Math-Net.Ru

Общероссийский математический портал

А. П. Семигродских, Е. В. Суханов, О замкнутых классах полиномов над конечными полями, *Дискрет. матем.*, 1997, том 9, выпуск 4, 50–62

DOI: <https://doi.org/10.4213/dm502>

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

Параметры загрузки:

IP: 35.173.137.237

26 апреля 2023 г., 07:41:37

О замкнутых классах полиномов над конечными полями

© 1997 г. А. П. Семигродских, Е. В. Суханов

Изучается строение решетки замкнутых классов k -значных функций. Пусть F — класс всех полиномов над полем из $k = p^n$ элементов, L^0 — класс линейных форм над этим полем. В работе дается полное описание всех замкнутых классов, лежащих в указанной решетке между L^0 и F . В частности указаны (конечные) базисы таких классов.

1. Основные обозначения и формулировки

Данная работа является продолжением [1] и посвящена классификации части замкнутых классов полиномов над полем Галуа $GF(p^n)$.

Приведем основные обозначения. Пусть R — произвольное конечное ассоциативно-коммутативное кольцо с единицей. Мы рассматриваем алгебраические многочлены над R от произвольного (конечного) числа переменных и замкнутые классы таких многочленов. Введем основные для нас замкнутые классы: F_R — класс всех полиномов над R ; F_R^0 — класс всех полиномов из F_R без свободного члена; L_R — класс всех линейных полиномов из F_R ; L_R^0 — класс всех линейных полиномов из L_R без свободного члена.

Так как замкнутые классы функций, отображающих декартовы степени R в R , образуют решетку по включению, упомянутую в начале классификацию можно понимать как задачу описания интересующей нас части в этой решетке. Отмеченные выше замкнутые классы изображены на рис. 1. Знаки вопросов означают, что указанные интервалы в решетке всех замкнутых классов могут содержать и другие замкнутые классы. Это зависит от алгебраических свойств кольца R .

Рис. 1

Рис. 2

В [1] было показано, что в случае кольца вычетов по любому модулю весь решеточный интервал $[L_R^0, F_R]$ есть подпрямое произведение интервалов $[L_R^0, F_R^0]$ и $[L_R^0, L_R]$. Соответствующее доказательство проходит и для произвольного кольца R . Поэтому исследование интервала $[L_R^0, F_R]$ в каком-то смысле сводится к изучению интервалов $[L_R^0, F_R^0]$ и $[L_R^0, L_R]$. Следуя этой идее, мы даем полное описание интервала $[L_R^0, F_R]$ в том важном случае, когда кольцо R является конечным полем, т. е. полем Галуа $GF(p^n)$. Это и есть основной результат работы.

В [1] для случая кольца вычетов показано, что интервалы $[L_R^0, L_R]$ и $[F_R^0, F_R]$ изоморфны решетке идеалов кольца R (а, значит, и между собой). Снова доказательство этого без изменений переносится на произвольное кольцо R . Поэтому интервал $[L_R^0, F_R]$ для поля $GF(p^n)$ имеет вид, изображенный на рис. 2. Так как всюду далее $R = GF(p^n)$, на рис. 2 и в дальнейшем мы опускаем индекс R .

Устройство интервала $[L, F]$ было выяснено в [2]. Там доказано, что $[L, F]$ без F дуально изоморфен решетке делителей числа n , а F выступает в роли внешне-присоединенного наибольшего элемента. Для каждого замкнутого класса из $[L, F]$, отличного от F , было указано порождающее множество. Кроме линейных функций в такое множество входит один полином вида x^{p^d} , где d есть делитель n .

Условимся об обозначениях. Пусть K — замкнутый класс из $[L^0, F]$. Тогда K может быть порожден совокупностью всех линейных форм (то есть полиномов из L^0) и какими-то функциями $f_1, f_2, \dots$, из F . В этом случае мы будем писать $K = \langle \langle f_1, f_2, \dots \rangle \rangle$. Всюду далее словосочетание замкнутый класс означает замкнутый класс из $[L^0, F]$, а полином или многочлен — полином над $GF(p^n)$. Каждый из изучаемых классов содержит L^0 , поэтому, рассматривая линейные комбинации элементов класса, мы не выйдем за его пределы. Это обстоятельство далее будет использоваться без оговорок.

Как обычно, через $\mathbf{N}$ обозначается множество всех натуральных чисел $\{1, 2, \dots\}$, и запись $k \mid l$ означает, что k является делителем l . При описании подрешеток из $[L^0, F]$ мы будем использовать обозначение $\mathbf{D}(m)$ для решетки делителей числа m с указанным отношением порядка $\mid$.

Из сказанного выше ясно, что основные наши усилия направлены на выяснение устройства интервала $[L^0, F^0]$. А именно, будет доказана следующая теорема.

Теорема 1. *Каждый класс из $[L^0, F^0]$ имеет вид*

$$(1) \langle \langle x_1 \dots x_{d+1} \rangle \rangle, \text{ где } d \in \mathbf{D}(p^n - 1),$$

$$(2) \langle \langle x^{p^d} \rangle \rangle, \text{ где } d \in \mathbf{D}(n).$$

Классы вида (1) и (2) образуют решетки $\mathcal{L}_1$ и $\mathcal{L}_2$ дуально изоморфные $\mathbf{D}(p^n - 1)$ и $\mathbf{D}(n)$ соответственно.

Интервалы вида $[\langle \langle x^{p^d} \rangle \rangle, \langle \langle x_1 \dots x_{p^d} \rangle \rangle]$, где $d \in \mathbf{D}(n)$ являются простыми.

Эта теорема позволяет изобразить диаграмму интервала $[L^0, F^0]$, представленную на рис. 3.

Здесь $\mathcal{L}_1 = [\langle \langle x_1 \dots x_{p^n} \rangle \rangle, F^0]$ и $\mathcal{L}_2 = [L^0, \langle \langle x^p \rangle \rangle]$ — решетки, упоминаемые в теореме, а прямолинейные отрезки символизируют интервалы. Штриховкой изображена решетка классов вида $\langle \langle x_1 \dots x_{p^d} \rangle \rangle$, где $d \in \mathbf{D}(n)$, изоморфная $\mathcal{L}_2$ и $\mathbf{D}(n)$. Интервал $I = [\langle \langle x_1 \dots x_p \rangle \rangle, F^0]$ дуально изоморфен $\mathbf{D}(p - 1)$. В частности, при $p = 2$ интервал I вырождается в точку.

Отметим, что частный случай теоремы, когда $n = 1$, был доказан в [1].

Рис. 3.

2. Вспомогательные утверждения

Данный параграф состоит из трех пунктов. В каждом из них есть утверждения двух видов, леммы и предложения. Леммами названы те из них, которые непосредственно используются в параграфе 3 для доказательства теоремы, остальные — предложения. В первом пункте мы сформулируем три теоретико-числовых утверждения, во втором получим сведения об одночленах некоторого специального вида и докажем, что каждый замкнутый класс определяется своими одночленами. В третьем пункте мы получим практически все леммы, необходимые для доказательства теоремы.

2.1. Теоретико-числовые утверждения

Прежде, чем сформулировать первое предложение, условимся говорить, что число K , удовлетворяющее некоторым условиям, можно выбрать сколь угодно большим (сколь угодно большим, чем $X \in \mathbb{N}$), если для любого числа M существует значение K большее, чем M (соответственно $X + M$).

Предложение 1. Пусть $b, a_1, \dots, a_l \in \mathbb{N}$ и d — наибольший общий делитель $(b, a_1, \dots, a_l)$. Тогда найдутся такие сколь угодно большие $K, K_1, \dots, K_l \in \mathbb{N}$, что K_1 сколь угодно больше, чем $K_2, \dots, K_l$ и $K_1 a_1 + \dots + K_l a_l - K b = d$.

Лемма 1. Пусть p — простое число и $k, n \in \mathbb{N}$. Тогда $k \mid n$ в том и только в том случае, когда $(p^k - 1) \mid (p^n - 1)$.

Эти утверждения мы считаем известными и не приводим их доказательства.

Предложение 2. Пусть p — простое число, $n, a_1, \dots, a_l \in \mathbb{N}$ и d — наибольший общий делитель $(n, a_1, \dots, a_l)$. Тогда в множестве

$$\{(p^{K_1 a_1 + \dots + K_l a_l} - 1) - K(p^n - 1) : K, K_1, \dots, K_l \in \mathbb{N} \cup \{0\}\}$$

есть число $p^d - 1$ и оно делит все его элементы.

Доказательство. Пусть $m > n$. Тогда

$$(p^m - 1) - p^{m-n}(p^n - 1) = p^{m-n} - 1$$

Если $m - n > n$, то

$$\begin{aligned} (p^m - 1) - (p^{m-n} + p^{m-2n})(p^n - 1) &= ((p^m - 1) - p^{m-n}(p^n - 1)) - p^{m-2n}(p^n - 1) \\ &= (p^{m-n} - 1) - p^{m-2n}(p^n - 1) = p^{m-2n} - 1. \end{aligned}$$

Продолжая по индукции, получим, что если $m - (j - 1)n > n$, то

$$(p^m - 1) - (p^{m-n} + \dots + p^{m-jn})(p^n - 1) = p^{m-jn} - 1.$$

Теперь, полагая $m = K_1 a_1 + \dots + K_l a_l$, $K = p^{m-n} + \dots + p^{m-jn}$, получим, что в множестве есть число

$$p^{K_1 a_1 + \dots + K_l a_l - jn} - 1.$$

По предложению 1 можно подобрать $K_1, \dots, K_l, j$ (а, значит, и K) так, что выполнено равенство $K_1 a_1 + \dots + K_l a_l - jn = d$. С учетом леммы 1 легко получаем, что $p^d - 1$ делит любой элемент множества.

2.2. Некоторые сведения об одночленах

Условимся обозначать переменные буквами x, y, u, v , быть может, с индексами. При рассмотрении многочлена как суммы одночленов мы считаем, что подобные члены в сумме приведены.

В $GF(p^n)$ выполняется тождество

$$x^{p^n} = x \quad (1)$$

Поэтому можно считать, что степенные показатели в многочленах меньше, чем p^n . В связи с этим мы формулируем предложение 3, которое в силу его простоты оставляем без доказательства.

Предложение 3. Любые две степени x^{d_1} и x^{d_2} , где $d_1 < d_2 < p^n$, различны как функции.

Если $k \geq n$, то существует единственное число $d < n$ такое, что $x^{p^d} = x^{p^k}$, при этом $d = k - sn$, $s \in \mathbb{N}$.

Следующее утверждение дает нам одно из важнейших свойств исследуемых классов.

Лемма 2. Каждый одночлен многочлена, лежащего в замкнутом классе, сам принадлежит этому классу.

Доказательство. Пусть C — замкнутый класс, $f \in C$ и f есть сумма одночленов $m_1, \dots, m_l$. Требуется доказать, что $m_1, \dots, m_l \in C$.

Обозначим через d_i показатель переменной x_1 в одночлене m_i (для всех значений $i \in \{1, \dots, l\}$) и докажем лемму индукцией по l . При $l = 1$ утверждение очевидно. Пусть теперь оно выполнено для меньших, чем l , значений. В этой ситуации

есть переменная, входящая в два одночлена с разными степенными показателями, так как подобные приведены. Не ограничивая общности, можно считать, что эта переменная есть x_1 , нужные нам одночлены есть m_1 и m_2 , а соответствующие показатели удовлетворяют неравенству $d_1 < d_2$.

При $d_1 = 0$, подставляя вместо x_1 константу $0 \in L^0 \subseteq C$, получим, что

$$h = f(0, x_2, \dots, x_r) = m_1(x_1, \dots, x_r) + \sum_{i=3}^l m_i(0, x_2, \dots, x_r) \in C.$$

Так как $d_2 > 0$, в $h \in C$ одночленов меньше, чем l . Значит, по предположению индукции $m_1 \in C$, $f - m_1 \in C$, и в $f - m_1 = m_2 + \dots + m_l$ меньше, чем l , одночленов. Теперь по предположению индукции $m_2, \dots, m_l \in C$ и, наконец, $m_1, m_2, \dots, m_l \in C$.

При $d_1 \neq 0$ существует такое $a \in GF(p^n)$, $a \neq 0$, что $a^{d_1} \neq a^{d_2}$ (предложение 3). Запишем одночлены в виде $m_i = x_1^{d_i} m'_i(x_2, \dots, x_r)$ и рассмотрим многочлен из C :

$$\begin{aligned} g &= a^{d_1} f(a^{-1} x_1, x_2, \dots, x_r) - f(x_1, \dots, x_r) \\ &= \sum_{i=1}^l (a^{d_1-d_i} - 1) x_1^{d_i} m'_i = \sum_{i=2}^l (a^{d_1-d_i} - 1) x_1^{d_i} m'_i. \end{aligned}$$

Здесь $(a^{d_1-d_2} - 1) x_1^{d_2} m'_2 \neq 0$ (a , значит, и $g \neq 0$), так как $a^{d_1} \neq a^{d_2}$. Очевидно, g — сумма не более, чем $l-1$, одночленов. По предположению индукции $(a^{d_1-d_2} - 1) m_2 \in C$, и поэтому

$$m_2 = (a^{d_1-d_2} - 1)^{-1} (a^{d_1-d_2} - 1) m_2 \in C.$$

Следовательно, $f - m_2 \in C$, и в $f - m_2$ не более $l-1$ одночленов. Аналогично случаю $d_1 = 0$ получаем, что $m_1, m_2, \dots, m_l \in C$.

Доказанная лемма дает нам основание утверждать, что каждый замкнутый класс определяется своими одночленами, поэтому целесообразно выделить наиболее простые одночлены, определяющие класс. В случае $GF(p)$ (см. [1]) это произведения переменных. В $GF(p^n)$ для любого $k \in \mathbb{N}$ выполняется тождество

$$(x + y)^{p^k} \equiv x^{p^k} + y^{p^k},$$

и мы не сможем применить для получения таких произведений использованный в [1] прием. С помощью следующего предложения мы сможем переходить от одночленов общего вида к одночленам, показатели степеней в которых имеют вид p^i , где $i \in \{0, \dots, n-1\}$. Дальнейшее упрощение будет произведено в леммах 3 и 4.

Предложение 4. Пусть

$$d = \sum_{i=0}^{n-1} a_i p^i, \quad a_i \in \{0, \dots, p-1\}.$$

Если C есть замкнутый класс и $x_1^d m(x_2, \dots, x_l) \in C$, то

$$m(x_2, \dots, x_l) (y_{0,1} \dots y_{0,a_0}) \dots (y_{n-1,1} \dots y_{n-1,a_{n-1}})^{p^{n-1}} = m \prod_{i=0}^{n-1} \prod_{j=1}^{a_i} y_{ij}^{p^i} \in C.$$

Доказательство. Очевидно, что

$$(u_1 + \dots + u_d) \in L^0 \subset C,$$

$$(u_1 + \dots + u_d)^d m \in C.$$

В $GF(p^n)$ справедливо равенство

$$(u_1 + \dots + u_d)^{p^i} = u_1^{p^i} + \dots + u_d^{p^i},$$

поэтому

$$(u_1 + \dots + u_d)^d m = (u_1 + \dots + u_d)^{a_0 p^0} \dots (u_1 + \dots + u_d)^{a_{n-1} p^{n-1}} m$$

$$= (u_1 + \dots + u_d)^{a_0} \dots (u_1^{p^{n-1}} + \dots + u_d^{p^{n-1}})^{a_{n-1}} m.$$

Воспользовавшись формулой возведения в степень a_i , в i -х скобках получим

$$\alpha_i \prod_{j=S_{i-1}+1}^{S_i} u_j^{p^i} + f_i,$$

где

$$S_k = \sum_{r=0}^k a_r,$$

α_i — ненулевой коэффициент и f_i не имеет членов, подобных первому слагаемому. Перемножая скобки, видим, что

$$\left(\left(\prod_{r=0}^{n-1} \alpha_i \right) \prod_{i=0}^{n-1} \prod_{j=S_{i-1}+1}^{S_i} u_j^{p^i} + g \right) m \in C,$$

где g не содержит слагаемых, подобных первому в скобках.

Согласно лемме 2

$$\left(\prod_{r=0}^{n-1} \alpha_i \right) m \prod_{i=0}^{n-1} \prod_{j=S_{i-1}+1}^{S_i} u_j^{p^i} \in C.$$

Умножая на

$$\left(\prod_{r=0}^{n-1} \alpha_i \right)^{-1},$$

получим, что

$$m \prod_{i=0}^{n-1} \prod_{j=S_{i-1}+1}^{S_i} u_j^{p^i} \in C.$$

Переименовав переменные, находим, что

$$m \prod_{i=0}^{n-1} \prod_{j=1}^{a_i} y_{ij}^{p^i} \in C,$$

что и требовалось.

Применяя это предложение к каждой переменной одночлена (аналогично x_1), получим следующее утверждение.

Следствие 1. Пусть C — замкнутый класс и $x_1^{d_1} \dots x_r^{d_r} \in C$. Если

$$d_s = \sum_{i=0}^{n-1} a_{s,i} p^i$$

и $a_{s,i} \in \{0, \dots, p-1\}$ для любых $s \in \{1, \dots, r\}$, $i \in \{0, \dots, n-1\}$, то

$$\prod_{i=0}^{n-1} \prod_{j=1}^{a_{1,i}} y_{1ij}^{p^i} \dots \prod_{i=0}^{n-1} \prod_{j=1}^{a_{ri,i}} y_{rij}^{p^i} = \prod_{s=1}^r \prod_{i=0}^{n-1} \prod_{j=1}^{a_{si,i}} y_{sij}^{p^i} \in C.$$

Данное следствие дает основание утверждать, что если в C есть одночлен, не имеющий вид ax^{p^i} , то в C есть одночлен вида $x_1^{p^{d_1}} x_2^{p^{d_2}} m(x_3, \dots, x_r)$.

2.3. О степенях одночленов и порождающих множествах замкнутых классов

В этом пункте будут доказаны две леммы, из которых сразу вытекает справедливость первого утверждения теоремы. Но вначале мы докажем лемму, которая используется при доказательстве основных утверждений данного пункта, а также в доказательстве второго и третьего утверждений теоремы.

Лемма 3. Пусть $m_1, \dots, m_l$ — одночлены положительных степеней $D_1, \dots, D_l$ соответственно, d наибольший общий делитель $(p^n - 1, D_1 - 1, \dots, D_l - 1)$ и $D_0 > 0$ есть степень одночлена из $\langle\langle m_1, \dots, m_l \rangle\rangle$. Тогда $D_0 - 1$ делится на d .

Доказательство. Рассмотрим алгебру $(P_{p^n}; \zeta, \tau, \Delta, \nabla, *)$, определенную в [3]. Напомним, что стандартные итеративные операции $\zeta, \tau, \Delta, \nabla, *$ действуют следующим образом:

при $N > 1$

$$\begin{aligned} (\zeta f)(x_1, \dots, x_N) &= f(x_2, \dots, x_N, x_1), \\ (\tau f)(x_1, x_2, x_3, \dots, x_N) &= f(x_2, x_1, x_3, \dots, x_N), \\ (\Delta f)(x_1, \dots, x_{N-1}) &= f(x_1, x_1, x_2, \dots, x_{N-1}), \\ (\nabla f)(x_1, \dots, x_{N+1}) &= f(x_2, \dots, x_{N+1}), \end{aligned}$$

при $N = 1$

$$\zeta f = \tau f = \Delta f = f$$

и, наконец,

$$(f * g)(x_1, \dots, x_m, x_{m+1}, \dots, x_{m+k-1}) = f(g(x_1, \dots, x_m), x_{m+1}, \dots, x_{m+k-1}).$$

Замкнутый класс $\langle\langle m_1, \dots, m_l \rangle\rangle$ является подалгеброй, порожденной множеством $L^0 \cup \{m_1, \dots, m_l\}$. Мы докажем лемму индукцией по построению этой подалгебры. База индукции очевидна. Переходя к шагу индукции, отметим, что операции ζ, τ, ∇ не изменяют степени одночленов. Поэтому достаточно рассмотреть действие на степени операций Δ и $*$.

При действии Δ степень может лишь уменьшиться на $p^n - 1$ в силу (1), так как если сумма степеней отождествляемых переменных превысит $p^n - 1$, то мы учтем, что $x^{p^n} \equiv x$.

При подстановке $m * f$, где $m = x_1^\alpha m'(x_2, \dots, x_s)$ — одночлен степени $1 + rd$, $f = m_1 + \dots + m_l$, m_i — одночлены, $\deg m_i = 1 + q_i d$, получаются одночлены со степенями вида $1 + qd$.

В самом деле,

$$(m_1 + \dots + m_l)^\alpha = \sum_{t=0}^T a_t m_1^{\beta_{1t}} \dots m_l^{\beta_{lt}},$$

где $\beta_{1t} + \dots + \beta_{lt} = \alpha$ для любого $t \in \{0, \dots, T\}$. Если $a_t \neq 0$, то слагаемое с номером t имеет степень

$$(1 + q_1 d)\beta_{1t} + \dots + (1 + q_l d)\beta_{lt} = \sum_{j=1}^l \beta_{jt} + d \sum_{j=1}^l \beta_{jt} q_j = \alpha + C_t d.$$

При подстановке $m * (m_1 + \dots + m_l)$ получим

$$(m_1 + \dots + m_l)^\alpha m' = \sum_{t=0}^T a_t m_1^{\beta_{1t}} \dots m_l^{\beta_{lt}} m'.$$

Здесь слагаемое с номером t имеет степень

$$\alpha + C_t d + (1 + rd - \alpha) = 1 + C_t d + rd,$$

так как $\deg m' = 1 + rd - \alpha$.

Как и в случае операции Δ , учитывая (1), получим степень вида

$$D_0 = 1 + K_1 d - K_2(p^n - 1).$$

Очевидно, что $D_0 - 1 = K_1 d - K_2(p^n - 1)$ делится на d .

Общие случаи применения операций Δ и $*$ сводятся к предыдущим, так как

$$\begin{aligned} \Delta(M_1 + \dots + M_s) &= \Delta M_1 + \dots + \Delta M_s, \\ (M_1 + \dots + M_s) * f &= M_1 * f + \dots + M_s * f. \end{aligned}$$

Лемма доказана.

Лемма 4. Если d — наибольший общий делитель $(n, a_1, \dots, a_l)$, то

$$\langle \langle x^{p^{a_1}}, \dots, x^{p^{a_l}} \rangle \rangle = \langle \langle x^{p^d} \rangle \rangle.$$

Доказательство. Одночлены замкнутого класса $\langle \langle x^{p^{a_1}}, \dots, x^{p^{a_l}} \rangle \rangle$ имеют вид

$$ax^{p^{K_1 a_1 + \dots + K_l a_l}},$$

так как

$$\begin{aligned} x^{p^k} * x^{p^m} &= x^{p^{k+m}}, \\ (x_1 + \dots + x_k)^{p^m} &= x_1^{p^m} + \dots + x_k^{p^m}. \end{aligned}$$

В силу (1) эти одночлены имеют вид

$$ax^{p^{K_1 a_1 + \dots + K_l a_l - K(p^n - 1)}}.$$

По предложению 2 $\langle\langle x^{p^{a_1}}, \dots, x^{p^{a_l}} \rangle\rangle \supseteq \langle\langle x^{p^d} \rangle\rangle$. Обратное включение очевидно, так как $d \mid a_1, \dots, d \mid a_l$ и

$$x^{p^{a_i}} = x^{p^{(a_i/d)d}} = x^{p^d} * \dots * x^{p^d},$$

где число множителей равно a_i/d .

Для доказательства оставшейся леммы нам понадобятся два предложения.

Предложение 5. Пусть $m = x_1^{p^{k_1}} x_2^{p^{k_2}} m_1(x_3, \dots, x_r)$ — одночлен, $m \neq 0$. Тогда существует такой одночлен $m_2(y_3, \dots, y_s) \neq 0$, что

$$y_1 y_2 m_2(y_3, \dots, y_s) \in \langle\langle m \rangle\rangle.$$

Доказательство. Ясно, что

$$(u_1^{p^{k_1}} u_2^{p^{k_2}} m_1)^{p^{k_1}} x_2^{p^{k_2}} m_1 = u_1^{p^{2k_1}} x_2^{p^{k_2}} m'_1 \in \langle\langle m \rangle\rangle,$$

где m'_1 не зависит от u_1 и x_2 . Аналогично, применяя суперпозицию и учитывая тождество (1), получим, что

$$u^{p^{a_{k_1} - b(p^n - 1)}} x_2^{p^{k_2}} \tilde{m}_1 \in \langle\langle m \rangle\rangle,$$

где $\tilde{m}_1$ не зависит от u и x_2 . По предложению 2

$$u^{p^d} x_2^{p^{k_2}} m''_1 \in \langle\langle m \rangle\rangle,$$

где d — наибольший общий делитель (k_1, n) . Опять производя суперпозиции, видим, что

$$u^{p^{(n:d)d}} x_2^{p^{k_2}} m'''_1 = u^{p^n} x_2^{p^{k_2}} m'''_1 = u x_2^{p^{k_2}} m'''_1 \in \langle\langle m \rangle\rangle.$$

Применив те же рассуждения к x_2 в последнем одночлене и переименовав переменные, получим, что $y_1 y_2 m_2 \in \langle\langle m \rangle\rangle$.

Предложение 6. Пусть $m = x_1 x_2 m_1(x_3, \dots, x_r)$ — одночлен, $m \neq 0$. Тогда существует сколь угодно большое число D такое, что

$$y_1 \dots y_D \in \langle\langle m \rangle\rangle.$$

Доказательство. Покажем, что для любого наперед заданного числа M существует $D > M$ с нужным свойством.

С помощью суперпозиций можно получить включение

$$u_1 \dots u_l m_2 \in \langle\langle m \rangle\rangle,$$

где m_2 не зависит от $u_1, \dots, u_l$. Положим $l > M + p^n$ и отождествим переменные в m_2 с v , откуда $u_1 \dots u_l v^r \in \langle\langle m \rangle\rangle$, где $r < p^n$. Отождествляя с v последние $p^n - r$ из переменных u_i , находим, что

$$u_1 \dots u_{l-p^n+r} v^{p^n} = u_1 \dots u_{l-p^n+r} v \in \langle\langle m \rangle\rangle.$$

Переименовав переменные, получим, что $y_1 \dots y_D \in \langle\langle m \rangle\rangle$. При этом $D = l - p^n + r + 1 > M + r + 1 > M$, что и требовалось доказать.

Лемма 5. Пусть $m_1, \dots, m_l$ — одночлены положительных степеней $D_1, \dots, D_l$ соответственно, хотя бы один из них не имеет вид ax^{p^k} и d — наибольший общий делитель $p^n - 1, D_1 - 1, \dots, D_l - 1$. Тогда

$$\langle\langle m_1, \dots, m_l \rangle\rangle = \langle\langle x_1 \dots x_{d+1} \rangle\rangle.$$

Доказательство. Не ограничивая общности, мы можем считать, что m_1 не имеет вид ax^{p^k} . По следствию 1 $\langle\langle m_1 \rangle\rangle$ есть одночлен вида $x_1^{p^{d_1}} x_2^{p^{d_2}} m(x_3, \dots, x_s)$. По предложению 5 в $\langle\langle m_1 \rangle\rangle$ имеется одночлен вида $x_1 x_2 m'(x_3, \dots, x_r)$, а по предложению 6 имеется одночлен $x_1 \dots x_D$. При этом по лемме 3 число $D - 1$ делится на наибольший общий делитель $p^n - 1$ и $D_1 - 1$. Легко видеть, что наибольший общий делитель чисел $D - 1, p^n - 1, D_1 - 1, \dots, D_l - 1$ равен d . Значит, по предложению 1 существуют $C, K, K_1, \dots, K_l$ такие, что

$$C(D - 1) + K_1(D_1 - 1) + \dots + K_l(D_l - 1) - K(p^n - 1) = d. \quad (2)$$

Здесь C можно выбрать сколь угодно большим числом $K_1, \dots, K_l$. Выберем $C > (K_1 + \dots + K_l + p^n)/(D - 1)$, то есть $C(D - 1) > (K_1 + \dots + K_l + p^n)$.

С помощью суперпозиций построим одночлен $u_1 \dots u_{C(D-1)+1}$. Очевидно, что

$$u_1 \dots u_{C(D-1)+1} \in \langle\langle m_1 \rangle\rangle \subseteq \langle\langle m_1, \dots, m_l \rangle\rangle,$$

так как $x_1 \dots x_D \in \langle\langle m_1 \rangle\rangle$.

Подставим вместо первых K_1 переменных в это произведение одночлен m_1 , вместо следующих K_2 одночлен m_2 и так далее до m_l . После этого отождествим все переменные в подставленных одночленах с v . Получим включение

$$v^r u_N u_{C(D-1)+1} \in \langle\langle m_1, \dots, m_l \rangle\rangle,$$

где

$$r < p^n, \quad N = 1 + \sum_{i=1}^l K_i.$$

Теперь отождествим $p^n - r$ из оставшихся переменных u_i с v и снова учтем, что $x^{p^n} \equiv x$. Мы построили произведение $1 + C(D - 1) - (K_1 + \dots + K_l + p^n - r) > 1$ переменных. Если степень полученного одночлена еще не равна $1 + d$, то, согласно (1) и (2), отождествляя переменные группами по p^n , получаем, что

$$x_1 \dots x_{d+1} \in \langle\langle m_1, \dots, m_l \rangle\rangle.$$

Значит, $\langle\langle m_1, \dots, m_l \rangle\rangle \supseteq \langle\langle x_1 \dots x_{d+1} \rangle\rangle$.

Так как обратное включение очевидно, лемма доказана.

3. Доказательство теоремы и заключительные замечания

Начнем с первого утверждения теоремы. Рассмотрим произвольный замкнутый класс.

Если все одночлены класса имеют вид ax^{p^k} , то из леммы 4 следует, что

$$\langle\langle a_1 x^{p^{k_1}}, \dots, a_l x^{p^{k_l}} \rangle\rangle = \langle\langle x^{p^d} \rangle\rangle,$$

где d — наибольший общий делитель чисел $n, k_1, \dots, k_l$.

Если хотя бы один из них не имеет вид ax^{p^k} , то разобьем все одночлены класса на группы в соответствии с делителями числа $p^n - 1$ следующим образом: в группу, отвечающую делителю d_i , одночлен степени D попадет тогда и только тогда, когда наибольший общий делитель чисел $D - 1$ и $p^n - 1$ равен d_i . Теперь, включив в порождающее множество исходный одночлен и по одному одночлену из каждой группы, получим по лемме 5 класс $\langle\langle x_1 \dots x_{d+1} \rangle\rangle$, где d есть наибольший общий делитель чисел $p^n - 1, D_1 - 1, \dots, D_l - 1$.

Так как каждый замкнутый класс по лемме 2 определяется своими одночленами, первое утверждение теоремы доказано.

Перейдем к доказательству второго утверждения теоремы. Рассмотрим классы $\langle\langle x_1 \dots x_{d_1+1} \rangle\rangle$ и $\langle\langle x_1 \dots x_{d_2+1} \rangle\rangle$, где $d_1, d_2 \in \mathbf{D}(p^n - 1)$.

Если $d_1 \mid d_2$, то $\langle\langle x_1 \dots x_{d_1+1} \rangle\rangle \supseteq \langle\langle x_1 \dots x_{d_2+1} \rangle\rangle$, так как для любого натурального k

$$x_1 \dots x_{kd_1+1} \in \langle\langle x_1 \dots x_{d_1+1} \rangle\rangle.$$

Если d_1 не делит d_2 , то по лемме 3 $x_1 \dots x_{d_2+1} \notin \langle\langle x_1 \dots x_{d_1+1} \rangle\rangle$, откуда

$$\langle\langle x_1 \dots x_{d_1+1} \rangle\rangle \not\supseteq \langle\langle x_1 \dots x_{d_2+1} \rangle\rangle.$$

Таким образом, решетка классов вида $\langle\langle x_1 \dots x_{d+1} \rangle\rangle$, где $d \in \mathbf{D}(p^n - 1)$, дуально изоморфна $\mathbf{D}(p^n - 1)$. Аналогично, используя леммы 1 и 3, получим, что классы вида $\langle\langle x^{p^d} \rangle\rangle$, где $d \in \mathbf{D}(n)$, образуют решетку дуально изоморфную $\mathbf{D}(n)$.

Осталось доказать третье утверждение теоремы. Очевидно, при $d \in \mathbf{D}(n)$

$$\langle\langle x_1 \dots x_{p^d} \rangle\rangle \supseteq \langle\langle x^{p^d} \rangle\rangle.$$

Если какой-то класс вида $\langle\langle x_1 \dots x_{D+1} \rangle\rangle$, где $D \in \mathbf{D}(p^n - 1)$, принадлежит интервалу $[\langle\langle x^{p^d} \rangle\rangle, \langle\langle x_1 \dots x_{p^d} \rangle\rangle]$, то согласно второму утверждению теоремы $(p^d - 1) \mid D$, так как $\langle\langle x_1 \dots x_{p^d} \rangle\rangle \supseteq \langle\langle x_1 \dots x_{D+1} \rangle\rangle$. Но

$$\langle\langle x_1 \dots x_{D+1} \rangle\rangle \supseteq \langle\langle x^{p^d} \rangle\rangle,$$

и $D \mid (p^d - 1)$ в силу леммы 3. Значит, $D = p^d - 1$ и

$$\langle\langle x_1 \dots x_{D+1} \rangle\rangle = \langle\langle x_1 \dots x_{p^d} \rangle\rangle.$$

Если

$$\langle\langle x^{p^{d_1}} \rangle\rangle \in [\langle\langle x^{p^d} \rangle\rangle, \langle\langle x_1 \dots x_{p^d} \rangle\rangle],$$

где $d_1 \in \mathbf{D}(n)$, то $d \mid d_1$ в силу лемм 1 и 3, и $d_1 \mid d$ в силу второго утверждения теоремы. Значит, $d_1 = d$ и простота интервала $[\langle\langle x^{p^d} \rangle\rangle, \langle\langle x_1 \dots x_{p^d} \rangle\rangle]$ установлена.

Этим доказательство теоремы закончено.

Приведем теперь некоторые замечания и комментарии.

Рис. 4.

Замечание 1. Прежде всего приведем диаграмму интервала $[L^0, F]$ (см. рис. 4).

На диаграмме $[L, \langle\langle 1, x^p \rangle\rangle]$ — интервал, описанный в [2]. Эту диаграмму можно использовать для получения информации о замкнутых классах между L^0 и F .

Замечание 2. Функции, которые мы изучали, определены на множестве из p^n элементов. Пусть теперь A — произвольное конечное множество такое, что $|A| = k$. Разложив число k на простые множители

$$k = p_1^{\alpha_1} \dots p_s^{\alpha_s},$$

можно считать, что $A = A_1 \times \dots \times A_s$, где $|A_i| = p^{\alpha_i}$, $i = 1, \dots, s$. Превратив A_i в поле Галуа $GF(p^{\alpha_i})$, мы тем самым превращаем A в (полу)простое кольцо. Теперь мы можем говорить о многочленах над A и рассматривать замкнутые классы таких многочленов. В частности, можно поставить вопрос о строении интервала $[L_A^0, F_A]$. Известно (см. в [4] Теорему 3.3.3 (ii)), что такой интервал будет прямым произведением аналогичных интервалов для полей A_i , $i = 1, \dots, s$. Так как строение последних нами выяснено, можно считать, что мы знаем и строение интервала $[L_A^0, F_A]$. В частности, мы видим, что этот интервал конечен. Здесь мы еще раз подчеркнем, что A состоит из произвольного (конечного) числа элементов.

Замечание 3. Отметим следующее обстоятельство. Изучению замкнутых классов полиномов ранее был посвящен целый ряд работ. Первые результаты в этом направлении были получены еще в 50-е годы С. В. Яблонским и А. В. Кузнецовым. Из работ 80-х годов отметим работы [5-7]. Данная работа является продолжением указанных исследований. Она показывает, что до сих пор в изучении замкнутых классов полиномов над фиксированным кольцом можно получать достаточно содержательные результаты. Вместе с тем, остаются открытыми некоторые интересные и естественные вопросы классификации таких замкнутых классов. В этом направлении нам представляется наиболее актуальной задача исследования интервала $[L_R^0, F_R]$ для той ситуации, когда R есть кольцо вычетов $\mathbf{Z}_m$ по модулю $m = p^n$.

Список литературы

1. Крохин А. А., Сафин К. Л., Суханов Е. В. О строении решетки замкнутых классов полиномов. *Дискретная математика* (1997) **9**, №2, 24–39.
2. Szendrei Á. On closed classes of quasilinear functions. *Czech. Math. J.* (1980) **30**, №3, 498–509.
3. Мальцев А. И. Итеративные алгебры Поста. Наука, Новосибирск, 1974.
4. Pöschel R., Kalužnin L. Funktionen- und Relationenalgebren. Ein Kapitel der diskreten Mathematik. VEB DVW, Berlin, 1979.
5. Мещанинов Д. Г. Некоторые условия представимости функций из P_k полиномами по модулю k . *Докл. АН СССР* (1988) **299**, №1, 50–53.
6. Ремизов А. Б. О надструктуре замкнутого класса полиномов по модулю k . *Дискретная математика* (1989) **1**, №1, 3–15.
7. Черепов А. Н. Описание структуры замкнутых классов в P_k , содержащих класс полиномов. *Проблемы кибернетики* (1983) **40**, 5–18.

Статья поступила 10.11.1996.