ого порядка удалось получить новое доказательство теоремы М. Н. Добровольского (старшего) о том, что для каждого порядка j существуют два основных полинома Туэ j-ого порядка, через которые выражаются все остальные. Основные полиномы определяются с точностью до унимодулярной многочленной матрицы над кольцом целочисленных многочленов.

В работе вводятся дробно-линейные преобразования ТДП-форм. Показано, что при переходе от ТДП-формы, связанной с алгебраическим числом α к ТДП-форме, связанной с остаточной дробью к алгебраическому числу α, ТДП-форма преобразуется по закону, аналогичному преобразованию минимальных многочленов, а числители и знаменатели соответствующих пар Туэ преобразуются с помощью дробно-линейного преобразования второго рода.

Ключевые слова: минимальный многочлен, приведённая алгебраическая иррациональность, остаточные дроби, цепные дроби, ТДП-форма, модули Туэ, пара Туэ, дробно-линейное преобразование второго рода.

Библиография: 37 названий.

ON FRACTIONAL LINEAR TRANSFORMATIONS OF FORMS A. TUE — M. N. DOBROVOLSKY — V. D. PODSYPININA

N. M. Dobrovol’skii, I. N. Balaba, I. Yu. Rebrova, N. N. Dobrovol’skii, E. A. Matveeva (Tula)

Abstract

The work builds on the algebraic theory of polynomials Tue. The theory is based on the study of submodules of $\mathbb{Z}[t]$-module $\mathbb{Z}[t]^2$. Considers submodules that are defined by one defining relation and one defining relation k-th order. More complex submodule is the submodule given by one polynomial relation. Sub par Tue j-th order are directly connected with polynomials Tue j-th order. Using the algebraic theory of pairs of submodules of Tue j-th order managed to obtain a new proof of the theorem of M. N. Dobrowolski (senior) that for each j there are two fundamental polynomial Tue j-th order, which are expressed through others. Basic polynomials

[1]Работа выполнена по грантам РФФИ № 15-01-01540-а, №16-41-710194

are determined with an accuracy of unimodular polynomial matrices over the ring of integer polynomials.

In the work introduced linear-fractional conversion of TDP-forms. It is shown that the transition from TDP-forms associated with an algebraic number α to TDP-the form associated with the residual fraction to algebraic number α, TDP-form is converted under the law, similar to the transformation of minimal polynomials and the numerators and denominators of the respective pairs of Tue is converted using the linear-fractional transformations of the second kind.

Keywords: the minimum polynomial of the given algebraic irrationality, residual fractions, continued fractions, TDP-shape, the modules Tue, couple Tue, linear-fractional transformation of the second kind.

Bibliography: 37 titles.

1. Введение

В последнее время в работах Тульской школы теории чисел [5]–[11], [15]–[17], [24], [28]–[30] продолжены исследования из работ [4], [18] — [20], в которых изложены результаты длительных совместных исследований М. Н. Добровольского и его научного руководителя В. Д. Подсыпанина по теории иррациональностей 3-ей и 4-ой степеней. В основе этих исследований лежала теория полиномов А. Туэ и матричные многочленные разложения алгебраических иррациональностей.

Периодический характер разложения иррациональностей второй степени в непрерывную дробь известен ещё со времени Л. Эйлера (1737 г. [31], 1748 г. [32]), Ж. Лагранжа (1770 г. [34]) и Э. Галуа (1828 г. [33]). Закономерности в разложении в непрерывную дробь иррациональностей более высоких степеней до сих пор не известны. Лишь для некоторых иррациональностей найдены разложения в обобщенные непрерывные дроби, которые имеют малое применение в виду плохих приближений, даваемых ими.

Вопрос о характере разложения алгебраического числа α в непрерывную дробь связан с оценкой разности $\left|\alpha - \frac{p}{q}\right|$. Первой оценкой этой разности снизу явился результат Ж. Лиувилля [35]. Усиление этой оценки было получено А. Туэ [37] с помощью специальных полиномов. В дальнейшем оценки А. Туэ были уточнены. Наиболее сильный результат в оценке этой разности снизу был получен К. Ф. Ротом [36].

В настоящей работе продолжены исследования М. Н. Добровольского и В. Д. Подсыпанина. Принципиальное отличие их подхода в исследовании полиномов Туэ заключалось в поиске явного вида этих полиномов. Принцип Дирихле, позволяющий установить существование таких полиномов с заданными свойствами, был заменен на рекуррентные соотношения для основных полиномов Туэ порядка j и $j + 1$.

Данная работа является переработанным вариантом статьи [5]. Основная цель настоящего исследования — поиск зависимости полиномов Туэ остаточных дробей.

Отметим, что в работах [5], [4], [18] — [20] использовались разные определения полиномов Туэ, поэтому в данной работе пришлось для полноты изложения привести достаточные значительные фрагменты из работы [5] с необходимыми изменениями, которые даются для развития стройной теории полиномов Туэ.

2. Обозначения и необходимые факты

Как обычно, $\mathbb{Z}$ — кольцо целых рациональных чисел (говорим просто целых), а $\mathbb{Z}[x]$ — кольцо многочленов с целыми коэффициентами.

Через $\mathbb{Z}^*[x]$ будем обозначать мультипликативный моноид многочленов с целыми коэффициентами и старшим коэффициентом равным 1 (унитарные неприводимые многочлены).

Пусть $n \geqslant 2$ и $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ — неприводимый многочлен n-ой степени с целыми коэффициентами, а $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ — его корни, являющиеся алгебраически сопряженными целыми алгебраическими числами n-ой степени. Таким образом $a_n = 1$ и $\deg f(x) = n > 1$.

Будем говорить, что имеет место особый случай, если найдутся два корня α_ν и α_μ такие, что $\alpha_\mu = \frac{P(\alpha_\nu)}{Q(\alpha_\nu)}$, где многочлены $P(x)$, $Q(x) \in \mathbb{Z}[x]$. Если таких корней нет, то будем говорить, что имеется общий случай унитарного неприводимого многочлена.

Общий случай неприводимого многочлена $g(x) = b_nx^n + b_{n-1}x^{n-1} + \ldots + b_1x + b_0$ с алгебраически сопряженными алгебраическими числами n-ой степени $\beta = \beta_1, \beta_2, \ldots, \beta_n$ сводится к предыдущему переходом к многочлену $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ с коэффициентами $a_j = b_jb_n^{n-1-j}$ $(j = 0, 1, \ldots, n)$ и алгебраически сопряженными корнями $\alpha_j = b_n\beta_j$ $(j = 1, 2, \ldots, n)$ — целыми алгебраическими числами. Поэтому дальше будем рассматривать случай целых алгебраических чисел и неприводимого многочлена $f(x) \in \mathbb{Z}^*[x]$.

Кольцо целых алгебраических чисел $\mathbb{Z}[\alpha_\nu]$ определяется равенством

$$\mathbb{Z}[\alpha_\nu] = \left\{ m_0 + m_1\alpha_\nu + \ldots + m_{n-1}\alpha_\nu^{n-1} \middle| \, m_0, \ldots, m_{n-1} \in \mathbb{Z} \right\},$$

так как $\alpha_\nu^n = -(a_0 + a_1\alpha_\nu + \ldots + a_{n-1}\alpha_\nu^{n-1})$. Все кольца $\mathbb{Z}[\alpha_1], \ldots, \mathbb{Z}[\alpha_n]$ изоморфны между собой, так как для любых двух колец $\mathbb{Z}[\alpha_\nu]$ и $\mathbb{Z}[\alpha_\mu]$ имеется естественный изоморфизм, задаваемый соответствием $m_0 + m_1\alpha_\nu + \ldots + m_{n-1}\alpha_\nu^{n-1} \leftrightarrow m_0 + m_1\alpha_\mu + \ldots + m_{n-1}\alpha_\mu^{n-1}$. В общем случае неприводимого многочлена $f(x)$ все кольца $\mathbb{Z}[\alpha_1]$, $\ldots$, $\mathbb{Z}[\alpha_n]$ — различные и пересекаются только по $\mathbb{Z}$.

Имеем n изоморфных расширений $\mathbb{Z}[\alpha_1][x], \ldots, \mathbb{Z}[\alpha_n][x]$ кольца многочленов $\mathbb{Z}[x]$.

$\mathbb{Z}[\alpha_\nu][x]$ — кольцо полиномов (многочленов) над кольцом целых алгебраических чисел $\mathbb{Z}[\alpha_\nu]$. В общем случае неприводимого многочлена $f(x)$ все кольца полиномов $\mathbb{Z}[\alpha_1][x], \ldots, \mathbb{Z}[\alpha_n][x]$ — различные и пересекаются только по кольцу многочленов $\mathbb{Z}[x]$.

Мы будем говорить многочлены для элементов кольца $\mathbb{Z}[x]$ и полиномы — для $\mathbb{Z}[\alpha_\nu][x]$, при этом все полиномы попадающие в $\mathbb{Z}[x]$ являются многочленами.

Для дальнейшего нам понадобится разложение в кольце $\mathbb{Z}[\alpha_\nu][x]$ на полиномиальные множители унитарного неприводимого многочлена $f(x) \in \mathbb{Z}^*[x]$.

Лемма 1. *Справедливо равенство*

$$f(x) = (x - \alpha_\nu)f_\nu(x), \quad f_\nu(x) = \sum_{l=0}^{n-1} x^l \sum_{k=l+1}^{n} a_k\alpha_\nu^{k-l-1}, \tag{1}$$

при этом $(x - \alpha_\nu) \nmid f_\nu(x)$.

Доказательство. Действительно,

$$x^j - \alpha_\nu^j = (x-\alpha_\nu)\left(\sum_{l=0}^{j-1} x^l \alpha_\nu^{j-1-l}\right),$$

поэтому, так как $a_n = 1$,

$$f(x) = a_0 + \sum_{j=1}^{n} a_j x^j = a_0 + \sum_{j=1}^{n} a_j \left(\alpha_\nu^j + (x-\alpha_\nu)\left(\sum_{l=0}^{j-1} x^l \alpha_\nu^{j-1-l}\right)\right) =$$
$$= f(\alpha_\nu) + (x-\alpha_\nu)\sum_{j=1}^{n} a_j \left(\sum_{l=0}^{j-1} x^l \alpha_\nu^{j-1-l}\right) = (x-\alpha_\nu)\sum_{l=0}^{n-1} x^l \sum_{j=l+1}^{n} a_j \alpha_\nu^{j-1-l}$$

и первое утверждение леммы доказано.

Предположим противное, что $f_\nu(x) = (x-\alpha_\nu)g_\nu(x)$, тогда

$$f(x) = (x-\alpha_\nu)^2 g_\nu(x), \quad f'(x) = (x-\alpha_\nu)\left(2g_\nu(x) + (x-\alpha_\nu)g'_\nu(x)\right).$$

Если $d(x) = (f(x), f'(x))$ — наибольший общий делитель многочленов с целыми коэффициентами $f(x)$ и $f'(x)$, то $(x-\alpha_\nu)|d(x)$. Следовательно, степень $d(x)$ не меньше 1, что противоречит неприводимости многочлена $f(x)$, и лемма полностью доказана. □

Если через $\theta^{(1)} \in \mathbb{Z}[\alpha_1]$, ..., $\theta^{(n)} \in \mathbb{Z}[\alpha_n]$ обозначать набор сопряженных целых алгебраических чисел, то, переходя к полиномам, мы можем говорить о полном наборе сопряженных полиномов, а именно,

$$\mathcal{P}^{(1)}(x) = \sum_{j=0}^{k} \gamma_j^{(1)} x^j, \quad \ldots, \quad \mathcal{P}^{(m)}(x) = \sum_{j=0}^{k} \gamma_j^{(m)} x^j, \quad \ldots, \quad \mathcal{P}^{(n)}(t) = \sum_{j=0}^{k} \gamma_j^{(n)} x^j.$$

Также, как полный набор сопряженных целых алгебраических чисел является стационарным $\theta = \theta^{(1)} = \ldots = \theta^{(n)}$ тогда и только тогда, когда θ — целое рациональное число, и полный набор сопряженных полиномов является стационарным, если они суть один и тот же многочлен с целыми коэффициентами.

Примерами полного набора сопряженных многочленов могут служить:

1. $x-\alpha_1$, ..., $x-\alpha_n$ — полиномы первой степени;
2. $f_1(x)$, ..., $f_n(x)$ — полиномы степени $n-1$ из леммы 1;
3. $f(x)$, ..., $f(x)$ — стационарный набор полиномов-многочленов степени n.

Дадим следующее определение.

Определение 1. *Для произвольного полинома*

$$\mathcal{P}^{(\nu)}(x) = \sum_{j=0}^{k} \gamma_j^{(\nu)} x^j \in \mathbb{Z}[\alpha_\nu][x]$$

его многочленным представлением называется выражение вида

$$\mathcal{P}^{(\nu)}(x) = \sum_{l=0}^{n-1} \alpha_\nu^l p_l(x), \quad p_l(x) \in \mathbb{Z}[x] \quad (l = 0, 1, \ldots, n-1).$$

Многочлен $p_l(x)$ называется l-ой многочленной компонентой полинома $\mathcal{P}^{(\nu)}(x)$.

Теорема 1. *Для любого полинома $\mathcal{P}^{(\nu)}(x) \in \mathbb{Z}[\alpha_\nu][x]$ многочленное представление существует и единственное.*

Доказательство. Действительно, если

$$\mathcal{P}^{(\nu)}(x) = \sum_{j=0}^{k} \gamma_j^{(\nu)} x^j \in \mathbb{Z}[\alpha_\nu][x]$$

и

$$\gamma_j^{(\nu)} = \sum_{l=0}^{n-1} m_{l,j}\alpha_\nu^l, \quad m_{l,j} \in \mathbb{Z} \quad (j = 0, \ldots, k;\, l = 0, \ldots, n-1),$$

то

$$p_l(x) = \sum_{j=0}^{k} m_{l,j} x^j \,(l = 0, 1, \ldots, n-1), \quad \mathcal{P}^{(\nu)}(x) = \sum_{l=0}^{n-1} \alpha_\nu^l p_l(x)$$

и существование многочленного представления доказано.

Предположим, что существует два представления

$$\mathcal{P}^{(\nu)}(x) = \sum_{l=0}^{n-1} \alpha_\nu^l p_l(x) = \sum_{l=0}^{n-1} \alpha_\nu^l q_l(x),$$

тогда

$$\sum_{l=0}^{n-1} \alpha_\nu^l (p_l(x) - q_l(x)) = 0$$

для любого x. Так как хотя бы одна разность $p_l(x) - q_l(x)$ — ненулевой многочлен, то найдется целое число x_0 такое, что многочлен

$$g(t) = \sum_{l=0}^{n-1} t^l (p_l(x_0) - q_l(x_0))$$

— ненулевой многочлен степени не выше $n-1$ и α_ν — его корень, что противоречит неприводимости многочлена $f(x)$. Единственность многочленного представления доказана, и доказательство теоремы завершено. □

Теорема 2. *Полином $\mathcal{P}^{(\nu)}(x) \in \mathbb{Z}[\alpha_\nu][x]$ делится на многочлен $\varphi(x)$ тогда и только тогда, когда каждая многочленная компонента полинома $\mathcal{P}^{(\nu)}(x)$ делится на многочлен $\varphi(x)$.*

Доказательство. Достаточность очевидна.

Пусть полином $\mathcal{P}^{(\nu)}(x)$ делится на многочлен $\varphi(x)$,

$$\mathcal{P}^{(\nu)}(x) = \varphi(x)\mathcal{R}^{(\nu)}(x), \quad \mathcal{R}^{(\nu)}(x) \in \mathbb{Z}[\alpha_\nu][x]$$

и $p_l(x)$ $(l = 0, 1, \ldots, n-1)$ — его многочленные компоненты, а $r_l(x)$ $(l = 0, 1, \ldots, n-1)$ — многочленные компоненты для $\mathcal{R}^{(\nu)}(x)$. Тогда для полинома $\mathcal{P}^{(\nu)}(x)$ имеем второе многочленное представление

$$\mathcal{P}^{(\nu)}(x) = \sum_{l=0}^{n-1} \alpha_\nu^l \varphi(x) r_l(x).$$

Отсюда в силу предыдушей теоремы получаем

$$p_l(x) = \varphi(x) r_l(x) \quad (l = 0, 1, \ldots, n-1),$$

что и доказывает утверждение теоремы. □

Использование многочленного представления позволяет легко доказать теорему о произведении полного набора сопряженных полиномов.

Теорема 3. *Пусть $\mathcal{P}^{(1)}(x)$, $\ldots$, $\mathcal{P}^{(m)}(x)$, $\ldots$, $\mathcal{P}^{(n)}(t)$ — полный набор сопряженных полиномов, тогда их произведение является многочленом:*

$$\mathcal{P}^{(1)}(x)\cdot\ldots\cdot\mathcal{P}^{(m)}(x)\cdot\ldots\cdot\mathcal{P}^{(n)}(t)\in\mathbb{Z}[t].$$

Доказательство. Рассмотрим многочленное представление сопряженных полиномов, которые в силу сопряженности имеют одни и те же многочленные компоненты,

$$\mathcal{P}^{(\nu)}(x)=\sum_{l=0}^{n-1}\alpha_\nu^l p_l(x),\quad p_l(x)\in\mathbb{Z}[x]\quad (l=0,1,\ldots,n-1,\,\nu=1,\ldots,n).$$

Тогда, если S_n — симметрическая группа степени n и π — произвольная перестановка из S_n, то

$$\prod_{\nu=1}^{n}\mathcal{P}^{(\nu)}(x)=\sum_{k=1}^{n}\sum_{0\leqslant l_1<\ldots<l_k\leqslant n}\sum_{\substack{\lambda_1,\ldots,\lambda_k\geqslant 1,\\ \lambda_1+\ldots+\lambda_k=n}}\left(\prod_{\mu=1}^{k}p_{l_\mu}^{\lambda_\mu}(x)\right)\sum_{\pi\in S_n}\prod_{\tau=1}^{k}\prod_{\sum_{\gamma=1}^{\tau-1}\lambda_\gamma<\nu\leqslant\sum_{\gamma=1}^{\tau}\lambda_\gamma}\alpha_{\pi(\nu)}^{l_\tau}=$$

$$=\sum_{k=1}^{n}\sum_{0\leqslant l_1<\ldots<l_k}\sum_{\substack{\lambda_1,\ldots,\lambda_k\geqslant 1,\\ \lambda_1+\ldots+\lambda_k=n}}\left(\prod_{\mu=1}^{k}p_{l_\mu}^{\lambda_\mu}(x)\right)A(l_1,\lambda_1,\ldots,l_k,\lambda_k),$$

где

$$A(l_1,\lambda_1,\ldots,l_k,\lambda_k)=\sum_{\pi\in S_n}\prod_{\tau=1}^{k}\prod_{\sum_{\gamma=1}^{\tau-1}\lambda_\gamma<\nu\leqslant\sum_{\gamma=1}^{\tau}\lambda_\gamma}\alpha_{\pi(\nu)}^{l_\tau}$$

— симметрическая функция от полного набора сопряженных целых алгебраических чисел, а как известно (см. [25], стр. 23) такие функции имеют целые значения, поэтому искомое произведение есть многочлен, и теорема доказана. □

Обозначим через $\mathcal{M}_2(\mathbb{Z})$ кольцо квадратных целочисленных матриц второго порядка. Через $\mathcal{M}_2^*(\mathbb{Z})$ будем обозначать мультипликативную полугруппу кольца $\mathcal{M}_2(\mathbb{Z})$, то есть множество всех невырожденных матриц, а через $\mathcal{U}_2(\mathbb{Z})$ — мультипликативную группу обратимых целочисленных матриц, то есть множество унимодулярных матриц. Таким образом, имеем

$$M=\begin{pmatrix}A&B\\C&D\end{pmatrix}\in\mathcal{M}_2(\mathbb{Z}),\quad\text{если}\quad A,B,C,D\in\mathbb{Z};$$
$$M\in\mathcal{M}_2^*(\mathbb{Z}),\quad\text{если}\quad\det M=AD-BC\neq 0;$$
$$M\in\mathcal{U}_2(\mathbb{Z}),\quad\text{если}\quad\det M=\pm1.$$

Аналогичные конструкции нам потребуются для целочисленных многочленов.

$\mathcal{M}_2(\mathbb{Z}[t])$ — кольцо квадратных матриц второго порядка с целочисленными многочленами:

$$M[t]=\begin{pmatrix}A(t)&B(t)\\C(t)&D(t)\end{pmatrix}\in\mathcal{M}_2(\mathbb{Z}[t]),\quad\text{если}\quad A(t),B(t),C(t),D(t)\in\mathbb{Z}[t].$$

$\mathcal{M}_2^*(\mathbb{Z}[t])$ — мультипликативная полугруппа кольца $\mathcal{M}_2(\mathbb{Z}[t])$, то есть множество всех невырожденных матриц целочисленных многочленов:

$$M[t]\in\mathcal{M}_2^*(\mathbb{Z}[t]),\quad\text{если}\quad\det M[t]=A(t)D(t)-B(t)C(t)\neq 0.$$

$\mathcal{U}_2(\mathbb{Z}[t])$ — мультипликативная группа обратимых матриц целочисленных многочленов, то есть множество унимодулярных матриц целочисленных многочленов:

$$M[t]\in\mathcal{U}_2(\mathbb{Z}[t]),\quad\text{если}\quad\det M[t]=\delta(M[t])=\pm1,$$
$$M^{-1}[t]=\delta(M[t])\begin{pmatrix}D(t)&-B(t)\\-C(t)&A(t)\end{pmatrix}\in\mathcal{U}_2(\mathbb{Z}[t]).$$

3. Базисы двумерной решетки многочленов

Имея в виду цель — перенести некоторые конструкции из геометрии чисел на $\mathbb{Z}[t]$-модуль $\mathbb{Z}[t]^2$ — модуль Туэ, которые нам важны для дальнейшего, дадим следующие ниже определения. Название модуль Туэ связано с тем, что как мы увидим в последующих разделах, этот модуль тесно связан со всей конструкцией полиномов Туэ, играющих важную роль при решении диофантовых проблем теории чисел, связанных с приближением алгебраических чисел.

Определение 2. *Упорядоченная пара многочленов с целыми коэффициентами*

$$T = \{P(t), Q(t)\}$$

называется парой Туэ. Многочлен $P(t)$ называется числителем пары Туэ. Через $m(T)$ обозначается степень числителя. Многочлен $Q(t)$ называется знаменателем пары Туэ. Через $l(T)$ обозначается степень знаменателя. Величина $k(T) = \max(m(T), l(T))$ называется степенью пары Туэ.

Ясно, что множество всех пар Туэ совпадает с $\mathbb{Z}[t]^2 = \mathbb{Z}[t] \times \mathbb{Z}[t]$.

Определение 3. *Модулем Туэ называется множество всех пар Туэ с естественной операцией сложения, когда числитель суммы двух пар Туэ равен сумме числителей слагаемых, а знаменатель суммы — сумме знаменателей. Числитель произведения пары Туэ на многочлен из $\mathbb{Z}[t]$ равен произведению числителя пары на этот многочлен, а знаменатель произведения — произведению знаменателя на тот же многочлен.*

Определение 4. *Пусть имеется k пар Туэ $T_1 = \{P_1(t), Q_1(t)\}, \ldots, T_k = \{P_k(t), Q_k(t)\}$. Говорят, что они линейно зависимые, если существуют многочлены с целыми коэффициентами $c_1(t), \ldots, c_k(t)$, не все равные нулю и такие, что имеет место равенство*

$$c_1(t)T_1 + \ldots + c_k(t)T_k = \{0, 0\}. \tag{2}$$

Замечание 1. *Линейная зависимость пар, вообще говоря, не позволяет выразить одну пару через другие, не выходя за пределы $\mathbb{Z}[t]$-модуля $\mathbb{Z}[t]^2$.*

Замечание 2. *Если среди k пар хотя бы одна нулевая, то, очевидно, что они линейно зависимы.*

Лемма 2. *Любые две пары $T_1 = \{P_1(t), 0\}$ и $T_2 = \{P_2(t), 0\}$ — линейно зависимы. Любые две пары $U_1 = \{0, Q_1(t)\}$ и $U_2 = \{0, Q_2(t)\}$ — линейно зависимы.*

Доказательство. В силу замечания 2 достаточно рассмотреть случай $P_1(t) \neq 0$ и $P_2(t) \neq 0$, но тогда

$$P_2(t)T_1 - P_1(t)T_2 = \{0, 0\}$$

и первое утверждение леммы доказано.

Второе утверждение доказывается аналогично. □

Так как любая пара Туэ $T = \{P(t), Q(t)\}$ однозначно представима в виде

$$T = P(t)\{1, 0\} + Q(t)\{0, 1\}$$

и пары $T_0 = \{1, 0\}$, $T_1 = \{0, 1\}$ — линейно независимые, то пары T_0 и T_1 образуют базис модуля Туэ.

Таким образом, модуль Туэ $\mathbb{Z}[t]^2$ является унитарным свободным модулем ранга 2 над кольцом многочленов $\mathbb{Z}[t]$, то есть $\mathbb{Z}[t]$-модулем. Это, в частности, означает, что

$$\mathbb{Z}[t]^2 \cong \mathbb{Z}[t] \oplus \mathbb{Z}[t].$$

Определение 5. *Базисной матрицей Туэ называется матрица $M[t]$ вида*

$$M[t] = \begin{pmatrix} P(t) & Q(t) \\ R(t) & S(t) \end{pmatrix}, \tag{3}$$

такая, что две пары Туэ $T = \{P(t), Q(t)\}$ и $U = \{R(t), S(t)\}$ являются базисом для модуля Туэ.

Нетрудно видеть, что множество базисных матриц совпадает с унимодулярной группой $\mathcal{U}_2(\mathbb{Z}[t])$, которая кроме этого образует группу матриц перехода от одного базиса модуля Туэ к другому.

Через $M(T, U)$ для пар Туэ $T = \{P(t), Q(t)\}$ и $U = \{R(t), S(t)\}$ будем обозначать матрицу

$$M(T, U) = \begin{pmatrix} P(t) & Q(t) \\ R(t) & S(t) \end{pmatrix}.$$

Лемма 3. *Две пары Туэ $T = \{P(t), Q(t)\}$ и $U = \{R(t), S(t)\}$ — линейно зависимые тогда и только тогда, когда*

$$\det M(T, U) = 0.$$

Доказательство. Действительно, если они линейно зависимые, то найдутся многочлены $c_1(t)$ и $c_2(t)$ одновременно неравные тождественно нулю, такие что $c_1(t)T + c_2(t)U = \{0, 0\}$ и, следовательно, $c_1(t)P(t) + c_2(t)R(t) = 0$ и $c_1(t)Q(t) + c_2(t)S(t) = 0$. Пусть $c_1(t) \neq 0$, тогда

$$c_1(t)\left(P(t)S(t) - R(t)Q(t)\right) = (-c_2(t)R(t))S(t) - R(t)(-c_2(t)S(t)) = 0.$$

Так как $\mathbb{Z}[t]$ — кольцо без делителей нуля, то $P(t)S(t) - R(t)Q(t) = 0$, и необходимость доказана.

Перейдём к доказательству достаточности. В силу замечания 2 и леммы 2 достаточно рассмотреть случай, когда следующие два многочлена $c_1(t) = S(t)P(t) = R(t)Q(t)$, $c_2(t) = -Q(t)P(t)$ отличны от нуля.

Пусть $P(t)S(t) - R(t)Q(t) = 0$, тогда

$$\begin{gathered} c_1(t)T + c_2(t)U = \{c_1(t)P(t) + c_2(t)R(t), c_1(t)Q(t) + c_2(t)S(t)\} = \\ = \{R(t)Q(t)P(t) - Q(t)P(t)R(t), S(t)P(t)Q(t) - Q(t)P(t)S(t)\} = \{0, 0\} \end{gathered}$$

и достаточность доказана, что заканчивает доказательство леммы. □

Определение 6. *Пара Туэ $T = \{P(t), Q(t)\}$ называется примитивной, если наибольший общий делитель числителя и знаменателя $(P(t), Q(t)) = 1$.*

Лемма 4. *Если пары Туэ $T = \{P(t), Q(t)\}$ и $U = \{R(t), S(t)\}$ — примитивные и $\det M(T, U) = 0$, то $T = U$.*

Доказательство. Действительно, из равенства $P(t)S(t) = R(t)Q(t)$ и факториальности кольца $\mathbb{Z}[t]$ в силу примитивности пар следует $P(t) = R(t)$ и $S(t) = Q(t)$, что и доказывает утверждение леммы. □

Определение 7. *Наибольшим делителем $d(T)$ пары Туэ $T = \{P(t), Q(t)\}$ называется наибольший общий делитель числителя и знаменателя:*

$$d(T) = (P(t), Q(t)).$$

Ясно, что любую пару Туэ $T = \{P(t), Q(t)\}$ можно представить в виде

$$T = d(T)\left\{\frac{P(t)}{d(T)}, \frac{Q(t)}{d(T)}\right\}$$

и пара Туэ $\left\{\frac{P(t)}{d(T)}, \frac{Q(t)}{d(T)}\right\}$ — примитивная пара, которую будем обозначать через $\frac{T}{d(T)}$.

Определение 8. *Если для двух пар Туэ*

$$T = \{P(t), Q(t)\} \quad \text{и} \quad U = \{R(t), S(t)\}$$

$\det M(T,U) \neq 0$, *то двумерной решеткой многочленов* $\Lambda(T,U)$ *с базисом* $/T,U/$, *базисной матрицей* $M(T,U)$ *и детерминантом решетки многочленов* $\det \Lambda(T,U) = \det M(T,U)$ *называется множество вида*

$$\Lambda(T,U) = \{c_1(t)T + c_2(t)U \,|\, c_1(t),\, c_2(t) \in \mathbb{Z}[t]\}\,.$$

Таким образом, в силу линейной независимости пар T и U двумерная решетка многочленов $\Lambda(T,U)$ является свободным $\mathbb{Z}[t]$-модулем ранга 2.

4. О $\mathbb{Z}[t]$-модуле $\mathbb{Z}[t]^2$ и его подмодулях с одним линейным определяющем соотношением

Через $< T,U >= \{c_1(t)T + c_2(t)U \,|\, c_1(t), c_2(t) \in \mathbb{Z}[t]\}$ будем обозначать подмодуль пар Туэ, порожденный парами T и U. Если T и U линейно независимые пары Туэ, то подмодуль $< T,U >$ — свободный $\mathbb{Z}[t]$-модуль ранга 2 (см. [13], стр. 164). Матрицу $M(T,U)$ будем называть базисной матрицей подмодуля $< T,U >$.

Таким образом, если пары T и U линейно независимые, то подмодуль $< T,U >$ является двумерной решеткой многочленов $\Lambda(T,U)$.

Теорема 4. *Если пары Туэ T и U линейно независимые и матрица*

$$C[t] = \begin{pmatrix} c_{1,1}(t) & c_{1,2}(t) \\ c_{2,1}(t) & c_{2,2}(t) \end{pmatrix} \in \mathcal{M}_2^*(\mathbb{Z}[t])\,,$$

то для пар $T_1 = c_{1,1}(t)T + c_{1,2}(t)U$, $U_1 = c_{2,1}(t)T + c_{2,2}(t)U$ и модуля $< T_1, U_1 >$ справедливы соотношения

$$\begin{cases} < T_1, U_1 >=< T,U >, & \text{если } C[t] \in \mathcal{U}_2(\mathbb{Z}[t])\,, \\ < T_1, U_1 >\subset< T,U >, & \text{если } C[t] \notin \mathcal{U}_2(\mathbb{Z}[t])\,, \end{cases}$$

и $M(T,U) = C[t]M(T_1,U_1)$.

Доказательство. Действительно, если $C[t] \in \mathcal{U}_2(\mathbb{Z}[t])$, то пары T и U линейно выражаются через пары T_1 и U_1 с помощью обратной матрицы из $\mathcal{U}_2(\mathbb{Z}[t])$, в противном случае её просто не существует. Все остальные утверждения непосредственно следуют из определений и свойств матричного умножения. □

Теорема 5. *Если пары Туэ T и U линейно зависимые, то справедливо равенство*

$$< T,U >= J \cdot V,$$

где $V = \frac{T}{d(T)} = \frac{U}{d(U)}$ — *примитивная пара Туэ, а* $J =< d(T), d(U) >$ — *идеал в кольце целочисленных многочленов* $\mathbb{Z}[t]$, *порожденный наибольшими делителями пар.*

Доказательство. Действительно,

$$\det M(T,U) = d(T)d(U)\det M\left(\frac{T}{d(T)}, \frac{U}{d(U)}\right).$$

Из линейной зависимости пар Туэ T и U и факториальности кольца $\mathbb{Z}[t]$ в силу леммы 3 следует линейная зависимость соответствующих примитивных пар. Поэтому по лемме 4 они равны. Следовательно, примитивная пара V корректно определена. Но тогда

$$< T,U >= \{c_1(t)d(T)V + c_2(t)d(U)V | c_1(t), c_2(t) \in \mathbb{Z}[t]\} = J \cdot V,$$

где идеал $J =< d(T), d(U) >$ порожден наибольшими делителями пар, и теорема доказана. □

Теорема 6. *Любые три пары Туэ линейно-зависимы.*

Доказательство. Пусть имеем три пары Туэ

$$T_1 = \{P_1(t), Q_1(t)\},\ T_2 = \{P_2(t), Q_2(t)\},\ T_3 = \{P_3(t), Q_3(t)\}.$$

Положим

$$c_1(t) = P_2(t)Q_3(t) - P_3(t)Q_2(t),\ c_2(t) = P_3(t)Q_1(t) - P_1(t)Q_3(t),\ c_3(t) = P_1(t)Q_2(t) - P_2(t)Q_1(t).$$

Достаточно рассмотреть случай когда среди этих трех пар нет нулевой пары и не для каких двух пар не выполнены условия леммы 3 (см. стр. 61), тогда все три многочлена $c_1(t)$, $c_2(t)$, $c_3(t)$ отличны от нуля.

Непосредственно убеждаемся, что

$$c_1(t)T_1 + c_2(t)T_2 + c_3(t)T_3 = \{0, 0\}$$

и теорема доказана. □

Определение 9. *Пусть $f(t)$ — унитарный, неприводимый многочлен с целыми коэффициентами, а $(f(t)) = f(t)\mathbb{Z}[t]$ — главный идеал в $\mathbb{Z}[t]$, порожденный многочленом $f(t)$. Пусть $a(t)$, $b(t)$ — произвольные многочлены из $\mathbb{Z}[t]$. Будем говорить, что пара Туэ $T = \{P(t), Q(t)\}$ удовлетворяет линейному определяющему соотношению, если $a(t)P(t) + b(t)Q(t) \in (f(x))$. Подмодулем с одним определяющим соотношением назовем множество*

$$M(a(t), b(t) \,|\, f(t)) = \{\{P(t), Q(t)\} \,|\, a(t)P(t) + b(t)Q(t) \in (f(x))\}$$

— всех пар Туэ, удовлетворяющих этому линейному определяющему соотношению.

Если $a(t) \equiv 0 \pmod{f(t)}$ и $b(t) \equiv 0 \pmod{f(t)}$, то определяющему соотношению удовлетворяют все пары Туэ, и этот тривиальный случай исключается из дальнейших рассмотрений.

Пусть $a(t) \equiv 0 \pmod{f(t)}$ и $b(t) \not\equiv 0 \pmod{f(t)}$, тогда на числитель пары не накладывается никаких ограничений, а знаменатель будет принадлежать главному идеалу $(f(t))$. Если $a(t) \not\equiv 0 \pmod{f(t)}$ и $b(t) \equiv 0 \pmod{f(t)}$, то числитель и знаменатель пары Туэ меняются ролями.

Поэтому все перечисленные тривиальные случаи исключаются, и дальше рассматриваем только случай $a(t)b(t) \not\equiv 0 \pmod{f(t)}$.

Далее заметим, что если

$$d(t) \not\equiv 0 \pmod{f(t)},\quad a(t) \equiv a_1(t) \pmod{f(t)},\quad b(t) \equiv b_1(t) \pmod{f(t)},$$

то справедливы равенства

$$M(a(t)d(t), b(t)d(t) \,|\, f(t)) = M(a(t), b(t) \,|\, f(t)) = M(a_1(t), b_1(t) \,|\, f(t)).$$

Поэтому, окончательно, выделяем для дальнейшего рассмотрения только случай

$$a(t) \not\equiv 0, \quad b(t) \not\equiv 0 \pmod{f(t)}, \quad \max(\deg a(t), \deg b(t)) < \deg f(t), \quad (a(t), b(t)) = 1. \tag{4}$$

Из определения непосредственно следует, что свободный модуль ранга 2

$$f(t)\mathbb{Z}[t]^2 \subset M(a(t), b(t) \,|\, f(t)).$$

В частности, линейно независимые пары $T_0 = \{f(t), 0\}$ и $T_1 = \{0, f(t)\}$ принадлежат $M(a(t), b(t)|f(t))$.

Нетрудно указать пару из $M(a(t), b(t) \,|\, f(t)) \setminus f(t)\mathbb{Z}[t]^2$. Такой парой будет пара

$$T_3 = \{b(t), -a(t)\}.$$

Более того, если через $M(a(t), b(t))$ обозначить вырожденный случай определяющего соотношения: $a(t)P(t) + b(t)Q(t) = 0$, то при $(a(t), b(t)) = 1$ имеем равенство

$$M(a(t), b(t)) = \{\{b(t)c(t), -a(t)c(t)\} \,|\, c(t) \in \mathbb{Z}[t]\} = \{b(t), -a(t)\} \cdot \mathbb{Z}[t].$$

Очевидно, что справедливо включение

$$M(a(t), b(t)) \subset M(a(t), b(t) \,|\, f(t))$$

для любого унитарного, неприводимого многочлена $f(t)$ с целыми коэффициентами.

Лемма 5. *Если $T = \{P(t), Q(t)\}$ и $U = \{R(t), S(t)\}$ — две пары Туэ из $M(a(t), b(t) \,|\, f(t))$, то*

$$P(t)S(t) - R(t)Q(t) = f(t)\varphi(t), \quad \varphi(t) \in \mathbb{Z}[t].$$

Доказательство. Так как T и U из $M(a(t), b(t) \,|\, f(t))$, то по определению

$$a(t)P(t) + b(t)Q(t) = c_1(t)f(t), \quad a(t)R(t) + b(t)S(t) = c_2(t)f(t),$$

где $c_1(t), c_2(t) \in \mathbb{Z}[t]$.

Пользуясь этими равенствами, получим

$$a(t)b(t)\left(P(t)S(t) - R(t)Q(t)\right) = a(t)b(t)P(t)S(t) - (c_1(t)f(t) - a(t)P(t))(c_2(t)f(t) - b(t)S(t)) =$$
$$= f(t)\left(c_1(t)b(t)S(t) + c_2(t)a(t)P(t) - c_1(t)c_2(t)f(t)\right).$$

Так как по условию $(a(t)b(t), f(t)) = 1$, то $a(t)b(t)|c_1(t)b(t)S(t) + c_2(t)a(t)P(t) - c_1(t)c_2(t)f(t)$ и

$$\varphi(t) = \frac{c_1(t)b(t)S(t) + c_2(t)a(t)P(t) - c_1(t)c_2(t)f(t)}{a(t)b(t)} \in \mathbb{Z}[t]$$

что и доказывает лемму. □

Лемма 6. *Если $T = \{P(t), Q(t)\}$ пара Туэ из $M(a(t), b(t) \,|\, f(t))$, то*

$$T + f(t) \cdot \mathbb{Z}^2[t] \subset M(a(t), b(t) \,|\, f(t)).$$

Доказательство. Так как $f(t) \cdot \mathbb{Z}^2[t] \subset M(a(t), b(t) \,|\, f(t))$ и

$$T = \{P(t), Q(t)\} \in M(a(t), b(t) \,|\, f(t)),$$

то по свойствам модуля получаем утверждение леммы. □

Теорема 7. *Существуют две линейно-независимые, примитивные пары Туэ T, U степени меньше n из $M(a(t), b(t) \mid f(t))$ такие, что любая пара Туэ V из $M(a(t), b(t) \mid f(t))$ однозначно представима в виде*

$$V = c_1(t)T + c_2(t)U, \tag{5}$$

где $c_1(t)$ и $c_2(t)$ — многочлены с целыми коэффициентами.

Доказательство. Возьмем в качестве T одну из пар Туэ, принадлежащих

$$M(a(t), b(t) \mid f(t)),$$

наименьшей степени m. Так как пара $\{b(t), -a(t)\} \in M(a(t), b(t)) \subset M(a(t), b(t) \mid f(t))$, то степень $m < n$. Пусть пара $T = \{P(t), Q(t)\}$. Если $d(T) \neq 1$, то $(d(T), f(t)) = 1$ и из равенства

$$a(t)P(t) + b(t)Q(t) = \varphi(t)f(t)$$

следует, что $d(T) \mid \varphi(t)$ и для $P_1(t) = \frac{P(t)}{d(T)}$, $Q_1(t) = \frac{Q(t)}{d(T)}$, $\varphi_1(t) = \frac{\varphi(t)}{d(T)} \in \mathbb{Z}[t]$ справедливо соотношение

$$a(t)P_1(t) + b(t)Q_1(t) = \varphi_1(t)f(t), \quad \{P_1(t), Q_1(t)\} \in M(a(t), b(t) \mid f(t)).$$

Поэтому можно без ограничения общности считать, что пара T — примитивная пара Туэ из $M(a(t), b(t) \mid f(t))$ наименьшей степени m. При этом, легко видеть, что такая примитивная пара Туэ не может иметь вид $\{P(t), 0\}$ или $\{0, Q(t)\}$.

Отсюда следует, что пары Туэ $T_0 = \{f(t), 0\}$ и $T_1 = \{0, f(t)\}$ из $M(a(t), b(t) \mid f(t))$ обе линейно независимы с T. Пусть для определенности степень этой пары Туэ $T = \{P(t), Q(t)\}$ равна степени числителя пары и старший коэффициент числителя равен p_0, а знаменателя — q_0, то есть

$$P(t) = p_0 t^m + P_1(t), \quad P_1(t) = \sum_{\nu=1}^{m} p_\nu t^{m-\nu}, \quad Q(t) = q_0 t^{m_1} + Q_1(t), \quad Q_1(t) = \sum_{\nu=1}^{m_1} q_\nu t^{m_1-\nu}, \quad m_1 \leqslant m.$$

Рассмотрим пару Туэ T', заданную равенством

$$T' = \begin{cases} \{t^{n-m}P(t) - p_0 f(t), t^{n-m}Q(t)\}, & \text{если } m_1 < m, \\ \{t^{n-m}P(t) - p_0 f(t), t^{n-m}Q(t) - q_0 f(t)\}, & \text{если } m_1 = m. \end{cases}$$

Ясно, что пара Туэ $T' \in M(a(t), b(t) \mid f(t))$ и линейно независима от пары Туэ $T = \{P(t), Q(t)\}$, кроме того её степень меньше n.

Следовательно, существуют пары Туэ из $M(a(t), b(t) \mid f(t))$ линейно независимые с T. Пусть U одна из этих пар Туэ наименьшей степени k. Из предыдущего следует, что $k < n$. Аналогично случаю пары T, можно считать, что U — примитивная пара Туэ из $M(a(t), b(t) \mid f(t))$ наименьшей степени k.

Пусть такие выбранные примитивные пары Туэ имеют вид:

$$T = \left\{ \sum_{\nu=0}^{m} g_\nu t^{m-\nu}, \sum_{\nu=0}^{m} h_\nu t^{m-\nu} \right\}, \quad U = \left\{ \sum_{\nu=0}^{k} u_\nu t^{k-\nu}, \sum_{\nu=0}^{k} v_\nu t^{k-\nu} \right\}.$$

По выбору пар $m \leqslant k < n$.

Далее для выбранных пар

$$g_0 v_0 - h_0 u_0 \neq 0, \tag{6}$$

так как в противном случае пара $u_0t^{k-m}T - g_0U = \{P(t), Q(t)\}$, где

$$P(t) = \sum_{\nu=0}^{m}(u_0g_\nu - g_0u_\nu)t^{k-\nu} - \sum_{\nu=m+1}^{k} g_0u_\nu t^{k-\nu} = \sum_{\nu=1}^{m}(u_0g_\nu - g_0u_\nu)t^{k-\nu} - \sum_{\nu=m+1}^{k} g_0u_\nu t^{k-\nu},$$

$$Q(t) = \sum_{\nu=0}^{m}(u_0h_\nu - g_0v_\nu)t^{k-\nu} - \sum_{\nu=m+1}^{k} g_0v_\nu t^{k-\nu} = \sum_{\nu=1}^{m}(u_0h_\nu - g_0v_\nu)t^{k-\nu} - \sum_{\nu=m+1}^{k} g_0v_\nu t^{k-\nu},$$

линейно независима с парой T и имеет степень меньшую k. Но это противоречит выбору пары U.

Предположим существование пар из $M(a(t), b(t) \mid f(t))$ и не представимых через T, U по формуле (5). Пусть W является такой парой наименьшей степени l и имеет вид

$$W = \left\{\sum_{\nu=0}^{l} p_\nu t^{l-\nu}, \sum_{\nu=0}^{l} q_\nu t^{l-\nu}\right\}.$$

Очевидно, что $l \geqslant k \geqslant m$.

Рассмотрим пару

$$\{R(t), S(t)\} = (u_0q_0 - p_0v_0)t^{l-m}T + (p_0h_0 - q_0g_0)t^{l-k}U + (g_0v_0 - u_0h_0)W$$

$$R(t) = (u_0q_0 - p_0v_0)\sum_{\nu=0}^{m} g_\nu t^{l-\nu} + (p_0h_0 - q_0g_0)\sum_{\nu=0}^{k} u_\nu t^{l-\nu} + (g_0v_0 - u_0h_0)\sum_{\nu=0}^{l} p_\nu t^{l-\nu} =$$

$$= (u_0q_0 - p_0v_0)\sum_{\nu=1}^{m} g_\nu t^{l-\nu} + (p_0h_0 - q_0g_0)\sum_{\nu=1}^{k} u_\nu t^{l-\nu} + (g_0v_0 - u_0h_0)\sum_{\nu=1}^{l} p_\nu t^{l-\nu},$$

$$S(t) = (u_0q_0 - p_0v_0)\sum_{\nu=0}^{m} h_\nu t^{l-\nu} + (p_0h_0 - q_0g_0)\sum_{\nu=0}^{k} v_\nu t^{l-\nu} + (g_0v_0 - u_0h_0)\sum_{\nu=0}^{l} q_\nu t^{l-\nu} =$$

$$= (u_0q_0 - p_0v_0)\sum_{\nu=1}^{m} h_\nu t^{l-\nu} + (p_0h_0 - q_0g_0)\sum_{\nu=1}^{k} v_\nu t^{l-\nu} + (g_0v_0 - u_0h_0)\sum_{\nu=1}^{l} q_\nu t^{l-\nu}.$$

Эта пара не представима через пары T, U и имеет степень меньшую l. Но это противоречит выбору пары W. Полученное противоречие доказывает утверждение теоремы. □

Из доказанной теоремы следует, что подмодуль с одним определяющим соотношением $M(a(t), b(t) \mid f(t))$ является двумерной решеткой многочленов $\Lambda(T, U)$ с базисом $/T, U/$, причём базис примитивный, то есть обе пары Туэ T и U являются примитивными парами, и степень каждой пары меньше n.

Теорема 8. *Для двумерной решётки многочленов $\Lambda(T, U) = M(a(t), b(t) \mid f(t))$ справедливо равенство*

$$\det \Lambda(T, U) = \det M(T, U) = \pm f(t). \tag{7}$$

Доказательство. Прежде всего, заметим, что пары $T_1 = \{f(t), 0\}$ и $T_2 = \{0, f(t)\}$ принадлежат решётке $\Lambda(T, U) = M(a(t), b(t) \mid f(t))$.

Пусть базис $/T, U/$ имеет вид $T = \{P(t), Q(t)\}$, $U = \{R(t), S(t)\}$, тогда, согласно лемме 5, имеем: $P(t)S(t) - Q(t)R(t) = \varphi_0(t)f(t)$ и найдутся целочисленные многочлены $c_{\nu,\mu}(t)$ ($\nu = 1, 2$; $\mu = 1, 2$) такие, что выполнены равенства

$$\left\{\begin{array}{l} c_{1,1}(t)P(t) + c_{1,2}(t)R(t) = f(t) \\ c_{1,1}(t)Q(t) + c_{1,2}(t)S(t) = 0 \\ c_{2,1}(t)P(t) + c_{2,2}(t)R(t) = 0 \\ c_{2,1}(t)Q(t) + c_{2,2}(t)S(t) = f(t) \end{array}\right. . \tag{8}$$

Отсюда следует, что

$$\begin{cases} c_{1,1}(t)(P(t)S(t)-Q(t)R(t)) = f(t)S(t) \\ c_{1,2}(t)(P(t)S(t)-Q(t)R(t)) = -f(t)Q(t) \\ c_{2,1}(t)(P(t)S(t)-Q(t)R(t)) = -f(t)R(t) \\ c_{2,2}(t)(P(t)S(t)-Q(t)R(t)) = f(t)P(t) \end{cases} . \tag{9}$$

Из (9) вытекает, что

$$\begin{cases} c_{1,1}(t)\varphi_0(t) = S(t) \\ c_{1,2}(t)\varphi_0(t) = -Q(t) \\ c_{2,1}(t)\varphi_0(t) = -R(t) \\ c_{2,2}(t)\varphi_0(t) = P(t) \end{cases} . \tag{10}$$

Из примитивности пар Туэ T и U делаем вывод, что $\varphi_0(t) = c(T,U) = \pm 1$ и теорема доказана. □

Дадим теперь обобщающее определение подмодуля с одним определяющим соотношением.

Определение 10. *Пусть $f(t)$ — унитарный, неприводимый многочлен с целыми коэффициентами, а $(f^k(t)) = f^k(t)\mathbb{Z}[t]$ — главный идеал в $\mathbb{Z}[t]$, порожденный k-ой степенью многочлена $f(t)$. Пусть $a(t)$, $b(t)$ — произвольные многочлены из $\mathbb{Z}[t]$. Будем говорить, что пара Туэ $T = \{P(t), Q(t)\}$ удовлетворяет линейному определяющему соотношению k-ого порядка, если $a(t)P(t) + b(t)Q(t) \in (f^k(x))$. Подмодулем с одним определяющим соотношением k-ого порядка назовем множество $M(a(t), b(t) \,|\, f^k(t))$ всех пар Туэ, удовлетворяющих этому линейному определяющему соотношению k-ого порядка.*

Если $a(t) \equiv 0 \pmod{f^k(t)}$ и $b(t) \equiv 0 \pmod{f^k(t)}$, то определяющему соотношению k-ого порядка удовлетворяют все пары Туэ, и этот тривиальный случай исключается из дальнейших рассмотрений.

Пусть $a(t) \equiv 0 \pmod{f^k(t)}$ и $b(t) \not\equiv 0 \pmod{f^k(t)}$, тогда на числитель пары не накладывается никаких ограничений, а знаменатель будет принадлежать главному идеалу $(f^k(t))$. Если $a(t) \not\equiv 0 \pmod{f^k(t)}$ и $b(t) \equiv 0 \pmod{f^k(t)}$, то числитель и знаменатель пары Туэ меняются ролями.

Поэтому все перечисленные тривиальные случаи исключаются, и дальше рассматриваем только случай $a(t)b(t) \not\equiv 0 \pmod{f(t)}$.

Далее заметим, что если

$$d(t) \not\equiv 0 \pmod{f(t)}, \quad a(t) \equiv a_1(t) \pmod{f^k(t)}, \quad b(t) \equiv b_1(t) \pmod{f^k(t)},$$

то справедливы равенства

$$M(a(t)d(t), b(t)d(t) \,|\, f^k(t)) = M(a(t), b(t) \,|\, f^k(t)) = M(a_1(t), b_1(t) \,|\, f^k(t)).$$

Поэтому, окончательно, выделяем для дальнейшего рассмотрения только случай

$$a(t) \not\equiv 0, \quad b(t) \not\equiv 0 \pmod{f(t)}, \quad \max(\deg a(t), \deg b(t)) < k \deg f(t), \quad (a(t), b(t)) = 1. \tag{11}$$

Из определения непосредственно следует, что свободный модуль ранга 2

$$f^k(t)\mathbb{Z}[t]^2 \subset M(a(t), b(t) \,|\, f^k(t)).$$

В частности, линейно независимые пары $T_0 = \{f^k(t), 0\}$ и $T_1 = \{0, f^k(t)\}$ принадлежат $M(a(t), b(t) \,|\, f^k(t))$.

Нетрудно указать пару из $M(a(t),b(t)\,|\,f^k(t))\setminus f^k(t)\mathbb{Z}[t]^2$. Такой парой будет пара

$$T_3=\{b(t),-a(t)\}.$$

Очевидно, что справедливо включение

$$M(a(t),b(t))\subset M(a(t),b(t)\,|\,f^{k+1}(t))\subset M(a(t),b(t)\,|\,f^k(t))\subset M(a(t),b(t)\,|\,f(t))$$

для любого унитарного, неприводимого многочлена $f(t)$ с целыми коэффициентами и любого натурального k.

Лемма 7. *Если $T=\{P(t),Q(t)\}$ и $U=\{R(t),S(t)\}$ — две пары Туэ из $M(a(t),b(t)\,|\,f^k(t))$, то*

$$P(t)S(t)-R(t)Q(t)=f^k(t)\varphi(t),\quad \varphi(t)\in\mathbb{Z}[t].$$

Доказательство. Так как T и U из $M(a(t),b(t)\,|\,f^k(t))$, то по определению

$$a(t)P(t)+b(t)Q(t)=c_1(t)f^k(t),\quad a(t)R(t)+b(t)S(t)=c_2(t)f^k(t),$$

где $c_1(t),c_2(t)\in\mathbb{Z}[t]$.

Пользуясь этими равенствами, получим

$$\begin{gathered}a(t)b(t)\left(P(t)S(t)-R(t)Q(t)\right)=\\=a(t)b(t)P(t)S(t)-(c_1(t)f^k(t)-a(t)P(t))(c_2(t)f^k(t)-b(t)S(t))=\\=f^k(t)\Big(c_1(t)b(t)S(t)+c_2(t)a(t)P(t)-c_1(t)c_2(t)f^k(t)\Big).\end{gathered}$$

Так как по условию $(a(t)b(t),f(t))=1$, то $a(t)b(t)|c_1(t)b(t)S(t)+c_2(t)a(t)P(t)-c_1(t)c_2(t)f^k(t)$ и

$$\varphi(t)=\frac{c_1(t)b(t)S(t)+c_2(t)a(t)P(t)-c_1(t)c_2(t)f^k(t)}{a(t)b(t)}\in\mathbb{Z}[t]$$

что и доказывает лемму. □

Лемма 8. *Если $T=\{P(t),Q(t)\}$ пара Туэ из $M(a(t),b(t)\,|\,f^k(t))$, то*

$$T+f^k(t)\cdot\mathbb{Z}^2[t]\subset M(a(t),b(t)\,|\,f^k(t)).$$

Доказательство. Так как $f^k(t)\cdot\mathbb{Z}^2[t]\subset M(a(t),b(t)\,|\,f^k(t))$ и

$$T=\{P(t),Q(t)\}\in M(a(t),b(t)\,|\,f^k(t)),$$

то по свойствам модуля получаем утверждение леммы. □

Теорема 9. *Существуют две линейно-независимые, примитивные пары Туэ T_k, U_k степени меньше nk из подмодуля с одним определяющим соотношением k-ого порядка $M(a(t),b(t)\,|\,f^k(t))$ такие, что любая пара Туэ V из $M(a(t),b(t)\,|\,f^k(t))$ однозначно представима в виде*

$$V=c_1(t)T_k+c_2(t)U_k, \tag{12}$$

где $c_1(t)$ и $c_2(t)$ — многочлены с целыми коэффициентами.

Доказательство. Возьмем в качестве T_k одну из пар Туэ, принадлежащих

$$M(a(t), b(t) \,|\, f^k(t)),$$

наименьшей степени m. Так как пара $\{b(t), -a(t)\} \in M(a(t), b(t)) \subset M(a(t), b(t) \,|\, f^k(t))$, то степень $m < n$. Пусть пара $T = \{P(t), Q(t)\}$. Если $d(T) \neq 1$, то $(d(T), f(t)) = 1$ и из равенства

$$a(t)P(t) + b(t)Q(t) = \varphi(t)f^k(t)$$

следует, что $d(T) \,|\, \varphi(t)$ и для $P_1(t) = \frac{P(t)}{d(T)}$, $Q_1(t) = \frac{Q(t)}{d(T)}$, $\varphi_1(t) = \frac{\varphi(t)}{d(T)} \in \mathbb{Z}[t]$ справедливо соотношение

$$a(t)P_1(t) + b(t)Q_1(t) = \varphi_1(t)f^k(t), \quad \{P_1(t), Q_1(t)\} \in M(a(t), b(t) \,|\, f^k(t)).$$

Поэтому можно без ограничения общности считать, что пара T — примитивная пара Туэ из $M(a(t), b(t) \,|\, f^k(t))$ наименьшей степени m. При этом, легко видеть, что такая примитивная пара Туэ не может иметь вид $\{P(t), 0\}$ или $\{0, Q(t)\}$.

Пары Туэ $T_{k,0} = \{f^k(t), 0\}$ и $T_{k,1} = \{0, f^k(t)\}$ из $M(a(t), b(t) \,|\, f^k(t))$ одновременно линейно независимы с T_k.

Пусть для определенности степень этой пары Туэ $T_k = \{P(t), Q(t)\}$ равна степени числителя пары и старший коэффициент числителя равен p_0, а знаменателя — q_0, то есть

$$P(t) = p_0t^m + P_1(t), \quad P_1(t) = \sum_{\nu=1}^{m} p_\nu t^{m-\nu}, \quad Q(t) = q_0t^{m_1} + Q_1(t), \quad Q_1(t) = \sum_{\nu=1}^{m_1} q_\nu t^{m_1-\nu}, \quad m_1 \leqslant m.$$

Рассмотрим пару Туэ T', заданную равенством

$$T' = \begin{cases} \{t^{nk-m}P(t) - p_0f^k(t), t^{nk-m}Q(t)\}, & \text{если } m_1 < m, \\ \{t^{nk-m}P(t) - p_0f^k(t), t^{nk-m}Q(t) - q_0f^k(t)\}, & \text{если } m_1 = m. \end{cases}$$

Ясно, что пара Туэ $T' \in M(a(t), b(t) \,|\, f^k(t))$ и линейно независима от пары Туэ $T_k = \{P(t), Q(t)\}$, кроме того её степень меньше nk.

Следовательно, существуют пары Туэ из $M(a(t), b(t) \,|\, f^k(t))$ линейно независимые с T_k. Пусть U_k одна из этих пар Туэ наименьшей степени s. Из предыдущего следует, что $s < nk$. Аналогично случаю пары T_k, можно считать, что U_k — примитивная пара Туэ из $M(a(t), b(t) \,|\, f^k(t))$ наименьшей степени $s < nk$.

Пусть такие выбранные пары Туэ имеют вид:

$$T_k = \left\{\sum_{\nu=0}^{m} g_\nu t^{m-\nu}, \sum_{\nu=0}^{m} h_\nu t^{m-\nu}\right\}, \quad U_k = \left\{\sum_{\nu=0}^{s} u_\nu t^{s-\nu}, \sum_{\nu=0}^{s} v_\nu t^{s-\nu}\right\}.$$

По выбору пар $m \leqslant s$.

Далее для выбранных пар

$$g_0v_0 - h_0u_0 \neq 0, \tag{13}$$

так как в противном случае пара $u_0t^{s-m}T_k - g_0U_k = \{P(t), Q(t)\}$, где

$$P(t) = \sum_{\nu=0}^{m}(u_0g_\nu - g_0u_\nu)t^{s-\nu} - \sum_{\nu=m+1}^{s} g_0u_\nu t^{s-\nu} = \sum_{\nu=1}^{m}(u_0g_\nu - g_0u_\nu)t^{s-\nu} - \sum_{\nu=m+1}^{s} g_0u_\nu t^{s-\nu},$$

$$Q(t) = \sum_{\nu=0}^{m}(u_0h_\nu - g_0v_\nu)t^{s-\nu} - \sum_{\nu=m+1}^{s} g_0v_\nu t^{s-\nu} = \sum_{\nu=1}^{m}(u_0h_\nu - g_0v_\nu)t^{s-\nu} - \sum_{\nu=m+1}^{s} g_0v_\nu t^{s-\nu},$$

линейно независима с парой T_k и имеет степень меньшую s. Но это противоречит выбору пары U_k.

Предположим существование пар из $M(a(t), b(t) \mid f(t))$ и не представимых через T_k, U_k по формуле (12). Пусть W является такой парой наименьшей степени l и имеет вид

$$W = \left\{ \sum_{\nu=0}^{l} p_\nu t^{l-\nu}, \sum_{\nu=0}^{l} q_\nu t^{l-\nu} \right\}.$$

Очевидно, что $l \geqslant s \geqslant m$.

Рассмотрим пару

$$\{R(t), S(t)\} = (u_0q_0 - p_0v_0)t^{l-m}T + (p_0h_0 - q_0g_0)t^{l-s}U + (g_0v_0 - u_0h_0)W$$

$$R(t) = (u_0q_0 - p_0v_0)\sum_{\nu=0}^{m} g_\nu t^{l-\nu} + (p_0h_0 - q_0g_0)\sum_{\nu=0}^{s} u_\nu t^{l-\nu} + (g_0v_0 - u_0h_0)\sum_{\nu=0}^{l} p_\nu t^{l-\nu} =$$

$$= (u_0q_0 - p_0v_0)\sum_{\nu=1}^{m} g_\nu t^{l-\nu} + (p_0h_0 - q_0g_0)\sum_{\nu=1}^{s} u_\nu t^{l-\nu} + (g_0v_0 - u_0h_0)\sum_{\nu=1}^{l} p_\nu t^{l-\nu},$$

$$S(t) = (u_0q_0 - p_0v_0)\sum_{\nu=0}^{m} h_\nu t^{l-\nu} + (p_0h_0 - q_0g_0)\sum_{\nu=0}^{s} v_\nu t^{l-\nu} + (g_0v_0 - u_0h_0)\sum_{\nu=0}^{l} q_\nu t^{l-\nu} =$$

$$= (u_0q_0 - p_0v_0)\sum_{\nu=1}^{m} h_\nu t^{l-\nu} + (p_0h_0 - q_0g_0)\sum_{\nu=1}^{s} v_\nu t^{l-\nu} + (g_0v_0 - u_0h_0)\sum_{\nu=1}^{l} q_\nu t^{l-\nu}.$$

Эта пара не представима через пары T_k, U_k и имеет степень меньшую l. Но это противоречит выбору пары W. Полученное противоречие доказывает утверждение теоремы. □

Из доказанной теоремы следует, что подмодуль с одним определяющим соотношением k-ого порядка $M(a(t), b(t) \mid f^k(t))$ является двумерной решеткой многочленов $\Lambda(T_k, U_k)$ с базисом $/T_k, U_k/$, причём базис примитивный, то есть обе пары Туэ T_k и U_k являются примитивными парами, и степень первой пары меньше n, а степень второй меньше nk.

Теперь можно утверждать, что имеет место бесконечная цепочка вложенных двумерных решёток многочленов:

$$\mathbb{Z}^2[t] \supset \Lambda(T_1, U_1) \supset \ldots \supset \Lambda(T_k, U_k) \supset \ldots. \tag{14}$$

Теорема 10. *Для двумерной решётки многочленов $\Lambda(T_k, U_k) = M(a(t), b(t) \mid f^k(t))$ справедливо равенство*

$$\det \Lambda(T, U) = \det M(T, U) = \pm f^k(t). \tag{15}$$

Доказательство. Прежде всего, заметим, что пары $V_1 = \{f^k(t), 0\}$ и $V_2 = \{0, f^k(t)\}$ принадлежат решётке $\Lambda(T, U) = M(a(t), b(t) \mid f^k(t))$.

Пусть базис $/T_k, U_k/$ имеет вид $T_k = \{P(t), Q(t)\}$, $U_k = \{R(t), S(t)\}$, тогда, согласно лемме 7, имеем: $P(t)S(t) - Q(t)R(t) = \varphi_0(t)f^k(t)$ и найдутся целочисленные многочлены $c_{\nu,\mu}(t)$ ($\nu = 1, 2$; $\mu = 1, 2$) такие, что выполнены равенства

$$\begin{cases} c_{1,1}(t)P(t) + c_{1,2}(t)R(t) = f^k(t) \\ c_{1,1}(t)Q(t) + c_{1,2}(t)S(t) = 0 \\ c_{2,1}(t)P(t) + c_{2,2}(t)R(t) = 0 \\ c_{2,1}(t)Q(t) + c_{2,2}(t)S(t) = f^k(t) \end{cases}. \tag{16}$$

Отсюда следует, что

$$\begin{cases} c_{1,1}(t)(P(t)S(t) - Q(t)R(t)) = f^k(t)S(t) \\ c_{1,2}(t)(P(t)S(t) - Q(t)R(t)) = -f^k(t)Q(t) \\ c_{2,1}(t)(P(t)S(t) - Q(t)R(t)) = -f^k(t)R(t) \\ c_{2,2}(t)(P(t)S(t) - Q(t)R(t)) = f^k(t)P(t) \end{cases}. \tag{17}$$

Из (17) вытекает, что

$$\begin{cases} c_{1,1}(t)\varphi_0(t) = S(t) \\ c_{1,2}(t)\varphi_0(t) = -Q(t) \\ c_{2,1}(t)\varphi_0(t) = -R(t) \\ c_{2,2}(t)\varphi_0(t) = P(t) \end{cases}. \tag{18}$$

Из примитивности пар Туэ T_k и U_k делаем вывод, что $\varphi_0(t) = c(T_k, U_k) = \pm 1$ и теорема доказана. □

5. Подмодули с k линейными определяющими соотношениями

Следующее определение является обобщением на случай k определяющих соотношений, когда одному и тому же определяющему соотношению удовлетворяет не только пара, но и её производные до порядка $k-1$.

Определение 11. *Пусть $f(t)$ — унитарный, неприводимый многочлен с целыми коэффициентами, а $(f(t)) = f(t)\mathbb{Z}[t]$ — главный идеал в $\mathbb{Z}[t]$, порожденный многочленом $f(t)$. Пусть $a(t)$, $b(t)$ — произвольные многочлены из $\mathbb{Z}[t]$. Будем говорить, что пара Туэ $T = \{P(t), Q(t)\}$ удовлетворяет k линейным определяющим соотношениям, если $a(t)P^{(\nu)}(t) + b(t)Q^{(\nu)}(t) \in (f(x))$ для $\nu = 0, \ldots, k-1$. Подмодулем с k определяющими соотношениями назовем множество*

$$M(a(t), b(t)\,|\,f(t), k) = \Big\{\{P(t), Q(t)\}\,|\,a(t)P^{(\nu)}(t) + b(t)Q^{(\nu)}(t) \in (f(x))\,(\nu = 0, \ldots, k-1)\Big\}$$

— всех пар Туэ, удовлетворяющих этим линейным определяющим соотношениям.

Если $a(t) \equiv 0 \pmod{f(t)}$ и $b(t) \equiv 0 \pmod{f(t)}$, то определяющим соотношениям удовлетворяют все пары Туэ, и этот тривиальный случай исключается из дальнейших рассмотрений.

Пусть $a(t) \equiv 0 \pmod{f(t)}$ и $b(t) \not\equiv 0 \pmod{f(t)}$, тогда на числитель пары не накладывается никаких ограничений, а знаменатель и его производные будут принадлежать главному идеалу $(f(t))$. Если $a(t) \not\equiv 0 \pmod{f(t)}$ и $b(t) \equiv 0 \pmod{f(t)}$, то числитель и знаменатель пары Туэ меняются ролями.

Лемма 9. *Необходимым и достаточным условием выполнения k соотношений*

$$g^{(\nu)}(t) \in (f(t)) \quad (\nu = 0, \ldots, k-1)$$

является выполнение соотношения $g(t) \in (f^k(t))$.

Доказательство. Достаточность. Проведём индукцию по k.

При $k = 1$ утверждение тривиально.

Пусть $k \geqslant 1$ и из $g(t) \in (f^k(t))$ следует $g^{(\nu)}(t) \in (f(t)) \quad (\nu = 0, \ldots, k-1)$ для любого многочлена $g(t)$.

Пусть $g(t) \in (f^{k+1}(t))$, тогда $g(t) = c(t)f^{k+1}(t)$. Поэтому

$$g'(t) = c'(t)f^{k+1}(t) + c(t)(k+1)f^k(t)f'(t) \in (f^k(t)).$$

Отсюда, в силу индукционного предположения, следует $(g'(t))^{(\nu)} \in (f(t))$ $(\nu = 0, \ldots, k-1)$. Но это означает, что $g(t)^{(\nu+1)} \in (f(t))$ и достаточность доказана.

Необходимость.

При $k = 1$ утверждение тривиально.

Пусть $k \geqslant 1$ и из $g^{(\nu)}(t) \in (f(t)) \quad (\nu = 0, \ldots, k-1)$ следует $g(t) \in (f^k(t))$ для любого многочлена $g(t)$.

Пусть $g^{(\nu)}(t) \in (f(t)) \quad (\nu = 0, \ldots, k)$, тогда $g(t) = c(t)f^k(t)$, $g'(t) = c_1(t)f^k(t)$. Поэтому

$$g'(t) = c'(t)f^k(t) + c(t)kf^{k-1}(t)f'(t) = c_1(t)f^k(t).$$

Отсюда, в силу неприводимости $f(t)$, следует $c(t) = c_2(t)f(t)$, $c_2(t) \in \mathbb{Z}[t]$. Но это означает, что $g(t) \in (f^{k+1}(t))$ и необходимость доказана.

□

Поэтому все перечисленные тривиальные случаи исключаются, и дальше рассматриваем только случай $a(t)b(t) \not\equiv 0 \pmod{f(t)}$.

По аналогии со случаем одного определяющего соотношения выделяем для дальнейшего рассмотрения только случай

$$a(t) \not\equiv 0, \quad b(t) \not\equiv 0 \pmod{f(t)}, \quad \max(\deg a(t), \deg b(t)) < \deg f(t), \quad (a(t), b(t)) = 1. \tag{19}$$

Из определения непосредственно следует, что свободный модуль ранга 2

$$f^k(t)\mathbb{Z}[t]^2 \subset M(a(t), b(t) \,|\, f(t), k).$$

В частности, линейно независимые пары $T_0 = \{f^k(t), 0\}$ и $T_1 = \{0, f^k(t)\}$ принадлежат $M(a(t), b(t)|f(t), k)$.

Лемма 10. *Множество $M(a(t), b(t) \,|\, f(t), k)$ является $\mathbb{Z}[t]$-подмодулем модуля $\mathbb{Z}^2[t]$.*

Доказательство. Пусть $T = \{P(t), Q(t)\}$ и $U = \{R(t), S(t)\}$ из $M(a(t), b(t) \,|\, f(t), k)$, тогда по определению

$$a(t)P^{(\nu)}(t) + b(t)Q^{(\nu)}(t) = c_{1,\nu}(t)f(t), \quad a(t)R^{(\nu)}(t) + b(t)S^{(\nu)}(t) = c_{2,\nu}(t)f(t) \quad (\nu = 0, \ldots, k-1),$$

где $c_{1,\nu}(t), c_{2,\nu}(t) \in \mathbb{Z}[t]$ $(\nu = 0, \ldots, k-1)$.

Пользуясь этими равенствами, получим

$$a(t)\left(P^{(\nu)}(t) + R^{(\nu)}(t)\right) + b(t)\left(Q^{(\nu)}(t) + S^{(\nu)}(t)\right) = f(t)\left(c_{1,\nu}(t) + c_{2,\nu}(t)\right) \quad (\nu = 0, \ldots, k-1),$$

что означает замкнутость $M(a(t), b(t) \,|\, f(t), k)$ относительно операции сложения.

Так как для любого $c(t) \in \mathbb{Z}[t]$ имеем:

$$(P(t)c(t))^{(\nu)} = \sum_{\mu=0}^{\nu} C_\nu^\mu P^{(\mu)}(t)c^{(\nu-\mu)}(t) \in \mathbb{Z}[t],$$

то

$$a(t)(P(t)c(t))^{(\nu)} + b(t)(Q(t)c(t))^{(\nu)} = \sum_{\mu=0}^{\nu} C_\nu^\mu c^{(\nu-\mu)}(t)\left(a(t)P^{(\mu)}(t) + b(t)Q^{(\mu)}(t)\right) =$$
$$= f(t)\sum_{\mu=0}^{\nu} C_\nu^\mu c^{(\nu-\mu)}(t)c_{1,\mu}(t) \quad (\nu = 0, \ldots, k-1),$$

что доказывает замкнутость $M(a(t), b(t) \,|\, f(t), k)$ относительно операции умножения на многочлен и доказывает лемму. □

Лемма 11. *Если $T = \{P(t), Q(t)\}$ пара Туэ из $M(a(t), b(t) \,|\, f(t), k)$, то*

$$T + f^k(t) \cdot \mathbb{Z}^2[t] \subset M(a(t), b(t) \,|\, f(t), k).$$

Доказательство. Так как $f^k(t) \cdot \mathbb{Z}^2[t] \subset M(a(t), b(t) \,|\, f(t), k)$ и

$$T = \{P(t), Q(t)\} \in M(a(t), b(t) \,|\, f(t), k),$$

то по свойствам модуля получаем утверждение леммы. □

Теорема 11. *Существуют две линейно-независимые пары Туэ T, U степени меньше nk из $M(a(t), b(t) \,|\, f(t), k)$ такие, что любая пара Туэ V из $M(a(t), b(t) \,|\, f(t), k)$ однозначно представима в виде*

$$V = c_1(t)T + c_2(t)U, \tag{20}$$

где $c_1(t)$ и $c_2(t)$ — многочлены с целыми коэффициентами.

Доказательство. Возьмем в качестве T одну из пар Туэ, принадлежащих

$$M(a(t), b(t) \,|\, f(t), k),$$

наименьшей степени m. В силу леммы 11 степень $m < nk$. Легко видеть, что такая примитивная пара Туэ не может иметь вид $\{P(t), 0\}$ или $\{0, Q(t)\}$.

Действительно, если $\{P(t), 0\} \in M(a(t), b(t) \,|\, f(t), k)$, то по лемме 9 $P(t) \in (f^k(t))$, что противоречит неравенству $m \leqslant nk$. Аналогичные рассуждения справедливы для пары Туэ $\{0, Q(t)\}$.

Отсюда следует, что пары Туэ $T_{k,0} = \{f^k(t), 0\}$ и $T_{k,1} = \{0, f^k(t)\}$ из $M(a(t), b(t) \,|\, f(t), k)$ обе линейно независимы с T. Пусть для определенности степень этой пары Туэ $T = \{P(t), Q(t)\}$ равна степени числителя пары и старший коэффициент числителя равен p_0, а знаменателя — q_0, то есть

$$P(t) = p_0 t^m + P_1(t), \quad P_1(t) = \sum_{\nu=1}^{m} p_\nu t^{m-\nu}, \quad Q(t) = q_0 t^{m_1} + Q_1(t), \quad Q_1(t) = \sum_{\nu=1}^{m_1} q_\nu t^{m_1-\nu}, \quad m_1 \leqslant m.$$

Рассмотрим пару Туэ T', заданную равенством

$$T' = \begin{cases} \{t^{nk-m}P(t) - p_0 f(t), t^{nk-m}Q(t)\}, & \text{если } m_1 < m, \\ \{t^{nk-m}P(t) - p_0 f(t), t^{nk-m}Q(t) - q_0 f(t)\}, & \text{если } m_1 = m. \end{cases}$$

Ясно, что пара Туэ $T' \in M(a(t), b(t) \,|\, f(t), k)$ и линейно независима от пары Туэ $T = \{P(t), Q(t)\}$, кроме того её степень меньше nk.

Следовательно, существуют пары Туэ из $M(a(t), b(t) \,|\, f(t), k)$ линейно независимые с T. Пусть U одна из этих пар Туэ наименьшей степени s. Из предыдущего следует, что $s < nk$.

Пусть такие выбранные пары Туэ имеют вид:

$$T = \left\{ \sum_{\nu=0}^{m} g_\nu t^{m-\nu}, \sum_{\nu=0}^{m} h_\nu t^{m-\nu} \right\}, \quad U = \left\{ \sum_{\nu=0}^{s} u_\nu t^{s-\nu}, \sum_{\nu=0}^{s} v_\nu t^{s-\nu} \right\}.$$

По выбору пар $m \leqslant s < nk$.

Далее для выбранных пар

$$g_0 v_0 - h_0 u_0 \neq 0, \tag{21}$$

так как в противном случае пара $u_0 t^{s-m} T - g_0 U = \{P(t), Q(t)\}$, где

$$P(t) = \sum_{\nu=0}^{m} (u_0 g_\nu - g_0 u_\nu) t^{s-\nu} - \sum_{\nu=m+1}^{s} g_0 u_\nu t^{s-\nu} = \sum_{\nu=1}^{m} (u_0 g_\nu - g_0 u_\nu) t^{s-\nu} - \sum_{\nu=m+1}^{s} g_0 u_\nu t^{s-\nu},$$

$$Q(t) = \sum_{\nu=0}^{m} (u_0 h_\nu - g_0 v_\nu) t^{s-\nu} - \sum_{\nu=m+1}^{s} g_0 v_\nu t^{s-\nu} = \sum_{\nu=1}^{m} (u_0 h_\nu - g_0 v_\nu) t^{s-\nu} - \sum_{\nu=m+1}^{s} g_0 v_\nu t^{s-\nu},$$

линейно независима с парой T и имеет степень меньшую s. Но это противоречит выбору пары U.

Предположим существование пар из $M(a(t), b(t) \,|\, f(t), k)$ и не представимых через T, U по формуле (20). Пусть W является такой парой наименьшей степени l и имеет вид

$$W = \left\{ \sum_{\nu=0}^{l} p_\nu t^{l-\nu}, \sum_{\nu=0}^{l} q_\nu t^{l-\nu} \right\}.$$

Очевидно, что $l \geqslant s \geqslant m$.

Рассмотрим пару

$$\{R(t), S(t)\} = (u_0 q_0 - p_0 v_0) t^{l-m} T + (p_0 h_0 - q_0 g_0) t^{l-s} U + (g_0 v_0 - u_0 h_0) W$$

$$R(t) = (u_0 q_0 - p_0 v_0) \sum_{\nu=0}^{m} g_\nu t^{l-\nu} + (p_0 h_0 - q_0 g_0) \sum_{\nu=0}^{s} u_\nu t^{l-\nu} + (g_0 v_0 - u_0 h_0) \sum_{\nu=0}^{l} p_\nu t^{l-\nu} =$$

$$= (u_0 q_0 - p_0 v_0) \sum_{\nu=1}^{m} g_\nu t^{l-\nu} + (p_0 h_0 - q_0 g_0) \sum_{\nu=1}^{s} u_\nu t^{l-\nu} + (g_0 v_0 - u_0 h_0) \sum_{\nu=1}^{l} p_\nu t^{l-\nu},$$

$$S(t) = (u_0 q_0 - p_0 v_0) \sum_{\nu=0}^{m} h_\nu t^{l-\nu} + (p_0 h_0 - q_0 g_0) \sum_{\nu=0}^{s} v_\nu t^{l-\nu} + (g_0 v_0 - u_0 h_0) \sum_{\nu=0}^{l} q_\nu t^{l-\nu} =$$

$$= (u_0 q_0 - p_0 v_0) \sum_{\nu=1}^{m} h_\nu t^{l-\nu} + (p_0 h_0 - q_0 g_0) \sum_{\nu=1}^{s} v_\nu t^{l-\nu} + (g_0 v_0 - u_0 h_0) \sum_{\nu=1}^{l} q_\nu t^{l-\nu}.$$

Эта пара не представима через пары T, U и имеет степень меньшую l. Но это противоречит выбору пары W. Полученное противоречие доказывает утверждение теоремы. □

Из доказанной теоремы следует, что подмодуль с k определяющими соотношениями $M(a(t), b(t) \,|\, f(t), k)$ является двумерной решеткой многочленов $\Lambda_2(T, U)$ с базисом $/T, U/$, причём степень каждой пары меньше nk.

Из определения подмодуля с k определяющими соотношениями $M(a(t), b(t) \,|\, f(t), k)$ сразу следует, что имеет место бесконечная цепочка вложенных подмодулей (двумерных решёток многочленов)

$$\mathbb{Z}^2[t] \supset M(a(t), b(t) \,|\, f(t), 1) \supset \ldots \supset M(a(t), b(t) \,|\, f(t), k) \supset \ldots. \tag{22}$$

6. Дробно-линейные преобразования двумерных решёток многочленов

Напомним определение (см. [7], [8] стр. 104) дробно-линейного преобразования M многочленов $f_{\vec{a}}(\vec{x})$, где

$$f_{\vec{a}}(\vec{x}) = \sum_{\nu=0}^{n} a_\nu x^\nu, \quad \vec{a} = (a_0, a_1, \ldots, a_n).$$

Напомним, что $\mathcal{U}_2(\mathbb{Z})$ — мультипликативная группа квадратных, унимодулярных, целочисленных матриц второго порядка. Таким образом, целочисленная матрица

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathcal{U}_2(\mathbb{Z})$$

тогда и только тогда, когда

$$A, B, C, D \in \mathbb{Z}, \quad \delta(M) = \det M = AD - BC = \pm 1.$$

Заметим, что для обратной матрицы M^{-1} справедливо равенство

$$M^{-1} = \delta(M) \begin{pmatrix} D & -B \\ -C & A \end{pmatrix} \in \mathcal{U}_2(\mathbb{Z}).$$

Определение 12. *Для произвольной матрицы $M \in \mathcal{U}_2(\mathbb{Z})$ дробно-линейным преобразованием M многочлена $f_{\vec{a}}(x)$ называется преобразование, заданное формулой*

$$M(f_{\vec{a}}(x)) = (Cx + D)^n f_{\vec{a}} \left(\frac{Ax + B}{Cx + D} \right).$$

Отсюда следует, что можно дать следующее определение дробно-линейного преобразования двумерных решёток многочленов.

Определение 13. *Для произвольной матрицы $M \in \mathcal{U}_2(\mathbb{Z})$ дробно-линейным преобразованием M первого рода двумерной решётки многочленов $\Lambda(T, U)$ называется преобразование, заданное формулой*

$$M(\Lambda(T, U)) = \Lambda(M(T), M(U)),$$

где для произвольной пары $T = \{P(t), Q(t)\}$ преобразование $M(T)$ первого рода определяется равенством $M(T) = \{M(P(t)), M(Q(t))\}$.

Лемма 12. *Для произвольной матрицы $M \in \mathcal{U}_2(\mathbb{Z})$ дробно-линейное преобразование M многочленов переводит линейно независимые пары Туэ T, U в линейно независимые пары Туэ $M(T), M(U)$.*

Доказательство. Предположим противное, что пары Туэ $M(T), M(U)$ — линейно зависимые, то есть существуют два многочлена $c_1(t)$ и $c_2(t)$ с целыми коэффициентами одновременно неравные нулю, что $c_1(t)M(T) + c_2(t)M(U) = \{0, 0\}$. Так как $M \in \mathcal{U}_2(\mathbb{Z})$, то существует обратная матрица $M^{-1} \in \mathcal{U}_2(\mathbb{Z})$. Применим её к последнему равенству для пар, получим: $M(c_1(t))T + M(c_2(t))U = \{0, 0\}$. Так как из $M(c(t)) = 0$ следует $c(t) = 0$, то получаем линейную зависимость пар Туэ T, U. Полученное противоречие доказывает утверждение леммы. □

Из доказанной леммы следует, что определение дробно-линейного преобразования M первого рода двумерной решётки многочленов $\Lambda(T, U)$ корректно.

Оказывается, что можно дать и другое определение преобразования двумерной решётки многочленов $\Lambda(T, U)$ с помощью матрицы M.

Определение 14. *Для произвольной матрицы $M \in \mathcal{U}_2(\mathbb{Z})$ дробно-линейным преобразованием $\tilde{M}$ второго рода двумерной решётки многочленов $\Lambda(T, U)$ называется преобразование, заданное формулой*

$$\tilde{M}(\Lambda(T, U)) = \Lambda(\tilde{M}(T), \tilde{M}(U)),$$

где для произвольной пары $T = \{P(t), Q(t)\}$ преобразование $\tilde{M}(T)$ второго рода определяется равенством $\tilde{M}(T) = \{D \cdot M(P(t)) - B \cdot M(Q(t)), A \cdot M(Q(t)) - C \cdot M(P(t))\}$.

Лемма 13. *Для произвольной матрицы $M \in \mathcal{U}_2(\mathbb{Z})$ и пары Туэ T справедливо равенство*

$$\tilde{M}^{-1}(\tilde{M}(T)) = T.$$

Доказательство. Действительно,

$$\tilde{M}^{-1}(\tilde{M}(T)) = \tilde{M}^{-1}(\{D\cdot M(P(t)) - B\cdot M(Q(t)), A\cdot M(Q(t)) - C\cdot M(P(t))\}) =$$
$$= \delta(M)\{A\cdot M^{-1}(D\cdot M(P(t)) - B\cdot M(Q(t))) + B\cdot M^{-1}(A\cdot M(Q(t)) - C\cdot M(P(t))),$$
$$D\cdot M^{-1}(A\cdot M(Q(t)) - C\cdot M(P(t))) + C\cdot M^{-1}(D\cdot M(P(t)) - B\cdot M(Q(t)))\} =$$
$$= \delta(M)\{(AD-BC)M^{-1}(M(P(t))), (AD-BC)M^{-1}(M(Q(t)))\} = \{P(t), Q(t)\} = T.$$

□

Из доказанной леммы следует, что дробно-линейное преобразование второго рода имеет обратное преобразование, а, значит, оно преобразует двумерную решётку многочленов $\Lambda(T,U)$ в двумерную решётку многочленов.

7. О полиномах Туэ

Напомним некоторые определения из работы [4], сделав необходимые для дальнейшего модификации.

Определение 15. *Пусть $f(x)$ — неприводимый многочлен n-ой степени с целыми коэффициентами и старшим коэффициентом равным 1, α_ν — корень этого многочлена, а $P(t)$ и $Q(t)$ — многочлены с целыми коэффициентами. Тогда $\mathcal{T}(t,\alpha_\nu) = P(t) - \alpha_\nu Q(t)$ называется полиномом Туэ для α_ν.*

Таким образом, многочлены $P(t)$ и $Q(t)$ из $\mathbb{Z}[t]$, а полином Туэ $\mathcal{T}(t,\alpha_\nu)$, вообще говоря, из его расширения $\mathbb{Z}[\alpha_\nu][t]$.

Другими словами можно сказать, что неприводимый многочлен $f(x) \in \mathbb{Z}^*[x]$ задает отображение Туэ из декартового квадрата $\mathbb{Z}[t]^2$ в кольцо полиномов $\mathbb{Z}[\alpha_\nu][t]$ ($\nu = 1,\ldots,n$). Образом произвольной пары многочленов $P(t)$ и $Q(t)$ с целыми коэффициентами и будет полином Туэ $\mathcal{T}(t,\alpha_\nu)$.

Ясно, что полиномы Туэ $\mathcal{T}(t,\alpha_1)$, ..., $\mathcal{T}(t,\alpha_\nu)$, ..., $\mathcal{T}(t,\alpha_n)$ образуют полный набор сопряженных полиномов.

Определение 16. *Порядком полинома Туэ называется наивысшая степень $(t-\alpha_\nu)$, на которую этот полином делится. Полином Туэ j-го порядка обозначается через $\mathcal{T}_j(t,\alpha_\nu)$. Полином $R_j(t,\alpha_\nu)$, удовлетворяющий равенству $\mathcal{T}_j(t,\alpha_\nu) = (t-\alpha_\nu)^j R_j(t,\alpha_\nu)$, называется множителем Туэ порядка j для α_ν, а упорядоченная пара многочленов $T_j = \{P_j(t), Q_j(t)\}$ — парой Туэ порядка j. Многочлен $P_j(t)$ называется числителем пары Туэ. Через m_j обозначается степень числителя. Многочлен $Q_j(t)$ называется знаменателем пары Туэ. Через l_j обозначается степень знаменателя. Величина $k_j = \max(m_j, l_j)$ называется степенью пары Туэ.*

Таким образом, для произвольной пары Туэ T и соответствующего полинома Туэ $\mathcal{T}(t,\alpha_\nu)$ определены четыре функции:

- $j(T)$ — порядок пары Туэ.
- $m(T)$ — степень числителя пары.
- $l(T)$ — степень знаменателя пары.
- $k(T)$ — степень пары.

Единственным полиномом Туэ бесконечного порядка является нулевой полином:

$$\mathcal{T}_\infty(t,\alpha_\nu) = 0 = (t-\alpha_\nu)^j \cdot 0$$

для любого $j \geqslant 0$, соответствующая пара Туэ будет обозначаться $T_\infty = \{0,0\}$. Примем естественное соглашение, что $j(\{0,0\}) = m(\{0,0\}) = l(\{0,0\}) = k(\{0,0\}) = \infty$.

Отметим пять простейших свойств полиномов Туэ, указанных в работе [4], и к ним добавим ещё шестое и седьмое свойства, которые сразу вытекают из определения полинома Туэ порядка j.

1. $f^j(t)$ является полиномом Туэ порядка j.
2. Существуют полиномы Туэ любого порядка.
3. Произведение полиномов Туэ j-го порядка на многочлен с целыми коэффициентами есть также полином Туэ порядка не ниже j.
4. Сумма двух полиномов Туэ является также полиномом Туэ и его порядок не ниже наименьшего из порядков слагаемых.
5. Если α — алгебраическое число степени не ниже второй и полином Туэ $\mathcal{T}_j(t,\alpha) = P_j(t) - \alpha Q_j(t)$ делится на многочлен $\varphi(t)$ с целыми коэффициентами, то $P_j(t)$ и $Q_j(t)$ делятся на $\varphi(t)$ и частное от деления $\mathcal{T}_j(t,\alpha)$ на $\varphi(t)$ есть многочлен Туэ порядка не выше j.
6. Степень полинома Туэ j-го порядка не меньше j.
7. Полином Туэ имеет порядок не ниже j тогда и только тогда, когда он сам и все его производные до порядка $j-1$ включительно являются полиномами Туэ порядка не ниже 1.

Прежде всего уточним свойство 1, а именно, многочлен $f^j(t)$ является полиномом Туэ для каждого алгебраического числа α_1, α_2, ..., α_n. Его парой Туэ порядка j является пара $T_j = \{f^j(t), 0\}$. Таким образом, полиномы Туэ $\mathcal{T}(t,\alpha_1) = f^j(t)$, ..., $\mathcal{T}(t,\alpha_\nu) = f^j(t)$, ..., $\mathcal{T}(t,\alpha_n) = f^j(t)$ образуют стационарный полный набор сопряженных полиномов, но соответствующий полный набор сопряженных полиномов-множителей Туэ $R_j(t,\alpha_1)$, ..., $R_j(t,\alpha_\nu)$, ..., $R_j(t,\alpha_n)$ не является стационарным, так как

$$R_j(t,\alpha_\nu) = \left(\sum_{l=0}^{n-1} t^l \sum_{k=l+1}^{n} a_k \alpha_\nu^{k-l-1}\right)^j = f_\nu^j(t).$$

Перейдем к обсуждению свойства 2. Тривиальными примерами пар Туэ порядка j являются уже упомянутая пара $T_{j,0} = \{f^j(t), 0\}$ и пара $T_{j,1} = \{0, f^j(t)\}$.[2] Свойство 2 является содержательным, так как кроме тривиальных примеров, указанных выше, для любого порядка $j > 0$ имеются нетривиальные примеры отличные от пар Туэ вида $T_j = f^j(1)T_0$, где T_0 — произвольная пара Туэ нулевого порядка. Именно на изучении таких нетривиальных примеров полиномов Туэ порядка j и были сосредоточены исследования М. Н. Добровольского и В. Д. Подсыпанина.

Например, парами Туэ порядка 1 является пара $T_{1,0} = \{t, 1\}$, которой соответствует полный набор сопряженных полиномов Туэ первого порядка

$$\mathcal{T}_{1,0}(t,\alpha_1) = t - \alpha_1, \quad \ldots, \quad \mathcal{T}_{1,0}(t,\alpha_n) = t - \alpha_n,$$

[2] Мы и далее полиномы Туэ и пары Туэ будем обозначать, как правило, с помощью двух индексов. Первый индекс указывает на порядок, а второй на номер, если речь идет сразу о нескольких полиномах или парах.

со стационарным набором множителей Туэ $R_{1,0}(t,\alpha_1)=1$, а также пара

$$T_{1,1}=\left\{-a_0, \sum_{j=1}^{n-1} a_j t^{j-1}+t^{n-1}\right\},$$

которая задает полиномы Туэ

$$\mathcal{T}_{1,1}(t,\alpha_\nu)=-a_0-\alpha_\nu\left(\sum_{j=1}^{n-1} a_j t^{j-1}+t^{n-1}\right) \quad (\nu=1,\dots,n).$$

Действительно, так как $a_n=1$, то

$$-a_0-\alpha_\nu\sum_{j=1}^{n} a_j t^{j-1}=-\alpha_\nu\sum_{j=2}^{n} a_j\left(t^{j-1}-\alpha_\nu^{j-1}\right)=$$

$$=-\alpha_\nu(t-\alpha_\nu)\sum_{j=2}^{n} a_j\sum_{l=0}^{j-2} t^l\alpha_\nu^{j-2-l}=(t-\alpha_\nu)R_{1,1}(t,\alpha_\nu),$$

где $R_{1,1}(t,\alpha_\nu)=-\alpha_\nu\sum\limits_{l=0}^{n-2} t^l\sum\limits_{j=l+2}^{n} a_j\alpha_\nu^{j-2-l}$ — множитель Туэ первого порядка для α_ν.

Свойства 3 и 4 позволят нам в следующих разделах на множестве всех пар Туэ порядка не ниже j задать алгебраическую структуру унитарного модуля над кольцом целочисленных полиномов $\mathbb{Z}[t]$.

Остановимся подробнее на свойстве 5, которое является частным случаем теоремы 2 (см. стр. 58). Действительно, полином Туэ $\mathcal{T}(t,\alpha_\nu)=P(t)-\alpha_\nu Q(t)$ имеет нулевую многочленную компоненту $P(t)$ и первую многочленную компоненту $-Q(t)$, что доказывает свойство 5.

Свойство 6 очевидно, так как полином Туэ порядка j отличен от нуля, а в кольце полиномов $\mathbb{Z}[\alpha_\nu][t]$ $(\nu=1,\dots,n)$ ненулевой полином делится на полином $(t-\alpha_\nu)^j$ тогда и только тогда, когда его степень не меньше j и он имеет корень α_ν кратности не меньше j. Эти рассуждения доказывают и свойство 7.

Лемма 14. *Для любого полинома Туэ $\mathcal{T}_j(t,\alpha)=P_j(t)-\alpha Q_j(t)$ порядка $j\geqslant 1$ соответствующая пара Туэ $T_j=\{P_j(t),Q_j(t)\}\in M(1,-t\,|\,f(t))$, то есть выполнены соотношения*

$$f(t)|(P_j(t)-tQ_j(t)).$$

Доказательство. Действительно,

$$\mathcal{T}_j(t,\alpha)=P_j(t)-\alpha Q_j(t)=(t-\alpha)Q_j(t)+\left(P_j(t)-tQ_j(t)\right).$$

Поэтому из делимости левой части на $(t-\alpha)$ следует делимость на этот бином последнего выражения в больших скобках. Но это выражение является многочленом с целыми коэффициентами, поэтому он будет делиться на многочлен $f(t)$. □

Легко вычислить произведение полного набора сопряженных многочленов Туэ.

Теорема 12. *Для любой пары многочленов $P_j(t)$ и $Q_j(t)$ из $\mathbb{Z}[t]$, задающих полный набор сопряженных полиномов Туэ j-ого порядка: $\mathcal{T}_j(t,\alpha_1)=P_j(t)-\alpha_1 Q_j(t)$, …, $\mathcal{T}_j(t,\alpha_\nu)=P_j(t)-\alpha_\nu Q_j(t)$, …, $\mathcal{T}_j(t,\alpha_n)=P_j(t)-\alpha_n Q_j(t)$ справедливо равенство*

$$\prod_{\nu=1}^{n}\mathcal{T}_j(t,\alpha_\nu)=Q_j^n(t)\cdot f\left(\frac{P_j(t)}{Q_j(t)}\right)=f^j(t)R_j(t), \tag{23}$$

где множитель Туэ $R_j(t)=\prod\limits_{\nu=1}^{n} R_j(t,\alpha_\nu)\in\mathbb{Z}[t]$.

Доказательство. Действительно,

$$\prod_{\nu=1}^{n}\mathcal{T}_j(t,\alpha_\nu)=Q_j^n(t)\prod_{\nu=1}^{n}\left(\frac{P_j(t)}{Q_j(t)}-\alpha_\nu\right)=Q_j^n(t)\cdot f\left(\frac{P_j(t)}{Q_j(t)}\right).$$

Так как $\prod\limits_{\nu=1}^{n}(t-\alpha_\nu)^j=f^j(t)$, то равенство (23) доказано, а из делимости двух многочленов из кольца $\mathbb{Z}[t]$ в расширенном кольце $\mathbb{Z}[\alpha_1,\ldots,\alpha_\nu,\ldots,\alpha_n][t]$ следует делимость в $\mathbb{Z}[t]$, что завершает доказательство теоремы. □

Определение 17. *Формой А. Туэ — М. Н. Добровольского — В. Д. Подсыпанина называется бинарная полиномиальная форма $\mathcal{F}(P(t),Q(t))$, задаваемая равенством*

$$\mathcal{F}(P(t),Q(t))=\sum_{\nu=0}^{n}a_\nu P^\nu(t)Q^{n-\nu}(t). \tag{24}$$

Из определения видно, что ТДП-форма задает отображение из декартового квадрата $\mathbb{Z}[t]^2$ в кольцо многочленов $\mathbb{Z}[t]$. Нетрудно видеть, что степень образа равна $n\cdot k$, где k — степень пары $\{P(t),Q(t)\}$.

Формулу (23) теперь можно переписать в виде

$$f\left(\frac{P_j(t)}{Q_j(t)}\right)=\frac{\mathcal{F}(P_j(t),Q_j(t))}{Q_j^n(t)}=f^j(t)\frac{R_j(t)}{Q_j^n(t)}. \tag{25}$$

Из этой формулы видно, что особый интерес представляют примитивные пары Туэ.

Определение 18. *Пара Туэ $T_j=\{P_j(t),Q_j(t)\}$ порядка j называется примитивной, если её числитель и знаменатель взаимно простые многочлены.*

Заметим, что ТДП-форма является однородной формой порядка n. Действительно,

$$\mathcal{F}(P(t)d(t),Q(t)d(t))=\sum_{\nu=0}^{n}a_\nu P^\nu(t)Q^{n-\nu}(t)d^n(t)=d^n(t)\mathcal{F}(P(t),Q(t)). \tag{26}$$

Пользуясь формулой (25), можно определить два типа итерационных последовательностей рациональных чисел.

Определение 19. *ТДП-последовательностью первого рода для примитивной пары Туэ $T_j=\{P_j(t),Q_j(t)\}$ порядка j называется последовательность несократимых дробей $\frac{p_0}{q_0}$, $\frac{p_1}{q_1}$, …, $\frac{p_l}{q_l}$, …, удовлетворяющих соотношениям*

$$d_l=\left(q_l^{m_j}P_j\left(\frac{p_l}{q_l}\right),q_l^{l_j}Q_j\left(\frac{p_l}{q_l}\right)\right),$$
$$p_{l+1}=d_l^{-1}q_l^{m_j}P_j\left(\frac{p_l}{q_l}\right),\quad q_{l+1}=d_l^{-1}q_l^{l_j}Q_j\left(\frac{p_l}{q_l}\right)\quad (l\geqslant 0). \tag{27}$$

Определение 20. *Последовательность $\{T_{j_\nu}=\{P_{j_\nu}(t),Q_{j_\nu}(t)\}\}_{\nu=0}^{\infty}$ примитивных пар Туэ называется монотонной, если $1\leqslant j_0\leqslant j_1\leqslant\ldots\leqslant j_\nu\leqslant\ldots$.*

Определение 21. *ТДП-последовательностью второго рода для монотонной последовательности $\{T_{j_\nu}=\{P_{j_\nu}(t),Q_{j_\nu}(t)\}\}_{\nu=0}^{\infty}$ примитивных пар Туэ называется последовательность несократимых дробей $\frac{p_0}{q_0}$, $\frac{p_1}{q_1}$, …, $\frac{p_l}{q_l}$, …, удовлетворяющих соотношениям*

$$d_\nu=\left(q_\nu^{m_j}P_{j_\nu}\left(\frac{p_\nu}{q_\nu}\right),q_\nu^{l_{j_\nu}}Q_{j_\nu}\left(\frac{p_l}{q_l}\right)\right),$$
$$p_{\nu+1}=d_\nu^{-1}q_\nu^{m_j}P_{j_\nu}\left(\frac{p_\nu}{q_\nu}\right),\quad q_{\nu+1}=d_\nu^{-1}q_\nu^{l_{j_\nu}}Q_{j_\nu}\left(\frac{p_l}{q_l}\right)\quad (l\geqslant 0). \tag{28}$$

Возникают естественные вопросы об условиях сходимости этих итерационных последовательностей.

8. Подмодули с одним полиномиальным определяющем соотношением порядка k

С помощью ТДП-формы дадим следующее определение.

Определение 22. *Пусть $f(t)$ — унитарный, неприводимый многочлен с целыми коэффициентами, а $(f^k(t)) = f^k(t)\mathbb{Z}[t]$ — главный идеал в $\mathbb{Z}[t]$, порожденный k-ой степенью многочлена $f(t)$. Пусть $\mathcal{F}(P(t), Q(t))$ — соответствующая ТДП-форма. Будем говорить, что пара Туэ $T = \{P(t), Q(t)\}$ удовлетворяет полиномиальному определяющему соотношению k-ого порядка, если $\mathcal{F}(P(t), Q(t)) \in (f^k(x))$. Подмодулем с одним определяющим полиномиальным соотношением k-ого порядка назовем множество $M(\mathcal{F}(P(t), Q(t)) \mid f^k(t))$ всех пар Туэ, удовлетворяющих этому полиномиальному определяющему соотношению k-ого порядка.*

Из определения непосредственно следует, что свободный модуль ранга 2

$$f^k(t)\mathbb{Z}[t]^2 \subset M(\mathcal{F}(P(t), Q(t)) \mid f^k(t)).$$

В частности, линейно независимые пары $T_0 = \{f^k(t), 0\}$ и $T_1 = \{0, f^k(t)\}$ принадлежат $M(\mathcal{F}(P(t), Q(t)) \mid f^k(t))$.

Очевидно, что справедливо включение

$$M(\mathcal{F}(P(t), Q(t)) \mid f^{k+1}(t)) \subset M(\mathcal{F}(P(t), Q(t)) \mid f^k(t)) \subset M(\mathcal{F}(P(t), Q(t)) \mid f(t))$$

для любого унитарного, неприводимого многочлена $f(t)$ с целыми коэффициентами и любого натурального k.

Лемма 15. *Для любого унитарного, неприводимого многочлена $f(t)$ из общего случая, если $T = \{P(t), Q(t)\}$ и $U = \{R(t), S(t)\}$ — две пары Туэ из*

$$M(\mathcal{F}(P(t), Q(t)) \mid f^k(t)),$$

то

$$P(t)S(t) - R(t)Q(t) = f^k(t)\varphi(t), \quad \varphi(t) \in \mathbb{Z}[t].$$

Доказательство. Прежде всего, заметим, что утверждение достаточно доказать для примитивных пар Туэ. Действительно,

$$\mathcal{F}(P(t), Q(t)) = d^n(T)\mathcal{F}\left(\frac{P(t)}{d(T)}, \frac{Q(t)}{d(T)}\right), \quad \mathcal{F}(R(t), S(t)) = d^n(U)\mathcal{F}\left(\frac{R(t)}{d(U)}, \frac{S(t)}{d(U)}\right),$$
$$P(t)S(t) - R(t)Q(t) = d(T)d(U)\left(\frac{P(t)}{d(T)}\frac{S(t)}{d(U)} - \frac{R(t)}{d(U)}\frac{Q(t)}{d(T)}\right).$$

Далее заметим, что если

$$T = \{P(t)f(t), Q(t)\} \in M(\mathcal{F}(P(t), Q(t)) \mid f^k(t)),$$

то $Q(t) = f(t)Q_1(t)$, $Q_1(t) \in \mathbb{Z}[t]$.

Поэтому, в силу выше сказанного, считаем, что $d(T) = d(U) = 1$,

$$P(t), Q(t), R(t), S(T) \notin (f(t)).$$

Так как T и U из $M(\mathcal{F}(P(t),Q(t))\,|\,f^k(t))$, то по определению

$$\mathcal{F}(P(t),Q(t)) = c_1(t)f^{k_1}(t), \quad \mathcal{F}(R(t),S(t)) = c_2(t)f^{k_2}(t), \quad k_1,k_2 \geqslant k,$$

где $c_1(t),c_2(t) \in \mathbb{Z}[t]$ и $(c_1(t),f(t)) = (c_2(t),f(t)) = 1$.

Разложим левую и правую части этих равенств в кольце многочленов

$$\mathbb{Z}[\alpha_1,\ldots,\alpha_\nu,\ldots,\alpha_n][t],$$

получим

$$\prod_{\nu=1}^{n}\left(\frac{P(t)-\alpha_\nu Q(t)}{(t-\alpha_\nu)^{k_1}}\right) = c_1(t), \quad \prod_{\nu=1}^{n}\left(\frac{R(t)-\alpha_\nu S(t)}{(t-\alpha_\nu)^{k_2}}\right) = c_2(t).$$

Заметим, что при $\nu \neq \mu$ имеем:

$$\lim_{t\to\alpha_\nu}\frac{P(t)-\alpha_\mu Q(t)}{(t-\alpha_\nu)^{k_1}} = \frac{P(\alpha_\nu)-\alpha_\mu Q(\alpha_\nu)}{(\alpha_\nu-\alpha_\mu)^{k_1}} \neq 0,$$

в силу общего случая унитарного, неприводимого многочлена $f(t)$.

Так как $c_1(\alpha_\nu) \neq 0$, $c_2(\alpha_\nu) \neq 0$ для любого $\nu = 1,\ldots,n$, то

$$P(t)-\alpha_\nu Q(t) = R_1(t,\alpha_\nu)(t-\alpha_\nu)^{k_1}, \quad R(t)-\alpha_\nu S(t) = R_2(t,\alpha_\nu)(t-\alpha_\nu)^{k_2},$$

где полиномы $R_1(t,\alpha_\nu)$, $R_2(t,\alpha_\nu) \in \mathbb{Z}[\alpha_\nu][t]$.

Положим $g(t,\alpha_\nu) = (t-\alpha_\nu)^{k_1-k}R_1(t,\alpha_\nu)$ и $h(t,\alpha_\nu) = (t-\alpha_\nu)^{k_2-k}R_2(t,\alpha_\nu)$. Тогда

$$P(t)S(t)-R(t)Q(t) = \Big((t-\alpha_\nu)^k g(t,\alpha_\nu)+\alpha_\nu Q(t)\Big)S(t)-$$
$$-\Big((t-\alpha_\nu)^k h(t,\alpha_\nu)+\alpha_\nu S(t)\Big)Q(t) = (t-\alpha_\nu)^k\left(g(t,\alpha_\nu)S(t)-h(t,\alpha_\nu)Q(t)\right). \qquad (29)$$

Формула (29) справедлива для любого $\nu = 1,\ldots,n$.

Таким образом, многочлен $P(t)S(t)-R(t)Q(t)$ делится на n взаимно простых полиномов $(t-\alpha_\nu)^k$ из кольца $\mathbb{Z}[\alpha_1,\ldots,\alpha_n][t]$, а значит делится на их произведение, равное $f^k(t)$, что и доказывает лемму. □

Теорема 13. *Для любого унитарного, неприводимого многочлена $f(t)$ с целыми коэффициентами множество $M(\mathcal{F}(P(t),Q(t))\,|\,f^k(t))$ всех пар Туэ, удовлетворяющих полиномиальному определяющему соотношению k-ого порядка $\mathcal{F}(P(t),Q(t)) \in (f^k(x))$, является свободным $\mathbb{Z}[t]$-модулем ранга 2.*

Доказательство. Прежде всего заметим, что если $\mathcal{T}(t,\alpha_\nu) = P(t)-\alpha_\nu Q(t)$ — полиномом Туэ для α_ν ($\nu = 1,\ldots,n$), то имеем разложение ТДП-формы $\mathcal{F}(P(t),Q(t))$ в произведение полиномов Туэ:

$$\mathcal{F}(P(t),Q(t)) = \prod_{\nu=1}^{n}\mathcal{T}(t,\alpha_\nu).$$

Отсюда следует, что если пара Туэ $T = \{P(t),Q(t)\} \in M(\mathcal{F}(P(t),Q(t))\,|\,f^k(t))$, то соответствующие полиномы Туэ $\mathcal{T}(t,\alpha_\nu) = P(t)-\alpha_\nu Q(t)$ будут иметь порядок не ниже k, и наоборот, если пара Туэ $T = \{P(t),Q(t)\}$ имеет порядок не ниже k, то она удовлетворяет полиномиальному определяющему соотношению k-ого порядка $\mathcal{F}(P(t),Q(t)) \in (f^k(x))$.

Таким образом, множество $M(\mathcal{F}(P(t),Q(t))\,|\,f^k(t))$ совпадает с множеством всех пар Туэ порядка не ниже k, которое является подмодулем $\mathbb{Z}[t]$-модуля $\mathbb{Z}^2[t]$.

Перейдём к доказательству того, что ранг этого свободного модуля равен 2. Для этого необходимо показать, что существуют две линейно-независимые пары Туэ T_k, U_k из $M(\mathcal{F}(P(t),Q(t))\,|\,f^k(t))$ такие, что любая пара Туэ V из $M(\mathcal{F}(P(t),Q(t))\,|\,f^k(t))$ однозначно представима в виде

$$V = c_1(t)T_k + c_2(t)U_k, \tag{30}$$

где $c_1(t)$ и $c_2(t)$ — многочлены с целыми коэффициентами.

Возьмем в качестве T_k одну из пар Туэ, принадлежащих

$$M(\mathcal{F}(P(t),Q(t))\,|\,f^k(t)),$$

наименьшей степени m.

Пары Туэ $T_{k,0} = \{f^k(t), 0\}$ и $T_{k,1} = \{0, f^k(t)\}$ из $M(\mathcal{F}(P(t),Q(t))\,|\,f^k(t))$ не могут быть одновременно линейно зависимыми с T_k. Следовательно, существуют пары Туэ из $M(\mathcal{F}(P(t),Q(t))\,|\,f^k(t))$ линейно независимые с T_k. Пусть U_k одна из этих пар Туэ наименьшей степени s.

Пусть такие выбранные пары Туэ имеют вид:

$$T_k = \left\{\sum_{\nu=0}^{m} g_\nu t^{m-\nu}, \sum_{\nu=0}^{m} h_\nu t^{m-\nu}\right\}, \quad U_k = \left\{\sum_{\nu=0}^{s} u_\nu t^{s-\nu}, \sum_{\nu=0}^{s} v_\nu t^{s-\nu}\right\}.$$

По выбору пар $m \leqslant s$.

Далее для выбранных пар

$$g_0v_0 - h_0u_0 \neq 0, \tag{31}$$

так как в противном случае пара $u_0t^{s-m}T_k - g_0U_k = \{P(t), Q(t)\}$, где

$$P(t) = \sum_{\nu=0}^{m}(u_0g_\nu - g_0u_\nu)t^{s-\nu} - \sum_{\nu=m+1}^{s} g_0u_\nu t^{s-\nu} = \sum_{\nu=1}^{m}(u_0g_\nu - g_0u_\nu)t^{s-\nu} - \sum_{\nu=m+1}^{s} g_0u_\nu t^{s-\nu},$$
$$Q(t) = \sum_{\nu=0}^{m}(u_0h_\nu - g_0v_\nu)t^{s-\nu} - \sum_{\nu=m+1}^{s} g_0v_\nu t^{s-\nu} = \sum_{\nu=1}^{m}(u_0h_\nu - g_0v_\nu)t^{s-\nu} - \sum_{\nu=m+1}^{s} g_0v_\nu t^{s-\nu},$$

линейно независима с парой T_k и имеет степень меньшую s. Но это противоречит выбору пары U_k.

Предположим существование пар из $M(\mathcal{F}(P(t),Q(t))\,|\,f(t))$ и не представимых через T_k, U_k по формуле (30). Пусть W является такой парой наименьшей степени l и имеет вид

$$W = \left\{\sum_{\nu=0}^{l} p_\nu t^{l-\nu}, \sum_{\nu=0}^{l} q_\nu t^{l-\nu}\right\}.$$

Очевидно, что $l \geqslant s \geqslant m$.

Рассмотрим пару

$$\{R(t), S(t)\} = (u_0q_0 - p_0v_0)t^{l-m}T + (p_0h_0 - q_0g_0)t^{l-s}U + (g_0v_0 - u_0h_0)W$$

$$R(t) = (u_0q_0 - p_0v_0)\sum_{\nu=0}^{m} g_\nu t^{l-\nu} + (p_0h_0 - q_0g_0)\sum_{\nu=0}^{s} u_\nu t^{l-\nu} + (g_0v_0 - u_0h_0)\sum_{\nu=0}^{l} p_\nu t^{l-\nu} =$$
$$= (u_0q_0 - p_0v_0)\sum_{\nu=1}^{m} g_\nu t^{l-\nu} + (p_0h_0 - q_0g_0)\sum_{\nu=1}^{s} u_\nu t^{l-\nu} + (g_0v_0 - u_0h_0)\sum_{\nu=1}^{l} p_\nu t^{l-\nu},$$
$$S(t) = (u_0q_0 - p_0v_0)\sum_{\nu=0}^{m} h_\nu t^{l-\nu} + (p_0h_0 - q_0g_0)\sum_{\nu=0}^{s} v_\nu t^{l-\nu} + (g_0v_0 - u_0h_0)\sum_{\nu=0}^{l} q_\nu t^{l-\nu} =$$
$$= (u_0q_0 - p_0v_0)\sum_{\nu=1}^{m} h_\nu t^{l-\nu} + (p_0h_0 - q_0g_0)\sum_{\nu=1}^{s} v_\nu t^{l-\nu} + (g_0v_0 - u_0h_0)\sum_{\nu=1}^{l} q_\nu t^{l-\nu}.$$

Эта пара не представима через пары T_k, U_k и имеет степень меньшую l. Но это противоречит выбору пары W. Полученное противоречие доказывает утверждение теоремы. □

Из доказанной теоремы следует, что подмодуль с одним определяющим полиномиальным соотношением k-ого порядка $M(\mathcal{F}(P(t), Q(t)) \mid f^k(t))$ является двумерной решеткой многочленов $\Lambda_1(T_k, U_k)$ с базисом $/T_k, U_k/$.

Теперь можно утверждать, что имеет место бесконечная цепочка вложенных двумерных решёток многочленов:

$$\mathbb{Z}^2[t] \supset \Lambda_1(T_1, U_1) \supset \ldots \supset \Lambda_1(T_k, U_k) \supset \ldots. \tag{32}$$

□

9. Модули $\mathbb{TDP}_j$ над кольцом $\mathbb{Z}[t]$ $(j = 0, 1, \ldots)$

Для изучения указанных выше итерационных последовательностей (см. опр. 19, 21) определим бесконечную последовательность вложенных модулей над кольцом $\mathbb{Z}[t]$.

Определение 23. *Модулем $\mathbb{TDP}_j$ называется множество всех пар Туэ порядка не ниже j с естественной операцией сложения, когда числитель суммы двух пар Туэ равен сумме числителей слагаемых, а знаменатель суммы — сумме знаменателей. Числитель произведения пары Туэ на многочлен из $\mathbb{Z}[t]$ равен произведению числителя пары на этот многочлен, а знаменатель произведения — произведению знаменателя на тот же многочлен.*

Из свойств 1. — 4. на стр. 77 следует, что каждое множество $\mathbb{TDP}_j$ не пусто и является унитарным модулем над кольцом многочленов $\mathbb{Z}[t]$. Из свойства 6 вытекает, что степень любой пары Туэ из $\mathbb{TDP}_j$ не меньше j. Таким образом, имеем бесконечную цепочку вложенных модулей

$$\mathbb{Z}[t]^2 = \mathbb{TDP}_0 \supset \mathbb{TDP}_1 \supset \ldots \supset \mathbb{TDP}_j \supset \ldots$$

над кольцом $\mathbb{Z}[t]$.

Из теоремы 13 (стр. 81) следует, что $\mathbb{TDP}_j = M(\mathcal{F}(P(t), Q(t)) \mid f^j(t))$, и, следовательно, существуют две линейно-независимые пары Туэ T_j, U_j из $\mathbb{TDP}_j$ такие, что любая пара Туэ V из $\mathbb{TDP}_j$ однозначно представима в виде

$$V = c_1(t)T_j + c_2(t)U_j, \tag{33}$$

где $c_1(t)$ и $c_2(t)$ — многочлены с целыми коэффициентами.

Если положить $\mathbb{TDP}_j^* = \{T \in \mathbb{TDP}_j | \, j(T) = j\}$, то множество $\mathbb{TDP}_j^*$ не является модулем, так как не замкнуто относительно сложения и операции умножения на многочлены. Справедливо очевидное разбиение модуля на непересекающиеся множества

$$\mathbb{TDP}_j = \bigcup_{\nu=j}^{\infty} \mathbb{TDP}_\nu^*,$$

причем в это разбиение входит и $\mathbb{TDP}^*_\infty = \{\{0,0\}\}$ — нулевой модуль.

Введем на множестве всех пар Туэ $\mathbb{Z}[t]^2$ линейный оператор дифференцирования $\frac{d}{dt}$ следующим образом.

Определение 24. *Для любой пары Туэ $T = \{P(t), Q(t)\}$ полагается $\frac{d}{dt}T = \{P'(t), Q'(t)\}$ — производная от пары Туэ. Другое обозначение оператора дифференцирования пары просто T'.*

Теорема 14. *Для любой пары Туэ $T = \{P(t), Q(t)\}$ с порядком $j(T) > 0$ справедливо равенство*

$$j(T') = j(T) - 1. \tag{34}$$

Доказательство. Действительно, если $j(T) > 0$, то соответствующий полином Туэ $\mathcal{T}(t,\alpha) = (t-\alpha)^{j(T)}R_{j(t)}(t,\alpha)$ и полином $R_{j(t)}(t,\alpha)$ взаимно прост с полиномом $(t-\alpha)$. Так как полином Туэ для пары T' равен производной полинома Туэ от исходной пары и

$$\mathcal{T}'(t,\alpha) = j(T)(t-\alpha)^{j(T)-1}R_{j(t)}(t,\alpha) + (t-\alpha)^{j(T)}R'_{j(t)}(t,\alpha),$$

то теорема доказана. □

Из доказанной теоремы следует, что оператор дифференцирования $\frac{d}{dt}$ отображает $\mathbb{TDP}^*_j$ в $\mathbb{TDP}^*_{j-1}$ при $j \geqslant 1$: $\frac{d}{dt}(\mathbb{TDP}_j) \subset \mathbb{TDP}_{j-1}$, $\frac{d}{dt}\left(\mathbb{TDP}^*_j\right) \subset \mathbb{TDP}^*_{j-1}$.

Замечание 3. *Если пара Туэ T имеет вид $T = U + \{a, b\}$, где для пары Туэ U её порядок $j(U) > 1$ и a, b — целые числа, то $j(T) = 0$, а $j(T') = j(U) - 1 > 0$, так как $T' = U'$.*

Непосредственно из определения оператора дифференцирования пар Туэ и из свойств дифференцирования многочленов вытекает следующая теорема.

Теорема 15. *Для дифференцирования пар Туэ справедливы следующие формулы дифференцирования:*

$$\begin{gathered}
\forall\, a, b \in \mathbb{Z} : \{a, b\}' = \{0, 0\},\\
\forall\, a, b \in \mathbb{Z} : (a \cdot T + b \cdot U)' = a \cdot T' + b \cdot U',\\
\forall\, a(t) \in \mathbb{Z}[t] : (a(t) \cdot T)' = a'(t) \cdot T + a(t) \cdot T',\\
\forall\, a(t) \in \mathbb{Z}[t] : \frac{d^k}{dt^k}(a(t) \cdot T) = \sum_{\nu=0}^{k} C_k^\nu \frac{d^\nu}{dt^\nu}\, a(t) \cdot \frac{d^{k-\nu}}{dt^{k-\nu}}\, T.
\end{gathered}$$

Теорема 16. *Пара Туэ $T = \{P(t), Q(t)\}$ имеет порядок не ниже j тогда и только тогда, когда выполнены следующие j условий:*

$$P^{(\nu)}(t) \equiv tQ^{(\nu)}(t) \pmod{f(t)} \quad (\nu = 0, \ldots, j-1). \tag{35}$$

Доказательство. Рассмотрим полином Туэ

$$\mathcal{T}(t,\alpha) = P(t) - \alpha Q(t) = (t-\alpha)Q(t) + P(t) - tQ(t)$$

для числа α, соответствующий паре Туэ T. Если $j(T) \geqslant 1$, то многочлен $P(t) - tQ(t)$ делится на $(t-\alpha)$, но в силу неприводимости унитарного многочлена $f(t)$, корнем которого является целое алгебраическое число α, отсюда следует сравнение (35) при $\nu = 0$. Согласно теореме 14 $j\left(\frac{d^k}{dt^k}T\right) = j(T) - k$ при $k \leqslant j(T)$, поэтому сравнение (35) выполнено для любого $\nu < j(T)$, и тем самым теорема доказана. □

Лемма 16. *Если* $T_{k,1} = \{P_{k,1}(t), Q_{k,1}(t)\}$ *и* $T_{m,2} = \{P_{m,2}(t), Q_{m,2}(t)\}$ — *две пары Туэ, имеющие порядок не ниже* j, *то*

$$P_{k,1}(t)Q_{m,2}(t) - P_{m,2}(t)Q_{k,1}(t) = f^j(t)\varphi(t), \quad \varphi(t) \in \mathbb{Z}[t].$$

Доказательство. Так как $k \geqslant j$ и $m \geqslant j$, то по определению

$$\mathcal{T}_{k,1}(t,\alpha_\nu) = P_{k,1}(t) - \alpha_\nu Q_{k,1}(t) = (t-\alpha_\nu)^j \left((t-\alpha_\nu)^{k-j} R_{k,1}(t,\alpha_\nu)\right),$$

где $R_{k,1}(t,\alpha_\nu)$ — множитель Туэ порядка k для алгебраического числа α_ν. Аналогично $\mathcal{T}_{m,2}(t,\alpha_\nu) = P_{m,2}(t) - \alpha_\nu Q_{m,2}(t) = (t-\alpha_\nu)^j \left((t-\alpha_\nu)^{m-j} R_{m,2}(t,\alpha_\nu)\right)$, где $R_{m,2}(t,\alpha_\nu)$ — множитель Туэ порядка m для алгебраического числа α_ν.

Положим $g(t,\alpha_\nu) = (t-\alpha_\nu)^{k-j} R_{k,1}(t,\alpha_\nu)$ и $h(t,\alpha_\nu) = (t-\alpha_\nu)^{m-j} R_{m,2}(t,\alpha_\nu)$. Тогда

$$\begin{aligned} P_{k,1}(t)Q_{m,2}(t) - P_{m,2}(t)Q_{k,1}(t) &= \left((t-\alpha_\nu)^j g(t,\alpha_\nu) - \alpha_\nu Q_{k,1}(t)\right) Q_{m,2}(t) - \\ &- \left((t-\alpha_\nu)^j h(t,\alpha_\nu) - \alpha_\nu Q_{m,2}(t)\right) Q_{k,1}(t) = \\ &= (t-\alpha_\nu)^j \left(g(t,\alpha_\nu)Q_{m,2}(t) - h(t,\alpha_\nu)Q_{k,1}(t)\right). \end{aligned} \tag{36}$$

Формула (36) справедлива для любого $\nu = 1, \ldots, n$.

Таким образом, многочлен $P_{k,1}(t)Q_{m,2}(t) - P_{m,2}(t)Q_{k,1}(t)$ делится на n взаимно простых полиномов $(t-\alpha_\nu)^j$ из кольца $\mathbb{Z}[\alpha_1, \ldots, \alpha_n][t]$, а значит делится на их произведение, равное $f^j(t)$, что и доказывает лемму. □

Определение 25. *Основными парами Туэ для порядка* j *назовем две пары Туэ* $T_{k,1}$ *и* $T_{m,2}$ *порядка не ниже* j, *для которых любая пара Туэ* $T_{l,3}$ *порядка не ниже* j *представляется по формуле*

$$T_{l,3} = c_1(t)T_{k,1} + c_2(t)T_{m,2}, \tag{37}$$

где $c_1(t)$, $c_2(t)$ — *многочлены с целыми коэффициентами. Соответствующие полиномы Туэ будут называться основными для порядка* j.

Из теоремы 13 (стр. 81) следует, что для любого порядка j существуют основные пары Туэ и соответствующие основные полиномы Туэ.

Замечание 4. *Так как через основные пары для порядка* j *выражаются пары Туэ порядка* j, *то по крайней мере одна из основных пар имеет порядок* j.

Теорема 17. *Основные полиномы Туэ для порядка* j *определяются с точностью до унимодулярной матрицы.*

Доказательство. Пусть $\mathcal{T}_{j_1,1}(t,\alpha)$, $\mathcal{T}_{j_2,2}(t,\alpha)$ — основные полиномы Туэ для порядка j, а полиномы $\mathcal{T}_{k_1,1}(t,\alpha)$, $\mathcal{T}_{k_2,2}(t,\alpha)$ выражаются по формулам

$$\begin{cases} \mathcal{T}_{k_1,1}(t,\alpha) = & \mathcal{T}_{j_1,1}(t,\alpha) \cdot c_{1,1}(t) + \mathcal{T}_{j_2,2}(t,\alpha) \cdot c_{1,2}(t) \\ \mathcal{T}_{k_2,2}(t,\alpha) = & \mathcal{T}_{j_1,1}(t,\alpha) \cdot c_{2,1}(t) + \mathcal{T}_{j_2,2}(t,\alpha) \cdot c_{2,2}(t) \end{cases}, \tag{38}$$

где $c_{1,1}(t)$, $c_{1,2}(t)$, $c_{2,1}(t)$, $c_{2,2}(t)$ — многочлены с целыми коэффициентами и

$$\begin{vmatrix} c_{1,1}(t) & c_{1,2}(t) \\ c_{2,1}(t) & c_{2,2}(t) \end{vmatrix} = c = \pm 1. \tag{39}$$

Тогда система разрешима относительно $\mathcal{T}_{j_1,1}(t,\alpha)$, $\mathcal{T}_{j_2,2}(t,\alpha)$:

$$\begin{cases} \mathcal{T}_{j_1,1}(t,\alpha) = & \mathcal{T}_{k_1,1}(t,\alpha)\cdot c^*_{1,1}(t) + \mathcal{T}_{k_2,2}(t,\alpha)\cdot c^*_{1,2}(t) \\ \mathcal{T}_{j_2,2}(t,\alpha) = & \mathcal{T}_{k_1,1}(t,\alpha)\cdot c^*_{2,1}(t) + \mathcal{T}_{k_2,2}(t,\alpha)\cdot c^*_{2,2}(t) \end{cases}, \tag{40}$$

где $c^*_{1,1}(t) = \frac{c_{2,2}(t)}{c}$, $c^*_{1,2}(t) = -\frac{c_{1,2}(t)}{c}$, $c^*_{2,1}(t) = -\frac{c_{2,1}(t)}{c}$, $c^*_{2,2}(t) = \frac{c_{1,1}(t)}{c}$ — многочлены с целыми коэффициентами.

Таким образом основные многочлены $\mathcal{T}_{j_1,1}(t,\alpha)$, $\mathcal{T}_{j_2,2}(t,\alpha)$ выражаются через многочлены $\mathcal{T}_{k_1,1}(t,\alpha)$, $\mathcal{T}_{k_2,2}(t,\alpha)$ порядка не ниже j, а следовательно через них выражаются все многочлены порядка не ниже j, и потому многочлены $\mathcal{T}_{k_1,1}(t,\alpha)$, $\mathcal{T}_{k_2,2}(t,\alpha)$ являются основными.

С другой стороны, если полиномы $\mathcal{T}_{j_1,1}(t,\alpha)$, $\mathcal{T}_{j_2,2}(t,\alpha)$, а также полиномы $\mathcal{T}_{k_1,1}(t,\alpha)$, $\mathcal{T}_{k_2,2}(t,\alpha)$ являются двумя парами основных полиномов для порядка j, то имеют место равенства (38), (40) и, следовательно,

$$\begin{pmatrix} c_{1,1}(t) & c_{1,2}(t) \\ c_{2,1}(t) & c_{2,2}(t) \end{pmatrix} \cdot \begin{pmatrix} c^*_{1,1}(t) & c^*_{1,2}(t) \\ c^*_{2,1}(t) & c^*_{2,2}(t) \end{pmatrix} = E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

то есть матрица

$$C[t] = \begin{pmatrix} c_{1,1}(t) & c_{1,2}(t) \\ c_{2,1}(t) & c_{2,2}(t) \end{pmatrix}$$

является унимодулярной. □

Теорема 18. *Если $T_{k,1} = \{P_{k,1}(t), Q_{k,1}(t)\}$ и $T_{m,2} = \{P_{m,2}(t), Q_{m,2}(t)\}$ — две пары Туэ, имеющие порядок не ниже j, и*

$$P_{k,1}(t)Q_{m,2}(t) - P_{m,2}(t)Q_{k,1}(t) = f^j(t),$$

то пары $T_{k,1}$ и $T_{m,2}$ являются основными для порядка j.

Доказательство. Пусть пара Туэ $T_{l,3} = \{P_{l,3}(t), Q_{l,3}(t)\}$ имеет порядок не ниже j.

Рассмотрим три многочлена

$$c_1(t) = P_{m,2}(t)Q_{l,3}(t) - P_{l,3}(t)Q_{m,2}(t), \quad c_2(t) = P_{l,3}(t)Q_{k,1}(t) - P_{k,1}(t)Q_{l,3}(t),$$
$$c_3(t) = P_{k,1}(t)Q_{m,2}(t) - P_{m,2}(t)Q_{k,1}(t).$$

Непосредственно убеждаемся, что

$$c_1(t)T_{k,1} + c_2(t)T_{m,2} + c_3(t)T_{l,3} = T_\infty = \{0,0\}. \tag{41}$$

По условию $c_3(t) = f^j(t)$, а по лемме 7 (стр. 68) многочлены $c_1(t)$ и $c_2(t)$ имеют вид $c_1(t) = f^j(t)\varphi(t)$ и $c_2(t) = f^j(t)\psi(t)$, где $\varphi(t)$ и $\psi(t)$ — многочлены с целыми коэффициентами. Тогда равенство (41) можно переписать в виде

$$f^j(t)\varphi(t)T_{k,1} + f^j(t)\psi(t)T_{m,2} + f^j(t)T_{l,3} = T_\infty = \{0,0\}.$$

Сокращая на $f^j(t)$, что возможно, так как кольцо $\mathbb{Z}[t]$ без делителей нуля, получим

$$\varphi(t)T_{k,1} + \psi(t)T_{m,2} + T_{l,3} = T_\infty = \{0,0\},$$

следовательно,

$$T_{l,3} = -\varphi(t)T_{k,1} - \psi(t)T_{m,2}.$$

Следовательно, данные пары Туэ являются основными для порядка j. □

Определение 26. *Матрицей Туэ для порядка j назовем матрицу MT_j вида*

$$MT_j = \begin{pmatrix} P_{k,1}(t) & Q_{k,1}(t) \\ P_{m,2}(t) & Q_{m,2}(t) \end{pmatrix}, \tag{42}$$

такую, что две пары Туэ $T_{k,1} = \{P_{k,1}(t), Q_{k,1}(t)\}$ и $T_{m,2} = \{P_{m,2}(t), Q_{m,2}(t)\}$ порядка не ниже j являются основными для порядка j.

Если выполнено дополнительное условие $\det MT_j = f^j(t)$, то матрицу Туэ MT_j будем называть основной для порядка j.

Замечание 5. *На первый взгляд построение основной матрицы Туэ для порядка j, а значит и основных пар Туэ для порядка j не вызывает затруднений, так как для матриц*

$$M = \begin{pmatrix} t & 1 \\ -a_0 & \frac{f(t)-a_0}{t} \end{pmatrix}, \quad M_1 = \begin{pmatrix} f(t) & 0 \\ t & 1 \end{pmatrix} \tag{43}$$

имеем $\det M = f(t)$, $\det M_1 = f(t)$ и пары $T_{1,1} = \{t, 1\}$ и $T_{1,2} = \left\{-a_0, \frac{f(t)-a_0}{t}\right\}$ для матрицы M, и пары $T_{1,3} = \{f(t), 0\}$ и $T_{1,4} = \{t, 1\}$ для матрицы M_1, являются основными для порядка $j = 1$, то есть $MT_{1,1} = M$ и $MT_{1,2} = M_1$ — основные матрицы Туэ для порядка $j = 1$. Но уже про матрицы $M_{j,1} = M^j$ и $M_{j,2} = M_1^j$ с $\det M_{j,1} = M_{j,2} = f^j(t)$ нельзя утверждать, что они являются матрицами Туэ. Например, $M_{2,2} = M_1^2 = \begin{pmatrix} f(t)^2 & 0 \\ t\,(f(t)+1) & 1 \end{pmatrix}$, пара Туэ $T_{2,3} = \{f^2(t), 0\}$ имеет порядок 2, а пара Туэ $T_{1,5} = \{t \cdot (f(t)+1), 1\}$ имеет порядок только 1.

Лемма 17. *Если для полинома Туэ $\mathcal{T}_l(t,\alpha) = P_l(t) - \alpha Q_l(t) = (t-\alpha)^l \cdot g(t,\alpha)$ выполнено соотношение*

$$f(t) | P_l^{(j-1)}(t) - tQ_l^{(j-1)}(t), \tag{44}$$

то полином $\mathcal{T}_l(t,\alpha)$ будет порядка не ниже j.

Доказательство. Действительно, $\mathcal{T}_l(t,\alpha) = (t-\alpha)^l \cdot g(t,\alpha)$, где многочлен $g(t,\alpha) \in \mathbb{Z}[\alpha][t]$ и $g(t,\alpha)$ не делится на $(t-\alpha)$.

$$\mathcal{T}_l^{(j-1)}(t,\alpha) = \sum_{\gamma=0}^{j-1} C_{j-1}^{\gamma} \left(\prod_{\nu=0}^{\gamma-1}(l-\nu)\right)(t-\alpha)^{l-\gamma} \cdot g^{(j-1-\gamma)}(t,\alpha) =$$

$$= (t-\alpha)\sum_{\gamma=0}^{j-2} C_{j-1}^{\gamma} \left(\prod_{\nu=0}^{\gamma-1}(l-\nu)\right)(t-\alpha)^{l-1-\gamma} \cdot g^{(j-1-\gamma)}(t,\alpha) + \left(\prod_{\nu=0}^{j-2}(l-\nu)\right)(t-\alpha)^{l-j+1} \cdot g(t,\alpha).$$

Так как последнее слагаемое делится на $(t-\alpha)$ только при $l-j+1 \geqslant 1$, то порядок $l \geqslant j$. □

Теорема 19. *Если $\mathcal{T}_{j_1,1}(t,\alpha) = P_{j_1,1}(t) - \alpha Q_{j_1,1}(t)$, $\mathcal{T}_{j_2,2}(t,\alpha) = P_{j_2,2}(t) - \alpha Q_{j_2,2}(t)$ — основные полиномы для порядка j, то*

$$P_{j_1,1}(t)Q_{j_2,2}(t) - P_{j_2,2}(t)Q_{j_1,1}(t) = f^j(t)c_j,$$

где постоянная $c_j = \pm 1$.

Доказательство. Ясно, что основными полиномами наименьшей степени для порядка 0 являются $\mathcal{T}_{0,1}(t,\alpha) = 1$, $\mathcal{T}_{0,2}(t,\alpha) = \alpha$ и $P_{0,1}(t)Q_{0,2}(t) - P_{0,2}(t)Q_{0,1}(t) = 1 \cdot 1 - 0 \cdot 0 = 1$. Поэтому данные основные полиномы наименьшей степени для порядка 0 удовлетворяют теореме. Следовательно, по теореме 17 ей удовлетворяют любые основные полиномы для порядка 0.

Пусть теорема доказана для основных полиномов для порядка $j-1$, и покажем её справедливость для основных полиномов для порядка j.

Пусть $\mathcal{T}_{k_1,1}(t,\alpha) = P_{k_1,1}(t) - \alpha Q_{k_1,1}(t)$, $\mathcal{T}_{k_2,2}(t,\alpha) = P_{k_2,2}(t) - \alpha Q_{k_2,2}(t)$ — основные полиномы для порядка $j-1$. Тогда любой полином $\mathcal{T}_l(t,\alpha) = P_l(t) - \alpha Q_l(t)$ порядка не ниже j представляется в виде

$$\mathcal{T}_l(t,\alpha) = \mathcal{T}_{k_1,1}(t,\alpha)\cdot a_l(t) + \mathcal{T}_{k_2,2}(t,\alpha)\cdot b_l(t),$$

где $a_l(t)$, $b_l(t)$ — целочисленные многочлены.

Полином $\mathcal{T}_l(t,\alpha)$ имеет делителем $(t-\alpha)^j$, следовательно, производная $j-1$ порядка имеет делителем $(t-\alpha)$.

Так как

$$\mathcal{T}_l^{(j-1)}(t,\alpha) = \sum_{\gamma=0}^{j-1} C_{j-1}^{\gamma}\left(\mathcal{T}_{k_1,1}^{(\gamma)}(t,\alpha)\cdot a_l^{(j-1-\gamma)}(t) + \mathcal{T}_{k_2,2}^{(\gamma)}(t,\alpha)\cdot b_l^{(j-1-\gamma)}(t)\right) =$$
$$= \sum_{\gamma=0}^{j-2} C_{j-1}^{\gamma}\left(\mathcal{T}_{k_1,1}^{(\gamma)}(t,\alpha)\cdot a_l^{(j-1-\gamma)}(t) + \mathcal{T}_{k_2,2}^{(\gamma)}(t,\alpha)\cdot b_l^{(j-1-\gamma)}(t)\right) +$$
$$+\mathcal{T}_{k_1,1}^{(j-1)}(t,\alpha)\cdot a_l(t) + \mathcal{T}_{k_2,2}^{(j-1)}(t,\alpha)\cdot b_l(t)$$

и производные $\mathcal{T}_{k_1,1}^{(\gamma)}(t,\alpha)$ и $\mathcal{T}_{k_2,2}^{(\gamma)}(t,\alpha)$ делятся на $(t-\alpha)^{j-\gamma}$ при $\gamma = 0,\ldots,j-2$, то на $(t-\alpha)$ должен делиться полином Туэ

$$\mathcal{T}(t,\alpha) = P(t) - \alpha Q(t) = \mathcal{T}_{k_1,1}^{(j-1)}(t,\alpha)\cdot a_l(t) + \mathcal{T}_{k_2,2}^{(j-1)}(t,\alpha)\cdot b_l(t),$$

где $P(t) = P_{k_1,1}^{(j-1)}(t)a_l(t) + P_{k_2,2}^{(j-1)}(t)b_l(t)$, $Q(t) = Q_{k_1,1}^{(j-1)}(t)a_l(t) + Q_{k_2,2}^{(j-1)}(t)b_l(t)$.

Следовательно, на $f(t)$ должно делиться выражение

$$\left(P_{k_1,1}^{(j-1)}(t) - t\cdot Q_{k_1,1}^{(j-1)}(t)\right)a_l(t) + \left(P_{k_2,2}^{(j-1)}(t) - t\cdot Q_{k_2,2}^{(j-1)}(t)\right)b_l(t). \tag{45}$$

Если последнее условие будет выполнено, то согласно леммы 17 полином $\mathcal{T}_l(t,\alpha)$ будет порядка не ниже j.

Пусть остатки от деления $P_{k_1,1}^{(j-1)}(t) - t\cdot Q_{k_1,1}^{(j-1)}(t)$ и $P_{k_2,2}^{(j-1)}(t) - t\cdot Q_{k_2,2}^{(j-1)}(t)$ на $f(t)$ будут $r_1(t)$ и $r_2(t)$. Рассмотрим два возможных случая.

I. Если оба основных полинома $j-1$ порядка, то $r_1(t)$ и $r_2(t)$ не равны 0. Действительно, если $r_1(t) = 0$, то условие (45) будет выполнено при $a_l(t) = 1$, $b_l(t) = 0$ и $\mathcal{T}_l(t,\alpha) = \mathcal{T}_{k_1,1}(t,\alpha)$ имеет порядок не ниже j. Аналогично, если $r_2(t) = 0$, то при $a_l(t) = 0$, $b_l(t) = 1$ получаем $\mathcal{T}_l(t,\alpha) = \mathcal{T}_{k_2,2}(t,\alpha)$ имеет порядок не ниже j.

Пусть

$$r_1'(t) = \frac{r_1(t)}{(r_1(t), r_2(t))}, \quad r_2'(t) = \frac{r_2(t)}{(r_1(t), r_2(t))},$$

и пусть многочлены $\varphi_1(t)$, $\varphi_2(t)$, $\psi_1(t)$, $\psi_2(t)$ являются решениями уравнений

$$\varphi_1(t) = r_2'(t), \quad \psi_1(t) = -r_1'(t), \quad r_1'(t)\varphi_2(t) + r_2'(t)\psi_2(t) = f(t).$$

Для них условие (45) выполнено. Действительно, если $P_{k_\nu,\nu}^{(j-1)}(t) - t\cdot Q_{k_\nu,\nu}^{(j-1)}(t) = q_\nu(t)f(t) + r_\nu(t)$ $(\nu = 1,2)$, то

$$\left(P_{k_1,1}^{(j-1)}(t) - t\cdot Q_{k_1,1}^{(j-1)}(t)\right)\varphi_1(t) + \left(P_{k_2,2}^{(j-1)}(t) - t\cdot Q_{k_2,2}^{(j-1)}(t)\right)\psi_1(t) =$$
$$= f(t)(q_1(t)\varphi_1(t) + q_2(t)\psi_1(t)) + r_1(t)\varphi_1(t) + r_2(t)\psi_1(t) = f(t)(q_1(t)\varphi_1(t) + q_2(t)\psi_1(t)).$$

Аналогично,

$$\left(P_{k_1,1}^{(j-1)}(t) - t\cdot Q_{k_1,1}^{(j-1)}(t)\right)\varphi_2(t) + \left(P_{k_2,2}^{(j-1)}(t) - t\cdot Q_{k_2,2}^{(j-1)}(t)\right)\psi_2(t) =$$
$$= f(t)(q_1(t)\varphi_2(t) + q_2(t)\psi_2(t)) + r_1(t)\varphi_2(t) + r_2(t)\psi_2(t) =$$
$$= f(t)(q_1(t)\varphi_1(t) + q_2(t)\psi_1(t) + (r_1(t), r_2(t))).$$

Поэтому полученные для них полиномы Туэ будут порядка не ниже j.

Обозначим эти полиномы через

$$\mathcal{T}_{j_1,1}(t,\alpha) = P_{j_1,1}(t) - \alpha Q_{j_1,1}(t), \quad \mathcal{T}_{j_2,2}(t,\alpha) = P_{j_2,2}(t) - \alpha Q_{j_2,2}(t).$$

Тогда

$$P_{j_1,1}(t)Q_{j_2,2}(t) - P_{j_2,2}(t)Q_{j_1,1}(t) = (P_{k_1,1}(t)Q_{k_2,2}(t) - P_{k_2,2}(t)Q_{k_1,1}(t))\cdot$$
$$\cdot(\varphi_1(t)\psi_2(t) - \varphi_2(t)\psi_1(t)) = c\cdot f^j(t).$$

Действительно, так как

$$\mathcal{T}_{j_1,1}(t,\alpha) = P_{j_1,1}(t) - \alpha Q_{j_1,1}(t) = \mathcal{T}_{k_1,1}(t,\alpha)\cdot\varphi_1(t) + \mathcal{T}_{k_2,2}(t,\alpha)\cdot\psi_1(t),$$
$$\mathcal{T}_{j_2,2}(t,\alpha) = P_{j_2,2}(t) - \alpha Q_{j_2,2}(t) = \mathcal{T}_{k_1,1}(t,\alpha)\cdot\varphi_2(t) + \mathcal{T}_{k_2,2}(t,\alpha)\cdot\psi_2(t),$$

то

$$P_{j_\nu,\nu}(t) = P_{k_1,1}(t)\cdot\varphi_\nu(t) + P_{k_2,2}(t)\cdot\psi_\nu(t),$$
$$Q_{j_\nu,\nu}(t) = Q_{k_1,1}(t)\cdot\varphi_\nu(t) + Q_{k_2,2}(t)\cdot\psi_\nu(t) \quad (\nu = 1,2)$$

и

$$P_{j_1,1}(t)Q_{j_2,2}(t) - P_{j_2,2}(t)Q_{j_1,1}(t) = \begin{vmatrix} P_{j_1,1}(t) & Q_{j_1,1}(t) \\ P_{j_2,2}(t) & Q_{j_2,2}(t)\end{vmatrix} =$$
$$= \begin{vmatrix} P_{k_1,1}(t)\cdot\varphi_1(t) + P_{k_2,2}(t)\cdot\psi_1(t) & Q_{k_1,1}(t)\cdot\varphi_1(t) + Q_{k_2,2}(t)\cdot\psi_1(t) \\ P_{k_1,1}(t)\cdot\varphi_2(t) + P_{k_2,2}(t)\cdot\psi_2(t) & Q_{k_1,1}(t)\cdot\varphi_2(t) + Q_{k_2,2}(t)\cdot\psi_2(t)\end{vmatrix} =$$
$$= \left|\begin{pmatrix}\varphi_1(t) & \psi_1(t) \\ \varphi_2(t) & \psi_2(t)\end{pmatrix}\cdot\begin{pmatrix}P_{k_1,1}(t) & Q_{k_1,1}(t) \\ P_{k_2,2}(t) & Q_{k_2,2}(t)\end{pmatrix}\right| =$$
$$= (P_{k_1,1}(t)Q_{k_2,2}(t) - P_{k_2,2}(t)Q_{k_1,1}(t))\cdot(\varphi_1(t)\psi_2(t) - \varphi_2(t)\psi_1(t)) =$$
$$= \left(c_{j-1}f^{j-1}(t)\right)\cdot f(t) = c\cdot f^j(t).$$

Следовательно, полиномы $\mathcal{T}_{j_1,1}(t,\alpha)$, $\mathcal{T}_{j_2,2}(t,\alpha)$ по теореме 18 являются основными и для них теорема справедлива.

Если один из основных полиномов будет порядка выше $j-1$, пусть это будет $\mathcal{T}_{k_2,2}(t,\alpha)$, то положим

$$\varphi_1(t) = f(t), \quad \psi_1(t) = 0, \quad \varphi_2(t) = 0, \quad \psi_2(t) = 1.$$

Для них условие (45) выполнено.

Действительно,

$$\left(P_{k_1,1}^{(j-1)}(t) - t\cdot Q_{k_1,1}^{(j-1)}(t)\right)\varphi_1(t) + \left(P_{k_2,2}^{(i-1)}(t) - t\cdot Q_{k_2,2}^{(j-1)}(t)\right)\psi_1(t) =$$
$$= f(t)\cdot\left(P_{k_1,1}^{(j-1)}(t) - t\cdot Q_{k_1,1}^{(j-1)}(t)\right).$$

Так как условие (45) является необходимым и достаточным, а

$$\mathcal{T}_{k_1,1}(t,\alpha)\cdot\varphi_2(t)+\mathcal{T}_{k_2,2}(t,\alpha)\cdot\psi_2(t)=\mathcal{T}_{k_2,2}(t,\alpha),$$

то условие (45) выполнено и для второго многочлена.

Поэтому полученные для них многочлены Туэ будут порядка не ниже j.

Обозначим эти многочлены через

$$\mathcal{T}_{j_1,1}(t,\alpha)=P_{j_1,1}(t)+\alpha Q_{j_1,1}(t),\quad \mathcal{T}_{j_2,2}(t,\alpha)=P_{j_2,2}(t)+\alpha Q_{j_2,2}(t).$$

Тогда

$$P_{j_1,1}(t)Q_{j_2,2}(t)-P_{j_2,2}(t)Q_{j_1,1}(t)=(P_{k_1,1}(t)Q_{k_2,2}(t)-P_{k_2,2}(t)Q_{k_1,1}(t))\cdot$$
$$\cdot(\varphi_1(t)\psi_2(t)-\varphi_2(t)\psi_1(t))=c\cdot f^j(t).$$

Действительно, так как

$$\mathcal{T}_{j_1,1}(t,\alpha)=P_{j_1,1}(t)+\alpha Q_{j_1,1}(t)=\mathcal{T}_{k_1,1}(t,\alpha)\cdot f(t),$$
$$\mathcal{T}_{j_2,2}(t,\alpha)=P_{j_2,2}(t)+\alpha Q_{j_2,2}(t)=\mathcal{T}_{k_2,2}(t,\alpha),$$

то $P_{j_1,1}(t)=P_{k_1,1}(t)\cdot f(t)$, $Q_{j_1,1}(t)=Q_{k_1,1}(t)\cdot f(t)$, $P_{j_2,2}(t)=P_{k_2,2}(t)$, и $Q_{j_2,2}(t)=Q_{k_2,2}(t)$ $(\nu=1,2)$, поэтому

$$P_{j_1,1}(t)Q_{j_2,2}(t)-P_{j_2,2}(t)Q_{j_1,1}(t)=f(t)P_{k_1,1}(t)Q_{k_2,2}(t)-P_{k_2,2}(t)Q_{k_1,1}(t)f(t))=$$
$$=\left(c_{j-1}f^{j-1}(t)\right)\cdot f(t)=c\cdot f^j(t).$$

Следовательно, многочлены $\mathcal{T}_{j_1,1}(t,\alpha)$, $\mathcal{T}_{j_2,2}(t,\alpha)$ по теореме 18 являются основными и для них теорема справедлива.

Таким образом, всегда существуют основные полиномы для порядка j, для которых теорема справедлива. Но в следствии теоремы 17 она тогда справедлива для любых основных полиномов Туэ для порядка j, что и доказывает теорему. □

Основные полиномы могут быть найдены следующим способом: пусть известны основные полиномы j-го порядка. Рассматриваем основные полиномы $j+1$-го порядка как полиномы j-го порядка. На основании теоремы 13 (стр. 81) они будут представлены через основные полиномы j-го порядка в виде (37) при определенных условиях, наложенных на множители $c_j(t)$. Таким образом, формула (37) дает нам рекуррентные соотношения для вычисления основных полиномов. Для её реального применения должны быть известны $c_j(t)$, которые зависят от основных полиномов и являются функциями t и j.

10. Дробно-линейные преобразования форм

Так как значением бинарной полиномиальной формы $\mathcal{F}(P(t),Q(t))$ является многочлен, то к нему можно применить дробно-линейное преобразование M многочленов с произвольной невырожденной матрицей M из $\mathcal{M}_2^*(\mathbb{Z})$:

$$M\left(\mathcal{F}(P(t),Q(t))\right)=\sum_{\nu=0}^{n}a_\nu(Ct+D)^{n\cdot k}P^\nu\left(\frac{At+B}{Ct+D}\right)Q^{n-\nu}\left(\frac{At+B}{Ct+D}\right),$$

где k — степень пары Туэ $\{P(t),Q(t)\}$.

Введем следующие обозначения:

$\alpha = \alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(n)}$ — полный набор алгебраически сопряженных чисел, корней неприводимого унитарного многочлена $f(x) = f_0(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 \in \mathbb{Z}[x]$, α — вещественный корень;

$$\alpha = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots + \cfrac{1}{q_m + \cfrac{1}{\ddots}}}}}$$

— разложение в бесконечную цепную дробь;

P_m, Q_m — числитель и знаменатель m-ой подходящей дроби, которые связаны рекуррентными соотношениями

$$\begin{cases} P_{-1} = 1, & P_{-2} = 0 \\ Q_{-1} = 0, & Q_{-2} = 1 \end{cases} \quad (m \geqslant 0), \quad \begin{cases} P_m = q_m P_{m-1} + P_{m-2} \\ Q_m = q_m Q_{m-1} + Q_{m-2} \end{cases};$$

$$\alpha_m = q_m + \cfrac{1}{q_{m+1} + \cfrac{1}{\ddots}}$$

— m-ая остаточная дробь, для которой справедливы соотношения

$$\alpha = \frac{P_{m-1}\alpha_m + P_{m-2}}{Q_{m-1}\alpha_m + Q_{m-2}}, \quad \alpha_m = \frac{Q_{m-2}\alpha - P_{m-2}}{-Q_{m-1}\alpha + P_{m-1}};$$

$$f_m(x) = (-1)^m (Q_{m-1}x + Q_{m-2})^n f_0\left(\frac{P_{m-1}x + P_{m-2}}{Q_{m-1}x + Q_{m-2}}\right)$$

— минимальный многочлен для остаточной дроби α_m;

$$\alpha_m^{(\nu)} = \frac{Q_{m-2}\alpha^{(\nu)} - P_{m-2}}{-Q_{m-1}\alpha^{(\nu)} + P_{m-1}} \quad (\nu = 1, \ldots, n)$$

— полный набор алгебраически сопряженных чисел, корней минимального многочлена $f_m(x)$.

Через $\mathcal{F}_m(P(t), Q(t))$ будем обозначать ТДП-форму, соответствующую минимальному многочлену $f_m(x)$. Если

$$f_m(x) = \sum_{k=0}^{n} a_{k,m} x^k \in \mathbb{Z}[x],$$

$$a_{n,m} = Q_{m-1}^n \left| f_0\left(\frac{P_{m-1}}{Q_{m-1}}\right)\right|, \quad a_{0,m} = -Q_{m-2}^n \left| f_0\left(\frac{P_{m-2}}{Q_{m-2}}\right)\right|,$$

$$a_{\nu,m} = Q_{m-1}^{\nu} Q_{m-2}^{n-\nu} \sum_{\mu=0}^{n-\nu} \frac{f_0^{(\mu)}\left(\frac{P_{m-1}}{Q_{m-1}}\right)}{\mu!} \frac{(-1)^{m+(m-1)\mu}}{(Q_{m-2}Q_{m-1})^{\mu}} C_{n-\mu}^{\nu} \quad (0 \leqslant \nu \leqslant n),$$

$$a_{n-1,m} = Q_{m-1}^{n-1} Q_{m-2} \left(n \left| f_0\left(\frac{P_{m-1}}{Q_{m-1}}\right)\right| - \frac{1}{Q_{m-2}Q_{m-1}} f_0'\left(\frac{P_{m-1}}{Q_{m-1}}\right)\right),$$

то справедливы равенства

$$\mathcal{F}_m(P(t),Q(t)) = a_{n,m}\prod_{\nu=1}^{n}\mathcal{T}(t,\alpha_m^{(\nu)})$$
$$\mathcal{T}(t,\alpha_m^{(\nu)}) = P(t) - \alpha_m^{(\nu)}Q(t)$$

— полином Туэ для алгебраического числа $\alpha_m^{(\nu)}$ $(\nu = 1,\ldots,n)$.

Теорема 20. *Справедливо равенство*

$$M\left(\mathcal{F}(P(t),Q(t))\right) = \mathcal{F}_m((Q_{m-2}M(P(t)) - P_{m-2}M(Q(t))),(P_{m-1}M(Q(t)) - Q_{m-1}M(P(t)))).$$

Доказательство. Действительно, рассмотрим унимодулярную матрицу

$$M = \begin{pmatrix} P_{m-1} & P_{m-2} \\ Q_{m-1} & Q_{m-2}\end{pmatrix}, \quad \det M = P_{m-1}Q_{m-2} - P_{m-2}Q_{m-1} = (-1)^m$$

и применим её к ТДП-форме $\mathcal{F}(P(t),Q(t))$, получим

$$M\left(\mathcal{F}(P(t),Q(t))\right) = \sum_{\nu=0}^{n} a_\nu(Q_{m-1}t+Q_{m-2})^{n\cdot k}P^\nu\left(\frac{P_{m-1}t+P_{m-2}}{Q_{m-1}t+Q_{m-2}}\right)\cdot$$
$$\cdot Q^{n-\nu}\left(\frac{P_{m-1}t+P_{m-2}}{Q_{m-1}t+Q_{m-2}}\right) = \left(M\left(Q(t)\right)\right)^n a_n\prod_{\nu=1}^{n}\left(\frac{M(P(t))}{M(Q(t))} - \alpha^{(\nu)}\right) =$$
$$= a_n\prod_{\nu=1}^{n}\Big(M(P(t)) - \alpha^{(\nu)}M(Q(t))\Big) = \frac{a_n}{\prod_{\nu=1}^{n}(Q_{m-1}\alpha_m^{(\nu)}+Q_{m-2})}\cdot$$
$$\cdot\prod_{\nu=1}^{n}\Big((Q_{m-1}\alpha_m^{(\nu)}+Q_{m-2})M(P(t)) - (P_{m-1}\alpha_m^{(\nu)}+P_{m-2})M(Q(t))\Big) =$$
$$= a_n\prod_{\nu=1}^{n}\frac{P_{m-1}-Q_{m-1}\alpha^{(\nu)}}{P_{m-1}Q_{m-2}-P_{m-2}Q_{m-1}}\cdot$$
$$\cdot\prod_{\nu=1}^{n}\Big((Q_{m-2}M(P(t)) - P_{m-2}M(Q(t))) - \alpha_m^{(\nu)}(P_{m-1}M(Q(t)) - Q_{m-1}M(P(t)))\Big) =$$
$$= \mathcal{F}_m((Q_{m-2}M(P(t)) - P_{m-2}M(Q(t))),(P_{m-1}M(Q(t)) - Q_{m-1}M(P(t)))),$$

что доказывает теорему. □

11. Заключение

Из материалов статьи видно, что ТДП-формы подчиняются более сложным законам преобразования, когда мы рассматриваем ТДП-формы остаточных дробей. Сама форма подчиняется дробно-линейному преобразованию как и минимальный многочлен, а пара Туэ преобразуется с помощью дробно-линейного преобразования второго рода.

В процессе исследования выяснилось, что особый случай, который связан с группой Галуа, требует специального рассмотрения.

В следующих статьях мы предполагаем продолжить данные исследования, сделав упор на изучении сходимости итерационных ТДП-последовательностей первого и второго рода.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. ван дер Варден Б. Л. Алгебра. — М.: Из-во " Наука" 1976.
2. Вейль Г. Алгебраическая теория чисел. — М.: ГИ И*Л 1947.
3. Гаусс К. Ф. Труды по теории чисел. Перевод Б. Б. Демьянова, общая редакция И. М. Виноградова, комментарии Б. Н. Делоне. — М.: Изд-во АН СССР, 1959. 978 с.
4. Добровольский М. Н. О разложении иррациональностей третьей степени в непрерывные дроби // Чебышевский сб. 2010. Т. XI, вып. 4(36). С. 4–24.
5. Н. М. Добровольский, Н. Н. Добровольский О формах А. Туэ — М. Н. Добровольского — В. Д. Подсыпанина // Чебышевский сб. 2010. Т. XI, вып. 4(36). С. 70–109.
6. Н. М. Добровольский, Н. Н. Добровольский О минимальных многочленах остаточных дробей для алгебраических иррациональностей // Чебышевский сб. 2015. Т. 16, вып. 3. С. 147–182.
7. Н. М. Добровольский, Н. Н. Добровольский, И. Н. Балаба, И. Ю. Реброва, Н. С. Полякова Дробно-линейные преобразования многочленов и линейные преобразования форм // Материалы XIII Международной конференции Алгебра, теория чисел и дискретная геометрия: современные проблемы и приложения, Дополнительный том. Тула: Изд-во Тул. гос. пед. ун-та им. Л. Н. Толстого. 2015. С. 134–149.
8. Н. М. Добровольский, Н. Н. Добровольский, Д. К. Соболев, В. Н. Соболева Классификация чисто-вещественных алгебраических иррациональностей // Чебышевский сб. 2017. Т. 18, вып. 2. С. 98–128.
9. Н. М. Добровольский, Д. К. Соболев, В. Н. Соболева О матричном разложении приведенной кубической иррациональности // Чебышевский сб. 2013. Т. 14, вып. 1. С. 34–55.
10. Н. М. Добровольский, Е. И. Юшина О приведенных алгебраических иррациональностях // Алгебра и приложения: труды Международной конференции по алгебре, посвященной 100-летию со дня рождения Л. А. Калужнина, Нальчик, 6–11 сентября 2014 г. – Нальчик: из-во КБГУ. С. 44–46.
11. Н. М. Добровольский, Н. Н. Добровольский, Е. И. Юшина О матричной форме теоремы Галуа о чисто периодических цепных дробях // Чебышевский сб. 2012. Т. 13, вып. 3. С. 47–52.
12. Дэвенпорт Г. Высшая арифметика. Введение в теорию чисел. — М. Из-во "Наука" 1965.
13. А. И. Кострикин Введение в алгебру. Часть III. Основные структуры: Учебник для вузов. — 2-е изд., исправл. — М.: Физико-математическая литература, 2001. — 272 с. — ISBN 5-9221-0166-8.
14. Лежен Дирихле П. Г. Лекции по теории чисел. — М.–Л.: ОНТИ НКТП СССР 1936.
15. Е. А. Морозова Многочлены Туэ для квадратичных иррациональностей // Алгебра, теория чисел и дискретная геометрия: Современные проблемы и приложения: Материалы XIII Междунар. конф., посвященной 85-летию содня рождения профессора Сергея Сергеевича Рышкова — Тула: Изд-во Тул. гос. пед. ун-та им. Л. Н. Толстого, 2015. С. 354–356.

16. Е. А. Морозова Многочлены Туэ для квадратичных иррациональностей // Алгебра, теория чисел и дискретная геометрия: Современные проблемы и приложения: Материалы XIII Междунар. конф.: [Доп. том]. — Тула: Изд-во Тул. гос. пед. ун-та им. Л. Н. Толстого, 2015. С. 161–168.

17. Е. А. Морозова Многочлены Туэ для квадратичных иррациональностей // Математика и информатика: Материалы Международной конференции (Москва. 14–18 марта 2016 г.) / — М.: МПГУ 2016. С. 127–130.

18. Подсыпанин В. Д. О разложении иррациональностей четвертой степени в непрерывную дробь // Материалы межвузовской научной конференции математических кафедр пединститутов Центральной зоны. Тула, 1968, С. 68–70.

19. Подсыпанин В. Д. О разложении иррациональностей четвертой степени в непрерывную дробь // Чебышевский сборник. 2007. Т. VIII, вып. 3(23). — Тула: Изд-во Тул. гос. пед. ун-та им. Л. Н. Толстого, С. 43–46.

20. Подсыпанин В. Д. О многочленах Туэ и разложении иррациональностей четвертой степени в непрерывную дробь // Чебышевский сборник. 2010. Т. XI, вып. 4(36). С. 25–69.

21. Подсыпанин Е. В. О разложении иррациональностей высших степеней в обобщенную непрерывную дробь (по материалам В. Д. Подсыпанина) рукопись 1970 // Чебышевский сборник. 2007. Т. 8, вып. 3(23). С. 47–49.

22. Е. В. Подсыпанин Об одном обобщении алгоритма цепных дробей, связанном с алгоритмом Вигго Бруна // Зап. научн. сем. ЛОМИ. 1977. Т. 67. С. 184–194.

23. А. К. Сушкевич Теория чисел. Элементарный курс. — 2-е изд. — Харьков: Изд-во Харьковского гос. ун-та им. А. М. Горького, 1956. — 204 с.

24. Е. В. Триколич, Е. И. Юшина Цепные дроби для квадратических иррациональностей из поля $\mathbb{Q}(\sqrt{5})$ // Чебышевский сб. 2009. Т. 10, вып. 1. С. 77–94.

25. Фельдман Н. И. Приближения алгебраических чисел. — М.: Изд-во Моск. ун-та, 1981. — 200 с.

26. Хинчин А. Я. Цепные дроби. — 2-е изд. — М.–Л.: ГИТТЛ, 1949. — 116 с.

27. Шмидт В. М. Диофантовы приближения: Пер. с англ. — М.: Мир, 1983. — 232 с.

28. Е. И. Юшина О некоторых приведенных алгебраических иррациональностях // Современные проблемы математики, механики, информатики: материалы Региональной научной студенческой конференции. Тула: ТулГУ 2015. С. 66–72.

29. Е. И. Юшина О некоторых обобщенных числах Пизо // Университет XXI века: исследования в рамках научных школ: материалы Всероссийской научно-практической конференции. Тула: ТГПУ им. Л. Н. Толстого 2015. С. 66–72.

30. Nikolai M. Dobrovol'skii, Nikolai N. Dobrovolsky, Irina N. Balaba, Irina Yu. Rebrova, Dmitrii K. Sobolev and Valentina N. Soboleva Generalized Pisot Numbers and Matrix Decomposition // Springer International Publishing Switzerland 2016 V. A. Sadovnichiy and M. Z. Zgurovsky (eds.), Advances in Dynamical Systems and Control, Studies in Systems, Decision and Control 69, DOI 10.1007/978-3-319-40673-2_5

31. Euler L. De fractinibus continuis // Comm. Acad. Sci. Imper. Petropol., 1737, v. 9.

32. Euler L. De relatione inter ternas pluresve quantitates instituenda // Petersburger Akademie Notiz. Exhib. August 14, 1775 // Commentationes arithmeticae collectae. V. II. St. Petersburg, 1849. P. 99-104.

33. Galois E. Théorème sur les fractions contiues périodiques — Annales de Mathematiques (Gergonne), 1828/29, t. 19, p. 294; Oeuvres mathematiques. — Paris: Gauthier Villars, 1951. [Имеется перевод: Галуа Э. Сочинения. — М.: ОНТИ, 1936.]

34. Lagrange J. L. Complement chez Elements d'algebre etc. par M.L. Euler, t. III, 1774.

35. Liouville J. Sur des classes très-étendues de quantités dont la irrationelles algébriques // C. R. Acad. Sci. Paris 18, 1844, C. 883–885, 910–911.

36. Roth K. F. Rational approximations to algebraic numbers // Mathematika. 1955. Vol. 2. P. 1–20. corrigendum: p. 168.

37. Thue A. Über Annäherungswerte algebraischer Zahlen // J. reine ang. Math. 1910. Vol. 135. PP. 284–305.

REFERENCES

1. Van der Waerden, B. L. 1976 *Algebra.* Moscow: Iz-in "Science".

2. Weyl G. 1947 *Algebraic number theory.* M .: GI I * L.

3. Gauss K. F. 1959 *Proceedings on the theory of numbers.* Translation of B. B. Demyanov, general edition I. M. Vinogradova, comments B. N. Delone. - Moscow: Publishing House of the USSR Academy of Sciences. 978 p.

4. Dobrovol'skii M. N. 2010 "On the decomposition of irrationalities of the third degree into continuous fractions" *Chebyshevsky Sb.* vol. XI, №. 4 (36). pp. 4–24.

5. Dobrovol'skii N. M., Dobrovolsky N. N. 2010, "On the forms of A. Thue M. N. Dobrovolsky — V. D. Podsypinina" *Chebyshevsky sb.* vol. XI, №. 4 (36). pp. 70–109.

6. N. M. Dobrovol'skii, N. N. Dobrovol'skii, 2015 "About minimal polynomial residual fractions for algebraic irrationalities", *Chebyshevskii Sb.*, 16:3, pp. 147–182

7. N. M. Dobrovol'skii, N. N. Dobrovol'skii, I. N. Balaba, I. Yu. Rebrova, N. S. Polyakova, 2015 "Fractional-linear transformations of polynomials and linear transformations of forms" *Proceedings of the XIII International Conference Algebra, number theory and discrete geometry: modern problems and applications, Supplementary volume.* Tula: Publishing house Tul. State. Ped. The university of L. N. Tolstoy. pp. 134–149.

8. N. M. Dobrovolsky, N. N. Dobrovolsky, D. K. Sobolev, V. N. Soboleva, 2017 "Classification of purely real algebraic irrationalities" , *Chebyshevsky Sb.* Vol. 18, no. 2. pp. 98–128.

9. N. M. Dobrovol'skii, D. K. Sobolev, V. N. Soboleva, 2013 "On matrix decomposition of one reduced cubic irrational", *Chebyshevskii Sb.*, 14:1, pp. 34–55

10. N. M. Dobrovol'skii, E. I. Yushina "On reduced algebraic irrationalities" *Algebra and Applications: Proceedings of the International Conference on Algebra LA Kaluzhnina, Nalchik, September 6-11, 2014 - Nalchik* Iz-in Kabardino-Balkarian State University. pp. 44–46.

11. N. M. Dobrovol'skii, N. N. Dobrovol'skii, E. I. Yushina, 2012 "On the matrix form of the Galois theorem on purely periodic continued fractions", *Chebyshevskii Sb.*, 13:3, 47–52

12. Davenport G. 1965 *Higher arithmetic. Introduction to number theory.* Iz-in From the "Science".

13. A. I. Kostrikin, 2001 *Introduction to Algebra. Part III. Basic structures: Textbook for high schools. — 2 nd ed., Correct.* M .: Physical and mathematical literature, — 272 p. — ISBN 5-9221-0166-8.

14. Lezhen Dirichlet P. G. 1936 *Lectures on number theory.* M — L .: ONTI NKTP of the USSR.

15. E. A. Morozova 2015 "Thue polynomials for quadratic irrationalities" *Algebra, number theory and discrete geometry: Contemporary problems and applications: Proceedings of the XIIIth International Conference. Conf., Dedicated to the 85th anniversary of the birth of Professor Sergey Sergeevich Ryshkov* Tula: Izd-vo Tul. State. Ped. Un-ta L. N. Tolstoy, pp. 354–356.

16. E. A. Morozova 2015 "Thue polynomials for quadratic irrationalities" *Algebra, number theory and discrete geometry: Contemporary problems and applications: Proceedings of the XIIIth International Conference. Conf .: [Ext. Tom].* Tula: Publishing House Tul. State. Ped. Un-ta them. L.N. Tolstoy, pp. 161-168.

17. E. A. Morozova 2016 "Thue polynomials for quadratic irrationalities" *Mathematics and Computer Science: Proceedings of the International Conference (Moscow, March 14-18, 2016)* / — M .: MPGU pp. 127–130.

18. Podsypanin V. D. 1968 "On the decomposition of irrationalities of the fourth degree into an continued fraction" *Materials of the Interuniversity Scientific Conference of Mathematical Departments Pedagogical institutes of the Central zone.* Tula, pp. 68–70.

19. Podsypanin V. D. 2007 "On the decomposition of irrationalities of the fourth power into an continued fraction *Chebyshevskii sbornik.* T. VIII, vol. 3 (23). — Tula: Izd-vo Tul. State. Ped. Un-ta them. L.N. Tolstoy, pp. 43–46.

20. Podsypanin V. D. 2010 "On Thue polynomials and the expansion of irrationalities of the fourth degree into a continued fraction"*Chebyshevskii sbornik.* T. XI, vol. 4 (36). pp. 25–69.

21. Podsypanin E. V. 2007 "On the decomposition of irrationalities of higher powers into a generalized continued fraction (On the materials of VD Podsypanin) manuscript 1970"*Chebyshevskii sbornik* T. 8, issue 3 (23). pp. 47–49.

22. E. V. Podsypinin 1977 "On a generalization of the algorithm of continued fractions associated with the Viggo Brun algorithm"*Zap. Scientific. Sem. LOMI.* T. 67. pp. 184–194.

23. A. K. Sushkevich 1956 *Number theory. Elementary course. — 2 nd ed.* — Kharkov: Publishing house of Kharkov state. Un-ta them. AM Gorky, — 204 p.

24. E .V .Trikolich, E. I. Yushina 2009 "Chain fractions for quadratic Irrationalities from the field $\mathbb{Q}(\sqrt{5})$" *Chebyshevsky sb.* T. 10, no. 1. pp. 77–94.

25. Feldman N. I. 1981 *Approximation of algebraic numbers.* — Moscow: Izd-vo Mosk. University, p. 200

26. Khinchin A. Ya. 1949 *Chain fractions. — 2 nd ed.* M .: — L .: GITTL, p. 116

27. Schmidt V. M. 1983 *Diophantine approximations: Per. With the English.* Moscow: Mir, — 232 p.

28. E. I. Yushina 2015 "On some reduced algebraic irrationalities" *Modern problems in mathematics, mechanics, informatics: materials of the Regional Scientific Student Conference.* Tula: Tula State University. pp. 66–72.

29. E. I. Yushina 2015 "On some generalized Piso numbers" *University of the XXI century: research within the framework of scientific schools: materials of the All-Russian Scientific and Practical Conference.* Tula: TSPU them. L.N. Tolstoy. pp. 66–72.

30. Nikolai M. Dobrovol'skii, Nikolai N. Dobrovolsky, Irina N. Balaba, Irina Yu. Rebrova, Dmitrii K. Sobolev and Valentina N. Soboleva Generalized Pisot Numbers and Matrix Decomposition // Springer International Publishing Switzerland 2016 V. A. Sadovnichiy and M. Z. Zgurovsky (eds.), Advances in Dynamical Systems and Control, Studies in Systems, Decision and Control 69, DOI 10.1007/978-3-319-40673-2_5

31. Euler L. De fractinibus continuis // Comm. Acad. Sci. Imper. Petropol., 1737, v. 9.

32. Euler L. De relatione inter ternas pluresve quantitates instituenda // Petersburger Akademie Notiz. Exhib. August 14, 1775 // Commentationes arithmeticae collectae. V. II. St. Petersburg, 1849. P. 99-104.

33. Galois E. Théorème sur les fractions contiues périodiques — Annales de Mathematiques (Gergonne), 1828/29, t. 19, p. 294; Oeuvres mathematiques. — Paris: Gauthier Villars, 1951. [Имеется перевод: Галуа Э. Сочинения. — М.: ОНТИ, 1936.]

34. Lagrange J. L. Complement chez Elements d'algebre etc. par M.L. Euler, t. III, 1774.

35. Liouville J. Sur des classes très-étendues de quantités dont la irrationelles algébriques // C. R. Acad. Sci. Paris 18, 1844, C. 883–885, 910–911.

36. Roth K. F. Rational approximations to algebraic numbers // Mathematika. 1955. Vol. 2. P. 1–20. corrigendum: p. 168.

37. Thue A. Über Annäherungswerte algebraischer Zahlen // J. reine ang. Math. 1910. Vol. 135. PP. 284–305.

Тульский государственный педагогический университет им. Л. Н. Толстого
Тульский государственный университет
Получено 02.03.2017 г.
Принято в печать 12.06.2017 г.