Math-Net.Ru

Общероссийский математический портал

А. А. Крохин, К. Л. Сафин, Е. В. Суханов, О строении решетки замкнутых классов полиномов, *Дискрет. матем.*, 1997, том 9, выпуск 2, 24–39

DOI: <https://doi.org/10.4213/dm469>

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: 54.80.97.219

26 апреля 2023 г., 13:52:58

О строении решетки замкнутых классов полиномов

© 1997 г. А. А. Крохин, К. Л. Сафин, Е. В. Суханов

В данной работе изучается строение решетки замкнутых классов полиномов по модулю k . Более точно, изучается строение интервала этой решетки от класса всех линейных полиномов без свободного члена до класса всех полиномов по модулю k . Доказывается, что этот интервал (как частично упорядоченное множество) есть подпрямое произведение двух своих подынтервалов и далее полностью выясняется его устройство для k , свободного от квадратов. Кроме того, для $k = 4$ (наименьшего k , содержащего квадрат) дано описание интервала от класса всех линейных полиномов до класса всех полиномов.

1. Введение

В работе изучаются замкнутые классы полиномов над кольцом Z_k вычетов по модулю $k \geq 3$. Пусть P_k — класс всех k -значных функций (т.е. отображений $f: Z_k^n \rightarrow Z_k$) и $\mathcal{L}(P_k)$ — решетка всех (включая $\emptyset$) замкнутых классов из P_k . Как известно, изучение свойств решетки $\mathcal{L}(P_k)$ представляет большой интерес как в теоретической кибернетике, так и в общей алгебре. С самого начала изучения строения решетки $\mathcal{L}(P_k)$ заметное внимание уделялось классификационным вопросам для замкнутых классов полиномов над Z_k (см. например [5]). Так, например, с 60-х годов ведутся исследования по перечислению замкнутых классов, состоящих из линейных над Z_k полиномов.

Пусть F_k — замкнутый класс полиномов по модулю k , а L_k — замкнутый класс линейных полиномов такого вида. Обозначим через $\mathcal{L}(F_k)$ решетку всех замкнутых классов из F_k . Надеяться на какое-либо описание (в разумном смысле этого слова) решетки $\mathcal{L}(F_k)$ не приходится по крайней мере из-за того, что $\mathcal{L}(F_p) = \mathcal{L}(P_p)$ для простого модуля p . Однако, по нашему мнению можно продвинуться в понимании устройства решетки $\mathcal{L}(F_k)$, рассматривая подходящие ее части. В этом и состоит цель данной работы.

Рассмотрим также замкнутый класс F_k^0 всех полиномов из F_k , сохраняющих константу 0 (т.е. полиномов без свободного члена) и замкнутый класс L_k^0 всех линейных полиномов из F_k^0 (т.е. линейных форм).

Более точно, наша цель состоит в изучении интервала $[L_k^0; F_k]$ решетки $\mathcal{L}(P_k)$ при помощи интервалов $[L_k^0; L_k]$, $[L_k^0; F_k^0]$, $[L_k; F_k]$ и $[F_k^0; F_k]$. Наглядно все эти интервалы представлены на рис. 1.

Стоит отметить, что объединением этих интервалов в общем случае не исчерпывается весь интервал $[L_k^0; F_k]$. Тем не менее, как мы увидим, знание устройства указанных интервалов ведет к лучшему пониманию строения решетки $[L_k^0; F_k]$.

Рис. 1.

Работа состоит из введения и трех параграфов. В §2 мы покажем, что строение $[L_k^0; F_k]$ сводится в определенном смысле к знанию устройства $[L_k^0; F_k^0]$ и $[L_k^0; L_k]$ (предложение 1). Затем мы дадим описание интервала $[L_k^0; L_k]$ для произвольного k (предложение 2) и опишем интервал $[L_k^0; F_k^0]$ для $k = p$, где p — простое число (теорема 1). После этого станет ясно, как в случае $k = p$ устроен весь исследуемый интервал $[L_k^0; F_k]$.

Пусть $k = p_1^{\alpha_1} \dots p_n^{\alpha_n}$ — разложение числа k на простые множители. Известно [2], что интервал $[L_k^0; F_k]$ является прямым произведением аналогичных интервалов для $p_i^{\alpha_i}$, $i = 1, \dots, n$ (существование этого прямого разложения вытекает также из теоремы 3.3.5 в [6]). Поэтому результаты §2 дают описание интервала $[L_k^0; F_k]$ для k , свободного от квадратов, т.е. для $k = p_1 \dots p_n$.

Таким образом, наименьшее из чисел k , которые теперь надо исследовать в нашей задаче, это $k = 2^2 = 4$. Этому и посвящены в нашей работе §3 и §4. К сожалению, нам не удалось описать строение интервала $[L_4^0; F_4^0]$. Поэтому вместо него мы рассматриваем интервал $[L_4; F_4]$ и полностью выясняем его устройство в теореме 2. Формулировка этой теоремы и первая половина доказательства помещены в §3. Последний §4 содержит другую половину доказательства.

Нетривиальность рассуждений при доказательстве теоремы 2 свидетельствует, как нам кажется, о достаточной сложности строения интервала $[L_4^0; F_4^0]$. В самом деле, из предложения 1 вытекает, что $[L_k; F_k]$ изоморфно вкладывается в $[L_k^0; F_k^0]$. Следовательно, $[L_k^0; F_k^0]$ устроен более сложно, чем $[L_k; F_k]$. В этой связи мы формулируем в явном виде вопрос: каково строение интервала $[L_4^0; F_4^0]$?

Формулировки основных результатов данной работы опубликованы в виде тезисов в [3, 4].

2. Интервал $[L_k^0; F_k]$

Пусть $Q = \{f_i \mid i \in I\}$ — замкнутый класс из $[L_k^0; F_k]$. Каждый полином f_i имеет вид $g_i + c_i$, где $g_i \in F_k^0$, а c_i — свободный член. Положим $Q^0 = \{g_i \mid i \in I\}$ и $Q^c = \{c_i \mid i \in I\}$. Если Q_1 и Q_2 — два класса полиномов из F_k , то через $Q_1 + Q_2$

обозначим (не обязательно замкнутый) класс $\{f_1 + f_2 \mid f_1 \in Q_1, f_2 \in Q_2\}$. Будем также считать, что $Z_k = F_k^c$.

Лемма 1. *Верны следующие соотношения:*

- (1) $Q^0 = F_k^0 \cap Q$;
- (2) $Q^c = Z_k \cap Q$;
- (3) Q^c — идеал в Z_k ;
- (4) $L_k^0 + Q^c = L_k \cap Q$;
- (5) $Q = Q^0 + Q^c$.

Доказательство. Все утверждения леммы проверяются непосредственно. Для примера проверим первое. Пусть $f \in Q$ и $f = g + c$. Подставляя в f вместо всех переменных константу 0 (а она есть в Q), получаем $c \in Q$. Теперь в $x_1 - x_2 \in Q$ подставляем f вместо x_1 и c вместо x_2 . Получаем, что $g \in Q$, откуда $Q^0 \subseteq F_k^0 \cap Q$. Обратное включение очевидно.

Рассмотрим интервалы $[L_k^0; F_k]$, $[L_k^0; F_k^0]$ и $[L_k^0; L_k]$ как частично упорядоченные множества. Другими словами, будем смотреть на них как на модели, а не как на алгебры.

Предложение 1. *Частично упорядоченное множество $[L_k^0; F_k]$ есть подпрямое произведение частично упорядоченных множеств $[L_k^0; F_k^0]$ и $[L_k^0; L_k]$.*

Доказательство. Достаточно проверить инъективность отображения

$$\phi: [L_k^0; F_k] \rightarrow [L_k^0; F_k^0] \times [L_k^0; L_k],$$

задаваемого правилом $\phi(Q) = (F_k^0 \cap Q, L_k \cap Q)$. Итак, пусть $\phi(Q_1) = \phi(Q_2)$, т.е. $(F_k^0 \cap Q_1, L_k \cap Q_1) = (F_k^0 \cap Q_2, L_k \cap Q_2)$. Согласно п. 1 и 4 леммы 1, получаем $(Q_1^0, L_k^0 + Q_1^c) = (Q_2^0, L_k^0 + Q_2^c)$, откуда $Q_1^0 = Q_2^0$ и $Q_1^c = Q_2^c$. Теперь согласно п. 5 леммы 1 $Q_1 = Q_1^0 + Q_1^c = Q_2^0 + Q_2^c = Q_2$, и инъективность установлена.

Отметим одну особенность этого предложения. Согласно ему, частично упорядоченное множество $[L_k^0; F_k]$ изоморфно части частично упорядоченного множества $[L_k^0; F_k^0] \times [L_k^0; L_k]$. И хотя $[L_k^0; F_k]$ есть решетка, она не является подрешеткой в прямом произведении решеток $[L_k^0; F_k^0]$ и $[L_k^0; L_k]$. Отчетливо это проявится, например, в следствии 2 ниже, где будет установлено, что для $k = p$ (p — простое число и $p \geq 3$) решетка $[L_p^0; F_p]$ недистрибутивна, в то время как решетка $[L_p^0; F_p^0] \times [L_p^0; L_p]$ (а, следовательно, и любая ее подрешетка) дистрибутивна. Это означает, что в формулировке предложения 1 словосочетание частично упорядоченное множество нельзя заменить на слово решетка.

Предложение 2. *Каждый из интервалов $[L_k^0; L_k]$ и $[F_k^0; F_k]$ изоморфен решетке идеалов кольца Z_k .*

Доказательство. Утверждение предложения для интервала $[L_k^0; L_k]$ вытекает из п. 1 и 5 леммы 1. В самом деле, для замкнутого класса Q из интервала $[L_k^0; L_k]$ формула п. 5 превращается в $Q = L_k^0 + Q^c$ (отметим, что то же самое получается, если к Q применить п. 4 леммы 1). А последнее как раз и означает, что замкнутые классы из интервала $[L_k^0; L_k]$ находятся во взаимно однозначном соответствии с идеалами из Z_k . Для полноты картины здесь, видимо, следует отметить, что для каждого идеала A из Z_k класс $L_k^0 + A$ замкнут, в чем нетрудно убедиться непосредственно.

Аналогичное рассуждение (со ссылкой на п. 3 и 5 леммы 1) проходит и для интервала $[F_k^0; F_k]$.

Следствие 1. Если интервал $[L_k^0; F_k^0]$ конечен или счетен, то таков же и интервал $[L_k^0; F_k]$.

Доказательство. Это непосредственно вытекает из предложений 1 и 2.

Теперь естественно возникает вопрос о строении интервала $[L_k^0; F_k^0]$. Как отмечено во введении, авторам пока неизвестно его устройство для произвольного k . Ниже мы выясним строение этого интервала для $k = p$, где p — простое число.

Введем сначала одно обозначение, которым будет удобно пользоваться в этом параграфе. Пусть $A, B \subseteq P_k$, т.е. A и B — два множества k -значных функций. Замкнутый класс, порожденный системой $A \cup L_k^0$, будем обозначать через $\langle A \rangle$, и будем писать $A \rightarrow B$, если $\langle A \rangle \supseteq B$. Иными словами, $A \rightarrow B$, если каждая функция из B может быть получена с помощью итеративных операций $\zeta, \tau, \Delta, \nabla, *$ (см. [1]) из функций системы $A \cup L_k^0$. Например, заметив, что $\sum \alpha_i x_i \in L_k^0$, получаем $f_1, \dots, f_n \rightarrow \sum \alpha_i f_i$ для произвольных $\alpha_i \in Z_k$. Это замечание мы будем использовать без специальных ссылок.

Переходя к выяснению строения интервала $[L_p^0; F_p]$ (p — простое), отметим следующие хорошо известные факты: интервалы $[L_p^0; L_p]$, $[L_p; F_p]$ и $[F_p^0; F_p]$ являются простыми, т.е. каждый из них имеет лишь два элемента. Но тогда по предложению 1 для полного описания интервала $[L_p^0; F_p]$ остается выяснить строение интервала $[L_p^0; F_p^0]$, что и будет сделано в теореме 1 ниже. Обозначим через $\mathcal{L}(Z_{p-1})$ решетку всех подгрупп группы $(Z_{p-1}, +)$, включая и пустую подгруппу. Другими словами, $\mathcal{L}(Z_{p-1})$ получается из обычной решетки подгрупп внешним добавлением нулевого элемента.

Теорема 1. Интервал $[L_p^0; F_p^0]$ изоморфен решетке $\mathcal{L}(Z_{p-1})$.

На рис. 2 изображены диаграммы всей решетки $[L_p^0; F_p]$ в общем случае и в случае $p = 3$.

Следствие 2. При любом простом $p \geq 3$ решетка $[L_p^0; F_p]$ недистрибутивна.

Доказательству теоремы 1 предположим несколько замечаний и одну лемму.

Если $f \in F_p^0$ и g — его нелинейная часть, то $\langle f \rangle = \langle g \rangle$. Поэтому в дальнейшем мы будем изучать лишь такие $f \in F_p^0$, у которых все одночлены нелинейны. Далее, так как в Z_p выполняется тождество $x^p = x$, степени всех переменных в f можно считать не превосходящими $p - 1$. Одночлен вида $x_1 \dots x_n$ будем называть элементарным произведением. Пусть $f \in F_p^0$. Каждому одночлену $ax_1^{\alpha_1} \dots x_n^{\alpha_n}$

Рис. 2.

из f сопоставим элементарное произведение $x_1 \dots x_m$ степени $m = \alpha_1 + \dots + \alpha_n$, и обозначим через A_f совокупность всех элементарных произведений, полученных таким образом по f .

Лемма 2. *Справедливо равенство $\langle f \rangle = \langle A_f \rangle$.*

Доказательство. Мы получим требуемое индукцией по числу одночленов в f .

Начнем с базы индукции. Пусть $f = x_1^{\alpha_1} \dots x_n^{\alpha_n}$. Подставляя вместо x_1 линейное выражение $y_1 + \dots + y_{\alpha_1}$, получим полином, в котором есть одночлен вида $ay_1 \dots y_{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$. При этом в других одночленах нет хотя бы одной из переменных $y_1, \dots, y_{\alpha_1}$. Осуществляя подходящим образом подстановки $y_1 = 0, \dots, y_{\alpha_1} = 0$ и вычитая получающиеся полиномы, получаем $f \rightarrow y_1 \dots y_{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$. Пропедев аналогичную процедуру с остальными переменными $x_2, \dots, x_n$, получим в конце концов $f \rightarrow y_1 \dots y_m$, где $m = \sum \alpha_i$. Обратно, отождествляя в $x_1 \dots x_m$ подходящие группы переменных, получаем $x_1 \dots x_m \rightarrow x_1^{\alpha_1} \dots x_n^{\alpha_n}$. Следовательно, $\langle f \rangle = \langle x_1 \dots x_m \rangle$.

Осуществим шаг индукции. Пусть $f = ax_1^{\alpha_1} \dots x_n^{\alpha_n} + g$ и x_1 имеет максимальную степень в одночлене $ax_1^{\alpha_1} \dots x_n^{\alpha_n}$. Используя процедуру, аналогичную проделанной при установлении базы индукции, получаем $f \rightarrow x_1 \dots x_m \rightarrow x_1^{\alpha_1} \dots x_n^{\alpha_n}$. Поэтому $f \rightarrow g$, а тогда по индуктивному предположению $g \rightarrow A_g$. Таким образом, $f \rightarrow x_1 \dots x_m, A_g$ и обратно, $x_1 \dots x_m, A_g \rightarrow f$. Значит, $\langle f \rangle = \langle A_f \rangle$, и лемма доказана.

Доказательство теоремы 1. Для удобства будем называть длиной одночлена $x_1 \dots x_m$ число $m - 1$. Пусть $K \in [L_p^0; F_p]$. Сопоставим каждому $f \in K$ систему A_f и рассмотрим $\{x_1 \dots x_{m_i} \mid i \in I\}$ — объединение всех таких систем. По лемме 2, $K = \langle \{x_1 \dots x_{m_i} \mid i \in I\} \rangle$. Обозначим теперь через $\mathcal{D}_k$ совокупность длин указанных элементарных произведений, т.е. $\mathcal{D}_k = \{m_i - 1 \mid i \in I\}$. Соответствие $K \leftrightarrow \mathcal{D}_k$ взаимно однозначно.

Если $K = L_p^0$, то $\mathcal{D}_k$ состоит из одного числа 0. Если же $K \neq L_p^0$, то множество неотрицательных чисел $\mathcal{D}_k$ обладает следующими свойствами.

$m, n \in \mathcal{D}_k \Rightarrow m + n \in \mathcal{D}_k$. В самом деле, если имеет место включение $m, n \in \mathcal{D}_k$, то $x_1 \dots x_{m+1}, x_1 \dots x_{n+1} \in K$. Подстановкой одного из этих полиномов в другой получаем, что $x_1 \dots x_{m+n+1} \in K$, откуда следует включение $m + n \in \mathcal{D}_k$.

$m \geq 0, m + p - 1 \in \mathcal{D}_k \Rightarrow m \in \mathcal{D}_k$. Действительно, беря одночлен $x_1 \dots x_{m+p} \in K$ и отождествляя в нем переменные $x_{m+1}, \dots, x_{m+p}$, получаем $x_1 \dots x_m x_{m+1}^p = x_1 \dots x_{m+1} \in K$.

$\mathcal{D}_k = \{md_K \mid m \in \mathbb{N}_0\}$, где d_K — наименьшее из положительных чисел в $\mathcal{D}_K$. Пусть $n \in \mathcal{D}_K$, тогда $n = qd_K + r$, где $q \geq 0, 0 \leq r < d_K$. Поскольку

$$n - qd_K \equiv n + (p - 2)qd_K \pmod{p - 1},$$

получаем, что

$$r + s(p - 1) = n + (p - 2)qd_K.$$

В этом равенстве правая часть есть число из $\mathcal{D}_k$ в силу первого свойства, а тогда $r \in \mathcal{D}_K$ в силу второго свойства. Если $r > 0$, то получаем противоречие с выбором d_K , поэтому $r = 0$ и $n = qd_K$. Этим доказано включение слева направо; обратное включение вытекает из первого свойства.

Теперь определим отображение $\Phi: [L_p^0; F_p^0] \rightarrow \mathcal{L}(Z_{p-1})$ правилом

$$\Phi(K) = \begin{cases} \text{пустая подгруппа,} & \text{если } K = L_p^0, \\ \text{нулевая подгруппа,} & \text{если } d_K = p - 1, \\ \text{подгруппа, порожденная числом } d_K, & \text{если } 1 \leq d_K \leq p - 2. \end{cases}$$

Непосредственная проверка показывает, что Φ инъективно. Докажем его сюръективность.

Возьмем в $\mathcal{L}(Z_{p-1})$ произвольную подгруппу. Можно считать, что она непустая и ненулевая. Обозначив через d ее образующий элемент, рассмотрим множество целых неотрицательных чисел $\mathcal{D} = \{md \mid m \in \mathbb{N}_0\}$ и систему $K_{\mathcal{D}}$ всех таких полиномов из F_p^0 , одночлены которых либо являются элементарными произведениями с длинами из $\mathcal{D}$, либо получаются из них отождествлениями некоторых переменных. Показав, что $K_{\mathcal{D}}$ замкнутый класс, мы и установим сюръективность, так как $\Phi(K_{\mathcal{D}}) = \mathcal{D}$.

Установим замкнутость $K_{\mathcal{D}}$ относительно суперпозиции (замкнутость относительно других итеративных операций очевидна). Суть дела хорошо видна уже в случае суперпозиции одночленов. Пусть $f, g \in K_{\mathcal{D}}, f = x_1^{\alpha_1} \dots x_n^{\alpha_n}, g = x_1^{\beta_1} \dots x_m^{\beta_m}$. Тогда $f * g = (y_1^{\beta_1} \dots y_m^{\beta_m})^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$. Так как $\sum \alpha_i - 1$ и $\sum \beta_j - 1$ суть числа из $\mathcal{D}$, величина

$$(\beta_1 + \dots + \beta_m)\alpha_1 + \alpha_2 + \dots + \alpha_n - 1 = \left(\sum \beta_j - 1\right)\alpha_1 + \left(\sum \alpha_i - 1\right)$$

также содержится в $\mathcal{D}$. Общий случай подстановки полинома в полином после проведения несложных выкладок сводится к аналогичному числовому равенству.

Итак, Φ — биекция $[L_p^0; F_p^0]$ на $\mathcal{L}(Z_{p-1})$. То, что Φ — изоморфизм, вытекает из монотонности отображений Φ и Φ^{-1} . Последнее проверяется непосредственно. Этим и завершается доказательство теоремы 1.

Рис. 3.

3. Интервал $[L_4; F_4]$

Всюду далее $\langle A \rangle$ обозначает замкнутый класс, порожденный системой $A \cup L_4$, а $A \rightarrow B$ означает, что $\langle A \rangle \supseteq B$. Это несколько отличается от употребления аналогичных символов в предыдущем параграфе.

Теорема 2. Интервал $[L_4; F_4]$ является решеткой, изображенной на рис. 3.

Доказательство теоремы 2 излагается в данном и следующем параграфах. В этом параграфе мы покажем, что все замкнутые классы, изображенные на рис. 3, попарно различны, и включения между ними таковы, как указано. В §4 будет установлено, что других замкнутых классов в $[L_4; F_4]$ нет.

Переходя к анализу диаграммы, приведем сначала два замечания. Так как в Z_4 справедливо тождество $x^4 = x^2$, можно считать, что степени переменных в любом полиноме над Z_4 не превосходят трех. Далее, в силу справедливости в Z_4 тождества $2x^2 = 2x$, можно считать, что каждый одночлен $2x_1^{\alpha_1} \dots x_n^{\alpha_n}$ имеет линейризованный вид, т.е. записывается в виде $2x_1 \dots x_n$.

Рассмотрим замкнутые классы, изображенные на рис. 3 лежащими между L_4 и $\langle x^2, 2x_1 \dots x_n \mid n \geq 2 \rangle$. Отметим здесь, что на диаграмме вместо замкнутого класса $\langle x^2, 2x_1x_2 \rangle$ указан замкнутый класс $\langle x^2 \rangle$ так как $\langle x^2, 2x_1x_2 \rangle = \langle x^2 \rangle$ (в силу равенства $2x_1x_2 = (x_1 + x_2)^2 - x_1^2 - x_2^2$ мы получаем $x^2 \rightarrow 2x_1x_2$).

Предложение 3. Пусть $n \geq 2$.

- (1) $f \in \langle 2x_1 \dots x_n \rangle$ тогда и только тогда, когда каждый нелинейный одночлен в f имеет вид $2y_1 \dots y_s$, где $2 \leq s \leq n$;
- (2) $f \in \langle x^2, 2x_1 \dots x_n \rangle$ тогда и только тогда, когда каждый нелинейный одночлен в f имеет вид ay_i^2 или $2y_1 \dots y_s$, где $2 \leq s \leq n$.

Доказательство. Справедливость утверждений 1 и 2 устанавливается сходными рассуждениями. Поэтому мы остановимся лишь на первом из них.

Обозначим через F совокупность всех полиномов из F_4 , нелинейные одночлены которых имеют вид $2y_1 \dots y_s$, где $2 \leq s \leq n$. Надо показать, что $\langle 2x_1 \dots x_n \rangle = F$. Подставляя в $2x_1 \dots x_n$ достаточное число констант 1, получим любой одночлен вида $2y_1 \dots y_s$. Поэтому $2x_1 \dots x_n \rightarrow F$, т.е. $\langle 2x_1 \dots x_n \rangle \supseteq F$. Так как F содержит все линейные полиномы и одночлен $2x_1 \dots x_n$, теперь для доказательства равенства $\langle 2x_1 \dots x_n \rangle = F$ достаточно проверить, что F является замкнутым классом. Последнее проверяется непосредственно. Главным в этой проверке будет тот факт, что в Z_4 произведение $2a$ будет равно либо 0, либо 2.

Из доказанного предложения можно сделать следующие выводы:

- (1) $L_4 \subset \langle 2x_1x_2 \rangle \subset \dots \subset \langle 2x_1 \dots x_n \mid n \geq 2 \rangle$;
- (2) $\langle x^2 \rangle \subset \langle x^2, 2x_1x_2x_3 \rangle \subset \dots \subset \langle x^2, 2x_1 \dots x_n \mid n \geq 2 \rangle$;
- (3) если $m < n$, то замкнутые классы $\langle x^2, 2x_1 \dots x_m \rangle$ и $\langle 2x_1 \dots x_n \rangle$ несравнимы.

Отсюда, в свою очередь, вытекает, что замкнутые классы, изображенные на рис. 3 лежащими между L_4 и $\langle x^2, 2x_1 \dots x_n \mid n \geq 2 \rangle$, попарно различны, а включения между ними именно те, которые указаны на этом рисунке.

Перейдем теперь к верхней части диаграммы, т.е. рассмотрим взаимоотношения классов $\langle x^2, 2x_1 \dots x_n \mid n \geq 2 \rangle$, $\langle x_1^2x_2^2 \rangle$, $\langle x^3 \rangle$ and F_4 . Для этого необходимо выяснить строение полиномов из $\langle x_1^2x_2^2 \rangle$ and $\langle x^3 \rangle$.

Предложение 4. Включение $f \in \langle x_1^2x_2^2 \rangle$ имеет место тогда и только тогда, когда каждый нелинейный одночлен в f имеет вид $ay_1^2 \dots y_t^2$ или $2y_1 \dots y_s$.

Рассуждения при доказательстве этого предложения такие же, как и в случае предложения 3. Поэтому мы их опустим и перейдем к рассмотрению замкнутого класса $\langle x^3 \rangle$. Здесь ситуация существенно сложнее, и мы проанализируем ее подробнее.

Полином f над Z_4 будем называть четным, если для произвольного набора переменных $y_1, \dots, y_s$, $s \geq 2$, число одночленов вида $ay_1^{\alpha_1} \dots y_s^{\alpha_s}$, $a \in \{1, 3\}$, в записи f является четным (в частности, равно нулю). Совокупность всех четных в этом смысле полиномов обозначим через H . Наша цель — установить равенство $\langle x^3 \rangle = H$. Она будет достигнута в предложениях 5–7.

Предложение 5. Справедливо включение $H \subseteq \langle x^3 \rangle$.

Доказательство. Надо установить, что $x^3 \rightarrow H$. Если $f \rightarrow g$, то будем ради удобства говорить, что из f выводится g . Пусть $h \in H$. Тогда нелинейная часть h состоит из одночленов вида

$$(1) ax^\alpha, a \in \{1, 3\}, \alpha \in \{2, 3\},$$

$$(2) 2x_1 \dots x_s, s \geq 2,$$

и двучленов вида

$$(3) bx_1^{\beta_1} \dots x_t^{\beta_t} + cx_1^{\gamma_1} \dots x_t^{\gamma_t}, b, c \in \{1, 3\}, \beta_i, \gamma_i \in \{1, 2, 3\}.$$

Для наших целей достаточно вывести из x^3 одночлены x^2 , $2x_1 \dots x_s$ и двучлены вида (3). При этом в последнем случае можно считать, что $b = c = 1$, так как $3x_1^{\alpha_1} \dots x_t^{\alpha_t} = 2x_1 \dots x_t + x_1^{\alpha_1} \dots x_t^{\alpha_t}$. Этим мы и займемся.

Ясно, что

$$x^3 \rightarrow (x+1)^3 - x^3 - 3x - 1 = 3x^2 \rightarrow 3(3x^2) = x^2.$$

Поэтому

$$x^3 \rightarrow x^2.$$

Очевидно, что

$$x^2 \rightarrow 2x_1x_2,$$

откуда

$$x^3 \rightarrow 2x_1x_2.$$

Далее,

$$x^3 \rightarrow (2x_1x_2 + x_3)^3 - x_3^3 = 2x_1x_2x_3^2 = 2x_1x_2x_3.$$

Продолжая этот процесс, получим, что

$$x^3 \rightarrow (2x_1x_2x_3 + x_4)^3 - x_4^3 = 2x_1x_2x_3x_4,$$

и т.д. Итак, указанная процедура доказывает, что

$$x^3 \rightarrow 2x_1 \dots x_s$$

для любого $s \geq 2$.

Для доказательства того, что $x^3 \rightarrow bx_1^{\beta_1} \dots x_t^{\beta_t} + cx_1^{\gamma_1} \dots x_t^{\gamma_t}$, рассмотрим частные случаи.

Вначале докажем, что $x^3 \rightarrow x_1x_2 + x_1x_2^2$. Начнем с тождества

$$x_1x_2 + x_1x_2^2 + x_1^2x_2 + x_1^2x_2^2 = 0,$$

которое проверяется непосредственно. Из этого тождества следует, что

$$x_1x_2 + x_1x_2^2 = -(x_1^2x_2 + x_1^2x_2^2) = 3(x_1^2x_2 + x_1^2x_2^2),$$

$$x_1x_2 + x_1^2x_2^2 = 3(x_1x_2 + x_1^2x_2^2).$$

Отсюда

$$x^3 \rightarrow (x_1 + x_2)^3 - x_1^3 - x_2^3 = 3(x_1^2x_2 + x_1x_2^2) = x_1^2x_2 + x_1x_2^2$$

и, следовательно,

$$x^3 \rightarrow (x_1)^2x_2 + (x_1^2)x_2^2 = x_1^2x_2 + x_1^2x_2^2 \rightarrow 3(x_1^2x_2 + x_1^2x_2^2) = x_1x_2 + x_1x_2^2.$$

Поэтому

$$x^3 \rightarrow x_1x_2 + x_1x_2^2.$$

Теперь установим, что

$$x^3, f(x_1, \dots, x_n) \rightarrow x_{n+1}f(x_1, \dots, x_n)$$

для любого двучлена

$$f = x_1^{\alpha_1} \dots x_n^{\alpha_n} + x_1^{\beta_1} \dots x_n^{\beta_n}, \quad n \geq 1.$$

Действительно, $f^2 = 0$, так как $f^2 = 2x_1^2 \dots x_n^2 + 2x_1 \dots x_n = 4x_1 \dots x_n = 0$. Отсюда,

$$x^3, f \rightarrow x_{n+1}f + x_{n+1}f^2 = x_{n+1}f.$$

Уместно отметить, что если $x^3 \rightarrow f$, то

$$x^3 \rightarrow x_{n+1}f = x_1^{\alpha_1} \dots x_n^{\alpha_n} x_{n+1} + x_1^{\beta_1} \dots x_n^{\beta_n} x_{n+1},$$

и можно повторить эту процедуру. Иными словами, в данной ситуации мы можем получить, что

$$x^3 \rightarrow (x_1^{\alpha_1} \dots x_n^{\alpha_n} + x_1^{\beta_1} \dots x_n^{\beta_n})x_{n+1} \dots x_{n+m}.$$

Следующим шагом докажем, что $x^3 \rightarrow x_1 \dots x_n + x_1^{\alpha_1} \dots x_n^{\alpha_n}$. В силу предыдущего можно считать, что $\alpha_i \neq 1$ для всех i . Так как $x^3 \rightarrow x + x^\alpha = f$, получим, что

$$x^3 \rightarrow x_1 x_2 \dots x_n + x_1^{\alpha_1} x_2 \dots x_n = g_1.$$

Чтобы вывести $x^3 \rightarrow x_1 x_2 x_3 \dots x_n + x_1 x_2^{\alpha_2} x_3 \dots x_n$, подставим $x_1^{\alpha_1}$ (т.е. x_1^2 или x_1^3) вместо x_1 , и получим, что

$$x^3 \rightarrow x_1^{\alpha_1} x_2 x_3 \dots x_n + x_1^{\alpha_1} x_2^{\alpha_2} x_3 \dots x_n = g_2.$$

Снова, чтобы вывести $x^3 \rightarrow x_1 x_2 x_3 x_4 \dots x_n + x_1 x_2 x_3^{\alpha_3} x_4 \dots x_n$, подставим x_1 вместо $x_1^{\alpha_1}$ и x_2 вместо $x_2^{\alpha_2}$, и получим, что

$$x^3 \rightarrow x_1^{\alpha_1} x_2^{\alpha_2} x_3 x_4 \dots x_n + x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3} x_4 \dots x_n = g_3,$$

и так далее. Так как $x^3 \rightarrow g_1 \dots g_n$, получаем, что

$$x^3 \rightarrow \sum_{k=1}^n g_k = x_1 \dots x_n + 2(n-1)x_1 \dots x_n + x_1^{\alpha_1} \dots x_n^{\alpha_n},$$

и следовательно,

$$x^3 \rightarrow x_1 \dots x_n + x_1^{\alpha_1} \dots x_n^{\alpha_n}.$$

Наконец, рассмотрим наиболее общую ситуацию:

$$f = x_1^{\alpha_1} \dots x_n^{\alpha_n} + x_1^{\beta_1} \dots x_n^{\beta_n}.$$

Так как

$$x^3 \rightarrow x_1 \dots x_n + x_1^{\alpha_1} \dots x_n^{\alpha_n}, x_1 \dots x_n + x_1^{\beta_1} \dots x_n^{\beta_n},$$

получаем, что

$$x^3 \rightarrow x_1^{\alpha_1} \dots x_n^{\alpha_n} + x_1^{\beta_1} \dots x_n^{\beta_n} + 2x_1 \dots x_n,$$

и

$$x^3 \rightarrow x_1^{\alpha_1} \dots x_n^{\alpha_n} + x_1^{\beta_1} \dots x_n^{\beta_n}.$$

Предложение 5 доказано.

Пусть f — полином из F_4 . Обозначим через $\tilde{f}$ сумму всех одночленов из f , зависящих более чем от одного аргумента, а через $\text{Im}(f)$ — множество значений f (как функции).

Предложение 6. *Справедливо соотношение $H = \{f \in F_4 \mid \text{Im}(\tilde{f}) \subseteq \{0, 2\}\}$.*

Доказательство. Пусть $f \in H$. Рассмотрим соответствующий ему полином $\tilde{f}$. Из определения H следует, что $2\tilde{f} = 0$. Это и означает, что $\text{Im}(\tilde{f}) \subseteq \{0, 2\}$. Пусть теперь $f \notin H$. Тогда для некоторого набора переменных $\{x_{i_1}, \dots, x_{i_n}\}$ число слагаемых вида $ax_{i_1}^{\alpha_1} \dots x_{i_n}^{\alpha_n}$ ($a \in \{1, 3\}$) в полиноме $\tilde{f}$ нечетно. Поэтому в полиноме $2\tilde{f}$ присутствует слагаемое $2x_{i_1} \dots x_{i_n}$, которое не может уничтожиться, поскольку другие слагаемые в $2\tilde{f}$ имеют другие наборы переменных. Таким образом, $2\tilde{f}$ не равен тождественно нулю, а это и означает, что $\text{Im}(\tilde{f}) \not\subseteq \{0, 2\}$.

Предложение 7. *Справедливо включение $\langle x^3 \rangle \subseteq H$.*

Доказательство. Поскольку x^3 и все линейные полиномы являются четными, то достаточно проверить замкнутость класса H . То, что H замкнут относительно перестановок и отождествлений переменных, а также добавления фиктивных переменных, очевидно. Необходимо доказать, что H замкнут относительно композиции. Этому и посвящено дальнейшее.

Пусть $f, g \in H$. Представим их в виде $f = \tilde{f} + f_1$, $g = \tilde{g} + g_1$, где каждое слагаемое в f_1 и g_1 зависит не более чем от одного аргумента. Рассмотрим полином $f * g$, где $*$ — операция суперпозиции (см. [1]). Этот полином можно представить в виде $(\tilde{f} * g) + (f_1 * g)$. В полиноме $\tilde{f} * g$ все слагаемые зависят от двух или большего числа аргументов. Поскольку $\text{Im}(f) \subseteq \{0, 2\}$, полином $\tilde{f} * g$ четный. Так как сумма четных полиномов снова является четным полиномом, осталось доказать, что $f_1 * g \in H$.

Пусть

$$f_1 = a_1 x_1^3 + a_2 x_1^2 + a_3 x_1 + f_2,$$

где f_2 не зависит от x_1 . Тогда

$$f_1 * g = a_1 g^3 + a_2 g^2 + a_3 g + f_2.$$

Так как полиномы $a_3 g$ и f_2 четные, осталось доказать, что g^2 и g^3 четные.

Рассмотрим первый из них. Ясно, что

$$g^2 = (\tilde{g} + g_1)^2 = (\tilde{g})^2 + 2\tilde{g}g_1 + g_1^2 = g_1^2$$

(в силу того, что $\text{Im}(\tilde{g}) \subseteq \{0, 2\}$ по предложению 6). Поскольку все слагаемые в g_1^2 , зависящие более чем от одного аргумента, имеют вид $2x_i x_j$, полином g_1 , а вместе с ним и g^2 , четный.

Теперь рассмотрим второй полином. Очевидно, что

$$g^3 = (\tilde{g} + g_1)^3 = (\tilde{g})^3 + 3(\tilde{g})^2 g_1 + 3\tilde{g}g_1^2 + g_1^3 = \tilde{g}g_1^2 + g_1^3.$$

В полиноме $\tilde{g}g_1^2$ все одночлены зависят более чем от одного аргумента, и $\text{Im}(\tilde{g}) \subseteq \{0, 2\}$. Следовательно,

$$(\widetilde{\tilde{g}g_1^2}) = \tilde{g}g_1^2, \quad \text{Im}(\tilde{g}g_1^2) \subseteq \{0, 2\},$$

откуда $\tilde{g}g_1^2 \in H$. Для завершения доказательства предложения 7, остается показать, что справедливо включение $g_1^3 \in H$, которое является следствием из следующего утверждения: для любого полинома $h \in F_4$, каждое слагаемое которого имеет вид $a_i x_i^{\alpha_i}$, выполняется включение $h^3 \in H$.

Докажем это утверждение индукцией по числу аргументов полинома h . База индукции очевидна. Перейдем к установлению шага индукции.

Пусть h зависит от $n > 1$ переменных, и пусть утверждение справедливо для любого полинома указанного вида, зависящего от меньшего числа переменных. Пусть среди аргументов h есть x_1 . Представим h в виде $h = h_1(x_1) + h_2$, где h_1 зависит только от x_1 , а h_2 , наоборот, от x_1 не зависит. Тогда

$$h^3 = (h_1 + h_2)^3 = h_1^3 + 3h_1^2 h_2 + 3h_1 h_2^2 + h_2^3.$$

Полином h_2^3 четный по предположению индукции. Включение $h_1^3 \in H$ очевидно. Рассмотрим полином $3h_1^2 h_2 + 3h_1 h_2^2$. Все его одночлены зависят более чем от одного аргумента. Теперь заметим, что $\text{Im}(3x_1^2 x_2 + 3x_1 x_2^2) \subseteq \{0, 2\}$, и значит, $\text{Im}(3h_1^2 h_2 + 3h_1 h_2^2) \subseteq \{0, 2\}$. По предложению 6, полином $3h_1^2 h_2 + 3h_1 h_2^2$ четный. Значит, $h^3 \in H$. Утверждение, а вместе с ним и предложение 7, доказано.

Итак, из предложений 4, 5 и 7 следует, что четыре замкнутых класса в верхней части рис. 3 попарно различны, и указанные включения выполняются.

4. Завершение доказательства

Для установления того, что рис. 3 изображает все элементы интервала $[L_4; F_4]$, нам потребуется еще один объект, свойства которого будут выявлены в леммах этого параграфа.

Полином $f(x_1, \dots, x_n)$ назовем нормальным, если в записи каждого его слагаемого участвуют все переменные $x_1, \dots, x_n$. Каждый полином g без свободного члена представим в виде $g = f_1 + \dots + f_s$, где каждый из полиномов f_i нормальный, и для любых различных i, j полином $f_i + f_j$ не является нормальным. В этих обозначениях справедливо следующее утверждение.

Лемма 3. *Справедливо равенство $\langle g \rangle = \langle f_1, \dots, f_s \rangle$.*

Доказательство. Доказательство проведем индукцией по s .

Начнем с установления базы индукции. Для $s = 1$ утверждение тривиально.

Выполним шаг индукции. Пусть $s > 1$, и f_1 — минимальный среди $f_1, \dots, f_s$ по количеству вхождений переменных. Подставив в g всюду $x_i = 0$, если x_i не входит в f_1 , получим в точности f_1 . Тогда в силу предположения индукции

$$\begin{aligned} g &\rightarrow g - f_1 = f_2 + \dots + f_s, \\ \langle g \rangle &= \langle f_1, f_2 + \dots + f_s \rangle = \langle f_1, f_2, \dots, f_s \rangle, \end{aligned}$$

и лемма 3 доказана.

Наша следующая цель — доказать, что каждый нормальный полином равен (как функция) некоторому нормальному полиному простого вида. Это будет сделано в следующих двух леммах.

Пусть

$$f = \sum_{i=1}^m x_1^{\alpha_1(i)} \dots x_n^{\alpha_n(i)}$$

— нормальный полином (слагаемые могут повторяться). Сопоставим ему матрицу M_f размера $m \times n$, строки которой есть n -ки вида $(\alpha_1(i), \dots, \alpha_n(i))$, $i = 1, \dots, m$. Отметим, что порядок строк нам не важен. Число n в этом случае назовем длиной полинома f и обозначим через $l(f)$.

Лемма 4. Пусть f — нормальный полином, $l(f) = 4t$, и в каждом столбце матрицы M_f количества единиц, двоек и троек четны. Тогда $f = 0$.

Доказательство. Доказательство проведем индукцией по числу n переменных в записи f .

Начнем с установления базы индукции. Пусть $n = 1$. В этом случае M_f есть m -мерный столбец, $m = 4t$. Пусть $2t_1$, $2t_2$ и $2t_3$, соответственно, — число единиц, двоек и троек в этом столбце. Тогда $2t_1 + 2t_2 + 2t_3 = 4t$. Вычислим f в точках 0, 1, 2 и 3. Напомним только, что в этих вычислениях все арифметические действия выполняются по модулю 4. Получим

$$\begin{aligned} f(0) &= 0, \\ f(1) &= 2t_1 + 2t_2 + 2t_3 = 4t = 0, \\ f(2) &= 2 \cdot 2t_1 + 2^2 \cdot 2t_2 + 2^3 \cdot 2t_3 = 0, \\ f(3) &= 3 \cdot 2t_1 + 3^2 \cdot 2t_2 + 3^3 \cdot 2t_3 = 4t = 0. \end{aligned}$$

Итак, $f(x) = 0$, и база индукции установлена.

Выполним индуктивный переход. Зафиксировав произвольные $x_1, \dots, x_{n-1}$, вычислим значения $f(x_1, \dots, x_{n-1}, x_n)$, подставляя $x_n = 0, 1, 2, 3$. Очевидно, что $f(x_1, \dots, x_{n-1}, 0) = 0$. Для проверки остальных значений x_n , рассмотрим представление

$$f(x_1, \dots, x_{n-1}, x_n) = x_n f_1(x_1, \dots, x_{n-1}) + x_n^2 f_2(x_1, \dots, x_{n-1}) + x_n^3 f_3(x_1, \dots, x_{n-1}).$$

Полином $f_1 + f_2 + f_3$ удовлетворяет условию леммы и имеет меньшее число переменных. В силу индуктивного предположения, $f_1 + f_2 + f_3 = 0$. Поэтому

$$f(x_1, \dots, x_{n-1}, 1) = f_1 + f_2 + f_3 = 0.$$

Теперь заметим, что в силу условий леммы каждый из нормальных полиномов f_1, f_2, f_3 имеет четное число слагаемых. Значит, то же самое можно сказать и о нормальном полиноме $f_1 + f_3$. Но для любого нормального полинома g с четным числом слагаемых имеет место тождество $2g = 0$, так как $2g(x_1, \dots, x_k) = 2l(g)x_1 \dots x_k = 0$ в силу четности числа $l(g)$. Применим это соображение к вычислению значений f для $x_n = 2$ и $x_n = 3$, и получим, что

$$f(x_1, \dots, x_{n-1}, 2) = 2f_1 + 2^2 f_2 + 2^3 f_3 = 2f_1 = 0$$

и

$$\begin{aligned}
 f(x_1, \dots, x_{n-1}, 3) &= 3f_1 + 3^2f_2 + 3^3f_3 \\
 &= 3f_1 + f_2 + 3f_3 \\
 &= 2(f_1 + f_3) + (f_1 + f_2 + f_3) = 0.
 \end{aligned}$$

Лемма доказана.

Лемма 5. Каждый нелинейный нормальный полином $f(x_1, \dots, x_n)$ без свободного члена равен (как функция) нормальному полиному одного из следующих четырех видов:

- (1) $2x_1 \dots x_n$;
- (2) $ax_1^2 \dots x_n^2$, $a \in \{1, 3\}$;
- (3) $x_1^{\alpha_1} \dots x_n^{\alpha_n} + ax_1^2 \dots x_n^2$, где a произвольно и $\alpha_i \neq 2$ для некоторого i ;
- (4) $x_1^{\alpha_1} \dots x_n^{\alpha_n} + x_1^{\beta_1} \dots x_n^{\beta_n} ax_1^2 \dots x_n^2$, где a произвольно, $\alpha_i \neq 2$, $\beta_j \neq 2$ для некоторого i, j , а если $\alpha_k = \beta_k$ для некоторого k , то $\alpha_k = \beta_k = 2$ и $\beta_1, \dots, \beta_n \in \{2, 3\}$.

Доказательство. Рассмотрим матрицу M_f . Пусть в каждом ее столбце четное число единиц и троек. Рассмотрим полином

$$f_1(x_1, \dots, x_n) = f(x_1, \dots, x_n) + ax_1^2 \dots x_n^2,$$

где число $l(f) + a$ делится на 4. Полином f_1 удовлетворяет условиям леммы 4. Следовательно, $f(x_1, \dots, x_n) + ax_1^2 \dots x_n^2 = 0$, и $f(x_1, \dots, x_n) = -ax_1^2 \dots x_n^2$, т.е. f равен полиному вида (1), если $a = 2$, и полиному вида (2), если $a \in \{1, 3\}$.

Пусть в некотором столбце матрицы M_f имеется нечетное число единиц или троек. Рассмотрим полином

$$f_2(x_1, \dots, x_n) = f(x_1, \dots, x_n) + 3x_1^{\alpha_1} \dots x_n^{\alpha_n},$$

где

$$\alpha_i = \begin{cases} 1, & \text{если число единиц в } i\text{-ом столбце } M_f \text{ нечетно,} \\ 3, & \text{если число единиц в } i\text{-ом столбце } M_f \text{ четно, а число троек нечетно,} \\ 2 & \text{в остальных случаях.} \end{cases}$$

В каждом столбце матрицы M_{f_2} число единиц четно. Если количество троек в каждом столбце M_{f_2} также четно, то, рассуждая как и в предыдущем случае, получаем, что

$$f(x_1, \dots, x_n) = x_1^{\alpha_1} \dots x_n^{\alpha_n} + ax_1^2 \dots x_n^2,$$

т.е. f равен полиному вида (3).

Пусть в некотором столбце матрицы M_{f_2} число троек нечетно. Тогда рассмотрим полином

$$f_3(x_1, \dots, x_n) = f_2(x_1, \dots, x_n) + 3x_1^{\beta_1} \dots x_n^{\beta_n},$$

где

$$\beta_i = \begin{cases} 3, & \text{если число троек в } i\text{-ом столбце } M_f \text{ нечетно,} \\ 2 & \text{в противном случае.} \end{cases}$$

Рассуждая, как и в начале доказательства этой леммы, получаем, что f равен некоторому полиному вида (4).

Перебор случаев закончен, и лемма доказана.

Лемма 6. Пусть полином f имеет один из видов, перечисленных в лемме 5. Тогда замкнутый класс $\langle f \rangle$ присутствует на рис. 3.

Доказательство. Если f зависит от одной переменной, то нетрудно понять, что замкнутый класс $\langle f \rangle$ есть либо $\langle x^2 \rangle$, либо $\langle x^3 \rangle$. Пусть f зависит от двух или более переменных. Если f — полином вида (1), то утверждение леммы тривиально. Если f имеет вид (2), то $\langle f \rangle = \langle x_1^2 x_2^2 \rangle$. Пусть f — полином вида (3) и $a \in \{1, 3\}$. Докажем, что $\langle f \rangle = \langle x^3 \rangle$. В самом деле, f — четный полином, поэтому $\langle f \rangle \subseteq \langle x^3 \rangle$. Покажем, что справедливо и обратное включение.

Если $\alpha_i = 3$ для некоторого i , то, подставив 1 вместо всех x_j , кроме x_i , получим $x_i^3 + ax_i^2$, откуда, как нам уже известно, выводится x^3 . Пусть все $\alpha_i \in \{1, 2\}$ и $\alpha_1 = 1$. Подставив $x_2 = \dots = x_n = 1$, получим $ax_1^2 + x_1$, где $a \in \{1, 3\}$, т.е. $f \rightarrow x^2$. Рассмотрим полином $f(x_1, x_1^2, 1, \dots, 1) = x^3 + ax^2$. Опять получаем $f \rightarrow x^3$, и обратное включение доказано.

Пусть теперь f — полином вида (3) и $a \in \{0, 2\}$. Докажем, что $\langle f \rangle = F_4$. Если $a = 2$, то

$$f = x_1^{\alpha_1} \dots x_n^{\alpha_n} + ax_1^2 \dots x_n^2 = 3x_1^{\alpha_1} \dots x_n^{\alpha_n}.$$

Как нам уже известно,

$$\langle f \rangle = \langle 3f \rangle = \langle x_1^{\alpha_1} \dots x_n^{\alpha_n} \rangle.$$

Поэтому можно считать, что $a = 0$. Рассмотрим случай, когда $\alpha_1 \neq 2$. Подставив 1 вместо $x_3, \dots, x_n$ в f , получим $x_1^{\alpha_1} x_2^{\alpha_2}$. При любом α_2

$$x_1^{\alpha_1} x_2^{\alpha_2} \rightarrow x^3.$$

Полином $x_1^{\alpha_1} x_2^{\alpha_2} + x_1 x_2$ четный, поэтому

$$x^3 \rightarrow x_1^{\alpha_1} x_2^{\alpha_2} + x_1 x_2.$$

Наконец,

$$x_1^{\alpha_1} x_2^{\alpha_2} + x_1 x_2, x_1^{\alpha_1} x_2^{\alpha_2} \rightarrow x_1 x_2.$$

Итак, $\langle f \rangle \supseteq \langle x_1 x_2 \rangle = F_4$, а значит, $\langle f \rangle = F_4$.

Осталось разобрать случай, когда f имеет вид (4).

Предположим, что $a \in \{0, 2\}$. Тогда f четный и $\langle f \rangle \supseteq \langle x^3 \rangle$. Покажем, что выполняется и обратное включение. В этой ситуации найдется некоторое i такое, что $\beta_i \neq 3$; пусть $\beta_1 \neq 3$ ($i = 1$). Тогда $\alpha_1 \neq 3$. Подставив 1 вместо $x_2, \dots, x_n$ в f , получим $x_1^{\alpha_1} + x_1^3 + ax_1^2$. Отсюда выводим x^3 . Таким образом, в этом случае $\langle f \rangle = \langle x^3 \rangle$.

Пусть $a \in \{1, 3\}$. Докажем, что $\langle f \rangle = F_4$. Если $\beta_1 = 3$, то, как и в предыдущем случае, получаем, что

$$f \rightarrow x_1^{\alpha_1} + x_1^3 + ax_1^2 \rightarrow x^3.$$

Подставив в f единицы вместо $x_3, \dots, x_n$, получим полином

$$g(x_1, x_2) = x_1^{\alpha_1} x_2^{\alpha_2} + x_1^1 x_2^{\beta_2} + a x_1 x_2.$$

Поскольку полином $g_1 = g(x_1, x_2) + a x_1 x_2$ четный, $g_1 \in \langle f \rangle$. Далее, $g, g_1 \rightarrow x_1 x_2$ и $\langle f \rangle = F_4$. Лемма 6 доказана.

Теперь мы в состоянии показать, что рис. 3 изображает все элементы интервала $[L_4; F_4]$. Действительно, в силу леммы 3 каждый замкнутый класс из $[L_4; F_4]$ может быть порожден нормальными полиномами вида (1)–(4). Поэтому в силу леммы 6 достаточно установить, что решеточная сумма замкнутых классов вида $\langle f \rangle$ на рис. 3 есть снова замкнутый класс, представленный на этом рисунке. Единственный нетривиальный случай, который нуждается в проверке, — это решеточная сумма $\langle x_1^2 x_2^2 \rangle \vee \langle x^3 \rangle$. Полином $x_1^2 x_2^2 + x_1 x_2$ четный, и поэтому $x^3 \rightarrow x_1^2 x_2^2 + x_1 x_2$. Следовательно, $x_1^2 x_2^2, x^3 \rightarrow x_1 x_2$. А так как $\langle x_1^2 x_2^2 \rangle = F_4$, получаем, что $\langle x_1^2 x_2^2 \rangle \vee \langle x^3 \rangle = F_4$. Этим завершено доказательство теоремы 2.

Список литературы

1. Мальцев А. И, *Итеративные алгебры Поста*. Наука, Новосибирск, 1976.
2. Ремизов А. Б. О надструктуре замкнутого класса полиномов по модулю k . *Дискретная математика* (1989) 1, №1, 3–15.
3. Сафин К. Л., Суханов Е. В. Клоны и полиномы над кольцом вычетов. В кн.: *Тез. докл. 3 Междунар. конф. по алгебре памяти М. И. Каргаполова*. Красноярск, 23–28 августа 1993, с. 294–295.
4. Суханов Е. В., Крохин А. А., Сафин К. Л. О некоторых замкнутых классах полиномов в k -значной логике. В кн.: *Тез. докл. 11 Межреспубл. конф. по матем. логике*. Казань, 1992, с. 137.
5. Яблонский С. В. Функциональные построения в k -значной логике. *Труды Матем. Института им. В. А. Стеклова* (1958) 51, 5–142.
6. R. Pöschel, L. A. Kalužnin, *Funktionen- und Relationenalgebren*. Ein Kapitel der diskreten Mathematik, Berlin, VEB DVW, 1979.

Статья поступила 05.01.1995.