С. Н. Селезнева, О некоторых свойствах многочленов над конечным полем, *Дискрет. матем.*, 2001, том 13, выпуск 2, 111–119

DOI: 10.4213/dm286

Дискретная математика

том 13 выпуск 2 * 2001

УДК 519.7

О некоторых свойствах многочленов над конечным полем

© 2001 г. С. Н. Селезнева

Рассматриваются многочлены над конечным полем. Многочлены от одной переменной называются преобразованиями. Изучаются многочлены от многих переменных, которые не изменяются при замещении каждой их переменной некоторым ее преобразованием. Такие многочлены называются инвариантными относительно преобразований переменных. Изучается строение многочленов, инвариантных относительно связных преобразований. Преобразование называется связным, если для произвольных элементов a_1 и a_2 поля найдутся такие числа m_1 и m_2, что m_1-кратная итерация преобразования над a_1 совпадает с m_2-кратной итерацией преобразования над a_2.

С каждым многочленом связан ряд целочисленных характеристик. В работе рассматриваются целочисленные характеристики, называемые рангом и весом многочлена от многих переменных. Доказано следующее свойство многочленов, инвариантных относительно связных преобразований: если r и w — соответственно ранг и вес многочлена, инвариантного относительно связных преобразований, то $w^q \geqslant 2^r$, где q — зависящая от преобразований постоянная, не большая числа элементов поля.

1. Основные понятия

Пусть F — поле из p^h элементов, где p — простое число, $h \geqslant 1$, характеристики p с операциями сложения и умножения, 0 и 1 — соответственно его нулевой и единичный элементы (см. [2]).

Обозначим $F[x_1, \ldots, x_n]$ кольцо многочленов над полем F, зависящих от переменных $x_1, \ldots, x_n$. Мы будем полагать, что в каждом многочлене приведены подобные слагаемые, отсутствуют слагаемые с нулевыми коэффициентами и степень каждой переменной каждого слагаемого не выше $p^h - 1$. Такой вид многочлена назовем приведенным. Каждый многочлен $f(x_1, \ldots, x_n)$ из $F[x_1, \ldots, x_n]$ определяет некоторое отображение из F^n в F, и наоборот, каждое отображение из F^n в F можно однозначно записать некоторым (приведенным) многочленом из $F[x_1, \ldots, x_n]$ (см. [1]). Поэтому мы будем отождествлять понятия многочлена и отображения, им определяемого. Многочлены из $F[x]$ будем называть преобразованиями (множества F). Заметим, что в определении преобразования не требуется взаимной однозначности отображения, определяемого многочленом из $F[x]$. Другими словами, рассматриваются в том числе и вырожденные преобразования множества F. Преобразование

$s(x)$ назовем связным, если для произвольных элементов $a, b \in F$ найдутся такие числа m_1 и m_2, что

$$s^{m_1}(a) = s^{m_2}(b),$$

где под записью $s^m(x)$ понимается m-кратная итерация $s(\dots s(x)\dots)$ преобразования $s(x)$, $m \geqslant 1$, $s^0(x) = x$.

Многочлен $f(x_1, \dots, x_n)$ из $F[x_1, \dots, x_n]$ назовем инвариантным относительно набора преобразований $s_1(x), \dots, s_n(x)$ из $F[x]$ (или просто инвариантным, подразумевая при этом некоторый набор преобразований), если

$$f(s_1(x_1), \dots, s_n(x_n)) = f(x_1, \dots, x_n).$$

Введем целочисленные характеристики многочленов. Назовем типом одночлена $x_{i_1}^{m_1} \dots x_{i_r}^{m_r}$ множество его переменных $\{x_{i_1}, \dots, x_{i_r}\}$. Произвольное подмножество типа назовем его подтипом. Рангом одночлена назовем мощность его типа. Под рангом многочлена будем понимать максимальный ранг его слагаемых. Весом многочлена назовем число попарно различных типов его слагаемых.

Каждому преобразованию $s(x)$ из $F[x]$ поставим в соответствие ориентированный граф (могущий содержать петли) $G(s)$ с множеством вершин F и множеством ребер $\{(a, s(a))\}$, где $a \in F$. Заметим, что граф $G(s)$ обладает тем свойством, что полустепень исхода каждой его вершины в точности равна единице (понятия, относящиеся к теории графов, можно найти, например, в [3]). Если преобразование $s(x)$ связно, то граф $G(s)$ связен. С использованием перечисленных двух свойств графа $G(s)$ несложно доказать, что в нем содержится в точности один ориентированный цикл. Число вершин в этом единственном цикле графа связного преобразования $s(x)$ назовем рангом преобразования $s(x)$. Рангом набора связных преобразований $s_1(x), \dots, s_n(x)$ назовем максимальный ранг составляющих его преобразований.

Мы докажем следующую теорему.

Теорема 1. *Пусть многочлен $f(x_1, \dots, x_n) \in F[x_1, \dots, x_n]$ не равен нулю и инвариантен относительно набора связных преобразований $s_1(x), \dots, s_n(x)$ ранга q, и пусть r и w — соответственно ранг и вес многочлена. Тогда $w^q \geqslant 2^r$.*

Теорема 1 является следствием теоремы 2. Пусть $T(f)$ обозначает множество всех типов слагаемых многочлена $f(x_1, \dots, x_n)$, а $T^l(f)$ — множество всех возможных пересечений l элементов (не обязательно различных) из $T(f)$.

Теорема 2. *Если многочлен $f(x_1, \dots, x_n) \in F[x_1, \dots, x_n]$ не равен нулю и инвариантен относительно набора связных преобразований $s_1(x), \dots, s_n(x)$ ранга q, то каждый подтип произвольного типа из $T(f)$ содержится в $T^q(f)$.*

В разделе 2 доказывается ряд лемм, на которых основываются доказательства теорем 1 и 2. Кроме того, этими леммами описываются свойства многочленов, инвариантных относительно связных преобразований.

2. О свойствах многочленов, инвариантных относительно связных преобразований

Пусть $s(x)$ — связное преобразование. Назовем элементы a и b из F эквивалентными относительно преобразования $s(x)$ и будем писать в этом случае $a \sim_s b$, если найдется такое число m, что $s^m(a) = s^m(b)$. Другими словами, если $a \sim_s b$, то в графе $G(s)$ найдутся пути одинаковой длины из вершин a и b соответственно к некоторой вершине. Введенное отношение является отношением эквивалентности на множестве F.

Лемма 1. *Пусть многочлен $f(x_1, \ldots, x_n)$ из $F[x_1, \ldots, x_n]$ инвариантен относительно набора связных преобразований $s_1(x), \ldots, s_n(x)$ и a, b — такие элементы F, что $a \sim_{s_i} b$. Тогда*

$$f_1(x_1, \ldots, x_{i-1}, a, x_{i+1}, \ldots, x_n) = f_2(x_1, \ldots, x_{i-1}, b, x_{i+1}, \ldots, x_n).$$

Доказательство. Положим для определенности, что $i = 1$.

Так как $a \sim_{s_1} b$, найдется такое число m, что $s_1^m(a) = s_1^m(b)$. Другими словами, в F существуют такие $2n(m+1)$ элементов

$$a^{(0)} = a, \quad a^{(1)} = s(a), \ldots, a^{(m)} = s^m(a), \tag{1}$$

$$b^{(0)} = b, \quad b^{(1)} = s(b), \ldots, b^{(m)} = s^m(b), \tag{2}$$

$$x_i^{(0)} = x_i, \quad x_i^{(1)} = s(x_i), \ldots, x_i^{(m)} = s^m(x_i),$$

для которых выполняются условия

$$s(a^{(j-1)}) = a^{(j)}, \quad s(b^{(j-1)}) = b^{(j)}, \quad s(x^{(j-1)}) = x^{(j)}$$

при $i = 2, \ldots, n$ и $j = 1, \ldots, m$. Так как $a^{(m)} = b^{(m)}$, справедливо тождество

$$f(a^{(m)}, x_2^{(m)}, \ldots, x_n^{(m)}) = f(b^{(m)}, x_2^{(m)}, \ldots, x_n^{(m)}).$$

Многочлен $f(x_1, \ldots, x_n)$ инвариантен относительно набора преобразований $s_1(x)$, $\ldots, s_n(x)$, поэтому верны равенства

$$f(a^{(m-1)}, x_2^{(m-1)}, \ldots, x_n^{(m-1)}) = f(a^{(m)}, x_2^{(m)}, \ldots, x_n^{(m)}),$$
$$f(b^{(m-1)}, x_2^{(m-1)}, \ldots, x_n^{(m-1)}) = f(b^{(m)}, x_2^{(m)}, \ldots, x_n^{(m)}),$$

откуда следует, что

$$f(a^{(m-1)}, x_2^{(m-1)}, \ldots, x_n^{(m-1)}) = f(b^{(m-1)}, x_2^{(m-1)}, \ldots, x_n^{(m-1)}).$$

Повторяя изложенные рассуждения m раз получаем, что

$$f(a^{(0)}, x_2^{(0)}, \ldots, x_n^{(0)}) = f(b^{(0)}, x_2^{(0)}, \ldots, x_n^{(0)})$$

или

$$f(a, x_2, \ldots, x_n) = f(b, x_2, \ldots, x_n).$$

Так как элементы $x_2, \ldots, x_n$ произвольны, лемма 1 доказана.

Преобразования $s_1(x)$ и $s_2(x)$ назовем эквивалентными, если для любых элементов a, b из F выполняются следующие условия:

(1) $a \sim_{s_1} b$ тогда и только тогда, когда $a \sim_{s_2} b$,

(2) $s_1(a) \sim_{s_1} s_2(a)$ (а в силу условия 1 и $s_1(a) \sim_{s_2} s_2(a)$).

Заметим, что если преобразования $s_1(x)$ и $s_2(x)$ эквивалентны, то из того, что $a \sim_{s_1} b$ (а значит, и $a \sim_{s_2} b$) следует, что $s_1(a) \sim_{s_1} s_2(b)$ (и $s_1(a) \sim_{s_2} s_2(b)$). Действительно, из соотношений

$$a \sim_{s_1} b \quad \text{и} \quad a \sim_{s_2} b$$

следует, что

$$s_1(a) \sim_{s_1} s_1(b), \qquad s_2(a) \sim_{s_2} s_2(b).$$

В силу первого условия в определении эквивалентных преобразований

$$s_2(a) \sim_{s_1} s_2(b) \tag{3}$$

и в силу второго условия

$$s_1(a) \sim_{s_1} s_2(a). \tag{4}$$

С учетом транзитивности отношения $\sim_{s_1}$ из первого и второго условий находим, что

$$s_1(a) \sim_{s_1} s_2(b).$$

Лемма 2. *Если многочлен $f(x_1, \ldots, x_n)$ инвариантен относительно набора связных преобразований $s_1(x), \ldots, s_n(x)$ и для некоторого i, $1 \leqslant i \leqslant n$, преобразования $s_i(x)$ и $s_i'(x)$ эквивалентны, то многочлен $f(x_1, \ldots, x_n)$ инвариантен относительно набора преобразований*

$$s_1(x), \ldots, s_{i-1}, s_i'(x), s_{i+1}, \ldots, s_n(x).$$

Доказательство. Положим для определенности, что $i = 1$.

Так как многочлен $f(x_1, \ldots, x_n)$ инвариантен относительно набора преобразований $s_1(x), \ldots, s_n(x)$, верно равенство

$$f(s_1(x_1), s_2(x_2), \ldots, s_n(x_n)) = f(x_1, x_2, \ldots, x_n). \tag{5}$$

Рассмотрим $f(s_1'(x_1), s_2(x_2), \ldots, s_n(x_n))$. Преобразования $s_1(x)$ и $s_1'(x)$ эквивалентны, поэтому по второму свойству определения эквивалентных преобразований $s_1(x_1) \sim_{s_1} s_1'(x_1)$. Тогда по лемме 1

$$f(s_1(x_1), s_2(x_2), \ldots, s_n(x_n)) = f(s_1'(x_1), s_2(x_2), \ldots, s_n(x_n)). \tag{6}$$

Из равенств (3) и (4) следует, что

$$f(s_1'(x_1), s_2(x_2), \ldots, s_n(x_n)) = f(x_1, x_2, \ldots, x_n),$$

то есть многочлен $f(x_1, \ldots, x_n)$ инвариантен относительно набора преобразований $s_1'(x), s_2(x), \ldots, s_n(x)$.

Лемма 2 доказана.

Пусть $s(x)$ — связное преобразование. Каждый элемент единственного цикла графа $G(s)$ назовем циклическим элементом преобразования $s(x)$. Отметим некоторые свойства циклических элементов преобразований. Если a — циклический элемент связного преобразования $s(x)$ ранга q, то

– для произвольного элемента b из F найдется такое число m, что $s^m(b) = a$,

– справедливо равенство $s^q(a) = a$,

– для произвольного числа m элемент $s^m(a)$ также является циклическим.

Перечисленные свойства циклических элементов следуют из свойств графа преобразования $G(s)$.

Зафиксируем некоторый циклический элемент a связного преобразования $s(x)$. Тогда для произвольного числа m найдется такой единственный циклический элемент b, что $s^m(b) = a$. Положим по определению, что $s^{-m}(a) = b$.

Лемма 3. *Если многочлен $f(x_1, \ldots, x_n)$ инвариантен относительно набора связных преобразований $s_1(x), \ldots, s_n(x)$, то для произвольного i, $1 \leqslant i \leqslant n$, найдется такое эквивалентное преобразованию $s_i(x)$ преобразование $s'_i(x)$ с нулевым циклическим элементом, что многочлен $f(x_1, \ldots, x_n)$ инвариантен относительно набора преобразований*

$$s_1(x), \ldots, s_{i-1}(x), s'_i(x), s_{i+1}(x), \ldots, s_n(x).$$

Доказательство. Рассмотрим преобразование $s_i(x)$, $1 \leqslant i \leqslant n$. Возможны две ситуации: либо 0 является циклическим элементом $s_i(x)$, либо нет. Если верна первая из них, то полагаем $s'_i(x) = s_i(x)$ и утверждение леммы верно.

Во втором случае, пусть a — некоторый циклический элемент $s_i(x)$. Так как $s_i(x)$ — связное преобразование, найдутся такие числа m_{i_1} и m_{i_2}, что $s_i^{m_{i_1}}(0) = s_i^{m_{i_2}}(a)$. Положим $m_{i_3} = m_{i_2} - m_{i_1}$. Тогда циклический элемент $s_i^{m_{i_3}}(a)$ эквивалентен элементу 0. Таким образом, мы обнаружили циклический элемент (обозначим его c), эквивалентный элементу 0.

Построим преобразование $s'_i(x)$ по следующим правилам. Полагаем $s'_i(0) = s_i(c)$, $s'_i(c) = s_i(0)$; если $s_i(x) = 0$, то полагаем $s'_i(x) = c$ и если $s_i(x) = c$, то $s'_i(x) = 0$. Во всех оставшихся возможными случаях преобразования $s'_i(x)$ и $s_i(x)$ совпадают.

Докажем, что преобразования $s'_i(x)$ и $s_i(x)$ эквивалентны. Другими словами, надо доказать справедливость двух условий определения эквивалентных преобразований. Их выполнение следует из того, факта, что так как $0 \sim_{s_i} c$, классы эквивалентности, на которые разбивают множество F преобразования $s_i(x)$ и $s'_i(x)$, совпадают и порядок следования их друг за другом при применении преобразований $s_i(x)$ и $s'_i(x)$ одинаков. Теперь более подробно.

Пусть $a \sim_{s_i} b$, то есть найдется такое число m, что $s_i^m(a) = s_i^m(b)$. Но тогда по определению преобразования s'_i по преобразованию $s_i(x)$ верно, что $(s'_i)^m(a) = (s'_i)^m(b)$. Аналогичное рассуждение проходит и в обратную сторону.

Пусть $a \in F$. Тогда если $a = 0$, то $s'_i(a) = s_i(a)$, и

$$s_i(a) \sim_{s_i} s_i, (a), \qquad s_i(a) \sim_{s'_i} s'_i(a),$$

случай $a = c$ рассматривается аналогично.

Если $s_i(a) = 0$, то $s'_i(a) = c$ и

$$0 \sim_{s_i} c, \qquad 0 \sim_{s'_i} c,$$

случай $s_i(a) = c$ рассматривается аналогично.

Если $s_i(a) \neq 0$ и $s_i(a) \neq c$, то $s_i(a) = s'_i(a)$, и значит,

$$s_i(a) \sim_{s_i} s'_i(a), \qquad s_i(a) \sim_{s'_i} s'_i(a).$$

Таким образом, преобразования $s_i(x)$ и $s'_i(x)$ эквивалентны и один из циклических элементов преобразования $s'_i(x)$ есть 0.

По лемме 2 многочлен $f(x_1, \ldots, x_n)$ инвариантен относительно набора преобразований

$$s_1(x), \ldots, s_{i-1}(x), s'_i(x), s_{i+1}(x), \ldots, s_n(x).$$

Лемма 3 доказана.

Леммы 1, 2 и 3 описывают функциональные свойства инвариантных относительно связных преобразований многочленов. В следующей лемме 4 представлено одно их структурное свойство.

Лемма 4. *Пусть многочлен $f(x_1, \ldots, x_n)$ не равен нулю, инвариантен относительно набора связных преобразований $s_1(x), \ldots, s_n(x)$ ранга q. Тогда $\varnothing \in T^q(f)$.*

Доказательство. В силу леммы 3 мы можем полагать, что элемент 0 является циклическим для каждого из преобразований $s_i(x)$, $i = 1, \ldots, n$.

Так как многочлен $f(x_1, \ldots, x_n)$ не равен 0, найдется такой ненулевой набор элементов $a_1, \ldots, a_n$ из F, что $f(a_1, \ldots, a_n) \neq 0$. Пусть $m_1, \ldots, m_n$ — такие числа, что $s_i^{m_i}(a_i)$, $i = 1, \ldots, n$, являются циклическими элементами. Пусть m — наибольшее из чисел $m_1, \ldots, m_n$. Положим $b_i = s^m(a_i)$. По замечанию к определению циклического элемента элементы $b_1, \ldots, b_n$ циклические.

Многочлен $f(x_1, \ldots, x_n)$ инвариантен относительно $s_1(x), \ldots, s_n(x)$, поэтому

$$f(b_1, \ldots, b_n) = f(a_1, \ldots, a_n) \neq 0.$$

Построим множества индексов $I_j \subseteq \{1, \ldots, n\}$, полагая, что $i \in F_j$ тогда и только тогда, когда $s_i^j(b_i) = 0$, $i = 1, \ldots, n$. Так как ранг набора преобразований $s_1(x), \ldots, s_n(x)$ равен q, число множеств I_j не превосходит q. Заметим также, что множества I_j попарно не пересекаются, а их объединение есть множество $\{1, \ldots, n\}$.

Рассмотрим непустое множество I_j. Ясно, что

$$f(s_1^j(b_1), \ldots, s_n^j(b_n)) = f(b_1, \ldots, b_n) \neq 0.$$

Следовательно, в многочлене $f(x_1, \ldots, x_n)$ найдется одночлен, не содержащий переменные с индексами из I_j. Обозначим его $X^{(j)}$. Пересечение типов всех таким образом построенных одночленов $X^{(j)}$ есть $\varnothing$. Так как их число не больше, чем q, верно, что $\varnothing \in T^q(f)$.

Лемма 4 доказана.

Каждому связному преобразованию $s(x)$ с нулевым циклическим элементом сопоставим функцию $t_s(x)$, построенную по правилу: $t_s(x) = m$, если m — наименьшее из всех таких чисел, что $s^m(x) = 0$. Назовем ее функцией расстояний преобразования $s(x)$. По определению функции расстояний $t_s(x)$ связного преобразования $s(x)$ с нулевым циклическим элементом справедливы равенства

$$s^{t_s(x)}(x) = 0, \qquad s^{t_s(0)}(x) = x.$$

Кроме того, если $s_1(x)$ — связное преобразование с нулевым циклическим элементом, $t_{s_1}(x)$ — его функция расстояний и $s_2(x)$ — связное преобразование, то

$$s_2^{t_{s_1}(s_1(x))}(s_2(y)) = s_2^{t_{s_1}(x)}(y).$$

Действительно,

$$s_2^{t_{s_1}(s_1(x))}(s_2(y)) = s_2^{t_{s_1}(s_1(x))+1}(y) = s_2^{t_{s_1}(x)}(y).$$

Лемма 5. *Многочлен $f(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$ инвариантен относительно набора связных преобразований $s_1(x), \ldots, s_n(x)$ с нулевыми циклическими элементами тогда и только тогда, когда для некоторого i, $1 \leqslant i \leqslant n$,*

$$f(x_1, \ldots, x_n) = h(s_1^{t_{s_i}(x_i)}(x_1), \ldots, s_{i-1}^{t_{s_i}(x_i)}(x_{i-1}), s_{i+1}^{t_{s_i}(x_i)}(x_{i+1}), \ldots, s_n^{t_{s_i}(x_i)}(x_n)),$$

где $h(y_1, \ldots, y_{n-1})$ — некоторый многочлен из $F[y_1, \ldots, y_{n-1}]$ и $t_{s_i}(x)$ — функция расстояний преобразования $s_i(x)$.

Доказательство. Положим для определенности, что $i = 1$. Докажем необходимость. Пусть многочлен $f(x_1, \ldots, x_n)$ инвариантен относительно набора связных преобразования $s_1(x), \ldots, s_n(x)$ с нулевыми циклическими элементами. Пусть $t_1(x)$ — функция расстояний преобразования $s_1(x)$.

Определим многочлен $h(y_1, \ldots, y_{n-1})$ как $f(0, y_1, \ldots, y_{n-1})$. Тогда

$$\begin{aligned} h(s_2^{t_1(x_1)}(x_2), \ldots, s_n^{t_1(x_1)}(x_n)) &= f(0, s_2^{t_1(x_1)}(x_2), \ldots, s_n^{t_1(x_1)}(x_n)) \\ &= f(s_1^{t_1(x_1)}(x_1), s_2^{t_1(x_1)}(x_2), \ldots, s_n^{t_1(x_1)}(x_n)) \\ &= f(x_1, \ldots, x_n). \end{aligned}$$

Докажем достаточность. Пусть для некоторого многочлена $h(y_1, \ldots, y_{n-1})$ из $F[y_1, \ldots, y_{n-1}]$ верно равенство

$$f(x_1, \ldots, x_n) = h(s_2^{t_1(x_1)}(x_2), \ldots, s_n^{t_1(x_1)}(x_n)).$$

Тогда можно заключить, что

$$\begin{aligned} f(s_1(x_1), s_2(x_2), \ldots, s_n(x_n)) &= h(s_2^{t_1(s_1(x_1))}(s_2(x_2)), \ldots, s_n^{t_1(s_1(x_1))}(s_n(x_n))) \\ &= h(s_2^{t_1(x_1)}(x_2), \ldots, s_n^{t_1(x_1)}(x_n)) \\ &= f(x_1, \ldots, x_n). \end{aligned}$$

Таким образом, многочлен $f(x_1, \ldots, x_n)$ инвариантен относительно набора преобразований $s_1(x_1), \ldots, s_n(x_n)$.

Лемма 5 доказана.

Лемма 5 представляет собой критерий инвариантности относительно связных преобразований с нулевыми циклическими элементами многочленов из $F[x_1,\dots,x_n]$.

На множестве многочленов $f(x_1,\dots,x_n)$ из $F[x_1,\dots,x_n]$, инвариантных относительно набора связных преобразований $s_1(x),\dots,s_n(x)$ с нулевыми циклическими элементами, введем функционал $f_{x_i}^{(x_j)}$, называемый производной по переменной x_i через переменную x_j, причем $i \neq j$.

Не ограничивая общности, положим, что $i = n$ и $j = 1$. По лемме 5

$$f(x_1,\dots,x_n) = h(s_2^{t_{s_1}(x_1)}(x_2),\dots,s_n^{t_{s_1}(x_1)}(x_n)),$$

причем $h(x_2,\dots,x_n) = f(0,x_2,\dots,x_n)$.

Пусть $g(x_2,\dots,x_n) = h'_{x_n}(x_2,\dots,x_n)$, то есть мы рассматриваем производную многочлена $h(x_2,\dots,x_n)$ по переменной x_n, которую можно ввести без применения понятия непрерывности (см., например, [2]). Тогда

$$f_{x_n}^{(x_1)} = g(s_2^{t_{s_1}(x_1)}(x_2),\dots,s_n^{t_{s_1}(x_1)}(x_n)).$$

Из последнего равенства с использованием леммы 5 получаем следующее утверждение.

Лемма 6. *Если многочлен $f(x_1,\dots,x_n)$ инвариантен относительно набора связных преобразований $s_1(x),\dots,s_n(x)$ с нулевыми циклическими элементами, то многочлен $f_{x_i}^{(x_j)}$ также инвариантен относительно преобразований $s_1(x),\dots,s_n(x)$.*

Лемма 7. *Пусть многочлен $f(x_1,\dots,x_n)$ не равен нулю, инвариантен относительно набора связных преобразований $s_1(x),\dots,s_n(x)$ с нулевыми циклическими элементами. Пусть X — одночлен, в котором переменная x_j не является сомножителем и переменные x_j и x_i различны. Если одночлен X является слагаемым многочлена $f_{x_i}^{(x_j)}(x_1,\dots,x_n)$, то одночлен x_iX является слагаемым многочлена $f(x_1,\dots,x_n)$.*

Доказательство. Положим для определенности, что $j = 1$. Многочлен $f(x_1,\dots,x_n)$ инвариантен относительно набора связных преобразований $s_1(x),\dots,s_n(x)$ с нулевыми циклическими элементами, поэтому по лемме 5

$$f(x_1,\dots,x_n) = h(s_2^{t_{s_1}(x_1)}(x_2),\dots,s_n^{t_{s_1}(x_1)}(x_n)).$$

Так как

$$s_2^{t_{s_1}(0)}(x_2) = x_2,\dots,s_n^{t_{s_1}(0)}(x_n) = x_n,$$

верно, что $h(x_2,\dots,x_n) = f(0,x_2,\dots,x_n)$. Таким образом,

$$f(x_1,\dots,x_n) = x_1g(x_1,\dots,x_n) + h(x_2,\dots,x_n),$$

где $g(x_1,\dots,x_n)$ — вполне определенный многочлен.

Производная может быть записана в виде

$$f_{x_i}^{(x_1)} = x_1g_1(x_1,\dots,x_n) + h'_{x_i}(x_2,\dots,x_n),$$

где $g_1(x_1,\dots,x_n)$ — вполне определенный многочлен.

Так как переменная x_1 не входит в качестве сомножителя в одночлен X, многочлен $h'_{x_i}(x_2,\dots,x_n)$ содержит одночлен X как слагаемое. Следовательно, по правилам взятия производной многочлен $h(x_2,\dots,x_n)$ содержит одночлен x_iX как слагаемое. Значит, одночлен x_iX является слагаемым многочлена $f(x_1,\dots,x_n)$.

Лемма 7 доказана.

Теперь мы докажем теоремы 1 и 2.

Доказательство теоремы 2. По лемме 3 мы можем полагать, что элемент 0 является циклическим для каждого из преобразований $s_i(x)$, $i=1,\dots,n$.

Если рассматриваемый подтип t есть $\{x_1,\dots,x_n\}$, то многочлен $f(x_1,\dots,x_n)$ содержит слагаемое вида $x_1^{m_1}\dots x_n^{m_n}$, $m_1,\dots,m_n\geqslant 1$, и, значит, $t\in T^q(f)$.

Рассмотрим слагаемое X многочлена $f(x_1,\dots,x_n)$. Пусть ранг одночлена X равен r, причем $1\leqslant r\leqslant n-1$. Рассмотрим подтип $t=\{x_{i_1},\dots,x_{i_{r_1}}\}$ типа одночлена X. Заметим, что $1\leqslant r_1\leqslant r$. Так как $r<n$, найдется некоторая переменная, не являющаяся сомножителем в одночлене X. Не ограничивая общности рассуждений, обозначим ее x_{r+1}.

Рассмотрим многочлен

$$g(x_1,\dots,x_n)=f^{(x_{r+1})\dots(x_{r+1})}_{x_{i_1}\dots x_{i_{r_1}}}(x_1,\dots,x_n).$$

Полученный многочлен $g(x_1,\dots,x_n)$ не равен нулю и по лемме 6 инвариантен относительно набора связных преобразований $s_1(x),\dots,s_n(x)$.

По лемме 5 найдутся слагаемые $X^{(1)},\dots,X^{(q)}$ многочлена $g(x_1,\dots,x_n)$, пересечение типов которых пусто. По лемме 7 слагаемые

$$x_{i_1}\dots x_{i_r}X^{(1)},\dots,x_{i_1}\dots x_{i_r}X^{(q)}$$

содержатся в многочлене $f(x_1,\dots,x_n)$. Несложно заметить, что пересечение их типов есть тип t.

Наконец, подтип $t=\varnothing$ типа одночлена X содержится в $T^q(f)$ согласно лемме 4.

Теорема 2 доказана.

Доказательство теоремы 1. Так как ранг многочлена $f(x_1,\dots,x_n)$ равен r, найдется слагаемое X многочлена $f(x_1,\dots,x_n)$ вида $x_{i_1}^{m_1}\dots x_{i_r}^{m_r}$. Имеется 2^r подтипов типа слагаемого X. В теореме 2, в частности, утверждается, что каждый подтип типа слагаемого X содержится в множестве $T^q(f)$. Мощность множества $T^q(f)$ не превосходит w^q. Следовательно, $w^q\geqslant 2^r$.

Теорема 1 доказана.

Список литературы

1. Лидл Р., Нидеррайтер Г., *Конечные поля*. Мир, Москва, 1988.

2. ван дер Варден Б. Л., *Алгебра*. Наука, Москва, 1979.

3. Зыков А. А., *Основы теории графов*. Наука, Москва, 1987.

Статья поступила 05.06.1999.