Московский государственный университет
имени М. В. Ломоносова

Механико-математический факультет

На правах рукописи
УДК 512.552.18, 512.552.332, 512.624.2

Кулямин Виктор Вячеславович

Об образах полиномиальных отображений в конечных кольцах матриц

Специальность 01.01.06 — математическая логика, алгебра и теория чисел

Диссертация на соискание учёной степени
кандидата физико-математических наук

Научный руководитель —
доктор физико-математических наук
профессор А. В. Михалёв

Москва 2000

Оглавление

Введение

Практически с самого зарождения теории колец большое значение для неё имело изучение свойств специфических многочленов. Роль, которую играет наличие таких многочленов для определения строения кольца, наиболее отчётливо была осознана в конце сороковых — начале пятидесятых годов этого века. Тогда, благодаря работам Капланского [1], Амицура [2, 3, 4], Левицкого [5], их совместным работам [6, 7] тождества, то есть многочлены, принимающие в кольце только значение 0, стали одним из основных инструментов исследований в данной области.

В связи с этим алгебры, обладающие нетривиальными тождествами, — так называемые PI-алгебры — стали важным объектом изучения и рассматривались как естественное обобщение коммутативных алгебр, удобное для распространения результатов структурной теории. Основные результаты о PI-алгебрах можно найти в классических монографиях Прочези [8], Джекобсона [9] и Роуэна [10].

Эти исследования показали, в частности, что важную роль в определении свойств алгебры, помимо тождеств, играют так называемые центральные многочлены — не являющиеся тождествами многочлены, образ которых целиком содержится в центре алгебры. Проблема существования центральных многочленов в наиболее важном случае, в полных матричных алгебрах, была поставлена Капланским ещё в 1956 году среди других проблем теории колец [11].

В случае конечности основного поля проблема Капланского была решена Латышевым и Шмелькиным [12] в 1969 году. Сам Капланский упоминал о частных её решениях в [13]. Полное положительное решение её было получено в 1971 году независимо Размысловым [14] и Форманеком [15], причём конструкция Размыслова с небольшими изменениями даёт центральный многочлен для полной матричной алгебры над произвольным коммутативным кольцом с единицей.

По-видимому, именно обсуждение различных аспектов проблемы существования центрального многочлена, побудило Капланского поставить следующую проблему: всегда ли образ некоммутативного полилинейного многочлена в полной матричной алгебре M над полем нулевой характеристики является линейным подпространством в M. В некоторых частных случаях, например, для многочленов от двух переменных, это, конечно же, так. Ответ на этот вопрос в общем случае до сих пор не известен.

Второй раз тема описания свойств образов многочленов возникла в работе Чуанга [16], появившейся в 1990 году. Пытаясь ответить на вопрос, поставленный Капланским, он получил характеризацию образов произвольных некоммутативных многочленов в полных матричных алгебрах над конечными полями. Подмножество A такой алгебры является образом многочлена с коэффициентами из основного поля тогда и только тогда, когда оно содержит скалярную матрицу и самоподобно, то есть $\alpha A \alpha^{-1} \subseteq A$ для всякой обратимой матрицы α.

В настоящей работе исследуются свойства образов многочленов в полных матричных алгебрах над конечными коммутативными кольцами. В первую очередь нас будут интересовать кольца наиболее близкие к полям по своим свойствам — так называемые кольца Галуа.

Кольцо Галуа — это конечное коммутативное локаль-

ное кольцо $\mathbb{K}$ главных идеалов с единицей, наибольший идеал которого $J(\mathbb{K})$ порождён характеристикой поля вычетов $\mathbb{K}/J(\mathbb{K})$. Такие кольца впервые были рассмотрены в работе Раджавендрана [17]. Они являются естественным обобщением колец вычетов по модулю, равному степени простого числа, и находятся с этими кольцами вычетов в таком же отношении, как поля Галуа с полями вычетов $\mathbb{Z}/p\mathbb{Z}$. Многие свойства колец Галуа были исследованы Нечаевым в статьях [18, 19, 20]. Изложение общих результатов, касающихся локальных колец и колец главных идеалов можно найти в книгах Нагаты [21] и Ятегаонкара [22].

Целью данной работы является исследование свойств образов многочленов в конечных алгебрах и распространение характеризации образов некоммутативных многочленов в полных матричных алгебрах, полученной Чуангом, на случай основного кольца, не являющегося полем.

В работе используются методы и результаты общей теории колец, теории PI-алгебр, арифметические свойства конечных полей и колец Галуа.

Основные результаты данной работы:

- Сформулирован ряд условий на подмножество произвольной алгебры над коммутативным кольцом, необходимых для того, чтобы это подмножество было образом некоммутативного многочлена с коэффициентами в этом кольце;

- Доказано, что упомянутые в предыдущем пункте условия на подмножество алгебры являются достаточными в том случае, если алгебра является конечной прямой суммой полных матричных алгебр над конечным полем, полной алгеброй матриц размера 2×2 над кольцом Галуа с радикалом степени нильпотентности 2 или над $\mathbb{Z}/8\mathbb{Z}$;

- Получен аналогичный результат для градуированного случая — сформулированы условия на однородное подмножество полной матричной алгебры над конечной коммутативной полугрупповой алгеброй над полем, необходимые и достаточные для того, чтобы это подмножество было образом градуированного многочлена с коэффициентами из основного поля.

Все полученные результаты являются новыми.

Работа носит теоретический характер. Её результаты могут быть использованы при исследовании ряда вопросов теории колец.

Результаты работы неоднократно обсуждались на семинаре «Кольца и модули» кафедры высшей алгебры механико-математического факультета МГУ под руководством профессора В. Н. Латышева и профессора А. В. Михалёва. Часть результатов докладывалась на конференции, посвящённой 70-летию кафедры высшей алгебры механико-математического факультета МГУ в 1999 году.

Основные результаты данной диссертации опубликованы в 3-х работах автора, список которых приводится в конце введения.

Диссертация состоит из введения, трёх глав, разбитых на параграфы, и списка литературы. Полный объём диссертации — 73 страницы, библиография содержит 35 наименований.

В первой главе данной работы обсуждаются общие свойства образов полиномиальных отображений в алгебрах над коммутативными кольцами. В первом её параграфе даются базовые определения, и формулируется основное свойство образов таких отображений, состоящее в устойчивости относительно эндоморфизмов алгебры. Дальнейшие исследования посвящены, в основном, выяснению того, в каких алгебрах

выполнения этого свойства для произвольного подмножества алгебры достаточно для существования многочлена, образ которого совпадает с этим подмножеством.

Во втором параграфе рассматривается влияние разложимости алгебры в прямую сумму на свойства образов многочленов в ней. Выявляется дополнительное условие, которому удовлетворяют образы многочленов в такой алгебре. Оно состоит в том, что для любых двух центральных ортогональных многочленов e_1 и e_2 образ многочлена A содержит множество e_1A+e_2A. Здесь же доказывается следующая теорема, позволяющая свести исследование вопроса о достаточности устойчивости множества относительно эндоморфизмов для того, чтобы оно было образом многочлена, к изучению алгебр над неразложимыми в прямую сумму кольцами.

Теорема 1. *Если R является алгеброй над кольцом $\mathbb{K} = \mathbb{K}_1 \oplus \cdots \oplus \mathbb{K}_n$ и для всякого $i \in [1, n]$ в алгебре ${}_{\mathbb{K}_i}(\mathbb{K}_i R)$ любое подмножество, устойчивое относительно эндоморфизмов этой алгебры является образом многочлена с коэффициентами из $\mathbb{K}_i$ и нулевым свободным членом, то всякое подмножество R, устойчивое относительно её эндоморфизмов и удовлетворяющее приведённому выше условию, также является образом некоторого многочлена с коэффициентами из $\mathbb{K}$ и нулевым свободным членом.*

В третьем параграфе приводится ряд примеров алгебр, в которых все устойчивые относительно эндоморфизмов подмножества являются образами многочленов. Во всех этих примерах соответствующие алгебры конечны. Несколько контрпримеров, также приведённых в третьем параграфе, демонстрируют, что в случае бесконечных алгебр требуются какие-то дополнительные ограничения.

Тут же доказано утверждение, показывающее что в алгебре, имеющей центральный многочлен, принимающий значе-

ние 1, объединение образов двух многочленов также является образом многочлена. Это даёт следующий метод для доказательства достаточности устойчивости подмножества алгебры относительно эндоморфизмов для того, чтобы оно являлось образом многочлена: сперва рассматриваем минимальные устойчивые подмножества и находим многочлены, чьими образами они являются, затем, используя конечность алгебры и сформулированное утверждение, получаем, что все устойчивые подмножества являются образами многочленов.

Во второй главе исследуются свойства образов многочленов в градуированных алгебрах. Первый её параграф содержит определения алгебры градуированных многочленов и образа градуированного многочлена, а также доказательство аналогичного неградуированному случаю свойства образов многочленов — образы градуированных многочленов устойчивы относительно эндоморфизмов, сохраняющих градуировку.

Второй параграф второй главы посвящён, в основном, доказательству следующего утверждения, являющегося некоторым обобщением результата Чуанга [16] на случай алгебр матриц над градуированным кольцом.

Теорема 2. *Пусть G — конечная коммутативная полугруппа с единицей, $\mathbb{K} = \mathbb{F}(G)$ — конечная полугрупповая алгебра над полем, $R = M_m(\mathbb{K})$ — кольцо матриц размера $m \times m$ над $\mathbb{K}$. Тогда на $\mathbb{K}$ определена естественная градуировка по G, которая переносится и на R. Однородное по этой градуировке множество $A \subseteq R$ является образом G-градуированного многочлена с нулевым свободным членом тогда и только тогда, когда $0 \in A$ и A самоподобно, то есть, переводится в себя всяким собственным автоморфизмом, соответствующим однородной обратимой матри-*

це.

Для доказательства используется описанный выше подход, при котором строятся многочлены, чьи образы совпадают с минимальными однородными содержащими 0 множествами — при этом используется результат Чуанга.

Третья глава данной работы посвящена распространению характеризации образов многочленов в полных матричных алгебрах над конечными полями, полученной Чуангом в [16], на матричные алгебры над кольцами Галуа. В первом её параграфе приводятся определение кольца Галуа и основные свойства таких колец.

Дальнейшее содержание этой главы составляет доказательство того, что все самоподобные и содержащие 0 подмножества полной алгебры матриц размера 2×2 над кольцом Галуа, радикал которого имеет степень нильпотентности 2, или же которое изоморфно $\mathbb{Z}/8\mathbb{Z}$, являются образами многочленов с коэффициентами из данного кольца и нулевым свободным членом. Доказательство это следует описанному выше пути — мы пытаемся сперва получить многочлены, образами которых являются минимальные самоподобные множества, или, по-другому, классы подобия.

В качестве вспомогательного средства для получения многочленов с определёнными подмножествами в качестве образов используются индикаторы. *Индикатором* подмножества A алгебры ${}_{\mathbb{K}}R$ называется многочлен $\chi(x, x_1, \ldots, x_n)$ с коэффициентами из $\mathbb{K}$, принимающий в R только значения 0 и 1, причём

$$a \notin A \Rightarrow \forall a_1, \ldots, a_n \in R \quad \chi_A(a, a_1, \ldots, a_n) = 0;$$

$$a \in A \Rightarrow \exists a_1, \ldots, a_n \in R \quad \chi_A(a, a_1, \ldots, a_n) = 1.$$

В [16] основной результат получен, фактически, как следствие следующего утверждения.

Лемма 3. *Всякое самоподобное множество* $A \subseteq R = M_m(\mathbb{K})$ *матриц над конечным полем обладает индикатором.*

Можно отметить как очевидный факт то, что всякое обладающее индикатором и содержащее 0 подмножество алгебры является образом многочлена. Если $\chi(x, x_1, \ldots, x_n)$ — его индикатор, в качестве такого многочлена подходит $x\chi(x, x_1, \ldots, x_n)$.

Во втором параграфе третей главы формулируется и доказывается критерий существования индикатора для подмножества полной матричной алгебры над кольцом Галуа. Оказывается, для такого подмножества индикатор существует в точности тогда, когда оно самоподобно и замкнуто по модулю радикала. Доказательство этого основано на сформулированной лемме.

Третий параграф содержит несколько вспомогательных результатов о подобии матриц размера 2×2 над кольцом Галуа. Здесь приводится классификация классов подобия таких матриц, полученная Нечаевым [20] и на её основе доказывается, что все матрицы из минимального самоподобного и замкнутого по модулю радикала множества после возведения в некоторую степень становятся либо скалярами по модулю радикала, либо образуют один класс подобия. В качестве подходящего показателя степени можно взять p^{n-1}, где $p = char(\mathbb{K}/J(\mathbb{K}))$ — характеристика поля вычетов по радикалу, а n обозначает степень нильпотентности радикала $J(\mathbb{K})$.

В четвёртом параграфе формулируются условия, при которых возведение матрицы 2×2 над кольцом Галуа в степень p^{n-1} даёт скалярную по модулю радикала матрицу.

Основное содержание пятого параграфа составляют процедуры построения многочленов, образы которых совпадают

с классами подобия, дополненными 0. При этом, во-первых, используются результаты трёх предыдущих параграфов, чтобы для каждого класса подобия матриц, p^{n-1}-ая степень которых нескалярна по модулю радикала, получить многочлен, чей образ равен этому классу в объединении с 0. Затем, при помощи некоторых специальных конструкций, вопрос о получении многочленов, образы которых давали бы все классы подобия, сводится, при некоторых ограничениях, к получению многочленов с образами, равными нескалярным по модулю радикала классам подобия матриц с нулевым следом, дополненным 0.

В шестом параграфе третьей главы полученные ранее результаты используются для доказательства теоремы, распространяющей результат Чуанга на алгебры матриц размера 2×2 над некоторыми кольцами Галуа.

Теорема 4. *Пусть $R = M_2(\mathbb{K})$ есть полная алгебра матриц размера 2×2 над кольцом Галуа $\mathbb{K}$, радикал которого имеет степень нильпотентности 2, или же которое само совпадает с $\mathbb{Z}/8\mathbb{Z}$. Тогда образами многочленов с коэффициентами из $\mathbb{K}$ и нулевым свободным членом в R являются самоподобные и содержащие 0 подмножества, и только они.*

Пока остаётся нерешённым вопрос о характеризации образов многочленов для матриц размера 2×2 над кольцами Галуа с радикалом, степень нильпотентности которого больше двух и для матриц большего размера. Однако ряд промежуточных результатов, полученных в данной работе, позволяют сформулировать алгоритм, способный проверить справедливость характеризации Чуанга для матриц размера 2×2 над одним из колец $\mathbb{Z}/p^n\mathbb{Z}$, где p — простое число. Этот алгоритм приведён в последнем параграфе данной работы. К сожалению, автору не удалось реализовать его достаточно

эффективно для того, чтобы на доступной вычислительной технике получить окончательный ответ для одного из колец, для которых этот ответ ещё не получен теоретически.

Автор выражает глубокую благодарность своему научному руководителю доктору физико-математических наук профессору А. В. Михалёву за постановку задач, постоянную поддержку и внимание к работе. Автор также признателен кандидату физико-математических наук доценту В. Т. Маркову и В. В. Острику за ряд ценных замечаний и полезные обсуждения.

Публикации автора по теме диссертации

[1] Кулямин В. В. Об образах многочленов в конечных кольцах матриц. Фунд. и прикл. математика 1997, т. 3, вып. 2, с. 469–485.

[2] Кулямин В. В. Об образах многочленов в кольце $M_2(\mathbb{Z}/8\mathbb{Z})$. Фунд. и прикл. математика 2000, т. 6, вып. 1, с. 275–280.

[3] Кулямин В. В. Образы градуированных многочленов в кольцах матриц над конечными групповыми алгебрами. УМН 2000, т. 55, вып. 2, с. 141–145.

[4] Кулямин В. В. Образы многочленов в кольцах матриц над кольцами Галуа. Международный алгебраический семинар, Москва, 1999, с. 36–37.

Глава 1.

Общие свойства образов многочленов

1.1. Определение образов многочленов в алгебрах

В этом разделе мы приведём определения основных понятий, а также ряд соглашений, которыми будем пользоваться всюду в дальнейшем. Всякая упоминаемая далее алгебра считается ассоциативной алгеброй над коммутативным кольцом с единицей, если не упомянуто обратное.

Некоммутативным многочленом или просто многочленом над коммутативным кольцом $\mathbb{K}$ будем называть элемент свободной ассоциативной алгебры с единицей над $\mathbb{K}$ со счётным множеством порождающих $\mathcal{K} = \mathbb{K}\{X\}$, где $X = \{x_0, x_1, \dots\}$ (см., например, [23]). Далее обозначение $\mathcal{K}$ мы всегда будем использовать для этой алгебры. Подалгебру многочленов с нулевым свободным членом в $\mathcal{K}$ мы будем обозначать $\mathcal{K}_0$ или $\mathbb{K}_0\{X\}$.

Образом $Im\, f$ некоммутативного многочлена f с нулевым свободным членом, зависящего от n переменных, в алгебре R над кольцом $\mathbb{K}$ будем называть образ соответствующего

полиномиального отображения $f : \underbrace{R \times \ldots \times R}_{\text{n times}} \to R$, то есть множество $\{x : \exists a_1, \ldots, a_n \in R \quad x = f(a_1, \ldots, a_n)\}$. Аналогично определяется образ многочлена $f + k$, где $f \in \mathcal{K}_0$ и $k \in \mathbb{K}$, но только в том случае, когда R имеет единицу. Очевидно, что тогда он получается из образа f поэлементным прибавлением $k1$, поэтому при изучении свойств образов многочленов достаточно рассматривать только многочлены с нулевым свободным членом.

В общей ситуации легко сформулировать условие, необходимое, чтобы некоторое подмножество алгебры над коммутативным кольцом было образом многочлена из $\mathcal{K}_0$.

Лемма 1. *Пусть $A \subseteq R$ есть подмножество некоторой алгебры R над коммутативным кольцом $\mathbb{K}$, являющееся образом многочлена $f(x_1, \ldots, x_n) \in \mathcal{K}_0$ с коэффициентами из кольца $\mathbb{K}$ и нулевым свободным членом, тогда это подмножество обладает следующим свойством:*

$$\forall \varphi \in End_{\mathbb{K}} R \quad \varphi(A) \subseteq A \tag{1.1}$$

Здесь через $End_{\mathbb{K}} R$ обозначено множество эндоморфизмов R как $\mathbb{K}$-алгебры.

Доказательство: Из определения эндоморфизма алгебры над кольцом непосредственно следует, что

$$\varphi(f(a_1, \ldots, a_n)) = f(\varphi(a_1), \ldots, \varphi(a_n)), \quad \forall a_1, \ldots, a_n \in R,$$

соответственно, если $a = f(a_1, \ldots, a_n)$, то и $\varphi(a) \in Im\, f$.□

Подмножества алгебры R, удовлетворяющие указанному условию будем называть *устойчивыми относительно эндоморфизмов.* Сразу отметим, что для образов многочленов с ненулевым свободным членом соответствующее условие тоже выполнено, если считать, что $End_{\mathbb{K}} R$ обозначает множество эндоморфизмов R как $\mathbb{K}$-алгебры с единицей.

1.2. Образы многочленов в разложимых в прямую сумму алгебрах

Рассмотрение свойств образов многочленов в алгебрах, являющихся прямыми суммами, даёт дополнительное условие, необходимое, чтобы подмножество алгебры было образом многочлена.

Лемма 2. *Пусть в алгебре R над коммутативным кольцом $\mathbb{K}$ есть два центральных идемпотента e_1 и e_2, произведение которых равно 0 (см. [24]). Пусть также множество $A \subseteq R$ — образ многочлена $f \in \mathcal{K}_0$. Тогда $e_1A + e_2A \subseteq A$.*

Доказательство: Пусть $a, b \in A$, причём a является значением f на элементах $a_1, \ldots, a_n$ и $b = f(b_1, \ldots, b_n)$. Тогда

$$f(e_1a_1, \ldots, e_1a_n) = \sum_{m,i_1,\ldots,i_m} f_{i_1,\ldots,i_m}(e_1a_{i_1})^{l_1} \ldots (e_1a_{i_m})^{l_m} =$$

$$= \sum_{m,i_1,\ldots,i_m} f_{i_1,\ldots,i_m} e_1^{l_1} a_{i_1}^{l_1} \ldots e_1^{l_m} a_{i_m}^{l_m} = \sum_{m,i_1,\ldots,i_m} e_1 f_{i_1,\ldots,i_m} a_{i_1}^{l_1} \ldots a_{i_m}^{l_m} =$$

$$= e_1 f(a_1, \ldots, a_n) = e_1 a.$$

Аналогично, $f(e_2b_1, \ldots, e_2b_n) = e_2b$. Рассмотрим теперь следующее выражение: $f(e_1a_1 + e_2b_1, \ldots, e_1a_n + e_2b_n)$.

$$f(e_1a_1 + e_2b_1, \ldots, e_1a_n + e_2b_n) =$$

$$= \sum_{m,i_1,\ldots,i_m} f_{i_1,\ldots,i_m}(e_1a_{i_1} + e_2b_{i_2})^{l_1} \ldots (e_1a_{i_m} + e_2b_{i_m})^{l_m} =$$

$$= \sum_{m,i_1,\ldots,i_m} f_{i_1,\ldots,i_m}(e_1a_{i_1}^{l_1} + e_2b_{i_1}^{l_1}) \ldots (e_1a_{i_m}^{l_m} + e_2b_{i_m}^{l_m}) =$$

$$= \sum_{m,i_1,\ldots,i_m} f_{i_1,\ldots,i_m}(e_1a_{i_1}^{l_1} \ldots e_1a_{i_m}^{l_m} + e_2b_{i_1}^{l_1} \ldots e_2b_{i_m}^{l_m}) =$$

$$= \sum_{m,i_1,\ldots,i_m} e_1 f_{i_1,\ldots,i_m} a_{i_1}^{l_1} \ldots a_{i_m}^{l_m} + \sum_{m,i_1,\ldots,i_m} e_2 f_{i_1,\ldots,i_m} b_{i_1}^{l_1} \ldots b_{i_m}^{l_m} =$$

$$= e_1 f(a_1, \ldots, a_n) + e_2 f(b_1, \ldots, b_n) = e_1 a + e_2 b.$$

Таким образом, для всяких $a, b \in A$ мы получили $e_1 a + e_2 b \in A$, что и требовалось.$\square$

Выделим полученное условие.

$$\forall e_1, e_2 \in Z(R)\ e_1^2 = e_1, e_2^2 = e_2, e_1 e_2 = 0 \Rightarrow e_1 A + e_2 A \subseteq A \tag{1.2}$$

Дальнейшее наше исследование в основном посвящено определению классов алгебр, в которых указанные необходимые условия (1.1) и (1.2) будут и достаточными. Упомянутый во Введении результат Чуанга означает, что в полных матричных алгебрах над конечными полями достаточно уже выполнения одного условия (1.1) (условие (1.2) в этом случае вырождено, поскольку в полных матричных алгебрах нет ортогональных центральных идемпотентов). Далее мы приведём ряд примеров алгебр, в которых указанных условий недостаточно.

Докажем одно вспомогательное утверждение.

Замечание 3. *Пусть R есть алгебра над коммутативным кольцом $\mathbb{K}$, раскладывающимся в прямую сумму, $\mathbb{K} = \mathbb{K}_1 \oplus \cdots \oplus \mathbb{K}_n$. Пусть также $e_1, \ldots, e_n \in \mathbb{K}$ — соответствующие центральные ортогональные идемпотенты, т.е. $\forall i \in [1, n]\quad \mathbb{K}_i \cong e_i \mathbb{K}$. Тогда $R \cong e_1 R \oplus \cdots \oplus e_n R$ и $e_i R$, $i \in [1, n]$ является алгеброй над $\mathbb{K}_i$ соответственно, причём $End_{\mathbb{K}} R \cong End_{\mathbb{K}_1} e_1 R \oplus \cdots \oplus End_{\mathbb{K}_n} e_n R$ (в категории полугрупп).*

Доказательство: Легко проверить, что $e_i R$ — подалгебра ${}_{\mathbb{K}}R$ для всякого $i \in [1, n]$. Для всякого $r \in R$

$$r = 1r = (e_1 + \cdots + e_n)r = e_1 r + \cdots + e_n r.$$

Отсюда $R = e_1R + \cdots + e_nR$. Кроме того, при $i \neq j$ имеем

$$r \in e_iR \cap e_jR \Rightarrow r = e_ir = e_jr \Rightarrow r = e_i^2r = e_ie_jr = 0r = 0.$$

Таким образом, R является прямой суммой алгебр ${}_{\mathbb{K}}e_iR$.

Структура $\mathbb{K}_i$ -алгебры на e_iR задаётся при помощи вложения $\mathbb{K}_i$ в $\mathbb{K}$ в качестве $e_i\mathbb{K}$. Рассмотрим $\varphi \in End_{\mathbb{K}}R$. Определим φ_i, $i \in [1,n]$ как сужение φ на e_iR. Тогда $\varphi_i \in End_{\mathbb{K}_i}e_iR$, поскольку $\varphi_i(e_ia) = \varphi(e_ia) = e_i\varphi(a) \in e_iR$. Свойства эндоморфизма для φ_i следуют из того, что φ является эндоморфизмом. Кроме того, $\forall a \in R \quad \varphi(a) = \varphi_1(e_1a) + \cdots + \varphi_n(e_na)$. Наоборот, по данным эндоморфизмам $\varphi_i \in End_{\mathbb{K}_i}e_iR$, $i \in [1,n]$ определяя $\varphi(a) = \varphi_1(e_1a) + \cdots + \varphi_n(e_na)$, получаем $\varphi \in End_{\mathbb{K}}R$, поскольку

$$\varphi(a+b) = \varphi_1(e_1a + e_1b) + \cdots + \varphi_n(e_na + e_nb) =$$

$$= \varphi_1(e_1a) + \varphi_1(e_1b) + \cdots + \varphi_n(e_na) + \varphi_n(e_nb) = \varphi(a) + \varphi(b),$$

а также

$$\varphi(ab) = \varphi_1(e_1ab) + \cdots + \varphi_n(e_nab) = \varphi_1(e_1ae_1b) + \cdots +$$

$$+\varphi_n(e_nae_nb) = \varphi_1(e_1a)\varphi_1(e_1b) + \cdots + \varphi_n(e_na)\varphi_n(e_nb) =$$

$$= \varphi_1(e_1a)\varphi_1(e_1b) + \cdots + \varphi_n(e_na)\varphi_n(e_nb) + \varphi_1(e_1a)\varphi_2(e_2b) + \cdots +$$

$$+\varphi_1(e_1a)\varphi_n(e_nb) + \cdots + \varphi_n(e_na)\varphi_1(e_1b) + \cdots +$$

$$+\varphi_n(e_na)\varphi_{n-1}(e_{n-1}b) = (\varphi_1(e_1a) + \cdots + \varphi_n(e_na)) \times$$

$$\times(\varphi_1(e_1b) + \cdots + \varphi_n(e_nb)) = \varphi(a)\varphi(b),$$

здесь использован тот факт, что при неравных индексах i и j из $[1,n]$ выполнено $\varphi_i(e_ia)\varphi_j(e_jb) = e_i\varphi_i(e_ia)e_j\varphi_j(e_jb) = e_ie_j\varphi_i(e_ia)\varphi_j(e_jb) = 0$.

Для всякого $k \in \mathbb{K}$

$$\varphi(ka) = \varphi_1(e_1ka) + \cdots + \varphi_n(e_nka) = e_1k\varphi_1(e_1a) + \cdots +$$

$$+e_nk\varphi_n(e_na) = (e_1k + \cdots + e_nk)\varphi_1(e_1a) + \cdots + (e_1k + \cdots +$$
$$+e_nk)\varphi_n(e_na) = k(\varphi_1(e_1a) + \cdots + \varphi_n(e_na)) = k\varphi(a),$$

здесь опять учитываем, что при $i \neq j$ верно $e_ik\varphi_j(e_ja) = e_ike_j\varphi_j(e_ja) = 0$.

Проверка того, что получившееся соответствие $\varphi \leftrightarrow (\varphi_1, \ldots, \varphi_n)$ — изоморфизм полугрупп, тривиальна.□

Теперь с помощью ряда предложений мы постараемся свести наше исследование свойств образов многочленов к алгебрам над кольцами, неразложимыми в прямые суммы.

Теорема 4. *Пусть R есть алгебра над конечной прямой суммой колец $\mathbb{K} = \mathbb{K}_1 \oplus \cdots \oplus \mathbb{K}_n$; пусть также в подалгебрах $R_i = \mathbb{K}_iR$ при рассмотрении их как алгебр над соответствующими кольцами $\mathbb{K}_i$ всякое подмножество, обладающее свойствами (1.1) и (1.2) является образом многочлена из $(\mathbb{K}_i)_0\{X\}$, т.е. с коэффициентами из $\mathbb{K}_i$ и нулевым свободным членом. Тогда и в R образы многочленов с коэффициентами из $\mathbb{K}$ и нулевым свободным членом — это множества, удовлетворяющие Условиям (1.1) и (1.2), и только они.*

Доказательство: Достаточно для произвольного подмножества A алгебры R, удовлетворяющего Условиям (1.1) и (1.2), указать многочлен, образом которого оно является.

Пусть e_i, $i \in [1, n]$ — набор идемпотентов в $\mathbb{K}$, соответствующий разложению $\mathbb{K} = \mathbb{K}_1 \oplus \cdots \oplus \mathbb{K}_n$. Рассмотрим множества e_iA, являющиеся подмножествами R_i. Для всякого эндоморфизма $\varphi \in End_{\mathbb{K}_i}R_i$, в соответствии с замечанием 3 дополняя φ тождественными эндоморфизмами на остальных слагаемых, можно построить эндоморфизм $\varphi' \in End_{\mathbb{K}}R$, такой что $\forall a \in R \quad \varphi'(a) = \varphi(e_ia) + (1 - e_i)a$. Значит, для всякого $a \in e_iA$ верно $\varphi(a) = \varphi(e_ia) = e_i\varphi(e_ia) = e_i\varphi'(a) \in e_iA$, следовательно $\forall \varphi \in End_{\mathbb{K}_i}R_i \quad \varphi(e_iA) \subseteq e_iA$. Это означает,

что при любом $i \in [1,n]$ множество e_iA устойчиво относительно эндоморфизмов алгебры ${}_{\mathbb{K}_i}R_i$.

Пусть h_1 и h_2 — центральные ортогональные идемпотенты в R_i. Тогда $h_1e_iA + h_2e_iA = e_i(h_1A + h_2A) \subseteq e_iA$. Таким образом, множество e_iA по условию должно быть образом многочлена $f_i(x_1,\ldots,x_{m_i})$ с коэффициентами из $\mathbb{K}_i$ и нулевым свободным членом в алгебре R_i. Посмотрим, каков образ этого многочлена, когда его переменные пробегают R.

$$f_i(a_1,\ldots,a_{m_i}) = \sum_{m,i_1,\ldots,i_m} f^{(i)}_{i_1,\ldots,i_m} a_{i_1}^{l_1}\ldots a_{i_m}^{l_m} =$$

$$= \sum_{m,i_1,\ldots,i_m} f^{(i)}_{i_1,\ldots,i_m} (e_ia_{i_1} + (1-e_i)a_{i_1})^{l_1}\ldots(e_ia_{i_m} + (1-e_i)a_{i_m})^{l_m} =$$

$$= \sum_{m,i_1,\ldots,i_m} f^{(i)}_{i_1,\ldots,i_m} (e_ia_{i_1}^{l_1} + (1-e_i)a_{i_1}^{l_1})\ldots(e_ia_{i_m}^{l_m} + (1-e_i)a_{i_m}^{l_m}) =$$

$$= \sum_{m,i_1,\ldots,i_m} f^{(i)}_{i_1,\ldots,i_m} e_ia_{i_1}^{l_1}\ldots a_{i_m}^{l_m} + \sum_{m,i_1,\ldots,i_m} f^{(i)}_{i_1,\ldots,i_m}(1-e_i)a_{i_1}^{l_1}\ldots a_{i_m}^{l_m}.$$

Вспомним, что f_i имеет коэффициенты в $e_i\mathbb{K}$, следовательно $f^{(i)}_{i_1,\ldots,i_m}(1-e_i) = 0$. Таким образом, второе слагаемое в этой сумме равно 0. Отсюда

$$f_i(a_1,\ldots,a_{m_i}) = \sum_{m,i_1,\ldots,i_m} f^{(i)}_{i_1,\ldots,i_m} e_ia_{i_1}^{l_1}\ldots a_{i_m}^{l_m} =$$

$$= \sum_{m,i_1,\ldots,i_m} f^{(i)}_{i_1,\ldots,i_m} (e_ia_{i_1})^{l_1}\ldots(e_ia_{i_m})^{l_m} = f_i(e_ia_1,\ldots,e_ia_{m_i}).$$

Полученное соотношение означает, что в алгебре R образ многочлена f_i по-прежнему равен e_iA.

Рассмотрим многочлен

$$F(x_1,\ldots,x_{m_1},x_{m_1+1},\ldots,x_{m_1+\cdots+m_n}) = f_1(x_1,\ldots,x_{m_1}) +$$

$$+f_2(x_{m_1+1},\ldots,x_{m_1+m_2}) + \cdots + f_n(x_{m_1+\cdots+m_{n-1}+1},\ldots,x_{m_1+\cdots+m_n}).$$

Очевидно, $F \in \mathcal{K}_0$. Из уже доказанного следует, что его образ совпадает с множеством $e_1A + \cdots + e_nA$. Заметим теперь, что $A = (e_1 + \cdots + e_n)A \subseteq e_1A + \cdots + e_nA \subseteq A$, следовательно, образ многочлена F равен A, что и требуется. $\square$

1.3. Несколько примеров

В этом разделе мы собрали несколько вспомогательных предложений, которые понадобятся в дальнейшем. Здесь же приведён ряд примеров алгебр, как таких, в которых все устойчивые относительно эндоморфизмов подмножества являются образами многочленов, так и таких, где это не так.

Для начала докажем следующую небольшую лемму.

Лемма 5. *Если G — конечная полугруппа, то существует $N \in \mathbb{N}$, такое что a^N является идемпотентом для всякого $a \in G$.*

Доказательство: (См. [16]) Для всякого $a \in G$ множество $\{a, a^2, \dots\}$ конечно, значит $a^{m+n} = a^m$ для каких-то $m, n \in \mathbb{N}$. Имеем

$$a^{mn+n} = a^{m(n-1)+m+n} = a^{m(n-1)}a^{m+n} = a^{m(n-1)}a^m = a^{mn}.$$

Отсюда

$$(a^{mn})^2 = a^{mn+mn} = a^{mn+n+(m-1)n} = a^{mn+(m-1)n} = \cdots = a^{mn},$$

то есть a^{mn} — идемпотент. Мы получили, таким образом, что для всякого $a \in G$ найдётся $n(a) \in \mathbb{N}$, такое, что $a^{n(a)}$ является идемпотентом. Беря в качестве N произведение $n(a)$ для всех $a \in G$, мы получаем искомое.$\square$

Лемма 6. *Пусть над кольцом $\mathbb{K}$ существует многочлен $E(z_1, \dots, z_t)$, принимающий в алгебре R только значения*

0 *и* 1, *и не равный на* R *константе. Если* $f(x_1, \ldots, x_k)$ *и* $g(y_1, \ldots, y_s)$ — *многочлены из* $\mathcal{K}_0$, *то образом многочлена*

$$h(x_1, \ldots, x_k, y_1, \ldots, y_s, z_1, \ldots, z_t) = E(z_1, \ldots, z_t) f(x_1, \ldots, x_k) +$$
$$+(1 - E(z_1, \ldots, z_t)) g(y_1, \ldots, y_s)$$

является объединение их образов. Кроме того, $h \in \mathcal{K}_0$.

Доказательство: Очевидно, что многочлен h принадлежит $\mathcal{K}_0$. Рассмотрим его значение на элементах $a_1, \ldots, a_k$, $b_1, \ldots, b_s, c_1, \ldots, c_t \in R$. Если $E(c_1, \ldots, c_t) = 0$, то значение h совпадает с $g(b_1, \ldots, b_s)$, если же $E(c_1, \ldots, c_t) = 1$, то значение h равно $f(a_1, \ldots, a_k)$. Отсюда получаем $Im\, h \subseteq Im\, f \cup Im\, g$.

Теперь докажем обратное включение. Поскольку E не равен на R константе, найдутся $c_1, \ldots, c_t, d_1, \ldots, d_t \in R$, такие, что $E(c_1, \ldots, c_t) = 0$ и $E(d_1, \ldots, d_t) = 1$. Поэтому

$$f(a_1, \ldots, a_k) = h(a_1, \ldots, a_k, b_1, \ldots, b_s, d_1, \ldots, d_t)$$

и

$$g(b_1, \ldots, b_s) = h(a_1, \ldots, a_k, b_1, \ldots, b_s, c_1, \ldots, c_t),$$

при любых $a_1, \ldots, a_k, b_1, \ldots, b_s \in R$. Таким образом, получаем $Im\, f \subseteq Im\, h$ и $Im\, g \subseteq Im\, h$.□

Многочлены, подобные упоминаемому в формулировке леммы $E(z_1, \ldots, z_t)$, играют важную роль при исследовании различных свойств PI-алгебр, поэтому приведём здесь соответствующее определение и теорему о существовании.

Многочлен $f(x_1, \ldots, x_k)$ от некоммутирующих переменных с коэффициентами из кольца $\mathbb{K}$ называется *центральным для* $\mathbb{K}$*-алгебры* R, если при подстановке в него элементов R он принимает значения в центре R, причем не все они равны 0.

Следующее утверждение показывает, что центральные многочлены встречаются достаточно часто.

Теорема 7. *Если* $\mathbb{K}$ *— коммутативное кольцо с единицей, то при любом* $m \in \mathbb{N}$ *для алгебры матриц* $M_m(\mathbb{K})$ *существует полилинейный центральный многочлен, среди значений которого есть единица* $\mathbb{K}$.

Доказательство см. в [25, Глава 6, § 6.1, Теорема 6.1.20].

Легко заметить, что в конечной матричной алгебре над кольцом, не имеющим нетривиальных идемпотентов Лемма 5 вместе с только что приведённой теоремой дают существование многочлена, имеющего в точности те же свойства, что и многочлен $E(z_1, \ldots, z_t)$ из Леммы 6.

Пример 1. Пусть $\mathbb{K}$ — конечное коммутативное кольцо с единицей, рассматриваемое как алгебра над собой, без нетривиальных, то есть, не равных 0 или 1 идемпотентов. Поскольку эндоморфизм ${}_{\mathbb{K}}\mathbb{K}$ однозначно задаётся образом единицы, являющимся идемпотентом, в данном случае нулём или единицей, единственными эндоморфизмами являются нулевой и тождественный. Соответственно, любое множество, содержащее 0, устойчиво относительно эндоморфизмов. Покажем, что все такие множества будут образами многочленов из $\mathcal{K}_0$.

По Лемме 5, существует такое $N \in \mathbb{N}$, что a^N — идемпотент, для всякого $a \in \mathbb{K}$, стало быть, многочлен $E(x) = x^N$ из $\mathcal{K}_0$ имеет образ $\{0, 1\}$. Всякое множество $\{0, a_1, \ldots, a_n\} \subseteq \mathbb{K}$ представим в виде $\{0, a_1\} \cup \cdots \cup \{0, a_n\}$. Теперь достаточно взять многочлены $a_i x^N$ и применить к ним Лемму 6.

Пример 2. Пусть $K \subseteq L$ — конечные поля. Рассмотрим L как K-алгебру. Эндоморфизмы ${}_K L$ — это автоморфизмы L, оставляющие на месте K, и нулевой эндоморфизм. Пусть множество $A \subseteq L$ устойчиво относительно эндоморфизмов ${}_K L$, и $a \in A$. Тогда все корни минимального многочлена a над K тоже принадлежат A (см., например, [26, Глава VII, § 5]). Следовательно, $A = \{0, a_1, \ldots, a_n\}$, где $a_1, \ldots, a_n$ — все

принадлежащие L корни некоторого многочлена g с коэффициентами в K.

Для всякого $a \in L \backslash A \quad g(a) \neq 0$. Соответственно, по Лемме 5, найдётся такое $N \in \mathbb{N}$, что $g^N(a) = 1$ для всякого $a \in L \backslash A$. Теперь рассмотрим многочлен $f(x) = x(1 - g^N(x)) \in K_0[x]$. Легко видеть, что при $a \in A$ выполнено $f(a) = a$, иначе $f(a) = 0$. Таким образом, $Im\, f$ совпадает с A.

Следующий пример уже упоминался в связи с историей вопроса о характеризации образов многочленов.

Назовём *самоподобным* множество матриц $A \subseteq M_m(\mathbb{K})$ над коммутативным кольцом, если оно обладает следующим свойством: для всякой обратимой матрицы $\alpha \in M_m(\mathbb{K})$ выполнено $\alpha A \alpha^{-1}$.

Пример 3. Пусть $\mathbb{K}$ — конечное поле, $R = M_m(\mathbb{K})$ — алгебра матриц размера $m \times m$ над ним. В работе [16] показано, что множество $A \subseteq R$ является образом многочлена из $\mathcal{K}_0$ тогда и только тогда, когда $0 \in A$ и A самоподобно. Поскольку кольцо эндоморфизмов матриц над полем состоит только из нулевого эндоморфизма и собственных автоморфизмов, указанные условия означают в точности, что множество A устойчиво относительно эндоморфизмов ${}_{\mathbb{K}}R$.

Далее нам пригодится следующая Лемма, доказательство которой легко извлечь из доказательства утверждения Примера 3 в [16].

Лемма 8. *Для всякого самоподобного множества $A \subseteq R = M_m(\mathbb{K})$ матриц над конечным полем существует многочлен от некоммутирующих переменных $\chi_A(x, x_1, \ldots, x_n)$, принимающий только значения 0 и 1, и такой, что*

$$a \notin A \Rightarrow \forall a_1, \ldots, a_n \in R \quad \chi_A(a, a_1, \ldots, a_n) = 0;$$

$$a \in A \Rightarrow \exists a_1, \ldots, a_n \in R \quad \chi_A(a, a_1, \ldots, a_n) = 1.$$

Многочлен, обладающий описанными свойствами, будем называть *индикатором* множества A. Про множество A в таком случае мы говорим, что оно обладает индикатором. Легко показать, что всякое обладающее индикатором подмножество полной матричной алгебры самоподобно.

В той же работе Чуанга [16] приведён следующий пример, показывающий, что в случае бесконечности основного поля устойчивости множества матриц относительно эндоморфизмов вообще говоря не достаточно для того, чтобы удовлетворяющее это множество являлось образом многочлена.

Пример 4. Пусть $\mathbb{K}$ обозначает бесконечное поле, а $A = \{a \in M_m(\mathbb{K}) : a^2 = 0\}$ есть множество матриц размера $m \times m$ над ним. Очевидно, что A содержит 0 и самоподобно. Пусть оно является образом многочлена $f \in \mathcal{K}_0$, тогда f^2 — тождество алгебры $M_m(\mathbb{K})$. По известной теореме Амицура (см., например, [27, Глава 20, § 20.5]), если $\theta_m \subseteq \mathcal{K}$ — множество тождеств $M_m(\mathbb{K})$, то факторалгебра $\mathcal{K}/\theta_m$ не содержит делителей нуля в случае бесконечного поля $\mathbb{K}$. Так как $f^2 \in \theta_m$, то и $f \in \theta_m$, но образ многочлена f содержит ненулевые элементы, если $m > 1$. Таким образом, множество A не может быть образом многочлена.

Можно привести и более простой пример, иллюстрирующий недостаточность указанного условия для бесконечных алгебр.

Пример 5. Рассмотрим бесконечное поле $\mathbb{K}$ как алгебру над собой. Поскольку эндоморфизмы ${}_{\mathbb{K}}\mathbb{K}$ исчерпываются нулевым и тождественным, любое подмножество $\mathbb{K}$, содержащее 0, замкнуто относительно эндоморфизмов.

Однако ни одно конечное множество $A = \{0, a_1, \ldots, a_k\} \subseteq$

$\mathbb{K}$, содержащее какие-нибудь ненулевые элементы, не может быть образом многочлена, так как, если $A = Im\, f$, то многочлен $f(f - a_1) \dots (f - a_k)$, будучи ненулевым, поскольку f не нулевой, должен однако быть тождественно равным 0 на $\mathbb{K}$.

Глава 2.

Образы многочленов в градуированных алгебрах

2.1. Алгебра градуированных многочленов и образы её элементов

Посмотрим, как введённые нами понятия и полученные результаты преобразуются в случае градуированных алгебр.

Прежде всего, надо понять, как «правильно» определить образ многочлена в градуированной по полугруппе G алгебре

$$R = \sum_{g \in G} R_g.$$

Наиболее логичным путём обобщения понятий, связанных с многочленами, на градуированные алгебры нам представляется явное выделение градуировки как элемента рассматриваемой структуры. Этот подхода придерживаются, например, работы [28, 29]. Поэтому для фиксированной полугруппы G рассмотрим *алгебру G-градуированных многочленов* над основным кольцом $\mathbb{K}$ — свободную ассоциативную алгебру с единицей $\mathbb{K}\{X\}$, порождённую G-градуированным множеством X, то есть множеством, представленным в виде

дизъюнктного объединения

$$X = \bigsqcup_{g \in G} X_g$$

компонент X_g, каждая из которых является счётным множеством $X_g = \{x_{g0}, x_{g1}, \dots\}$. Далее в этом разделе будем обозначать эту алгебру как $\mathcal{K}^G$, а подалгебру многочленов с нулевым свободным членом в ней как $\mathcal{K}_0^G$.

Определим каноническую градуировку по полугруппе G на алгебре $\mathcal{K}_0^G$. Если основное кольцо $\mathbb{K}$ не является G-градуированным, моном $kx_{i_1} \dots x_{i_t}$ будем называть однородным степени $g \in G$, если $x_{i_j} \in X_{g_j}$ для всякого $j \in [1, t]$ и $g = g_1 \dots g_t$ в G. Многочлен будем считать g-однородным, если он является суммой g-однородных мономов.

В том случае, когда $\mathbb{K}$ является G-градуированным коммутативным кольцом, можно следующим образом определить каноническую G-градуировку на $\mathcal{K}^G$. Моном $kx_{i_1} \dots x_{i_t}$ будем считать однородным степени $g \in G$, если $k \in \mathbb{K}_{g_0}$ — однородный степени g_0 элемент $\mathbb{K}$, для всякого $j \in [1, t]$ x_{i_j} является элементом X_{g_j} и $g = g_0 g_1 \dots g_t$ в полугруппе G. Многочлен, как и в предыдущем случае, будем считать однородным степени g, если он является суммой g-однородных мономов.

Легко проверить, что определённые таким образом множества однородных элементов действительно задают G-градуировку в обоих случаях. При этом во втором случае $\mathcal{K}_0^G$ является G-градуированной подалгеброй $\mathcal{K}^G$.

Образ многочлена f в обычной алгебре R является множеством образов f как элемента свободной ассоциативной алгебры при всевозможных гомоморфизмах этой алгебры в R. Аналогично определим образ G-градуированного многочлена в G-градуированной алгебре.

Обозначим сперва через $Hom^G_{\mathbb{K}}(R,S)$ множество гомоморфизмов G-градуированной $\mathbb{K}$-алгебры R в G-градуированную $\mathbb{K}$-алгебру S, сохраняющих градуировку, то есть, удовлетворяющих условию

$$\forall g \in G \quad \varphi(R_g) \subseteq S_g.$$

Будем называть их также *G-градуированными гомоморфизмами.* Соответствующим образом определяются G-градуированные эндоморфизмы, множество которых будем обозначать $End^G_{\mathbb{K}}(R)$. *Образом* градуированного многочлена f из $\mathcal{K}^G_0$ в G-градуированной алгебре R назовём следующее множество

$$Im\, f = \{a \in R : \exists \varphi \in Hom^G_{\mathbb{K}}(\mathcal{K}^G_0, R) \quad \varphi(f) = a\}.$$

В этом определении мы считаем $\mathcal{K}^G_0$ градуированной каноническим образом. Это означает, что при взятии образа градуированного многочлена мы подставляем в многочлен вместо переменных $x_{gi} \in X_g$ всевозможные однородные элементы степени g из R.

Далее для $a \in R$ будем обозначать через a_g его однородную компоненту степени g, а для $A \subseteq R$ через A_g — его проекцию на R_g, то есть, множество g-однородных компонент элементов A.

Теперь логично рассмотреть обобщение условия устойчивости относительно эндоморфизмов на градуированный случай. Множество $A \subseteq R$ элементов G-градуированной алгебры R будем называть *устойчивым относительно эндоморфизмов,* если

$$\forall \varphi \in End^G_{\mathbb{K}}(R) \quad \varphi(A) \subseteq A.$$

Сформулируем утверждение, являющееся аналогом Леммы 1 для случая градуированных алгебр.

Лемма 9. *Пусть R есть G-градуированная алгебра над кольцом $\mathbb{K}$ (всё равно, градуированным или нет), $f \in \mathcal{K}_0^G$ — G-градуированный многочлен с нулевым свободным членом. Тогда его образ $Im\, f$ в алгебре R устойчив относительно G-градуированных эндоморфизмов R.*

Доказательство: В соответствии с данными выше определениями, $a \in Im\, f$ эквивалентно тому, что найдётся $\varphi \in Hom_{\mathbb{K}}^G(\mathcal{K}_0^G, R)$, такой, что $\varphi(f) = a$. Рассмотрим $a \in Im\, f$ и $\xi \in End_{\mathbb{K}}^G(R)$. Пусть $b = \xi(a)$. Поскольку $\xi\varphi$ тоже является элементом $Hom_{\mathbb{K}}^G(\mathcal{K}_0^G, R)$ и $\xi\varphi(f) = \xi(a) = b$, получаем, что $b \in Im\, f$, что нам и требовалось.□

2.2. Характеризация образов градуированных многочленов

Следующее предложение показывает, что в некоторых случаях удаётся из характеризации образов многочленов в однородных частях градуированной алгебры получить характеризацию образов градуированных многочленов в ней самой.

Предложение 10. *Пусть G — конечная полугруппа, состоящая только из идемпотентов, R — конечная G-градуированная алгебра над коммутативным кольцом*

$$R = \sum_{g \in G} R_g,$$

обладающая градуированным многочленом $E \in \mathcal{K}_0^G$, принимающим значения 0 и 1, и только их. Пусть также каждое однородное слагаемое R_g (заметим, что, поскольку g идемпотент, R_g само является алгеброй) обладает тем свойством, что всякое его устойчивое относительно эндоморфизмов подмножество является образом многочлена

из $\mathcal{K}_0$. Тогда всякое устойчивое относительно градуированных эндоморфизмов подмножество R является образом многочлена из $\mathcal{K}_0^G$.

Доказательство: Сперва покажем, что в рассматриваемом случае градуированные эндоморфизмы R однозначно соответствуют наборам эндоморфизмов однородных слагаемых $\{\varphi_g\}_{g\in G}$, более того,

$$End_{\mathbb{K}}^G(R) \cong \bigoplus_{g\in G} End_{\mathbb{K}}(R_g).$$

Очевидно, что каждое сужение градуированного эндоморфизма R на её однородную компоненту является эндоморфизмом последней. Наоборот, по набору $\{\varphi_g\}_{g\in G}$ построим градуированный эндоморфизм φ, определив его на каждой компоненте как φ_g, а на остальных элементах по линейности. Ясно, что так мы получили взаимно однозначное соответствие между эндоморфизмами R и наборами эндоморфизмов её однородных слагаемых, которое, как легко проверить, является изоморфизмом полугрупп.

Пусть теперь $M \subseteq R$ есть минимальное, непустое и не равное $\{0\}$, устойчивое относительно градуированных эндоморфизмов подмножество градуированной алгебры R. Тогда для всякого $g \in G$ проекция этого множества на g-однородную компоненту $M_g = \{x \in R_g : \exists m \in M \quad m = \sum_{h\in G} m_h$ и $m_g = x\} \subseteq R_g$ устойчива относительно эндоморфизмов в R_g, так как любой из них можно продолжить до градуированного эндоморфизма R. Кроме того, M_g является минимальным (может быть, равным $\{0\}$) устойчивым множеством.

Иначе, пусть в нём имеются два элемента, не переводимых друг в друга ни одним эндоморфизмом R_g. Тогда и их классы сопряжённости A_{g1} и A_{g2} входят в M_g. Рассмотрим

подмножество R, состоящее из элементов, g-й компонентой которых является член A_{g1} или 0. Очевидно, из сказанного выше, что это множество устойчиво относительно градуированных эндоморфизмов, значит, и его пересечение с M, которое строго меньше M, поскольку в g-й проекции последнего есть ещё элементы из A_{g2}. Полученное противоречие с минимальностью M показывает, что M_g также минимально, или равно $\{0\}$.

Далее, среди множеств $\{M_g\}_{g\in G}$ только одно не равно $\{0\}$. Иначе, если $M_g \neq \{0\}$ и $M_h \neq \{0\}$, причём $g \neq h$, то рассматривая устойчивое относительно градуированных эндоморфизмов множество, состоящее из всех элементов R с нулевой h-й компонентой, опять получим, что его пересечение с M — устойчивое, не равное $\{0\}$, строго меньшее M множество.

Теперь, пусть $M_g \neq \{0\}$ является единственной ненулевой проекцией M. Так как M_g устойчиво относительно эндоморфизмов в R_g, можно выбрать многочлен $f(x_1, \ldots, x_n)$ из $\mathcal{K}_0$, образ которого в R_g совпадает с M_g. Взяв многочлен f' с теми же коэффициентами, но от переменных $x_{g1}, \ldots, x_{gn}$ из g-й компоненты множества X, получим, что $f' \in \mathcal{K}_0^G$ и образ f' в R совпадает с M.

Поскольку алгебра R конечна, каждое устойчивое относительно градуированных эндоморфизмов подмножество может быть получено объединением конечного числа минимальных таких подмножеств. Поэтому, в соответствии с Леммой 6, можно построить многочлен из $\mathcal{K}_0^G$, образом которого является это подмножество. Предложение доказано.□

Приведём ещё один результат, расширяющий характеризацию Чуанга на полные матричные алгебры над конечными полугрупповыми алгебрами с естественной градуировкой.

До конца этого раздела R будет обозначать полную

матричную алгебру над конечной коммутативной полугрупповой алгеброй $\mathbb{K} = \mathbb{F}(G)$ над конечным полем $\mathbb{F}$. На $\mathbb{K}$, а следовательно, и на R определена естественная G-градуировка — $\mathbb{K}_g = \mathbb{F}g$ и $R_g = M_m(\mathbb{K}_g)$.

Множество матриц $A \in R$, удовлетворяющее условию $\alpha A \alpha^{-1} \subseteq A$ для всякой обратимой однородной матрицы $\alpha \in R$, будем называть *самоподобным.*

Под *классом подобия* в R будем понимать минимальное непустое самоподобное множество. Назовём класс подобия матриц $C \subseteq R$ *разложимым,* если он является суммой своих проекций на однородные компоненты R, то есть, если $G = \{g_1, \ldots, g_k\}$, и $a_1, \ldots, a_k \in C$, то $\sum_{g \in G} a_{ig_i} \in C$. Очевидно, что класс подобия, состоящий из однородных матриц одной степени однородности, является разложимым — все его проекции, кроме одной, равны $\{0\}$.

Лемма 11. *Пусть G есть конечная коммутативная полугруппа с единицей e. Для всякого разложимого класса подобия матриц $C \subseteq R = M_m(\mathbb{K})$ над конечной полугрупповой алгеброй $\mathbb{K} = \mathbb{F}(G)$ над полем множество $C \cup \{0\}$ является образом градуированного многочлена из $\mathcal{K}_0^G$ в R.*

Доказательство: Пусть $G = \{g_1, \ldots, g_k\}$. Рассмотрим проекцию C на однородную компоненту R степени g_i. Эту проекцию C_{g_i} можно представить в виде $C_{(g_i)}g_i$, где $C_{(g_i)}$ — некоторое множество матриц над $\mathbb{F}$. Пусть $a \in C_{(g_i)}$, тогда a является g_i-однородной частью некоторого элемента $a' \in C$. Для всякой обратимой матрицы $\alpha \in M_m(\mathbb{F})$ αe является обратимым однородным элементом R. Поскольку C самоподобно, $(\alpha e)a'(\alpha^{-1}e) \in C$. Следовательно, $\alpha a \alpha^{-1} \in C_{(g_i)}$. Таким образом, $C_{(g_i)}$ представляет собой самоподобное множество матриц над $\mathbb{F}$.

По Лемме 8, $C_{(g_i)}$ имеет индикатор $\chi_i(x_i, x_{i1}, \ldots, x_{im_i})$ в

кольце матриц над $\mathbb{F}$. Рассмотрим многочлен

$$h(y_1, \dots y_k, x_{11}, \dots, x_{km_k}) =$$

$$= (g_1 y_1 + \dots + g_k y_k) \prod_{i \le k} \chi_i(y_i, x_{i1}, \dots, x_{im_i}),$$

в котором степень однородности переменных $y_i, x_{i1}, \dots, x_{im_i}$ равна e. Ясно, что он лежит в $\mathcal{K}_0^G$. Очевидно также, что если значение y_i для какого-нибудь i не лежит в $C_{(g_i)}$, то h принимает значение 0, если же для всякого i значение y_i является элементом $C_{(g_i)}$, то значение h равно сумме произведений их значений на соответствующие элементы группы G, и, следовательно, в силу разложимости C, лежит в C. Беря в качестве $g_i y_i$ однородные компоненты произвольного элемента C, легко показать, что C лежит в образе многочлена h. Таким образом, $Im\, h = C \cup \{0\}$.□

Теперь легко получить следующий результат.

Теорема 12. *Пусть G — конечная коммутативная полугруппа с единицей, $R = M_m(\mathbb{K})$ — кольцо матриц размера $m \times m$ над конечной алгеброй $\mathbb{K} = \mathbb{F}(G)$ над полем с естественной градуировкой. Однородное множество $A \subseteq R$ является образом G-градуированного многочлена из $\mathcal{K}_0^G$ тогда и только тогда, когда $0 \in A$ и A самоподобно.*

Доказательство: Всякое однородное множество $A \subseteq R$ является объединением конечного числа однородных классов подобия, поскольку R конечно. Однородный класс подобия, как уже отмечалось, является разложимым, значит, есть многочлен из $\mathcal{K}_0^G$, образ которого равен объединению этого однородного класса подобия с $\{0\}$.

По Лемме 6, A также является образом многочлена из $\mathcal{K}_0^G$. Необходимый для применения этой леммы градуированный многочлен, имеющий образ $\{0, 1\}$ можно получить, взяв

обычный многочлен, обладающий этим свойством в соответствующей алгебре матриц над $\mathbb{F}$ (его существование обсуждалось в последнем параграфе предыдущей главы) и объявив все переменные, от которых он зависит, переменными степени однородности e.

То, что всякий однородный образ многочлена из $\mathcal{K}_0^G$ содержит 0 и самоподобен следует из его устойчивости относительно эндоморфизмов.$\square$

Глава 3.

Образы многочленов в матричных алгебрах над кольцами Галуа

3.1. Основные свойства колец Галуа

Нашей дальнейшей целью является обобщение утверждения Примера 3 на случай полных матричных алгебр над кольцами, не являющимися полями. В свете приведённых выше примеров наиболее подходят для первоначального изучения неразложимые в прямую сумму конечные кольца, как можно более близкие к полям по своим свойствам.

Далее везде через $\mathbb{K}$ мы будем обозначать *кольцо Галуа,* то есть, конечное коммутативное локальное кольцо главных идеалов, имеющее единицу, наибольший идеал которого порождён элементом $p \in \mathbb{K}$, отождествляемым с характеристикой поля вычетов $\mathbb{K}/J(\mathbb{K})$ (см. [19]). Чтобы не повторяться, введём ещё несколько обозначений: $M = M_m(\mathbb{K})$ — алгебра матриц над $\mathbb{K}$ размера $m \times m$; $\mathcal{K}$ и $\mathcal{K}_0$ сохраняют свой смысл алгебр всех многочленов от некоммутирующих переменных $X = \{x_0, x_1, x_2, \dots\}$ с коэффициентами из $\mathbb{K}$ и многочленов с нулевым свободным членом соответственно.

Мы будем использовать те же буквы с верхней чертой

для обозначения соответствующих объектов, относящихся к полю вычетов $\overline{\mathbb{K}} = \mathbb{K}/J(\mathbb{K})$. Например, $\overline{M} = M_m(\overline{\mathbb{K}})$, $\overline{\mathcal{K}} = \overline{\mathbb{K}}\{X\}$, если $a \in \mathbb{K}$, то $\overline{a} \in \overline{\mathbb{K}}$ — вычет a по модулю радикала $J(\mathbb{K})$; если $A \subseteq M$, то $\overline{A} \subseteq \overline{M}$ — соответствующее множество матриц над $\overline{\mathbb{K}}$, и т.д.

Из свойств колец Галуа нам понадобятся следующие:

1) $J(\mathbb{K}) = p\mathbb{K}$ и $p^n = 0$ при некотором $n \in \mathbb{N}$. $\mathbb{K}$ изоморфно $(\mathbb{Z}/p^n\mathbb{Z})[x]/(f)$, где f — унитарный неприводимый по модулю p многочлен степени $t \in \mathbb{N}$; при этом $\overline{\mathbb{K}} = GF(p^t)$.

2) Всякий элемент a из $\mathbb{K}$ представляется в виде ряда $a = \sum_{k=0}^{n-1} a_k p^k$, где $a_k, 0 \leq k < n$ — элементы заранее фиксированной системы представителей смежных классов по модулю p (с натяжкой можно считать их элементами $\overline{\mathbb{K}}$), однозначно определяющиеся элементом a (см. [19]).

Обозначим теперь через $C(x_1, \ldots, x_c)$ полилинейный центральный многочлен для алгебры M, существующий по Теореме 7. N будет обозначать такое число, что для всякого $a \in M$ a^N — идемпотент (оно существует согласно Лемме 5). Через $E(x_1, \ldots, x_c)$ будем обозначать многочлен C^N, который, очевидно, имеет образом $\{0, 1\}$ и лежит в $\mathcal{K}_0$, поскольку C полилинеен.

3.2. Критерий существования индикатора для множества матриц над кольцом Галуа

Попытаемся теперь получить критерий существования индикатора для множеств матриц над кольцом Галуа, аналогичный Лемме 8.

Замечание 13. *Для любого идеала $I \lhd M$, для любого многочлена $f(x_1, \ldots, x_k) \in \mathcal{K}$, если $a_1, \ldots, a_k \in M$; $b_1, \ldots, b_k \in I$, то*

$$f(a_1 + b_1, a_2 + b_2, \ldots, a_k + b_k) - f(a_1, a_2, \ldots, a_k) \in I.$$

Доказательство: Сперва рассмотрим моном $x_{i_1}^{l_1} \ldots x_{i_r}^{l_r}$ и будем изменять значение только одной переменной x_{i_j}.

$$a_{i_1}^{l_1} \ldots (a_{i_j} + b_{i_j})^{l_j} \ldots a_{i_r}^{l_r} - a_{i_1}^{l_1} \ldots a_{i_j}^{l_j} \ldots a_{i_r}^{l_r} = a_{i_1}^{l_1} \ldots B \ldots a_{i_r}^{l_r}.$$

Здесь через B обозначено выражение $(a_{i_j}+b_{i_j})^{l_j} - a_{i_j}^{l_j}$, представляющее собой сумму всех возможных произведений значений a_{i_j} и b_{i_j} длины l_j, за исключением $a_{i_j}^{l_j}$. Таким образом, $B \in I$, следовательно, и всё выражение является элементом идеала I.

Далее можно применить очевидную индукцию по числу переменных, а затем линейность указанного соотношения.□

Теорема 14. *Множество матриц $A \subseteq M$ обладает индикатором $\chi_A(x, x_1, \ldots, x_s) \in \mathcal{K}_0$ тогда и только тогда, когда оно самоподобно и замкнуто по модулю p, то есть $A + pM \subseteq A$.*

Доказательство:

1) Докажем сперва прямое утверждение. Если $a \in A$, то в M найдутся $a_1, \ldots, a_s$ такие, что $\chi_A(a, a_1, \ldots, a_s) = 1$; следовательно, для любого обратимого $\alpha \in M$

$$\chi_A(\alpha a \alpha^{-1}, \alpha a_1 \alpha^{-1}, \ldots, \alpha a_s \alpha^{-1}) =$$

$$= \alpha \chi_A(a, a_1, \ldots, a_s) \alpha^{-1} = 1.$$

Поскольку при $b \notin A$ должно быть $\chi_A(b, a_1, \ldots, a_s) = 0$ при любых $a_1, \ldots, a_s \in M$, то $\alpha a \alpha^{-1} \in A$. Значит A самоподобно.

Согласно Замечаниею 13, разность $\chi_A(a+pb, a_1, \ldots, a_s)$ и $\chi_A(a, a_1, \ldots, a_s)$ лежит в pM, а поскольку значениями индикатора могут быть только 0 или 1, $\chi_A(a + pb, a_1, \ldots, a_s) = 1$; значит $(a + pb) \in A$ и $A + pM \subseteq A$.

2) Обратно, пусть $A \subseteq M$ самоподобно и замкнуто по модулю p. Рассмотрим $\overline{A}$, соответствующее подмножество $\overline{M}$. Имеем $A = \overline{A}+pM$, кроме того, $\overline{A}$ самоподобно. Согласно Лемме 8, $\overline{A}$ обладает индикатором $\chi_{\bar{A}} \in \overline{\mathcal{K}}$. Рассмотрим теперь многочлен

$$\chi_A(x, x_1, \ldots, x_k, y_1, \ldots, y_c) =$$
$$= E(y_1, \ldots, y_c)\chi_{\bar{A}}^N(x, x_1, \ldots, x_k).$$

Если $a \notin A$, то $a \notin (\overline{A} + pM)$, значит $\overline{a} \notin \overline{A}$ и для всех $a_1, \ldots, a_k \in M$ выполнено $\chi_{\bar{A}}(\overline{a}, \overline{a}_1, \ldots, \overline{a}_k) = 0$. По Замечаниею 13, $\chi_{\bar{A}}(a, a_1, \ldots, a_k) \in pM$, а поскольку возведение в степень N всегда дает идемпотенты, $(\chi_{\bar{A}}(a, a_1, \ldots, a_k))^N = 0$.

Если $a \in A$, то $\overline{a} \in \overline{A}$, и найдутся такие $a_1, \ldots, a_k \in M$, что $\chi_{\bar{A}}(\overline{a}, \overline{a}_1, \ldots, \overline{a}_k) = 1$. Тогда $\chi_{\bar{A}}(a, a_1, \ldots, a_k) \in (1 + pM)$ и $(\chi_{\bar{A}}(a, a_1, \ldots, a_k))^N = 1$.

Поскольку E лежит в $\mathcal{K}_0$, значит и $\chi_A \in \mathcal{K}_0$. Из всего сказанного заключаем, что χ_A обладает всеми требуемыми свойствами.□

Сформулируем ещё несколько вспомогательных утверждений.

Лемма 15. *Если $f(y_1, \ldots, y_k) \in \mathcal{K}$, и $A \subseteq M$ обладает индикатором $\chi_A(x, x_1, \ldots, x_s)$, то образом многочлена*

$$g(y_1, \ldots, y_k, x_1, \ldots, x_s) =$$
$$= f(y_1, \ldots, y_k)\chi_A(f(y_1, \ldots, y_k), x_1, \ldots, x_s)$$

является пересечение образа f и A, в объединении с $\{0\}$.

Доказательство: Легко видеть, что значение g на элементах $a_1, \ldots, a_k, b_1, \ldots, b_s$ равно 0, если $f(a_1, \ldots, a_k) \notin A$; когда же $f(a_1, \ldots, a_k) \in A$, по определению индикатора, найдутся такие $b_1, \ldots, b_s \in M$, что

$$\chi_A(f(a_1, \ldots, a_k), b_1, \ldots, b_s) = 1.$$

Следовательно, значение g при этом совпадает со значением f, что нам и требуется.□

Обозначим через $f(A_1, \ldots, A_k)$ множество значений, принимаемых многочленом $f(x_1, \ldots, x_k) \in \mathcal{K}$, когда x_1 пробегает $A_1, \ldots, x_k$ пробегает A_k. При этом, очевидно, $Im\, f$ совпадает с множеством $f(M, \ldots, M)$.

Замечание 16. *1) Пусть $f(x) \in \mathbb{K}[x]$, и A — класс подобия матриц, т.е. минимальное непустое самоподобное множество, тогда $f(A)$ — тоже класс подобия.*

2) Пусть $f(x_1, \ldots, x_k) \in \mathcal{K}$, и $A_1, \ldots, A_k$ — классы подобия, тогда $f(A_1, \ldots, A_k)$ есть объединение нескольких классов подобия или, попросту, непустое самоподобное множество.

Доказательства этих утверждений очевидны.

3.3. Подобие матриц 2×2 над кольцом Галуа

С этого момента будем считать, что $m = 2$, то есть, $M = M_2(\mathbb{K})$. Сформулируем ещё один известный результат (см. [20], частный случай этого утверждения можно найти в [30]).

Теорема 17. *Не равная 0 по модулю p матрица из M подобна одной из следующих:*

1) $\begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix}$, $a, b \in \mathbb{K}$;

2) $\begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix}$, $r \in \mathbb{K},\ r \neq 0 (mod\, p)$;

3) $\begin{pmatrix} r & p^k \\ p^k a & r + p^k b \end{pmatrix}$, $r, a, b \in \mathbb{K},\ r \neq 0 (mod\, p)$.

Причём a, b в случае 1), r в случае 2), $k \in [1, n-1], p^k a, p^k b$ и $p^{n-k} r$ в случае 3) определяются однозначно.

Следствие 18. *Если матрицы $a, b \in M$ нескалярны по модулю p, то они подобны в том и только в том случае, если у них равны следы и определители.*

Доказательство: По условию обе матрицы нескалярны по модулю p. Из предыдущего утверждения следует, что для таких матриц $a \approx \begin{pmatrix} 0 & 1 \\ -det(a) & tr(a) \end{pmatrix}$, поэтому

$$a \approx b \quad \Leftrightarrow \quad tr(a) = tr(b) \quad \& \quad det(a) = det(b),$$

что и требуется.□

Далее нам будет необходима

Лемма 19. *Рассмотрим действие конечной группы, порожденной циклом $(12 \ldots p^l)$ на множестве слов длины p^l, составленных из $m = p^j s$ (p не делит s) букв b и $(p^l - m)$ букв a. При этом длина любой орбиты этого действия будет степенью p, причем минимальная длина орбиты равна p^{l-j}.*

Доказательство: Запишем произвольную орбиту в виде

$$\begin{array}{ccccccc} b_1 & a^{k_1} & b_2 & a^{k_2} & \ldots & b_m & a^{k_m} \\ a^{k_1} & b_2 & a^{k_2} & b_3 & \ldots & a^{k_m} & b_1 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a & b_{i+1} & a^{k_{i+1}} & b_{i+2} & \ldots & b_i & a^{k_i - 1} \end{array}$$

Здесь различные вхождения b мы пометили индексами, a^k означает $\underbrace{aa\ldots a}_{k}$, и еще одно применение цикла должно привести к повторениям, то есть, i — минимальное число, такое что $k_1 = k_{i+1},\ k_2 = k_{i+2},\ \ldots\ , k_m = k_i$.

Отсюда следует, что i является периодом последовательности $k_1, k_2, \ldots, k_m$ и m делится на i, будем считать $m = qi$. Значит

$$p^l = 1+k_1+1+k_2+\cdots+1+k_m = q(1+k_1+1+k_2+\cdots+1+k_i) = qr;$$

здесь $r = i + k_1 + \cdots + k_i$ — длина нашей орбиты. q и r делят p^l, значит оба эти числа являются степенями p; причем q не превосходит p^j, поэтому r — степень p, не меньшая, чем p^{l-j}.

Рассматривая слово, построенное так: сперва s букв b, затем $(p^{l-j} - s)$ букв a, затем эта группа повторяется, всего p^j раз, видим, что минимальная орбита имеет длину в точности p^{l-j}.$\square$

Лемма 20. *Для матрицы a размера 2×2 над коммутативным кольцом с 1 и для всякого натурального m выполнено следующее соотношение*

$$tr^m(a) = \sum_{k=0}^{[m/2]} C_m^k tr(a^{m-2k}) det^k(a).$$

В записи этой формулы считаем, что $tr(a^0)$ обозначает 1.

Доказательство: Доказательство проводится по индукции. При $m = 0, 1$ утверждение Леммы выполнено.

Пусть это утверждение выполнено для $m = t$ при некотором $t > 1$. Рассмотрим правую часть доказываемого равенства при $m = t + 1$ и используем теорему Гамильтона-Кэли для a (см. её доказательство, например, в [31, Глава VII, § 5,

п. 4]): $a^2 - tr(a)a + det(a) = 0$.

$$\sum_{k=0}^{[(t+1)/2]} C_{t+1}^k tr(a^{t+1-2k}) det^k(a) = C_{t+1}^0 tr(a^{t+1}) +$$

$$+C_{t+1}^1 tr(a^{t-1}) det(a) + \cdots = C_t^0 (tr(a)tr(a^t) - det(a)tr(a^{t-1})) +$$

$$+C_{t+1}^1 tr(a^{t-1}) det(a) + \cdots = C_t^0 tr(a)tr(a^t) +$$

$$+ \left(C_{t+1}^1 - C_t^0\right) tr(a^{t-1}) det(a) + \cdots =$$

$$= C_t^0 tr(a)tr(a^t) + C_t^1 tr(a^{t-1}) det(a) + \ldots$$

Здесь a^{t+1} выражено через предыдущие степени a в соответствии с теоремой Гамильтона-Кэли, а затем использовано одно из свойств биномиальных коэффициентов.

Далее будем на k-ом шаге раскладывать a^{t+1-2k} по теореме Гамильтона-Кэли и складывать вторую часть получаемого выражения с $k+1$-м членом суммы. Получим

$$\cdots + C_t^k tr(a^{t+1-2k}) det^k(a) + C_{t+1}^{k+1} tr(a^{t-1-2k}) det^{k+1}(a) + \cdots =$$

$$= \cdots + C_t^k (tr(a)tr(a^{t-2k}) det^k(a) - tr(a^{t-1-2k}) det^{k+1}(a)) +$$

$$+C_{t+1}^{k+1} tr(a^{t-1-2k}) det^{k+1}(a) + \cdots =$$

$$= \cdots + C_t^k tr(a)tr(a^{t-2k}) det^k(a) + \left(C_{t+1}^{k+1} - C_t^k\right) \times$$

$$\times tr(a^{t-1-2k}) det^{k+1}(a) + \cdots =$$

$$= \cdots + C_t^k tr(a)tr(a^{t-2k}) det^k(a) + C_t^{k+1} tr(a^{t-1-2k}) det^{k+1}(a) + \ldots$$

Теперь рассмотрим последний шаг. В случае чётного t в последнем члене присутствует $tr(a)$, поэтому выкладки в точности совпадают с общими. Если же t нечётно, имеем

$$\cdots + C_t^{(t-1)/2} tr(a^2) det^{(t-1)/2}(a) + C_{t+1}^{(t+1)/2} det^{(t+1)/2}(a) =$$

$$= \cdots + C_t^{(t-1)/2} (tr^2(a) det^{(t-1)/2}(a) - 2det^{(t+1)/2}(a)) +$$

$$+C_{t+1}^{(t+1)/2}det^{(t+1)/2}(a) = \cdots + C_t^{(t-1)/2}tr^2(a)det^{(t-1)/2}(a)+$$
$$+\left(C_{t+1}^{(t+1)/2} - 2C_t^{(t-1)/2}\right)det^{(t+1)/2}(a) =$$
$$= \cdots + C_t^{(t-1)/2}tr^2(a)det^{(t-1)/2}(a).$$

Таким образом, получаем

$$\sum_{k=0}^{[(t+1)/2]} C_{t+1}^k tr(a^{t+1-2k})det^k(a) =$$

$$= tr(a)\left(\sum_{k=0}^{[t/2]} C_t^k tr(a^{t-2k})det^k(a)\right).$$

С учётом предположения индукции это означает, что Лемма доказана.□

Основной в этом разделе является следующая теорема.

Теорема 21. *1) Если $a, b \in M$; $k, l \in \mathbb{N}$; $k > 0, l > 0, k + l \geq n$ и $\overline{a}^{p^l}$ нескалярна, то $(a + p^k b)^{p^l} \approx a^{p^l}$.*

2) Если $\overline{a}^{p^l}$ нескалярна, то $\overline{a}^{p^l} \approx \overline{a}$.

3) Если $a, b \in M$ и $\overline{a}^{p^{n-1}}$ нескалярна, то $(a+pb)^{p^{n-1}} \approx a^{p^{n-1}}$.

Доказательство: Отметим прежде всего, что третий пункт — следствие первого.

1) Поскольку $\overline{(a + p^k b)}^{p^l} = \overline{a}^{p^l}$, обе матрицы в формулировке первого пункта нескалярны по модулю p, и для доказательства их подобия достаточно применить Следствие 18 — проверить равенство следов и определителей. Имеем

$$det\left((a + p^k b)^{p^l}\right) = \left(det(a + p^k b)\right)^{p^l} = \left(det(a) + p^k B\right)^{p^l} =$$

$$= det(a)^{p^l} + p^{k+l}C = det\left(a^{p^l}\right).$$

Здесь мы воспользовались разложением определителя по степеням p, формулой бинома и тем фактом, что p^n равно 0.

Для следа имеем

$$tr\left((a+p^k b)^{p^l}\right) = tr\left(a^{p^l} + p^k\left(a^{p^l-1}b + a^{p^l-2}ba + \cdots + \right.\right.$$

$$\left.\left. + ba^{p^l-1}\right) + p^{2k}\left(a^{p^l-2}b^2 + \cdots + b^2a^{p^l-2}\right) + \cdots + p^{kp^l}b^{p^l}\right).$$

В последнем выражении в скобках при p^{mk} стоят произведения m множителей b и $(p^l - m)$ множителей a. При действии циклических сдвигов на такие произведения след сохраняется, поэтому, воспользовавшись линейностью следа, мы получим сумму, в которой будут участвовать, кроме $tr(a^{p^l})$, следы представителей орбит, умноженные на p^{mk} и на длины соответствующих орбит.

Используя Лемму 19, видим, что множители эти будут иметь вид p^{mk+l-r}, где r — показатель степени p в разложении m на простые множители. Осталось показать, что $mk + l - r \geq k + l$ или $(m-1)k \geq r$. Но m делится на p^r, следовательно, по крайней мере $r < m$ или $r \leq (m-1)$. Таким образом, с точностью до суммы, делящейся на p^{k+l}, а значит равной 0 в $\mathbb{K}$,

$$tr\left((a+p^k b)^{p^l}\right) = tr\left(a^{p^l}\right).$$

2) Если $\overline{a}^{p^l}$ нескалярна, то $\overline{a}$ — тем более, и, как и в первом пункте, для доказательства их подобия достаточно проверить равенство следов и определителей, причем

только по модулю p. Имеем

$$det\left(\overline{a}^{p^l}\right) = (det(\overline{a}))^{p^l} = det(\overline{a})(mod\, p).$$

Для следов по Лемме 20 получаем

$$tr(a) = tr^{p^l}(a)(mod\, p) =$$

$$= \sum_{k=0}^{[p^l/2]} C_{p^l}^k tr\left(a^{p^l-2k}\right) det^k(a)\,(mod\, p) = tr\left(a^{p^l}\right)(mod\, p),$$

поскольку при любом k, $0 < k < p^l$ $\binom{p^l}{k}$ делится на p.$\square$

3.4. Критерий скалярности p^l-ой степени матрицы

Этот раздел посвящён доказательству следующей теоремы.

Теорема 22. *1) Если $a, b \in \mathbb{K}$; $k \in \mathbb{N}$, то*

$$\begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix}^k = \begin{pmatrix} ab_{k-1} & b_k \\ ab_k & b_{k+1} \end{pmatrix},$$

где $b_0 = 0$, $b_1 = 1$ и $b_{k+2} = ab_k + bb_{k+1}$.

2) Если $p = char(\overline{\mathbb{K}}) \neq 2$ и $\overline{b}^2 + 4\overline{a} \neq 0$, то для всех натуральных k выполнено

$$\overline{b}_k = \frac{1}{\sqrt{\overline{b}^2 + 4\overline{a}}}\left(\left(\frac{\overline{b} + \sqrt{\overline{b}^2 + 4\overline{a}}}{2}\right)^k - \left(\frac{\overline{b} - \sqrt{\overline{b}^2 + 4\overline{a}}}{2}\right)^k\right).$$

Эта формула верна в расширении $\overline{\mathbb{K}}(\sqrt{\overline{b}^2 + 4\overline{a}})$.

3) Если $p \neq 2$ *и* $\overline{b}^2 + 4\overline{a} = 0$, *то для всех натуральных* k

$$\overline{b}_k = k \left(\frac{\overline{b}}{2} \right)^{k-1}.$$

4) При произвольном p

$$\overline{b}_p = 0 \quad \Leftrightarrow \quad \overline{b}^2 + 4\overline{a} = 0 \text{ в } \overline{\mathbb{K}}.$$

5) Матрица

$$\begin{pmatrix} 0 & 1 \\ \overline{a} & \overline{b} \end{pmatrix}^p$$

скалярна тогда и только тогда, когда $\overline{b}^2 + 4\overline{a} = 0$ *в* $\overline{\mathbb{K}}$.

6) Матрица

$$\begin{pmatrix} 0 & 1 \\ \overline{a} & \overline{b} \end{pmatrix}^p$$

скалярна тогда, и только тогда, когда найдется $r \in \overline{\mathbb{K}}$ *такой, что*

$$\begin{pmatrix} 0 & 1 \\ \overline{a} & \overline{b} \end{pmatrix} \approx \begin{pmatrix} r & 1 \\ 0 & r \end{pmatrix}.$$

7) Для матрицы $c \in \overline{M}$ *ее* p^l*-ая степень скалярна тогда же, когда и* c^p.

8) Итог: матрица $c \in M$, *возведенная в степень* p^l *будет нескалярной по модулю* p *тогда, и только тогда, когда найдутся* $a, b \in \mathbb{K}$ *такие, что* $b^2 + 4a \neq 0 (mod\, p)$ *и*

$$c \approx \begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix}.$$

Доказательство:

1) Доказательство проводится по индукции. При $k = 1$ утверждение этого пункта выполнено, поскольку $b_2 = ab_0 + bb_1 = b$. Пусть оно выполнено при $k = t$, тогда при $k = t + 1$ имеем

$$\begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix}^{t+1} = \begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix}\begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix}^{t} = \begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix}\begin{pmatrix} ab_{k-1} & b_k \\ ab_k & b_{k+1} \end{pmatrix} =$$

$$= \begin{pmatrix} ab_k & b_{k+1} \\ a(ab_{k-1} + bb_k) & ab_k + bb_{k+1} \end{pmatrix} = \begin{pmatrix} ab_k & b_{k+1} \\ ab_{k+1} & b_{k+2} \end{pmatrix}.$$

Утверждение доказано.

2) Последовательность $\overline{b}_k$ задается условиями $\overline{b}_0 = 0$, $\overline{b}_1 = 1$, $\overline{b}_{k+2} = \overline{ab}_k + \overline{bb}_{k+1}$. Отсюда

$$\overline{b}_k = C\lambda_1^k + D\lambda_2^k,$$

где λ_1, λ_2 — различные корни уравнения

$$\lambda^2 - \overline{b}\lambda - \overline{a} = 0. \tag{3.1}$$

а коэффициенты C и D удовлетворяют системе

$$\begin{cases} C + D & = & 0 \\ C\lambda_1 + D\lambda_2 & = & 1. \end{cases}$$

Решая их, получаем нужное выражение.

3) В случае $\overline{b}^2 + 4\overline{a} = 0$

$$\overline{b}_k = (Ck + D)\,\lambda^k,$$

где λ — на этот раз единственный корень уравнения (3.1), равный $\overline{b}/2$. C и D опять получаем из соответствующей системы.

4) При $p = 2$ имеем

$$\overline{b}_p = \overline{b}_2 = \overline{b} = 0 \quad \Leftrightarrow \quad \overline{b}^2 + 4\overline{a} = \overline{b}^2 = 0.$$

При $p \neq 2$, если $\overline{b}^2 + 4\overline{a} \neq 0$, то в расширении $\overline{\mathbb{K}}(\sqrt{\overline{b}^2 + 4\overline{a}})$ верно $x = \sqrt{\overline{b}^2 + 4\overline{a}} \neq 0$, а

$$\overline{b}_p = \frac{1}{x}\left(\left(\frac{\overline{b}+x}{2}\right)^p - \left(\frac{\overline{b}-x}{2}\right)^p\right) = 0$$

влечёт $\left(\frac{\overline{b}+x}{2}\right)^p = \left(\frac{\overline{b}-x}{2}\right)^p$. Отсюда $(\overline{b}+x)^p = (\overline{b}-x)^p$, и, поскольку возведение в степень p — автоморфизм $\overline{\mathbb{K}}(x)$, получаем $\overline{b} + x = \overline{b} - x$, следовательно $x = 0$. Получилось противоречие, поэтому в рассматриваемом случае $\overline{b}_p \neq 0$.

При $\overline{b}^2 + 4\overline{a} = 0$, согласно третьему пункту,

$$\overline{b}_p = p\left(\frac{\overline{b}}{2}\right)^{p-1} = 0 (mod\, p).$$

Таким образом, равенства $\overline{b}^2 + 4\overline{a} = 0$ и $\overline{b}_p = 0$ равносильны.

5) Согласно первому пункту

$$\begin{pmatrix} 0 & 1 \\ \overline{a} & \overline{b} \end{pmatrix}^p = \begin{pmatrix} \overline{ab}_{p-1} & \overline{b}_p \\ \overline{ab}_p & \overline{b}_{p+1} \end{pmatrix}.$$

Поскольку $\overline{b}_{p+1} = \overline{ab}_{p-1} + \overline{b}\overline{b}_p$, эта матрица скалярна в том, и только в том случае, когда $\overline{b}_p = 0$; из четвертого пункта видим, что это бывает в точности тогда, когда $\overline{b}^2 + 4\overline{a} = 0$.

6) Необходимое и достаточное условие скалярности матрицы вида $\begin{pmatrix} 0 & 1 \\ \overline{a} & \overline{b} \end{pmatrix}^p$ — равенство $\overline{b}^2 + 4\overline{a} = 0$. При $p \neq 2$ можно положить $r = \overline{b}/2$, тогда $r^2 = -\overline{a}$. При $p = 2$ равенство $\overline{b}^2 + 4\overline{a} = 0$ выполнено тогда и только тогда, когда $\overline{b} = 0$. В этом случае, поскольку $\overline{\mathbb{K}}$ — поле характеристики 2, любой его элемент будет квадратом; в частности, найдется r, такой, что $r^2 = -\overline{a}$. Автоматически $2r = 0 = \overline{b}$. Итак, в любом случае есть $r \in \overline{\mathbb{K}}$ такой, что $2r = \overline{b}$ и $r^2 = -\overline{a}$.

Обратно, если существует $r \in \overline{\mathbb{K}}$, удовлетворяющий этим условиям, то $\overline{b}^2 + 4\overline{a} = 4r^2 - 4r^2 = 0$. Значит, матрица $\begin{pmatrix} 0 & 1 \\ \overline{a} & \overline{b} \end{pmatrix}^p$ скалярна в точности тогда, когда в $\overline{\mathbb{K}}$ найдется r, такой, что $2r = \overline{b}$ и $r^2 = -\overline{a}$.

Рассмотрим теперь матрицу $\begin{pmatrix} r & 1 \\ 0 & r \end{pmatrix}$. Ее след $2r$ равен $\overline{b}$, ее определитель r^2 равен $-\overline{a}$; это в точности след и определитель матрицы $\begin{pmatrix} 0 & 1 \\ \overline{a} & \overline{b} \end{pmatrix}$. Кроме того, обе эти матрицы нескалярны, значит по Следствию 18, они подобны.

7) Если наша матрица $c^p \in \overline{M}$ скалярна, то любая ее степень тоже скалярна, значит скалярна матрица $c^{p^l} = (c^p)^{p^{l-1}}$. Если же c^p нескалярна, то, согласно пункту 2) Теоремы 21, $c^p \approx c$. Отсюда

$$c^{p^l} \approx c^{p^{l-1}} \approx \cdots \approx c^p$$

— нескалярная матрица.

8) Осталось сказать только, что для любой $c \in M$ тот факт, что c^{p^l} нескалярна по модулю p, означает, что c

тем более такова, а значит, подобна $\begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix}$ для некоторых $a, b \in \mathbb{K}$; причем, так как $\overline{c}^p$ нескалярна, то $b^2 + 4a = \overline{b}^2 + 4\overline{a}(mod\, p) \neq 0(mod\, p)$.

Теорема доказана полностью.□

3.5. Многочлены с образами специального вида

Далее везде через $[a]$ мы будем обозначать класс подобия, содержащий матрицу $a \in M$, а через $[a]'$ — объединение $\{0\}$ с этим классом, $[a]' = [a] \cup \{0\}$.

Замечание 23. *Если* $\overline{a}, \overline{b} \in \overline{\mathbb{K}}$; $\overline{b}^2 + 4\overline{a} \neq 0$, *то существуют* $a, b \in \mathbb{K}$, *такие, что* $a = \overline{a}(mod\, p), b = \overline{b}(mod\, p)$, *и существует* $f \in \mathcal{K}_0$, *для которого*

$$Im\, f = \left[\begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix} \right]'.$$

Доказательство: Рассмотрим множество матриц

$$A = \left\{ c \in M : \overline{c} \approx \begin{pmatrix} 0 & 1 \\ \overline{a} & \overline{b} \end{pmatrix} \right\}.$$

Очевидно, что оно замкнуто по модулю p; кроме того, по Теореме 17, оно самоподобно. Согласно Теореме 14, оно обладает индикатором $\chi_A \in \mathcal{K}_0$. С другой стороны, по Теореме 22, $\forall c \in A \quad c^{p^{n-1}}$ — нескалярна по модулю p, а значит, воспользовавшись Теоремой 21, можно получить, что

1) $\forall c, d \in A \quad c^{p^{n-1}} \approx d^{p^{n-1}}$;

2) $\forall c \in A \quad \overline{c}^{p^{n-1}} \approx \overline{c}$.

Отсюда следует, что найдутся $a, b \in \mathbb{K}$ такие, что $a = \overline{a}(mod\, p), b = \overline{b}(mod\, p)$ и для всех $c \in A$

$$c^{p^{n-1}} \approx \begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix}.$$

Значит, многочлен $f(x, x_1, \ldots, x_k) = x^{p^{n-1}} \chi_A(x, x_1, \ldots, x_k)$ имеет образом $\left[\begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix}\right]'$, что и требовалось.$\square$

Лемма 24. *Для любых $a, b \in \mathbb{K}$, таких, что $b^2 + 4a \neq 0(mod\, p)$ существует многочлен $f \in \mathcal{K}_0$, образ которого равен $\left[\begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix}\right]'$.*

Доказательство: Согласно предыдущему утверждению, такой многочлен есть для некоторых a' и b', удовлетворяющих условиям $a' = a(mod\, p)$ и $b' = b(mod\, p)$.

1) Докажем сперва следующее: для любых $a, b, a', b' \in \mathbb{K}$, для которых выполнены указанные условия, существуют $r, s \in \mathbb{K}$, такие, что

$$\left(\begin{pmatrix} 0 & 1 \\ a' & b' \end{pmatrix} + \begin{pmatrix} pr & 0 \\ 0 & pr \end{pmatrix}\right)(1 + ps) \approx \begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix}.$$

Имеем

$$(1 + ps)\left(\begin{pmatrix} 0 & 1 \\ a' & b' \end{pmatrix} + \begin{pmatrix} pr & 0 \\ 0 & pr \end{pmatrix}\right) \approx$$

$$\approx (1 + ps)\begin{pmatrix} 0 & 1 \\ a' - prb' - p^2r^2 & b' + 2pr \end{pmatrix} \approx \begin{pmatrix} 0 & 1 \\ A & B \end{pmatrix},$$

где

$$A = a' + p(2sa' - rb') + p^2(s^2a' - 2srb' - r^2) -$$

$$-p^3(s^2rb' + 2sr^2) - p^4s^2r^2;$$
$$B = b' + p(sb' + 2r) + 2p^2sr.$$

Наше утверждение свелось к разрешимости относительно r и s системы уравнений

$$\begin{cases} a' + p(2sa' - rb') + p^2(s^2a' - 2srb' - r^2) - \\ \qquad -p^3(2sr^2 + s^2rb') - p^4s^2r^2 = a \\ \qquad b' + p(sb' + 2r) + 2p^2sr = b. \end{cases}$$

Если разложить a, b, a', b', r, s в ряды по степеням p (например, $a = \sum_{k=0}^{n-1} a_k p^k$), то, приравнивая коэффициенты при равных степенях и отбросив выполненные по условию равенства $a'_0 = a_0$ и $b'_0 = b_0$, получим для $0 < k < n$

$$\begin{cases} a'_k + \sum\limits_{i+j=k-1}(2s_ia'_j - r_ib'_j) - \sum\limits_{i+j=k-2} r_ir_j + \sum\limits_{i+j+l=k-2} s_i(s_ja'_l - 2r_jb'_l) - \\ \qquad -2\sum\limits_{i+j+l=k-3} s_ir_jr_l - \sum\limits_{i+j+l+m=k-3} s_is_jr_lb'_m - \sum\limits_{i+j+l+m=k-4} s_is_jr_lr_m = a_k \\ \qquad b'_k + 2r_{k-1} + \sum\limits_{i+j=k-1} s_ib'_j + 2\sum\limits_{i+j=k-2} s_ir_j = b_k \end{cases}$$

Заметим, что в этой системе в каждом уравнении помимо s_{k-1}, r_{k-1} присутствуют только s_i, r_i с $i < k-1$, поэтому ее можно решать, рассматривая систему для каждого k как линейную относительно s_{k-1}, r_{k-1} с коэффициентами из $\overline{\mathbb{K}}$ и выражая их через все предыдущие s_i и r_i. Такие линейные системы для всех k имеют одну и ту же матрицу — $\begin{pmatrix} 2a'_0 & -b'_0 \\ b'_0 & 2 \end{pmatrix}$, определитель которой

$$4a'_0 + (b'_0)^2 = \overline{b}^2 + 4\overline{a} \neq 0.$$

Поэтому они разрешимы, а, следовательно, указанная выше система — тоже.

2) Поскольку мы имеем многочлен $g \in \mathcal{K}_0$ такой, что $Im\, g = \left[\begin{pmatrix} 0 & 1 \\ a' & b' \end{pmatrix}\right]'$, образом $h = (1+ps)(g+pr)$, где r и s получены описанным выше способом, будет

$$\left[\begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix}\right] \cup \left[\begin{pmatrix} pr(1+ps) & 0 \\ 0 & pr(1+ps) \end{pmatrix}\right].$$

Если A — множество $\left\{c \in M : \overline{c} \approx \begin{pmatrix} 0 & 1 \\ \overline{a} & \overline{b} \end{pmatrix}\right\}$, то искомый многочлен можно получить так:

$$f(y_1, \ldots, y_k, x_1, \ldots, x_l) =$$

$$= h(y_1, \ldots, y_k)\chi_A(h(y_1, \ldots, y_k), x_1, \ldots, x_l).$$

Его образом будет в точности $\left[\begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix}\right]'$.□

Замечание 25. *Образ многочлена* $f = xyx + xy$ *при* x, *принимающем значения в классе подобия* $\left[\begin{pmatrix} 0 & 1 \\ pt & -1 \end{pmatrix}\right]$, *и* y, *пробегающем* $\left[\begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix}\right]$, *содержит только один класс подобия, состоящий из не равных* 0 *по модулю* p *матриц* — $\left[\begin{pmatrix} 0 & 1 \\ p^2t^2a & ptb \end{pmatrix}\right]$.

Доказательство: Рассмотрим значение, которое многочлен $xyx+xy = xy(x+1)$ принимает на матрицах $\begin{pmatrix} 0 & 1 \\ pt & -1 \end{pmatrix}$ и $\begin{pmatrix} x & y \\ z & v \end{pmatrix}$.

$$\begin{pmatrix} 0 & 1 \\ pt & -1 \end{pmatrix}\begin{pmatrix} x & y \\ z & v \end{pmatrix}\begin{pmatrix} 1 & 1 \\ pt & 0 \end{pmatrix} = \begin{pmatrix} z & v \\ -z+ptx & -v+pty \end{pmatrix} \times$$

$$\times \begin{pmatrix} 1 & 1 \\ pt & 0 \end{pmatrix} = \begin{pmatrix} z+ptv & z \\ -z+pt(x-v)+p^2t^2y & -z+ptx \end{pmatrix}$$

След последней матрицы равен $pt(x+v) = pt\,tr\begin{pmatrix} x & y \\ z & v \end{pmatrix}$, а её определитель равен $-z^2+ptz(x-v)+p^2t^2xv-(-z^2+ptz(x-v)+p^2t^2yz) = p^2t^2(xv-yz) = p^2t^2\,det\begin{pmatrix} x & y \\ z & v \end{pmatrix}$. Таким образом, если $tr\begin{pmatrix} x & y \\ z & v \end{pmatrix} = b$ и $det\begin{pmatrix} x & y \\ z & v \end{pmatrix} = -a$, значение f либо лежит в указанном классе подобия (при $z \neq 0(mod\,p)$), либо равно $0(mod\,p)$ (при $z = 0(mod\,p)$). Поскольку в классе подобия $\left[\begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix}\right]$, очевидно, есть матрицы с $z \neq 0(mod\,p)$, замечание доказано.□

Следствие 26. *Если* $p^3 = 0$ *в* $\mathbb{K}$, *то* $\forall a, b \in \mathbb{K}$ *существует* $f \in \mathcal{K}_0$ *имеющий образ* $\left[\begin{pmatrix} 0 & 1 \\ p^2a & pb \end{pmatrix}\right]'$.

Доказательство: Для всех a, b, таких, что b^2+4a не равно 0 по модулю p, это непосредственно вытекает из предыдущих утверждений. Если же $b^2+4a = 0(mod\,p)$, то найдётся такое $r \in \mathbb{K}$, что $a = -r^2+pc$ и $b = 2r+pd$. Мы уже имеем многочлен $f \in \mathcal{K}_0$ с образом $\left[\begin{pmatrix} 0 & 1 \\ 0 & pd \end{pmatrix}\right]'$, так как при $d \neq 0(mod\,p)$ это следует из только что сказанного, а при $d = p^kd'$, где $d' \neq 0(mod\,p)$, достаточно использовать Замечаниее 25 с $a = 0,\ b = d'$ и $t = p^{k-1}$. Отметим ещё, что прибавив pr к матрице, подобной $\begin{pmatrix} 0 & 1 \\ 0 & p^2d \end{pmatrix}$, мы получим

$$\begin{pmatrix} pr & 1 \\ 0 & pr+p^2d \end{pmatrix} \approx \begin{pmatrix} 0 & 1 \\ -p^2r^2-p^3rd & p(2r+pd) \end{pmatrix} =$$

$$= \begin{pmatrix} 0 & 1 \\ -p^2r^2 + p^3c & p(2r + pd) \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ p^2a & pb \end{pmatrix}.$$

Предпоследний переход учитывает, что $p^3 = 0$.

Непосредственно к f прибавить многочлен с образом $[pr]'$ нельзя, поскольку оба образа содержат 0, и в образе суммы будет содержаться класс $\left[\begin{pmatrix} 0 & 1 \\ 0 & p^2d \end{pmatrix}\right]'$ неразличимый с нужным нам по $mod\, p$, поэтому прибавим сперва многочлен с образом $[1]'$, затем, пересекая полученный образ с множеством матриц подобных $\begin{pmatrix} 1 & 1 \\ 0 & 1 + p^2d \end{pmatrix}$ по $mod\, p$ по Лемме 15, получим многочлен с образом $\left[\begin{pmatrix} 1 & 1 \\ 0 & 1 + p^2d \end{pmatrix}\right]'$, затем прибавим к нему многочлен с образом $[pr - 1]'$ и повторим процедуру пересечения, отделяя нужный нам класс $\left[\begin{pmatrix} 0 & 1 \\ p^2a & pb \end{pmatrix}\right]$.□

Далее мы часто будем использовать описанный в доказательстве приём для получения новых классов подобия путём прибавления скаляров равных 0 по $mod\, p$, не вдаваясь каждый раз в подробности.

Докажем теперь несколько утверждений, помогающих получить одни классы подобия из других.

Лемма 27. *Если в $\mathcal{K}_0$ для всякого $a \in \mathbb{K}$ существует многочлен с образом $\left[\begin{pmatrix} 0 & 1 \\ pa & 0 \end{pmatrix}\right]'$ в случае $p \neq 2$, или $\left[\begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix}\right]'$ в случае $p = 2$, то для всех $a, b \in \mathbb{K}$ найдётся многочлен из $\mathcal{K}_0$ с образом $\left[\begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix}\right]'$.*

Доказательство: Лемма 24 даёт нам искомый многочлен при $b^2 + 4a \neq 0(mod\, p)$. Если же это не так, можно найти r,

такое что $b = 2r$ — при $p \neq 2$ просто берём $r = b/2$, при $p = 2$ условие $b^2 + 4a = 0(mod\, p)$ эквивалентно $b = 0(mod\, p)$, следовательно $b = 2r$.

В случае $p = 2$ имеем

$$\begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix} \approx \begin{pmatrix} r & 1 \\ a + r^2 & r \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ a + r^2 & 0 \end{pmatrix} + r.$$

Согласно условию, существует многочлен $f \in \mathcal{K}_0$, имеющий образ $\left[\begin{pmatrix} 0 & 1 \\ a + r^2 & 0 \end{pmatrix}\right]'$, следовательно, прибавляя к нему r, и умножая сумму на $E(x_1, \ldots, x_c)$, мы получим многочлен с образом $\left[\begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix}\right]'$.

В случае $p \neq 2$, поскольку $4r^2 + 4a = 0(mod\, p)$, имеем $a = -r^2 + pa'$ и

$$\begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix} \approx \begin{pmatrix} r & 1 \\ pa' & r \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ pa' & 0 \end{pmatrix} + r.$$

Опять искомый многочлен легко получается из существующего по условию.□

При $p \neq 2$ это утверждение можно значительно усилить.

Лемма 28. *В случае $p \neq 2$ обозначим какой-нибудь из представителей единственного неединичного смежного класса группы обратимых элементов $\mathbb{K}$ по подгруппе обратимых квадратов через ε. Если существуют многочлены из $\mathcal{K}_0$ с образами $\left[\begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix}\right]'$ и $\left[\begin{pmatrix} 0 & 1 \\ \varepsilon p & 0 \end{pmatrix}\right]'$, то для всяких $a, b \in \mathbb{K}$ в $\mathcal{K}_0$ найдётся многочлен с образом $\left[\begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix}\right]'$.*

Доказательство:

1) Для всякого $a \neq 0(mod\, p)$ можно получить многочлен с образом $\left[\begin{pmatrix} 0 & 1 \\ pa & 0 \end{pmatrix}\right]'$ при помощи умножения на скаляр одного из существующих по условию многочленов, в зависимости от того, является ли a квадратом или нет, поскольку

$$\alpha \begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix} \approx \begin{pmatrix} 0 & 1 \\ p\alpha^2 & 0 \end{pmatrix} \text{ и}$$

$$\alpha \begin{pmatrix} 0 & 1 \\ p\varepsilon & 0 \end{pmatrix} \approx \begin{pmatrix} 0 & 1 \\ p\varepsilon\alpha^2 & 0 \end{pmatrix}.$$

2) По Лемме 24 для всякого $a \neq 0(mod\, p)$ существует многочлен с образом $\left[\begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix}\right]'$, а Замечаниее 25 позволяет получить из него многочлен с образом $\left[\begin{pmatrix} 0 & 1 \\ p^2a & 0 \end{pmatrix}\right]'$. Применяя теперь Замечаниее 25 к полученным в этом и предыдущем пунктах многочленам, можно получить последовательно многочлены с образами $\left[\begin{pmatrix} 0 & 1 \\ p^ka & 0 \end{pmatrix}\right]'$ для всех $a \neq 0(mod\, p)$ и $0 < k < n$. Это значит, что выполнено условие Леммы 27, применяя которую, мы завершаем доказательство этого утверждения.□

Лемма 29. *Пусть $p \neq 2$, либо $\overline{\mathbb{K}}$ является собственным расширением $\mathbb{Z}/2\mathbb{Z}$, либо $p^4 = 0$ в $\mathbb{K}$, пусть также $\forall a, b \in \mathbb{K}$ имеется многочлен из $\mathcal{K}_0$ с образом $\left[\begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix}\right]'$. Тогда для всякого класса сопряжённости скалярного по $mod\, p$ найдётся многочлен из $\mathcal{K}_0$, образ которого равен этому классу в объединении с $\{0\}$.*

Доказательство: Согласно Теореме 17, всякий класс подобия матриц размера 2×2 над $\mathbb{K}$, скалярный и не равный

0 по $mod\, p$, имеет вид $\left[\begin{pmatrix} r & p^k \\ p^k a & r+p^k b \end{pmatrix}\right]$, где $r, a, b \in \mathbb{K}$, $r \neq 0(mod\, p)$ и $0 < k < n$ (n — минимальное число, такое что $p^n = 0$ в $\mathbb{K}$.)

1) Пусть $a \neq 0(mod\, p)$, тогда, поскольку для матриц, подобных $\begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix}$ выполнено тождество $x^2 = bx+a$, нужный нам многочлен может быть получен в виде

$$ra^{-1}f^2 + (p^k - ra^{-1}b)f,$$

где f — многочлен с образом $\left[\begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix}\right]'$.

2) Пусть теперь $b \neq -1(mod\, p)$, тогда, аналогичным образом получаем искомый многочлен в виде

$$(r-p^k)(-b-1+a)^{-1}f^2+(p^k-(r-p^k)(-b-1+a)^{-1}(b+2))f,$$

беря в качестве f многочлен с образом, равным множеству $\left[\begin{pmatrix} 0 & 1 \\ -b-1+a & b+2 \end{pmatrix}\right]'$. Точно так же, в случае $b \neq 1(mod\, p)$, в качестве f возьмём многочлен с образом $\left[\begin{pmatrix} 0 & 1 \\ b-1+a & b-2 \end{pmatrix}\right]'$ и получим искомый многочлен в виде

$$(r+p^k)(b-1+a)^{-1}f^2+(p^k-(r+p^k)(b-1+a)^{-1}(b-2))f.$$

3) Остался случай $b = 1 = -1(mod\, p)$, т.е. $p = 2$, и $a = 0(mod\, p)$. Если в $\overline{\mathbb{K}}$ есть элемент $\alpha \neq 0, 1$, то, поскольку $b = 1(mod\, p)$, имеем $-\alpha^2 - b\alpha + a \neq 0(mod\, p)$. В качестве f возьмём многочлен с образом,

равным $\left[\begin{pmatrix} 0 & 1 \\ -\alpha^2 - b\alpha + a & 2\alpha + b \end{pmatrix}\right]'$. Тогда искомый многочлен можно получить в виде

$$(r - p^k\alpha)(-\alpha^2 - b\alpha + a)^{-1}f^2 +$$

$$+(p^k - (r - p^k\alpha)(-\alpha^2 - b\alpha + a)^{-1}(2\alpha + b))f.$$

Используется та же идея, что и в предыдущих случаях.

4) Теперь пусть $\overline{\mathbb{K}} = \mathbb{Z}/2\mathbb{Z}$, т.е. $\mathbb{K} = \mathbb{Z}/2^m\mathbb{Z}$. По условию $m \leq 4$, кроме того $a = 0(mod\, p)$ и $b = 1(mod\, p)$. Напомним, что многочлен $xyx + y$, если в качестве x в него подставить матрицу $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, переводит $\begin{pmatrix} r + p^k u & p^k v \\ p^k w & r + p^k t \end{pmatrix}$ в $\begin{pmatrix} r + p^k u & p^k(v + w) \\ p^k w & r + p^k t \end{pmatrix}$. Так как в результате мы хотим получить матрицу подобную $\begin{pmatrix} r & p^k \\ p^k a & r + p^k b \end{pmatrix}$, в качестве исходной надо брать подобную $\begin{pmatrix} r & p^k \\ p^k(a-1) & r + p^k b \end{pmatrix}$. Все такие матрицы получаются умножением матриц подобных $\begin{pmatrix} 0 & 1 \\ a-1 & b \end{pmatrix}$ на p^k и прибавлением r. Таким образом, получаем следующие требования на u, v, w и t :

$$\begin{cases} u + t = b(mod\, p^3), \\ wv - ut = (a-1)(mod\, p^3), \\ wv - ut + w^2 = a(mod\, p^3) \end{cases}$$

Вспомним, что $b = 1(mod\, p)$, значит, $u + t = b = 1(mod\, p)$. Поскольку $p = 2$, заключаем, что u и t не равны по $mod\, p$ и, следовательно, $ut = 0(mod\, p)$. Теперь, так как $a - 1 = 1(mod\, p)$, получаем, что $w =$

$1(mod\, p)$ и $v = 1(mod\, p)$. Отсюда следует, что всегда $w^2 = 1(mod\, 8)$, что нам и нужно. Итак, мы построили многочлен с образом $\left[\begin{pmatrix} r & p^k \\ p^k a & r + p^k b \end{pmatrix}\right]'$ для всех r, a и b из $\mathbb{Z}/2^m\mathbb{Z}$, при $m \leq 4$, что и требовалось в условии.□

Лемма 30. *Для каждого $a \in \mathbb{K}$ существует многочлен $f \in \mathcal{K}_0$, имеющий образом $\bigcup\limits_{b\in\mathbb{K}} \left[\begin{pmatrix} 0 & 1 \\ pa & pb \end{pmatrix}\right]'$.*

Доказательство:

1) Сперва покажем, что для всякого $a \in \mathbb{K}$ найдется $c \in \mathbb{K}$, такой, что $c(1+pc) = a$. Сделать это можно также, как и в Лемме 24, разложив a и c в ряды по степеням p и решая получающиеся уравнения.

$$c_k + \sum_{i+j=k-1} c_i c_j = a_k.$$

Из этих равенств видно, что каждое c_k выражается через a_k, a_i и c_i при $i < k$, поэтому нужное нам c существует.

2) Согласно Лемме 24, существует многочлен $g \in \mathcal{K}_0$, чей образ равен $\left[\begin{pmatrix} 0 & 1 \\ -pa & 1 \end{pmatrix}\right]'$, поскольку $1^2 - 4pa \neq 0(mod\, p)$. Аналогично, при $p \neq 2$ существует $h \in \mathcal{K}_0$ с образом $\left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right]'$, так как $0^2 + 4 \neq 0(mod\, p)$; а при $p = 2$ — с образом $\left[\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\right]'$, так как $1^2+4 \neq 0(mod\, 2)$ — обозначим его тоже h.

Возьмем теперь c, такое, что $c(1 + pc) = -a$. Тогда,

очевидно,

$$\begin{pmatrix} 1+pc & 0 \\ pb & -pc \end{pmatrix} \approx \begin{pmatrix} 1+pc & 0 \\ p(b+c) & -pc \end{pmatrix} \approx \begin{pmatrix} 0 & 1 \\ -pa & 1 \end{pmatrix};$$

$$\begin{pmatrix} 1+pc & 0 \\ pb & -pc \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}=\begin{pmatrix} 0 & 1+pc \\ -pc & pb \end{pmatrix}\approx\begin{pmatrix} 0 & 1 \\ pa & pb \end{pmatrix};$$

$$\begin{pmatrix} 1+pc & 0 \\ p(b+c) & -pc \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1+pc \\ -pc & pb \end{pmatrix}.$$

Значит множество $A = \bigcup\limits_{b\in\mathbb{K}} \left[\begin{pmatrix} 0 & 1 \\ pa & pb \end{pmatrix}\right]'$ содержится в образе произведения gh. Заметим также, что, если B обозначает множество $\left\{c \in M : \overline{c} \approx \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\right\}$, то пересечение B с образом gh в точности равно A, поскольку определитель любой ненулевой матрицы из $Im\, gh$ равен $-pa$. Отсюда, в соответствии с Леммой 15, многочлен

$$f(x_1,\dots,x_k,y_1,\dots,y_l,z_1,\dots,z_m) = g(x_1,\dots,x_k)\times$$

$$\times h(y_1,\dots,y_l)\chi_B(g(x_1,\dots,x_k)h(y_1,\dots,y_l),z_1,\dots,z_m)$$

имеет образом множество A.□

3.6. Случай $p^2 = 0$ и $\mathbb{Z}/8\mathbb{Z}$

В этих случаях удаётся доказать достаточность условия (1.1) для того, чтобы множество являлось образом многочлена из алгебры $\mathcal{K}_0$.

Лемма 31. *В случае $p^2 = 0$ в $\mathbb{K}$ для всякого $a \in \mathbb{K}$ существует многочлен $f \in \mathcal{K}_0$ с образом $\left[\begin{pmatrix} 0 & 1 \\ pa & 0 \end{pmatrix}\right]'$.*

Доказательство: По Лемме 24 есть многочлен $g \in \mathcal{K}_0$, имеющий образом $\left[\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}\right]'$, а по Лемме 30 существует $h \in \mathcal{K}_0$ с образом $\bigcup\limits_{b\in\mathbb{K}} \left[\begin{pmatrix} 0 & 1 \\ -pa & pb \end{pmatrix}\right]'$. Рассмотрим многочлен, являющийся их коммутатором

$$w(x_1,\ldots,x_k,y_1,\ldots,y_l) = g(x_1,\ldots,x_k)h(y_1,\ldots,y_l) - \\ -h(y_1,\ldots,y_l)g(x_1,\ldots,x_k)$$

и самоподобное, замкнутое по модулю p множество

$$A = \left\{ c \in M : \overline{c} \approx \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \right\}.$$

Поскольку

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \approx \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix},$$

можно получить все значения w следующим образом

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} x & y \\ z & t \end{pmatrix} - \begin{pmatrix} x & y \\ z & t \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & y \\ -z & 0 \end{pmatrix}.$$

При этом $x + t = pb, \quad xt - zy = pa$, и значение w лежит в A только если $yz = pc$, следовательно, $pa = x(pd - x) - pc$ и $x^2 = p(dx - a - c)$. Отсюда $x = 0(mod\, p)$ и, так как $p^2 = 0$, то $0 = p(a + c)$, т.е. $yz = -pa$. Получаем, что образ w пересекает A по множеству $\left[\begin{pmatrix} 0 & 1 \\ pa & 0 \end{pmatrix}\right]$, искомый многочлен получается так:

$$f(x_1,\ldots,x_k,y_1,\ldots,y_s) =$$

$$= w(y_1,\ldots,y_s)\chi_A(w(y_1,\ldots,y_s),x_1,\ldots,x_k).$$

Утверждение леммы доказано.□

Теперь мы в состоянии доказать следующую теорему.

Теорема 32. *Множество матриц $A \subseteq M_2(\mathbb{K})$ размера 2×2 над кольцом Галуа $\mathbb{K}$, для которого $J(\mathbb{K})^2 = 0$, является образом многочлена из $\mathcal{K}_0 = \mathbb{K}_0\{x_0, x_1, \dots\}$ тогда и только тогда, когда оно устойчиво относительно эндоморфизмов $M_2(\mathbb{K})$, то есть, содержит 0 и самоподобно.*

Доказательство: Условие $J(\mathbb{K})^2 = 0$ эквивалентно $p^2 = 0$. Сопоставляя теперь Лемму 31, Лемму 27, Лемму 29 и Теорему 17, можно заметить, что мы умеем получать многочлен из $\mathcal{K}_0$ с образом $[a]'$ для любой не равной 0 по модулю p матрицы $a \in M$, если только она не скалярная. Для скалярных матриц, таким многочленом, очевидно, будет E, умноженный на соответствующий скаляр.

Матрицы, равные 0 по модулю p подобны в том и только в том случае, когда есть подобные матрицы, из которых они получаются умножением на p, поэтому для таких матриц соответствующие многочлены можно построить, умножая уже имеющиеся на p.

Таким образом, для всякой матрицы $a \in M$ есть многочлен из $\mathcal{K}_0$, имеющий образ $[a]'$. Используя Лемму 6 и то, что M — конечное множество, можно теперь для любого самоподобного множества, содержащего 0, «склеивая» многочлены, образы которых совпадают с классами подобия, входящими в это множество, получить многочлен, чей образ равен этому множеству.

Необходимость условий теоремы была получена ещё при доказательстве Леммы 1.□

Замечание 33. *Если $\mathbb{K} = \mathbb{Z}/8\mathbb{Z}$, то для всякого $a \in \mathbb{K}$ существует многочлен из $\mathcal{K}_0$, имеющий образ $\left[\begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix}\right]'$.*

Доказательство: Рассмотрим многочлен $xyx + y$, в котором первый аргумент пробегает класс $\left[\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\right]$. Подста-

вляя в качестве второго произвольную матрицу, получим

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b+c \\ c & d \end{pmatrix}.$$

Таким образом, след результата совпадает со следом исходной матрицы, а определитель изменился на c^2.

Поскольку $c^2 = 0$, 4 или 1 при $c \in \mathbb{Z}/8\mathbb{Z}$, мы можем, подставляя вместо y многочлен с образом $\left[\begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix}\right]'$, а вместо x — многочлен с образом $\left[\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\right]'$, и используя затем Лемму 15, получить многочлен, имеющий образом $\left[\begin{pmatrix} 0 & 1 \\ a+1 & b \end{pmatrix}\right]'$. Применяя эту конструкцию к уже имеющемуся многочлену с образом $\left[\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\right]'$ несколько раз, мы будем последовательно получать $\left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right]'$, $\left[\begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}\right]'$, и т.д.□

Объединяя результаты Замечаниея 33, лемм 27, 29 и Теоремы 17, легко видеть, что всякое множество вида $[a]'$, где a — нескалярная и не равная 0 по модулю 2 матрица из $M_2(\mathbb{Z}/8\mathbb{Z})$, является образом многочлена с коэффициентами из $\mathbb{Z}/8\mathbb{Z}$ и нулевым свободным членом. Дополняя этот результат рассуждениями, аналогичными проведённым в доказательстве Теоремы 32, получаем следующую Теорему

Теорема 34. *Подмножество $M_2(\mathbb{Z}/8\mathbb{Z})$ является образом многочлена из $(\mathbb{Z}/8\mathbb{Z})\{X\}$ с нулевым свободным членом тогда и только тогда, когда оно устойчиво относительно эндоморфизмов $M_2(\mathbb{Z}/8\mathbb{Z})$, то есть, содержит 0 и самоподобно.*

3.7. Алгоритм поиска многочленов с образами специального вида в матричных алгебрах над $\mathbb{Z}/p^n\mathbb{Z}$

В этом разделе M обозначает $M_2(\mathbb{K})$, а $\mathbb{K}$ — произвольное кольцо Галуа.

На основании Лемм 28 и 29, а также рассуждений, при помощи которых доказывались основные теоремы в предыдущем разделе, можно утверждать, что при $p \neq 2$ достаточно найти два многочлена из $\mathcal{K}_0$, имеющие в качестве образов в M множества $\left[\begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix}\right]'$ и $\left[\begin{pmatrix} 0 & 1 \\ \varepsilon p & 0 \end{pmatrix}\right]'$, чтобы доказать аналогичную теорему для подмножеств M : всякое самоподобное и содержащее 0 множество матриц 2×2 над кольцом Галуа $\mathbb{K}$ является образом многочлена из $\mathcal{K}_0$.

Покажем сначала, что такие многочлены стоит искать только среди многочленов, зависящих не более чем от трёх переменных.

Замечание 35. *Если существует многочлен f с нулевым свободным членом, имеющий в качестве образа в M нескалярный класс подобия, объединённый с $\{0\}$, то существует многочлен из $\mathcal{K}_0$ с тем же образом, зависящий не более чем от трёх переменных.*

Доказательство: Пусть f зависит от k переменных. Существует нескалярная матрица b, такая что $Im\, f = [b] \cup \{0\}$. Найдутся $a_1, \ldots, a_k \in M$, для которых $b = f(a_1, \ldots, a_k)$. Выберем четыре матрицы r_i, $0 \leq i \leq 3$ из M, включающие $r_0 = e$ (единицу M) и составляющие базис M как $\mathbb{K}$-модуля. Тогда $a_j = \sum_{0 \leq i \leq 3} c_{ji} r_i$, где все c_{ij} — элементы $\mathbb{K}$.

Рассмотрим теперь многочлен

$$g(x_1, x_2, x_3) = f(c_{00}e + \sum_{1 \le i \le 3} c_{0i}x_i, \ldots, c_{k0}e + \sum_{1 \le i \le 3} c_{ki}x_i).$$

Это многочлен с коэффициентами из $\mathbb{K}$, образ его, очевидно, содержит $b = g(r_1, r_2, r_3)$. Кроме того, $Im\, g$ является самоподобным множеством и подмножеством $Im\, f$. Поскольку $Im\, f = [b] \cup \{0\}$, образ g может быть равен $[b]$ или $Im\, f$. Далее, $g(0,0,0) \in Im\, g$ является скалярной матрицей, следовательно, $g \in \mathcal{K}_0$ и $Im\, g = Im\, f$.$\square$

Выделим следующее свойство многочленов, образы которых в M равны $\left[\begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix}\right]'$ и $\left[\begin{pmatrix} 0 & 1 \\ \varepsilon p & 0 \end{pmatrix}\right]'$

Замечание 36. *Если многочлен f из $\mathcal{K}_0$ имеет в M образ $\left[\begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix}\right]'$, а $g \in \mathcal{K}_0$ имеет в M образ $\left[\begin{pmatrix} 0 & 1 \\ \varepsilon p & 0 \end{pmatrix}\right]'$, то f^2 и g^2 — центральные многочлены в M. При этом $Im\, f^2 = \{0, p\}$ и $Im\, g^2 = \{0, \varepsilon p\}$.*

Доказательство: Это утверждение становится очевидным, если заметить, что всякая матрица a из $\left[\begin{pmatrix} 0 & 1 \\ b & c \end{pmatrix}\right]$ удовлетворяет тождеству $a^2 = ca + b$.$\square$

Замечание 37. *Если $f, g \in \mathcal{K}_0$ — центральные многочлены в M, $Im\, f = \{0, p\}$ и $Im\, g = \{0, \varepsilon p\}$ в M. Пусть также $f = f_1^2$ и $g = g_1^2$ по модулю тождеств M, причём образы f_1 и g_1 содержат, кроме $\{0\}$, только один класс подобия. Тогда в M $Im\, f_1$ равен $\left[\begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix}\right]'$ и $Im\, g_1$ $\left[\begin{pmatrix} 0 & 1 \\ \varepsilon p & 0 \end{pmatrix}\right]'$.*

Доказательство: Поскольку f и g не являются тождествами M, то f_1 и g_1 тоже не тождества. Кроме того, очевидно, что f_1 и g_1 не будут тождествами и по модулю p.

Рассмотрим ненулевой класс подобия, входящий в образ f_1. Если $0 \neq r \in Im\, f_1$, и $r \cong \left[\begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix}\right]$, то $r^2 = br + a \in Im\, f$. Следовательно, $b = 0$ и $a = 0$ или $a = p$. Поскольку образ f содержит p, остаётся только случай $a = p$. Если же r скалярно по модулю p, то r^2 — тоже. Так как, f_1 не тождество по модулю p, $r \neq 0(mod\, p)$, значит и $r^2 \neq 0(mod\, p)$.

Таким образом, $Im\, f_1$ может быть равен только множеству $\left[\begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix}\right]'$. Аналогично доказывается, что $Im\, g_1 = \left[\begin{pmatrix} 0 & 1 \\ \varepsilon p & 0 \end{pmatrix}\right]'$.□

Теперь очевидно, что существование в $\mathcal{K}_0$ многочленов с образами $\left[\begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix}\right]'$ и $\left[\begin{pmatrix} 0 & 1 \\ \varepsilon p & 0 \end{pmatrix}\right]'$ эквивалентно существованию центральных многочленов от не более чем трёх переменных со свойствами, перечисленными в Замечании 37.

Можно сформулировать следующий алгоритм, дающий для заданного кольца Галуа $\mathbb{K}$, удовлетворяющего условию $p = char(\overline{\mathbb{K}}) \neq 2$, ответ на вопрос, все ли самоподобные и содержащие 0 подмножества $M = M_2(\mathbb{K})$ являются образами многочленов из $\mathcal{K}_0$.

Сначала находим все центральные в M многочлены из $\mathcal{K}_0$, зависящие не более чем от трёх переменных. Выделяем те из них, которые принимают только значения 0 и p (или 0 и εp). Затем из полученных выбираем являющиеся квадратами в M. На последнем шаге надо определить, есть ли среди квадратных корней из оставшихся многочленов такие, что их образ содержит, помимо $\{0\}$, только один класс подобия. Если на каком-то шаге множество выбранных многочленов окажется пустым, то соответствующее множество

$\left[\begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix}\right]'$ (или $\left[\begin{pmatrix} 0 & 1 \\ \varepsilon p & 0 \end{pmatrix}\right]'$) даёт пример самоподобного содержащего 0 подмножества M, не являющегося образом многочлена. Если же и на последнем шаге указанное множество многочленов непусто, то, в силу предшествующих замечаний и лемм, всякое самоподобное и содержащее 0 подмножество M является образом многочлена из $\mathcal{K}_0$.

Литература

[1] Kaplansky I. Rings with a Polynomial Identity, Bull. Amer. Math. Soc., 1948, No. 54, p. 575–580.

[2] Amitsur S. Nil PI-Rings, Proc. Amer. Math. Soc., 1951, No. 2, p. 538–540.

[3] Amitsur S. The Identities of PI-Rings, Proc. Amer. Math. Soc., 1953, No. 4, p. 27–34.

[4] Amitsur S. On Rings with Identities, J. London Math. Soc., 1955, No. 30, p. 464–470.

[5] Levitzki J. A Theorem on Polynomial Identities, Proc. Amer. Math. Soc., 1950, No. 1, p. 334–341.

[6] Amitsur S., Levitzki J. Minimal Identities for Algebras, Proc. Amer. Math. Soc., 1950, No. 1, p. 449–463.

[7] Amitsur S., Levitzki J. Remarks on Minimal Identities for Algebras, Proc. Amer. Math. Soc., 1951, No. 2, p. 320–327.

[8] Procesi C. Rings with Polynomial Identities, Marcel Dekker, New York, 1973.

[9] Jacobson N. *P.I.*-Algebras, An Introduction, Lecture Notes in Mathematics, vol. 441. Springen-Verlag, Berlin — Heidelberg — New York, 1975.

[10] Rowen L. H. Polynomial identities in ring theory. Academic Press, New York, 1980.

[11] Kaplansky I. Problems in the theory of rings. In report of a conference on linear algebras. Nat. Acad. Sci. Nat. Res. Cons. publ. 502, 1957, p. 1–3.

[12] Латышев В. Н., Шмелькин А. Л. Об одной проблеме Капланского. Алгебра и Логика, 1969, т. 8, № 4, с. 447–448.

[13] Kaplansky I. "Problems in the theory of rings" revisited. Amer. Math. Monthly, 1970, No. 77, p. 445–454.

[14] Размыслов Ю. П. Об одной проблеме Капланского. Изв. АН СССР, Сер. мат. 1973, т. 37, № 3, с. 483–501.

[15] Formanek E. Central polynomials for matrix rings, Jour. of Algebra, 1972, No. 23, p. 129–133.

[16] Chuang C.-L. On ranges of polinomials in finite matrix rings. Proc. Amer. Math. Soc., October 1990, vol. 110(2), p. 293–302

[17] Radhgavendran R. Finite associative rings, Compositio math., 1969, vol. 21, No. 2, p. 195–229.

[18] Нечаев А. А. О строении конечных коммутативных колец с единицей. Мат. заметки, 1971, т. 10, № 6, с. 679–688.

[19] Нечаев А. А. Конечные кольца главных идеалов. Мат. сборник, 1973, т. 91, № 3, с. 350–366.

[20] Нечаев А. А. О подобии матриц над коммутативным локальным артиновым кольцом. Труды сем. им. И. Г. Петровского, 1983, вып. 9, с. 81–101.

[21] Nagata M. Local rings, Interscience tracts in pure and applied math., 13. New York, 1962.

[22] Jategaonkar A. V. Left principal ideal rings, Lecture Notes in math., vol. 123, 1970.

[23] Джекобсон Н. Строение колец. Москва, ИЛ, 1961.

[24] Джекобсон Н. Теория колец. Москва, ИЛ, 1947.

[25] Rowen L. H. Ring Theory, vol. II. Academic Press, New York, 1983.

[26] Ленг С. Алгебра. Москва, Мир, 1968.

[27] Пирс Р. Ассоциативные алгебры. Москва, Мир, 1986.

[28] Bahturin Yu. A., Mikhalev A. A., Petrogradsky V. M., Zaicev M. V. Infinite Dimensional Lie Superalgebras. de Gruyter Expositions in Mathematics 7, Berlin — New York, 1992.

[29] Vasilovsky S. Yu. $\mathbb{Z}$-graded polynomial identities of the full matrix algebra. Comm. in Algebra, 1998, vol. 26(2), p. 601–612

[30] Петров Е. Е. О классах сопряжённых элементов группы $SL(2, \mathbb{Z}/p^\lambda\mathbb{Z})$, $p \neq 2$. Изв. вузов. матем., 1980, № 8, с. 85–88.

[31] Бурбаки Н. Алгебра. Модули, кольца, формы. Москва, Наука, 1966.

Публикации автора по теме диссертации

[32] Кулямин В. В. Об образах многочленов в конечных кольцах матриц. Фунд. и прикл. математика 1997, т. 3, вып. 2, с. 469–485.

[33] Кулямин В. В. Об образах многочленов в кольце $M_2(\mathbb{Z}/8\mathbb{Z})$. Фунд. и прикл. математика 2000, т. 6, вып. 1, с. 275–280.

[34] Кулямин В. В. Образы градуированных многочленов в кольцах матриц над конечными групповыми алгебрами. УМН 2000, т. 55, вып. 2, с. 141–145.

[35] Кулямин В. В. Образы многочленов в кольцах матриц над кольцами Галуа. Международный алгебраический семинар, Москва, 1999, с. 36–37.