ИЗВЕСТИЯ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ

2000 МАТЕМАТИКА № 7 (458)

УДК 512

А.П. СЕМИГРОДСКИХ

О КЛОНАХ ПОЛИНОМОВ НАД БЕСКОНЕЧНЫМИ ПОЛЯМИ

1. Введение

Данная работа является продолжением [1] и посвящена задаче классификации части замкнутых классов полиномов над бесконечными полями.

Введем основные понятия. Пусть дан класс функций, отображающих декартовы степени множества K в K. Этот класс называется замкнутым, если он замкнут относительно суперпозиций. Более точно, для m-местной функции f и n-местной функции g определим r-местную функцию $h = f * g$ $(r = m + n - 1)$, положив

$$h(x_1, \ldots, x_r) = f(g(x_1, \ldots, x_n), x_{n+1}, \ldots, x_r)$$

для всех $x_1, \ldots, x_r \in K$. Далее определим операции ζ, τ, Δ и ∇, полагая при $m > 1$

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

для всех $x_1, \ldots, x_{m+1} \in K$, и $\zeta f = \tau f = \Delta f = f$ при $m = 1$. Класс функций C называется замкнутым, если он замкнут относительно операций $*$, ζ, τ, Δ и ∇. Такой подход, предложенный А.И. Мальцевым, позволяет рассматривать замкнутые классы как алгебры относительно введенных операций (см. [2]). Замкнутый класс называется клоном, если он содержит все проекции, т. е. функции вида $e_i^n(x_1, \ldots, x_n) = x_i$, $1 \le i \le n$.

Пусть теперь K — произвольное ассоциативное коммутативное кольцо с единицей. Мы рассматриваем алгебраические полиномы над K от произвольного (конечного) числа переменных и замкнутые классы, образуемые такими полиномами. Рассмотрим основные для нас замкнутые классы

F_K — класс всех полиномов над K;

F_K^0 — класс всех полиномов из F_K без свободного члена;

L_K — класс всех линейных полиномов из F_K;

L_K^0 — класс всех линейных полиномов из L_K без свободного члена.

Поставим задачу классификации клонов из интервала $[L_K^0, F_K]$ решетки всех клонов. Будем понимать это как задачу выяснения решеточной структуры указанного интервала, который изображен на диаграмме 1. Знаки вопросов на ней означают, что указанные интервалы могут содержать замкнутые классы, не совпадающие с четырьмя отмеченными. Это зависит от свойств кольца K.

В [3] было показано, что в случае кольца вычетов по любому модулю весь решеточный интервал $[L_K^0, F_K]$ есть подпрямое произведение интервалов $[L_K^0, F_K^0]$ и $[L_K^0, L_K]$. Соответствующее доказательство проходит и для произвольного кольца K. Поэтому исследование интервала $[L_K^0, F_K]$ в каком-то смысле сводится к изучению интервалов $[L_K^0, F_K^0]$ и $[L_K^0, L_K]$. В [2] для случая кольца вычетов показано, что интервалы $[L_K^0, L_K]$ и $[F_K^0, F_K]$ изоморфны решетке идеалов

кольца K (а значит, и между собой). Доказательство и этого факта без изменений переносится на произвольное кольцо K. Поэтому, если K — поле, то интервал $[L_K^0, F_K]$ имеет вид, изображенный на диаграмме 2.

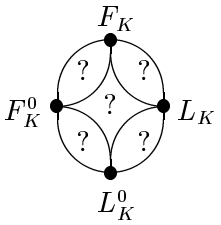

Диаграмма 1

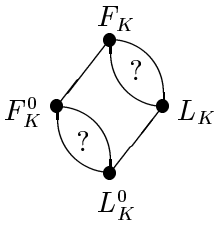

Диаграмма 2

Пусть C — замкнутый класс из $[L_K^0, F_K]$. Тогда C может быть порожден совокупностью всех линейных форм (т. е. полиномов из L_K^0) и какими-то функциями $f_1, f_2, \dots$ из F_K. В этом случае будем писать $C = \langle\langle f_1, f_2, \dots \rangle\rangle$ и говорить, что C порожден функциями $f_1, f_2, \dots$ (не упоминая L_K^0). Если при этом множество $\{f_1, f_2, \dots\}$ конечно, то класс C будем называть конечнопорожденным. Всюду далее словосочетание "замкнутый класс" означает *замкнутый класс из* $[L_K^0, F_K]$, а "полином" или "многочлен" — *полином над* K. Каждый из изучаемых классов содержит L_K^0, поэтому, рассматривая линейные комбинации элементов класса, мы не выйдем за его пределы. Это обстоятельство далее будет использоваться без оговорок.

Как обычно, через $\mathbb{N}$ обозначается множество всех натуральных чисел $\{1, 2, \dots\}$. Решетка подполугрупп полугруппы натуральных чисел по сложению обозначается через $\mathbf{Sub}(\mathbb{N}; +)$.

С точки зрения изучения свойств интервала $[L_K^0, F_K]$ бесконечные поля простой характеристики значительно отличаются от конечных и полей характеристики 0. Этому сложному случаю будет посвящена отдельная работа.

2. Об одночленах замкнутых классов

В данном параграфе будет доказана лемма, позволяющая, в частности, сделать вывод о том, что для полей каждый из исследуемых классов порождается своими одночленами.

Везде далее через K обозначаем поле. Считаем, что в полиноме как сумме одночленов подобные члены приведены. Если $K = GF(p^n)$, то полагаем, что переменные входят в многочлены в степенях меньших, чем p^n.

Сформулируем без доказательства следующее простое

Утверждение. Пусть d_1 и d_2 — различные натуральные числа (меньшие, чем p^n, если $K = GF(p^n)$). Тогда существует ненулевое $a \in K$ такое, что $a^{d_1} \neq a^{d_2}$.

Лемма 1. *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 $m_1, \dots, m_l \in C$. Докажем лемму индукцией по l. При $l = 1$ утверждение очевидно. Пусть теперь оно выполнено для меньших, чем l, значений. Обозначим через d_i показатель переменной x_1 в одночлене m_i (для всех $i \in \{1, \dots, l\}$). В этой ситуации есть переменная, входящая в два одночлена с разными степенными показателями, т. к. подобные одночлены приведены. Не ограничивая общности, можно считать, что эта переменная есть x_1, что эти одночлены суть m_1 и m_2, а соответствующие показатели удовлетворяют неравенству $d_1 < d_2$.

В случае $d_1 = 0$ выполняется равенство $m_1(0, \dots, x_r) = m_1(x_1, \dots, x_r)$. Подставляя вместо x_1 константу $0 \in L_K^0$, получим следующий многочлен из C:

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

Так как $d_2 > 0$, то в $h \in C$ одночленов меньше, чем l. Значит, по предположению индукции $m_1 \in C$, $f - m_1 \in C$, и в многочлене $f - m_1 = \sum\limits_{i=2}^{l} m_i$ число одночленов меньше, чем l. Теперь по предположению индукции $m_2, \ldots, m_l \in C$ и, наконец, $m_1, m_2, \ldots, m_l \in C$.

Пусть теперь $d_1 \neq 0$. Тогда по предыдущему утверждению существует такое ненулевое $a \in K$, что $a^{d_1} \neq a^{d_2}$. Запишем одночлены в виде $m_i = x_1^{d_i} m_i^{\#}(x_2, \ldots, x_r)$ и построим полином из C

$$g = a^{d_1} f(a^{-1}x_1, x_2, \ldots, x_r) - f(x_1, \ldots, x_r) = \sum_{i=1}^{l} (a^{d_1 - d_i} - 1) x_1^{d_i} m_i^{\#} = \sum_{i=2}^{l} (a^{d_1 - d_i} - 1) x_1^{d_i} m_i^{\#}.$$

Здесь $(a^{d_1 - d_2} - 1) x_1^{d_2} m_2^{\#} \not\equiv 0$, т. к. $a^{d_1} \neq a^{d_2}$. 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 $m_1, m_2, \ldots, m_l \in C$.

Доказанная лемма дает основание утверждать, что каждый замкнутый класс порождается своими одночленами. Поэтому целесообразно выделить наиболее простые одночлены, определяющие класс. Для полей характеристики 0 это будет проделано в следующем параграфе.

3. Случай полей характеристики 0

В данном параграфе под K понимается поле характеристики 0, и можно считать, что K содержит поле рациональных чисел $\mathbb{Q}$. Как будет показано, для таких полей интервал $[L_K^0, F_K^0]$ изоморфен решетке $\mathbf{Sub}(\mathbb{N}; +)$, а интервал $[L_K, F_K]$ прост (см. диаграмму 3).

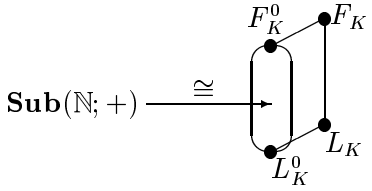

Диаграмма 3

Как показано в предыдущем параграфе, каждый замкнутый класс порождается своими одночленами. Определим достаточно простые множества таких одночленов. В связи с этим введем несколько понятий.

Одночлен вида $x_1 \ldots x_n$, являющийся произведением n различных переменных, будем называть простым (1 также считаем простым одночленом).

Лемма 2. *Если замкнутый класс содержит одночлен степени D, то он содержит и простой одночлен той же степени.*

Доказательство. Возьмем произвольный одночлен m из замкнутого класса C. Не ограничивая общности, можно считать, что $m = x_1^d m_1(x_2, \ldots, x_r)$, $d > 0$. Подставив вместо x_1 сумму из d переменных $y_1 + \cdots + y_d \in L_K^0$, получим

$$(y_1 + \cdots + y_d)^d m_1 = (k \cdot y_1 \ldots y_d + g) m_1 \in C,$$

где $k \in \mathbb{N}$ и многочлен g не содержит одночленов, подобных $y_1 \ldots y_d$. По лемме 1 имеем $k y_1 \ldots y_d m_1 \in C$. Подставляя вместо переменной y_1 одночлен $k^{-1} y_1 \in L_K^0 \subset C$ ($k^{-1} \in \mathbb{Q} \subset K$), получим

$$y_1 \ldots y_d m_1(x_2, \ldots, x_r) \in C.$$

Применяя к переменным $x_2, \ldots, x_r$ в полученном одночлене рассуждения, аналогичные проведенным для x_1, получим

$$y_1 \ldots y_D \in C. \quad \square$$

Отождествляя подходящим образом переменные в простом одночлене, с помощью итеративных операций легко получить любые одночлены той же степени. Поэтому доказанная лемма дает основание утверждать, что любой замкнутый класс порождается своими *простыми* одночленами.

Следствие 1. Интервал $[L_K, F_K]$ прост.

Доказательство. Пусть C — замкнутый класс из $[L_K, F_K]$, отличный от L_K. Покажем, что $C = F_K$. Класс C содержит одночлен степени $l > 1$, т. к. $C \neq L_K$. По лемме 2 он содержит одночлен $x_1 \dots x_l$. Подставляя вместо $l-2$ последних переменных $1 \in L_K$, получим $x_1 x_2 \in C$. Заметим, что

$$x_1x_2 * x_1x_2 = x_1x_2x_3,$$
$$x_1x_2x_3 * x_1x_2 = x_1x_2x_3x_4,$$
$$\dots$$
$$x_1x_2 \dots x_{n-1} * x_1x_2 = x_1x_2x_3 \dots x_n,$$
$$\dots$$

где $*$ — итеративная операция подстановки (см. § 1). Класс C содержит все простые одночлены. Значит, $C = F_K$.

Итак, интервал $[L_K, F_K]$ прост. Осталось выяснить устройство интервала $[L_K^0, F_K^0]$. До конца данного параграфа слова "замкнутый класс" будут обозначать замкнутый класс из $[L_K^0, F_K^0]$.

Назовем длиной одночлена его степень без единицы.

Лемма 3. *Положительные длины одночленов из замкнутого класса суть в точности элементы подполугруппы из* $\mathbb{N}$*, порожденной длинами одночленов из произвольного порождающего множества этого замкнутого класса.*

Доказательство. Рассмотрим замкнутый класс $C = \langle\langle f_1, \dots, f_k, \dots \rangle\rangle$, где $f_1, \dots, f_k, \dots$ — одночлены с ненулевыми длинами $l_1, \dots, l_k, \dots$, и пусть $S = \langle l_1, \dots, l_k, \dots \rangle$ — подполугруппа, порожденная этими длинами. Класс C является подалгеброй, порожденной множеством $L_K^0 \cup \{f_1, \dots, f_k, \dots\}$ с помощью операций ζ, τ, Δ, ∇, $*$. Докажем индукцией по построению этой подалгебры, что длины всех одночленов из C лежат в S. База индукции очевидна. Переходя к шагу индукции, отметим, что операции ζ, τ, Δ, ∇ не изменяют степени одночленов. Поэтому достаточно рассмотреть действие на степени операции $*$.

При подстановке $m * f$, где $m = x_1^\alpha m^\#(x_2, \dots, x_s)$ — одночлен степени $1+q$, $f = m_1 + \dots + m_r$, m_i — одночлены, $\deg m_i = 1 + q_i$, $q, q_1, \dots, q_r \in S$, получаются одночлены с длинами вида $k_0 q + k_1 q_1 + \dots + k_l q_r \in S$. В самом деле,

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

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

$$(1+q_1)\beta_{1t} + \dots + (1+q_r)\beta_{rt} = \sum_{j=1}^{r} \beta_{jt} + \sum_{j=1}^{r} \beta_{jt} q_j = \alpha + q_1\beta_{1t} + \dots + q_r\beta_{rt}.$$

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

$$(m_1 + \dots + m_r)^\alpha m^\# = \sum_{t=0}^{T} a_t m_1^{\beta_{1t}} \dots m_r^{\beta_{rt}} m^\#.$$

Здесь слагаемое с номером t имеет степень

$$\alpha + q_1\beta_{1t} + \dots + q_r\beta_{rt} + (1 + q - \alpha) = 1 + q_1\beta_{1t} + \dots + q_r\beta_{rt} + q,$$

т. к. $\deg m^{\#} = 1 + q - \alpha$. Таким образом, длины всех вновь полученных одночленов лежат в S.

Общий случай сводится к предыдущему, т. к. $\Delta(M_1 + \cdots + M_s) = \Delta M_1 + \cdots + \Delta M_s$, $(M_1 + \cdots + M_s) * f = M_1 * f + \cdots + M_s * f$.

Чтобы доказать, что положительные длины одночленов из C принимают *все* значения из S, рассмотрим простые одночлены с длинами $l_1, \ldots, l_k, \ldots$ По лемме 2 такие одночлены в C есть. Заметим теперь, что длины простых одночленов при подстановке складываются

$$x_1 \ldots x_{L_1+1} * x_1 \ldots x_{L_2+1} = x_1 \ldots x_{L_1+L_2+1}.$$

Это, в частности, означает, что длины простых одночленов из C пробегают всю полугруппу S.

Основной результат данной работы дает

Теорема. *Интервал* $[L_K^0, F_K^0]$ *изоморфен решетке* $\mathbf{Sub}(\mathbb{N}; +)$.

Доказательство. Каждый замкнутый класс порожден своими простыми одночленами. Поставим в соответствие каждой подполугруппе $S \in \mathbf{Sub}(\mathbb{N}; +)$ замкнутый класс $\phi(S)$, порожденный всеми простыми одночленами, длины которых принимают значения из S. По лемме 3 положительные длины одночленов из замкнутого класса суть в точности элементы подполугруппы из $\mathbb{N}$ порожденной длинами одночленов из порождающего множества этого замкнутого класса. В силу леммы 2 эти длины задают длины простых одночленов замкнутого класса, которые в свою очередь определяют сам класс. Таким образом, построенное соответствие есть взаимно однозначное отображение на $[L_K^0, F_K^0]$. Легко видеть, что оно сохраняет все включения:

$$\forall S_1, S_2 \in \mathbf{Sub}(\mathbb{N}; +)\ (S_1 \subset S_2 \Leftrightarrow \phi(S_1) \subset \phi(S_2)). \quad \square$$

Следствие 2. Любой класс из $[L_K^0, F_K]$ конечнопорожден.

Доказательство. Очевидно, $L_K = \langle\langle 1 \rangle\rangle$ и $F_K = \langle\langle 1, x_1 x_2 \rangle\rangle$ конечнопорождены. Известно также, что любая полугруппа из $\mathbf{Sub}(\mathbb{N}; +)$ конечнопорождена. В качестве порождающего множества для класса из $[L_K^0, F_K^0]$ возьмем множество всех тех простых одночленов этого класса, длины которых принимают все значения из произвольного *конечного* порождающего множества соответствующей ему полугруппы. Длины таких одночленов при подстановке складываются и порождают таким образом исходную подполугруппу, которая и определяет класс. Значит, классы из $[L_K^0, F_K^0]$ также конечнопорождены.

4. Заключительные замечания

Первые результаты о замкнутых классах полиномов были получены еще в 50-е годы, в частности, С.В. Яблонским [4] и А.В. Кузнецовым [5]. С тех пор этой теме был посвящен ряд работ, продолжением которого является и данная работа. Несколько необычной для данной тематики является бесконечность полей, над которыми рассматриваются полиномы.

В случае полей характеристики 0 удалось описать интервал $[L_K^0, F_K]$ с точностью до строения решетки $\mathbf{Sub}(\mathbb{N}; +)$, хорошо известной в теории полугрупп. Ее строением еще в 60-е годы заинтересовались в ходе изучения свойств полугрупп с решетками подполугрупп, удовлетворяющими нетривиальному тождеству. Вопрос о том, удовлетворяет ли $\mathbf{Sub}(\mathbb{N}; +)$ какому-либо нетривиальному тождеству, был поставлен Л.Н. Шевриным ([6], задача 2.74). Задача была решена в [7]. В статье [8] было отмечено, что конечные подрешетки из $\mathbf{Sub}(\mathbb{N}; +)$ — это в точности все конечные ограниченные снизу решетки. Полное доказательство этого факта приведено в ([9], теорема 28.1). Также важным для нас свойством решетки $\mathbf{Sub}(\mathbb{N}; +)$ является ее счетность.

В заключение автор выражает благодарность Е.В. Суханову, Л.Н. Шеврину и всем, кто высказал свои замечания по данной работе.

Литература

1. Семигродских А.П., Суханов Е.В. *О замкнутых классах полиномов над конечным полем* // Дискрет. матем. – 1997. – Т. 9. – № 4. – С. 50–62.
2. Мальцев А.И. *Итеративные алгебры Поста.* – Новосибирск: Изд-во Новосибирск. ун-та, 1974. – 80 с.
3. Крохин А.А., Сафин К.Л., Суханов Е.В. *О строении решетки замкнутых классов полиномов* // Дискрет. матем. – 1997. – Т. 9. – № 2. – С. 24–39.
4. Яблонский С.В. *Функциональные построения в k-значной логике* // Тр. Матем. ин-та АН СССР. – М., 1958. – Т. 51. – С. 5–142.
5. Кузнецов А.В. *О бесповторных контактных схемах и бесповторных суперпозициях функций алгебры логики* // Тр. Матем. ин-та АН СССР. – М., 1958. – Т. 51. – С. 186–225.
6. *Свердловская тетрадь. Нерешенные задачи теории полугрупп.* – Свердловск: Уральск. ун-т, 1979. – Вып. 3. – 41 с.
7. Репницкий В.Б., Кацман С.И. *Коммутативные полугруппы, решетка подполугрупп которых удовлетворяет нетривиальному тождеству* // Матем. сб. – 1988. – Т. 137. – № 4. – С. 462–482.
8. Repnitskiĭ V.B. *On finite lattices which are embeddable in subsemigroup lattices* // Semigroup Forum. – 1993. – V. 46. – P. 388–397.
9. Shevrin L.N., Ovsyannikov A.J. *Semigroups and their subsemigroup lattices.* – Dordrecht–Boston–London: Kluwer Acad. Publ., 1996. – 390 p.

Уральский государственный университет

Поступила
09.01.1998