ISSN 1512–1712

Академия Наук Грузии
Институт Кибернетики

СОВРЕМЕННАЯ МАТЕМАТИКА И ЕЕ ПРИЛОЖЕНИЯ

Том 13

АЛГЕБРА

Тбилиси
2004

СОВРЕМЕННАЯ МАТЕМАТИКА И ЕЕ ПРИЛОЖЕНИЯ

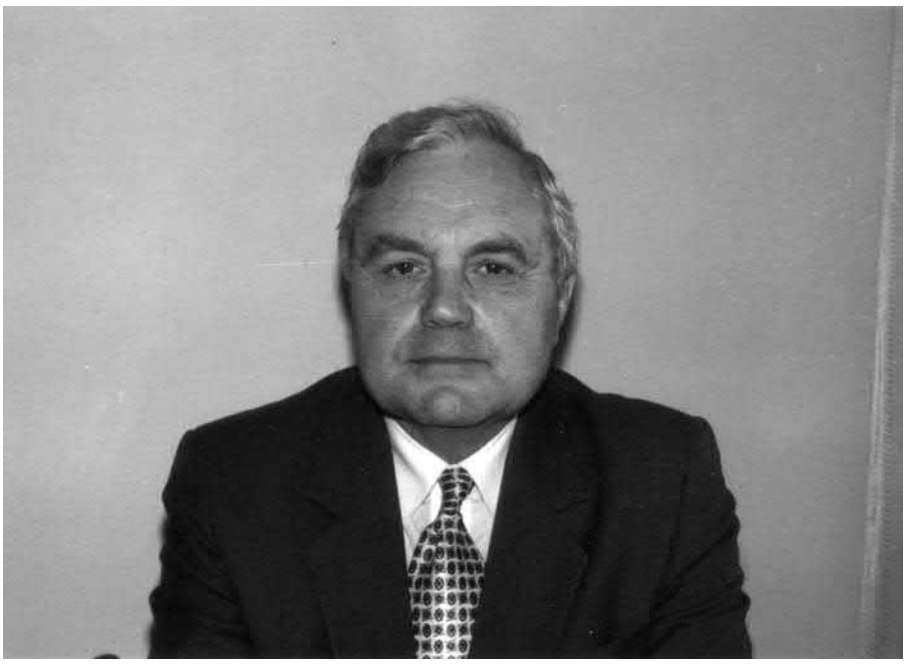
Том 13

АЛГЕБРА

Посвящается семидесятилетнему юбилею профессора Виктора Николаевича Латышева

კიბერნეტიკის ინსტიტუტი
თბილისი
2004

ОГЛАВЛЕНИЕ



Виктор Николаевич Латышев

Девятого февраля 2004 года исполняется 70 лет со дня рождения одного из ведущих российских математиков, ныне главы кафедры алгебры механико-математического факультета московского Университета, профессора Виктора Николаевича Латышева.

В. Н. Латышев своими работами, деятельностью созданной им научной школы оказал существенное влияние на развитие современной алгебры. Ему принадлежат фундаментальные результаты в изучении ассоциативных и лиевых алгебр с полиномиальными тождествами, в теории симплификации и стандартных базисов, в области алгоритмических проблем алгебры.

Любой из его учеников в первую очередь непременно отметит неповторимую атмосферу творчества, доброжелательности и одновременно требовательности, созданную на кафедре стараниями Виктора Николаевича, его талантом и мудростью.

В. Н. Латышев родился в 1934 г. в Москве, окончил механико-математический факультет МГУ в 1958 г. В 1961 г. после окончания аспирантуры начал свой преподавательский путь на кафедре высшей алгебры МГУ. В 1979 г. после защиты докторской диссертации он становится профессором этой кафедры, с 1992 г. — заместителем заведующего, а в 2001 г. Виктор Николаевич возглавил кафедру высшей алгебры.

Научные исследования В. Н. Латышева были начаты работами по теории алгебр Ли и ассоциативных алгебр с полиномиальными тождествами. Исследования В. Н. Латышева продолжили линию, начатую работами А. И. Мальцева и А. И. Ширшова, который являлся его научным руководителем. Класс алгебр с полиномиальными тождествами, или PI-алгебр, является естественным обобщением классических случаев коммутативных и конечномерных алгебр. В теории PI-алгебр в центре внимания на протяжении многих лет была проблема Шпехта, сформулированная в 1950 г.: будут ли тождества произвольной ассоциативной алгебры следовать из конечного числа тождеств?

На другом языке, будет ли произвольный T-идеал в свободной ассоциативной алгебре (или соответствующее ему многообразие алгебр) конечно базируемым?

Надо сказать, что в большинстве других алгебраических структур (например, в группах) аналогичная проблема решается отрицательно. Специфика класса ассоциативных колец и алгебр заключается в том, что многие общие проблемы в нем решаются положительно. Ко времени начала научной работы В. Н. Латышева в области PI-алгебр известны были лишь отдельные положительные результаты в частных случаях. Например, если T-идеал содержит тождество лиевой нильпотентности третьей степени, то он конечно базируем. Этот результат был обобщен В. Н. Латышевым для случая лиевой нильпотентности произвольной степени.

Поскольку не видно было подходов к решению проблемы Шпехта в общем случае, интересно было найти достаточно большие классы многообразий, в которых проблема Шпехта решается положительно. Прежде всего, наиболее интересен случай многообразий алгебр над полем нулевой характеристики, порожденных конечно порожденной алгеброй. В теории PI-алгебр определено понятие сложности T-идеала: это максимальное n такое, что T-идеал содержится в идеале тождеств алгебры матриц размера n. Многообразия сложности 1 называют нематричными многообразиями, поскольку они содержат тождество, которое не выполняется в алгебре матриц размера 2.

Нематричные многообразия представляют собой хотя и наиболее простой, но тем не менее достаточно общий класс многообразий, в котором проявляются все закономерности, присущие самому общему случаю. Поэтому наиболее серьезным продвижением в направлении положительного решения проблемы Шпехта явился следующий результат В. Н. Латышева: любое нематричное многообразие над полем нулевой характеристики, порожденное конечно-порожденной алгеброй, конечно базируемо. Этот результат составил основу его докторской диссертации. Доказательство этого результата дает больше, чем просто шпехтовость таких многообразий: фактически, в нем содержится классификация нематричных многообразий конечного базисного ранга.

Впоследствии проблема Шпехта для алгебр над полем нулевой характеристики и для конечно-порожденных алгебр над полем характеристики p была решена положительно. Решение проблемы Шпехта следует считать результатом коллективной работы многих математиков: В. Н. Латышева, Ю. П. Размыслова, А. Р. Кемера, А. Я. Белова и др.

Следует отметить и методическую работу В. Н. Латышева в этой области, связанную с нахождением ясных и изящных доказательств известных фактов. Так, принадлежащее Латышеву доказательство теоремы Регева о росте PI-алгебр входит во многие монографии. При изучении нематричных многообразий В. Н. Латышев предложил канонический базис в свободной алгебре, который оказался более удобным, чем использовавшийся до этого базис Холла. Наконец, во многих работах Латышева рассматривается связь между ассоциативными алгебрами и алгебрами Ли. Например, он ввел класс SPI-алгебр Ли, т.е. алгебр Ли, которые вкладываются в ассоциативные PI-алгебры. Впоследствии Ю. А. Бахтурин показал, что на класс SPI-алгебр Ли переносится большинство свойств конечномерных алгебр Ли. В теории универсальных обертывающих алгебр, как продемонстрировал В.Н.Латышев, хорошо работает техника базисов Гребнера (можно отметить красивое доказательство теоремы Пуанкаре—Биркгофа—Витта, а также результат Латышева об отсутствии нетривиальных PI-подалгебр в универсальных обертывающих в случае поля нулевой характеристики).

В более поздний период научной деятельности Виктора Николаевича выделилась вторая большая область его интересов, связанная с комбинаторными вопросами алгебры, если понимать под этим изучение свойств алгебр, заданных образующими и определяющими соотношениями, а также с некоторыми областями компьютерной алгебры. А именно, В. Н. Латышевым предложена обобщенная версия теории стандартных базисов (или базисов Гребнера), охватывающая большинство из ранее разработанных частных случаев. В книге по мономиальным алгебрам, написанной В. Н. Латышевым в соавторстве с А. Я. Беловым и В. В. Борисенко, собраны многие новые факты, проясняющие свойства этих алгебр, большинство из которых получено авторами. Обширен круг работ В. Н. Латышева и его учеников (Т. Гатевой-Ивановой, Н. Иыуду и др.), посвященных распознаваемости свойств алгебр, которые задаются соотношениями определенного типа. Примерами таких классов служат мономиальные алгебры, универсальные обертывающие алгебр Ли, некоторые

квадратичные алгебры, возникающие в физике, биномиальные квадратичные алгебры, некоторые геометрические кольца. Идеей В. Н. Латышева было выделение и изучение класса алгебр с ограниченной переработкой, являющегося аналогом класса групп с малыми сокращениями, над чем сейчас работают его ученики.

Нельзя не отметить педагогический талант Виктора Николаевича, удивительную стройность и продуманность его лекций. У большинства студентов, слушавших его лекции на 1-2 курсах, навсегда остается воспоминание об этой ясности и доходчивости.

Созданная Виктором Николаевичем кафедра алгебро-геометрических вычислений в Ульяновском филиале МГУ (ныне Ульяновский государственный университет) являет собой пример уникального коллектива, в котором живет атмосфера увлеченности и преданности науке.

От имени авторов сборника и всех, кто знает и любит В. Н. Латышева, мы поздравляем Виктора Николаевича и желаем ему неиссякающей бодрости, успехов во всех начинаниях и еще многих мгновений творческой радости.

В. В. Борисенко, Е. С. Голод, Н. К. Иыуду,
А. В. Михалев, А. Л. Шмелькин

Список научных трудов В. Н. Латышева

1. О делителях нуля в конечномерных антикоммутативных алгебрах// Изв. высш. уч. зав. — 1961. — *2*. — С. 100–108.
2. Об алгебрах с тождественными соотношениями// Докл. АН СССР. — 1962. — *146*, № 5. — С. 1003–1006.
3. Об алгебрах Ли с тождественными соотношениями// Сиб. мат. ж. — 1963. — *4*, № 4. — С. 821–829.
4. О делителях нуля и нильэлементах в алгебре Ли// Сиб. мат. ж. — 1963. — *4*, № 4. — С. 830–835.
5. Два замечания о PI-алгебрах Ли// Сиб. мат. ж. — 1963. — *4*, № 5. — С. 1120–1121.
6. О выборе базы в одном Т-идеале// Сиб. мат. ж. — 1963. — *4*, № 5. — С. 1122–1127.
7. О конечной порожденности Т-идеала с элементом $[x_1, x_2, x_3, x_4]$// Сиб. мат. ж. — 1965. — *4*, № 6. — С. 1432–1434.
8. Обобщение теоремы Гильберта о конечности базисов// Сиб. мат. ж. — 1966. — *7*, № 6. — С. 1422–1424.
9. Об одной проблеме Капланского// Алгебра и логика. — 1969. — *8*, № 4. — С. 447–448 (в соавторстве с А. Л. Шмелькиным).
10. О шпехтовости некоторых многообразий ассоциативных алгебр// Алгебра и логика. — 1969. — *8*, № 4. — С. 660–673.
11. Шпехтовость Т-идеала $T = [x_1, \ldots, x_{n-2}, [x_{n-1}, x_n]]$// Докл. АН СССР. — 1972. — *207*, № 4. — С. 777–780.
12. К теореме Регева о тождествах тензорного произведения PI-алгебр// Усп. мат. наук. — 1972. — *27*, № 4. — С. 213–214.
13. О некоторых многообразиях ассоциативных алгебр// Изв. АН СССР. — 1973. — *37*, № 5. — С. 1010–1037.
14. Алгебры с тождественными соотношениями// в сб.: Кольца II. — Ин-т математики СО АН СССР, 1973. — С. 29–36.
15. Булевы матрицы и тождества// Усп. мат. наук. — 1975. — *31*, № 3. — С. 189–198.
16. Частично упорядоченные множества и нематричные многообразия ассоциативных алгебр// Алгебра и логика. — 1976. — *18*, № 1. — С. 53–70.
17. Частично упорядоченные множества и нематрич-ные тождества ассоциативных алгебр// III Всесоюзный симпозиум по теории колец, алгебр и модулей/ Тезисы сообщений. — Тарту, 1976.

18. Алгебра с полиномиальными тождествами/ Мат. энциклопедия. — М., 1976.
19. Т-идеал/ Мат. энциклопедия. — М., 1976.
20. Конечная базируемость тождеств некоторых колец// Усп. мат. наук. — 1977. — *32*, № 4. — С. 259–260.
21. О сложности нематричных многообразий ассоциативных алгебр, I// Алгебра и логика. — 1977. — *16*, № 2. — С. 149–183.
22. О сложности нематричных многообразий ассоциативных алгебр, II// Алгебра и логика. — 1977. — *16*, № 2. — С. 184–199.
23. О сложности нематричных многообразий ассоциативных алгебр// XIV Всесоюзная алгебраическая конференция/ Тезисы сообщений. — Новосибирск, 1977.
24. Многообразия ассоциативных алгебр// Всесоюзная конференция по многообразиям алгебраических систем/ Тезисы докладов. — Барнаул.
25. Нематричные многообразия ассоциативных алгебр// Мат. заметки. — 1980. — *27*, № 1. — С. 147–156.
26. Об универсальном дифференцировании свободной алгебры// в кн.: Алгебра. — Изд-во МГУ, 1980. — С. 50–52.
27. Об устойчивых идеалах тождеств// XVI Всесоюзная алгебраическая конференция/ Тезисы сообщений. — Ленинград, 1981.
28. Устойчивые идеалы тождеств// Алгебра и логика. — 1981. — *20*, № 5. — С. 563–571.
29. Памяти А. И. Ширшова// Усп. мат. наук. — 1981. — *36*, № 5 (221). — С. 153–157 (с соавторами).
30. Коммутативность PI-алгебр полиномиального типа// в кн.: Алгебра. — Изд-во МГУ, 1982. — С. 86–95.
31. Практикум по алгебре. — Изд-во МГУ, 1983 (с соавторами).
32. Сборник задач по алгебре. Вып. 1. Основы алгебры. — Изд-во МГУ, 1983 (с соавторами).
33. Построение канонического симплификатора в модулях над кольцами полиномов// Вестн. КГУ. — 1985. — *27*. — С. 65–67.
34. Об алгоритме равенства в лиево нильпотентных ассоциативных алгебрах// Вестн. КГУ. — 1985. — *27*. — С. 67–69.
35. Сравнение сложностей некоторых алгебраических алгоритмов// в сб.: Выч. инварианта в теории алгебраических систем. — Новосибирск: СО АН СССР, 1987. — С. 80–90.
36. Комбинаторная теория колец. Сложность алгебраических алгоритмов. — Изд-во МГУ, 1987.
37. Сборник задач по алгебре. — Наука, 1987 (с соавторами).
38. Комбинаторная теория колец. Стандартные базисы. — Изд-во МГУ, 1988.
39. On the recognizable properties of associative algebras// J. Symb. Comp. — 1988. — *6*. — С. 371–388 (соавтор Т. Гатева-Иванова).
40. On the standard finite presented algebras// Inst. Math. Bulg. Acad. Sci. — 1990 (соавтор Т. Гатева-Иванова).
41. Линейная алгебра и геометрия/ Учебное пособие. — Ульяновск, 1990.
42. Results of A. I. Shirshov and his school// Международная конференция по алгебре/ Тезисы докладов, 1991 (с соавторами).
43. Выпуклые многогранники и линейное программирование/ Учебное пособие. — Ульяновск, 1992.
44. Об одном примере квадратичной полугруппы// III Междунар. конференция по алгебре/ Сборник тезисов. — Красноярск, 1993.
45. Общая теория исключения и некоторые ее приложения// Алгебраические структуры и теория сингулярных возмущений/ Материалы зимней мат. школы (25–30 января 1993 г.). — М., 1993.
46. О распознавании делителей нуля/ в кн.: Фундаментальные проблемы математики и механики. — Изд-во МГУ, 1994.
47. Сборник задач по алгебре. Изд. 2. — М.: Факториал, 1995 (с соавторами).

48. Замечание о центральных элементах разрешимых алгебр// Алгебраические структуры и теория сингулярных возмущений/ Материалы зимней мат. школы (25–30 января 1996 г.). — М., 1996.
49. Замечание о центральных элементах разрешимых алгебр// Математические методы и приложения/ Труды 3 математических чтений МГСУ (24–29 января 1995 г.). — М.: 1995. — С. 41–43.
50. Стандартные базисы и проблема равенства в многообразиях алгебр// Математические методы и приложения. — М.: МГСУ, 1996. — С. 69-72.
51. Lie nilpotency recognition and word problem// First International Tainan–Moscow Algebra Workshop. — Berlin, New York, 1996. — С. 237–241.
52. Some estimations for Groebner bases of ideals in Noetherian algebras// Тр. Междунар. конф. по алгебре, посвященной памяти Д. К. Фаддеева. — СПб: ПОМИ, 1997. — С. 81.
53. Отрицательные утверждения о стандартных базисах// Математические методы и приложения/ Труды 6 математических чтений МГСУ. — М.: 1998. — С. 167–170.
54. Распознавание тождеств в факторах универсальных обертывающих алгебр Ли// Международный алгебраический семинар/ Тезисы докладов. — М.: МГУ, 1999. — С. 37–38.
55. General version of standard bases in linear structures// Int. algebr. conf. dedicated to memory of A. G. Kurosh. — Moscow, 2000. — С. 215–227.
56. Combinatorical complexity of Groebner bases// Jour. Math. Sci. — Conf. Math., 1999. — С. 156–160.
57. Распознавание нематричных тождеств в факторах универсальных обертывающих алгебр Ли// Математические методы и приложения. — М.: МГСУ, 2000. — С. 68–69.
58. Сборник задач по алгебре. Изд. 3. — М.: Физматлит, 2001 (с соавторами).
59. Производные структуры алгебр со строгой фильтрацией// Математические методы и приложения/ Труды 9 математических чтений МГСУ. — М., 2002. — С. 123–127.
60. An improved version of standard bases. Formal power series and algebraic combinatorics// Proc. 12 Int. Conf., FPSAC'00, Moscow, June 2000. — С. 496–506.
61. Canonization and standard bases of filtered structures// Lie algebras, rings, and related topics. — Hong Kong: Sprinder-Verlag, 2000. — С. 61–80.
62. Алгебры со строгой фильтрацией и стандартные базисы// Тр. мат. центра им. Н. И. Лобачевского. — Казань: ДАС, 2001. — *12*. — С. 3–18.
63. Мономиальные алгебры// Итоги науки и техники. Современная математика и ее приложения. Тематические обзоры. — М.: ВИНИТИ, 2002. — *26*. — С. 35–214 (соавторы А. Я. Белов, В. В. Борисенко). Пер. на англ. яз.: Monomial Algebras// J.Math. Sci. — 1997. — *87*, № 3. — С. 3463–3575.
64. О сумме локально разрешимых идеалов алгебр Ли// Вестн. Моск. ун-та. Сер. 1. Мат., мех. — 2003. — *3*. — С. 29–32 (соавторы А. В. Михалев, С. А. Пихтильков).
65. Алгоритмическое распознавание полиномиальных тождеств// Математические вопросы кибернетики. — М.: 2002. — *11*. — С. 5–15.
66. General version of standard basis and its application to T-ideal// Тр. Междунар. конф. по алгебре. — Красноярск, 2003.

Современная математика и ее приложения. Том 13 (2004). С. 8–23

УДК 512.55

ПЕРЕСТАНОВОЧНЫЕ МОДУЛИ КОНЕЧНЫХ (АФФИННЫХ) ЛИНЕЙНЫХ ГРУПП

© 2004 г. **К. АБДУХАЛИКОВ**

Аннотация. Изучены перестановочные представления конечных полных линейных и аффинных групп на множестве векторов стандартного модуля. Перестановочные модули рассматриваются над полями и локальными кольцами.

СОДЕРЖАНИЕ

1. Введение

Пусть $q = p^t$ — степень простого числа и $V = \mathbb{F}_q^m$ — m-мерное векторное пространство над полем $\mathbb{F}_q$ из q элементов. Пусть $G_m = AGL_m(q) = V \cdot GL_m(q)$ — аффинная полная линейная группа степени m. Пусть R_p — кольцо целых элементов в неразветвленном расширении поля p-адических чисел $\mathbb{Q}_p$ со свойством $R_p/pR_p \cong \mathbb{F}_q$. Группа G_m действует на V (дважды транзитивно); следовательно, она действует на групповом кольце $\mathcal{A} = R_p[V]$. Нашей целью является изучение структур $GL_m(q)$- и $AGL_m(q)$-подмодулей модуля $\mathcal{A}$. Это исследование имеет несколько важных следствий. Во-первых, с помощью теории Галуа мы получаем комбинаторное описание G_m-инвариантных подрешеток естественных G_m-перестановочных решеток $A = \mathbb{Z}_p[V]$ и $\mathbb{Z}[V]$ (описание инвариантных решеток в $\mathbb{Z}[V]$ является локальной проблемой, см. подробнее в [2]). Этот набор решеток включает в себя множество унимодулярных решеток с интересными свойствами. Важным примером является то, что знаменитая решетка Барнса—Уолла может быть весьма просто реализована такой конструкцией.

Во-вторых, редукцией по модулю p мы получаем результаты, относящиеся к теории кодирования. Расширенный циклический код длины p^n (т.е. инвариантный относительно $GL_1(p^n)$) называется аффинно инвариантным, если он инвариантен относительно группы V. Такие коды были охарактеризованы в [18]. Этот результат был позже передоказан в [15] с помощью групповых алгебр. Далее, известно [13], что перестановочная группа $\mathrm{Per}(C)$ аффинно инвариантного кода C является либо симметрической группой $\mathrm{Sym}(p^n)$, либо знакопеременной группой $\mathrm{Alt}(p^n)$, $p = 2$, либо удовлетворяет условию

$$AGL_m(p^t) \subseteq \mathrm{Per}(C) \subseteq A\Gamma L_m(p^t)$$

с некоторым числом m, $n = mt$, где

$$A\Gamma L_m(p^t) = AGL_m(p^t) \cdot \mathrm{Gal}(\mathbb{F}_{p^t}/\mathbb{F}_p)$$

является полуаффинной полной линейной группой. Кроме того, группа автоморфизмов аффинно инвариантного кода C над полем F может быть легко получена из перестановочной группы [14]: $\mathrm{Aut}(C) \cong F^* \times \mathrm{Per}(C)$. Следовательно, описание $AGL_m(p^t)$-инвариантных кодов решает вопрос вычисления групп автоморфизмов аффинно инвариантных кодов. Этот результат был получен Дельсартом [16]; он дал необходимое и достаточное условие (в терминах определяющих множеств) инвариантности кодов относительно группы $GL_m(p^t)$. Недавно в [13] было найдено другое

ISSN 1512–1712

условие, эквивалентное условию Дельсарта. В [9] мы дали новое подробное описание $AGL_m(p^t)$-инвариантных кодов и использовали эти результаты в [4, 7] для получения простого описания определяющих множеств таких кодов.

В-третьих, из описания R_pG_m-инвариантных подмодулей в $\mathcal{A}$ с помощью теории Галуа можно получить описание $\mathbb{Z}_pG_m$-инвариантных подмодулей в A, и, следовательно, описание G_m-инвариантных подмодулей (кодов) в A/p^kA над кольцом $\mathbb{Z}_p/p^k\mathbb{Z}_p \cong \mathbb{Z}/p^k\mathbb{Z}$. В последнее время возрастает интерес к кодам над $\mathbb{Z}/p^k\mathbb{Z}$, в частности, над $\mathbb{Z}/4\mathbb{Z}$; было показано, что коды над $\mathbb{Z}/p^k\mathbb{Z}$ представляют собой систематическое средство для построения хороших бинарных кодов. Например, знаменитые коды Кердока и Препараты являются нелинейными бинарными кодами, которые содержат больше кодовых слов, чем любые другие сравнимые линейные коды, известные к настоящему времени. Недавно было показано [17], что коды Кердока и Препараты могут быть построены как бинарные образы линейных кодов над $\mathbb{Z}/4\mathbb{Z}$ относительно некоторого отображения, называемого отображением Грея. Этот факт стимулировал исследования линейных кодов над $\mathbb{Z}/4\mathbb{Z}$. Коды Кердока и Препараты, рассматриваемые как линейные коды (модули) над $\mathbb{Z}/4\mathbb{Z}$, являются аналогами классических кодов Рида—Маллера: они имеют размерность (ранг) p^n и инвариантны относительно аффинной группы G_1. Алгебраическая структура перестановочного модуля над $\mathbb{F}_qGL_m(q)$ изучена в [11]. Нам требуется более детальное исследование, которое проведено в разделе 2. Перестановочные модули и решетки для некоторых других групп рассмотрены также в [8, 20, 21].

Описание инвариантных подмодулей приведено в разделе 3 (см. теоремы 3.2, 3.3). Частные случаи $m = 1$ и $t = 1$ были подробно рассмотрены в [5, 6]. Аналогичные конструкции решеток изучены в [1–3, 19]. Результаты работы [9] использованы в [4, 7] для описания $AGL_m(q)$-инвариантных кодов над кольцами $\mathbb{Z}/p^k\mathbb{Z}$.

Результаты этого исследования получены при содействии фонда Александра фон Гумбольдта. Я благодарен профессору Р. Шарлау за стимулирующие обсуждения и гостеприимство.

2. Предварительные рассмотрения

Рассмотрим групповое кольцо $\mathcal{A} = R_p[V]$ в виде

$$\mathcal{A} = \left\{ \sum_{v\in V} a_v X^v \;\middle|\; a_v \in R_p \right\}.$$

Естественное действие группы $G_m = AGL_m(q) = V \cdot GL_m(q)$ на $\mathcal{A}$ определено следующим образом:

$$\begin{aligned} \widehat{u}(X^v) &= X^{u+v}, \qquad u \in V, \\ \widehat{g}(X^v) &= X^{gv}, \qquad g \in GL_m(q). \end{aligned}$$

Таким образом, проблема описания G_m-инвариантных R_p-подмодулей модуля $\mathcal{A}$ эквивалентна проблеме описания $GL_m(q)$-инвариантных идеалов кольца $\mathcal{A}$. Отображение Фробениуса σ на $\mathbb{F}_q \cong R_p/pR_p$ может быть продолжено единственным образом до отображения из R_p в R_p; тогда мы имеем

$$A = \{a \in \mathcal{A} \mid \widehat{\sigma}(a) = a\},$$

где действие отображения σ на $\mathcal{A}$ определено формулой

$$\widehat{\sigma}\left(\sum a_v X^v \right) = \sum \sigma(a_v) X^v.$$

Начнем с изучения G_m-модуля $\mathcal{A}/p\mathcal{A}$ над $\mathbb{F}_q \cong R_p/pR_p$. Для этого введем векторное пространство

$$\mathcal{F} = \left\{ \sum_{v\in V} a_v X^v \;\middle|\; a_v \in \mathbb{F}_q \right\}$$

над полем $\mathbb{F}_q$. Нашей первой целью является описание $\mathbb{F}_q$-подпространств в $\mathcal{F}$, инвариантных относительно группы $G_m = AGL_m(q)$. Имеются две интерпретации элементов модуля $\mathcal{F}$: как функций из V в $\mathbb{F}_q$ и как элементов групповой алгебры. Как функция, элемент $\sum a_v X^v$ отображает $v \in V$ в элемент a_v. В пп. 2.1 и 4.1 мы опишем структуру $\mathcal{F}$ как множества функций и как групповой

алгебры соответственно. Оказывается, что реализация функциями более подходит для изучения инвариантности относительно линейной группы $GL_m(q)$, а реализация групповой алгеброй более подходит для изучения инвариантности относительно группы V аффинных сдвигов.

2.1. Структура пространства $\mathcal{F}$ функций над аффинной группой. Рассмотрим полиномиальные функции

$$x_0^{i_0}\cdots x_{m-1}^{i_{m-1}} = \sum_{\alpha_0,\dots,\alpha_{m-1}\in\mathbb{F}_q} \alpha_0^{i_0}\cdots\alpha_{m-1}^{i_{m-1}} X^{\alpha_0 e_0+\cdots+\alpha_{m-1}e_{m-1}}.$$

Поскольку $\alpha^q = \alpha$ при $\alpha\in\mathbb{F}_q$, полиномиальные функции могут быть редуцированы по модулю $x_s^q - x_s$. Мономы $x_0^{i_0}\cdots x_{m-1}^{i_{m-1}}$, $0\leqslant i_s\leqslant q-1$, $s=0,1,\dots,m-1$, образуют базис векторного пространства $\mathcal{F}$ над $\mathbb{F}_q$. В этом разделе мы опишем $AGL_m(q)$-инвариантные подпространства в терминах этих базисных мономов.

Определим модули

$$\mathcal{M}(\lambda_0,\dots,\lambda_{t-1}) = \Big\langle x_0^{i_{00}+i_{01}p+\cdots+i_{0,t-1}p^{t-1}}\cdots x_{m-1}^{i_{m-1,0}+i_{m-1,1}p+\cdots+i_{m-1,t-1}p^{t-1}} \;\Big|\; i_{0j}+i_{1j}+\cdots+i_{m-1,j}\leqslant\lambda_j,\ j=0,1,\dots,t-1\Big\rangle,$$

где

$$0\leqslant\lambda_j\leqslant m(p-1),\quad 0\leqslant i_{sj}\leqslant m(p-1).$$

Заметим, что, вообще говоря, мономы в этом определении могут не быть базисными (но мы можем редуцировать их до базисных). Легко видеть, что

$$\mathcal{M}(m(p-1),\dots,m(p-1)) = \mathcal{F},\qquad \mathcal{M}(0,\dots,0)=\langle 1\rangle,$$
$$\mathcal{M}(\lambda_0,\dots,\lambda_{t-1})\supseteq\mathcal{M}(\lambda_0,\dots,\lambda_j-1,\dots,\lambda_{t-1}).$$

Далее, если $i_{sj}>p-1$ при некоторых s, j, то

$$i_{s0}+\cdots+i_{sj}p^j+\cdots+i_{s,t-1}p^{t-1} = i_{s0}+\cdots+(i_{sj}-p)p^j+(i_{s,j+1}+1)p^{j+1}\cdots+i_{s,t-1}p^{t-1},$$

поэтому

$$\mathcal{M}(\lambda_0,\dots,\lambda_{t-1})\supseteq\mathcal{M}(\lambda_0,\dots,\lambda_j-p,\lambda_{j+1}+1,\dots,\lambda_{t-1}).$$

Теорема 2.1 (см. [9]). *Модуль $\mathcal{M}(\lambda_0,\dots,\lambda_{t-1})$ инвариантен относительно аффинной группы $AGL_m(q)$. Кроме того, любой $AGL_m(q)$-инвариантный подмодуль в $\mathcal{F}$ равен сумме некоторых модулей вида $\mathcal{M}(\lambda_0,\dots,\lambda_{t-1})$.*

Для любых целых $j\geqslant 0$ и s, d таких, что $0\leqslant s,d\leqslant m-1$, определим линейные преобразования δ_s^j и $\epsilon_{s,d}^j$ модуля $\mathcal{F}$ следующим образом:

$$\delta_s^j(x_0^{i_0}\cdots x_{m-1}^{i_{m-1}}) = \binom{i_s}{j} x_0^{i_0}\cdots x_s^{i_s-j}\cdots x_{m-1}^{i_{m-1}}, \tag{1}$$

$$\epsilon_{s,d}^j(x_0^{i_0}\cdots x_{m-1}^{i_{m-1}}) = \binom{i_s}{j} x_0^{i_0}\cdots x_s^{i_s-j}\cdots x_d^{i_d+j}\cdots x_{m-1}^{i_{m-1}}. \tag{2}$$

Напомним, что $\binom{i_s}{j} = 0$ при $i_s<j$. Следующая лемма взята из [10] (она также следует из результатов [11]).

Лемма 2.2. *Подпространство $\mathcal{M}\subseteq\mathcal{F}$ инвариантно относительно аффинной группы $AGL_m(q)$ тогда и только тогда, когда*

1) *$\mathcal{M}$ инвариантно относительно преобразований δ_s^j и $\epsilon_{s,d}^j$ при $s\neq d$, $0\leqslant s,d\leqslant m-1$, $0\leqslant j\leqslant q-1$, и*
2) *$\mathcal{M}$ порождено мономами.*

В частности, лемма утверждает, что если модуль $\mathcal{M}$ инвариантен относительно $AGL_m(q)$ и

$$x_0^{i_{00}+i_{01}p+\cdots+i_{0,t-1}p^{t-1}} x_1^{i_{10}+i_{11}p+\cdots+i_{1,t-1}p^{t-1}} \cdots x_{m-1}^{i_{m-1,0}+i_{m-1,1}p+\cdots+i_{m-1,t-1}p^{t-1}} \in \mathcal{M},$$

где

$$0 \leqslant i_{ab} \leqslant p-1, \quad 0 \leqslant a \leqslant m-1, \quad 0 \leqslant b \leqslant t-1,$$

и $i_{sj} > 0$ для некоторых s и j, то

$$x_0^{i_{00}+\cdots+i_{0,t-1}p^{t-1}} \cdots x_s^{i_{s0}+\cdots+(i_{sj}-1)p^j+\cdots+i_{s,t-1}p^{t-1}} \cdots x_{m-1}^{i_{m-1,0}+\cdots+i_{m-1,t-1}p^{t-1}} \in \mathcal{M},$$

$$x_0^{i_{00}+\cdots} \cdots x_s^{i_{s0}+\cdots+(i_{sj}-1)p^j+\cdots+i_{s,t-1}p^{t-1}} \cdots x_d^{i_{d0}+\cdots+(i_{dj}+1)p^j+\cdots+i_{d,t-1}p^{t-1}} \cdots x_{m-1}^{i_{m-1,0}+\cdots} \in \mathcal{M}.$$

Пусть $\bar{S} = \bigoplus\limits_{\lambda=0}^{m(p-1)} \bar{S}^\lambda$ обозначает срезанное полиномиальное кольцо

$$S(V^*)/(V^{*(p)}) \cong \mathbb{F}_q[x_0, \ldots, x_{m-1}]/(x_i^p)_{i=0}^{m-1}$$

и $\bar{S}^{(p^j)}$ обозначает то же кольцо, но переменные x_i заменены их p^j-ми степенями. Модуль $\bar{S}^{(p^j)}$ изоморфен j-му кручению Фробениуса модуля $\bar{S}$. Далее, модули

$$S(\lambda_0, \ldots, \lambda_{t-1}) = \bigotimes_{j=0}^{t-1} (\bar{S}^{\lambda_j})^{(p^j)}$$

являются простыми модулями над $GL_m(q)$ и над $SL_m(q)$ согласно теореме Стейнберга о тензорном произведении.

Теорема 2.3 (см. [9]). *Справедливы следующие утверждения.*

(i) *Модуль $\mathcal{M}(\lambda_0, \ldots, \lambda_{t-1})$ имеет единственный максимальный подмодуль*

$$\sum_{j=0}^{t-1} \mathcal{M}(\lambda_0, \ldots, \lambda_j - 1, \ldots, \lambda_{t-1}) + \sum_{j=0}^{t-1} \mathcal{M}(\lambda_0, \ldots, \lambda_j - p, \lambda_{j+1} + 1, \ldots, \lambda_{t-1}),$$

где индексы j рассматриваются по модулю t и предполагается, что

$$\mathcal{M}(\ldots, -1, \ldots) = 0, \quad \mathcal{M}(\ldots, m(p-1)+1, \lambda_{j+2}, \ldots) = \mathcal{M}(\ldots, (m-1)(p-1), \lambda_{j+2}+1, \ldots).$$

(ii) *Модуль $\mathcal{M}(\lambda_0, \ldots, \lambda_{t-1})$ неразложим как $AGL_m(q)$-модуль, максимальный полупростой фактормодуль которого изоморфен $S(\lambda_0, \ldots, \lambda_{t-1})$.*

2.2. Структура модуля $\mathcal{F}$ над линейной группой. Модуль $\mathcal{F}$ может быть разложен в прямую сумму $GL_m(q)$-подмодулей:

$$\mathcal{F} = \bigoplus_{k=0}^{q-1} \mathcal{F}^k,$$

$$\mathcal{F}^k = \Big\{ f : V \to \mathbb{F}_q \;\Big|\; f(\beta\alpha_0, \ldots, \beta\alpha_{m-1}) = \beta^k f(\alpha_0, \ldots, \alpha_{m-1}),\ \beta \in \mathbb{F}_q \Big\}.$$

В частности,

$$\mathcal{F}^k = \Big\langle x_0^{i_0} \cdots x_{m-1}^{i_{m-1}} \;\Big|\; i_0 + \cdots + i_{m-1} \equiv k \pmod{q-1},\ i_0 + \cdots + i_{m-1} > 0 \Big\rangle$$

при $k > 0$ и

$$\mathcal{F}^0 = \langle x_0^0 \cdots x_{m-1}^0 \rangle = \langle 1 \rangle.$$

Для k, $0 \leqslant k \leqslant q-1$, пусть $k = k_0 + k_1 p + \cdots + k_{t-1}p^{t-1}$ — его p-адическое представление, $0 \leqslant k_i \leqslant p-1$. Для $k > 0$ пусть $\mathcal{H}[k]$ обозначает множество всех целых t-строк $(r_0, \ldots, r_{t-1})$, удовлетворяющих условиям

1) $0 \leqslant r_j \leqslant m-1$,
2) $0 \leqslant k_j + p r_{j+1} - r_j \leqslant m(p-1)$ (индексы по модулю t).

Кроме того, пусть $\mathcal{H}[0]$ состоит из одной t-строки $(0,\dots,0)$.

Существует естественное частичное упорядочение в $\mathcal{H}[k]$: $(r_1,\dots,r_{t-1}) \leqslant (r'_1,\dots,r'_{t-1})$ тогда и только тогда, когда $r_j \leqslant r'_j$ для всех j. Далее, $\bar r < \bar r'$ тогда и только тогда, когда $\bar r \leqslant \bar r'$ и $\bar r \neq \bar r'$. Существует аналогичное естественное частичное упорядочение для t-строк $(k_0,\dots,k_{t-1})$, где $k = k_0+k_1p+\dots+k_{t-1}p^{t-1}$, $0 \leqslant k_i \leqslant p-1$, является p-адическим представлением k, $0 \leqslant k \leqslant q-1$.

Положим

$$\mathcal{M}[k](\bar r) = \mathcal{M}[k_0,\dots,k_{t-1}](r_0,\dots,r_{t-1}) = \mathcal{F}^k \cap \mathcal{M}(\dots, k_j + pr_{j+1} - r_j, \dots).$$

Предположим, что

$$f = x_0^{i_{00}+\dots+i_{0,t-1}p^{t-1}} \cdots x_{m-1}^{i_{m-1,0}+\dots+i_{m-1,t-1}p^{t-1}}, \quad i_{0j} + i_{1j} + \dots + i_{m-1,j} = k_j + pr_{j+1} - r_j$$

для всех $j = 0,1,\dots,t-1$. Если $0 \leqslant i_{sd} \leqslant p-1$ для всех s, d, то $f \in \mathcal{M}[k](\bar r)$. Далее, если $i_{sd} > p-1$ для некоторых s, d, то $f \in \mathcal{M}[k](r_0,\dots,r_d-1,\dots,r_{t-1}) \subseteq \mathcal{M}[k](\bar r)$. Следовательно,

$$\mathcal{M}[k](\bar r) = \sum_{\bar r' \leqslant \bar r} \Big\langle x_0^{i_{00}+\dots+i_{0,t-1}p^{t-1}} \cdots x_{m-1}^{i_{m-1,0}+\dots+i_{m-1,t-1}p^{t-1}} \;\Big|$$

$$i_{0j} + \dots + i_{m-1,j} = k_j + pr'_{j+1} - r'_j;\ 0 \leqslant i_{sd} \leqslant p-1 \Big\rangle.$$

Отметим, что

$$\mathcal{F}^k = \mathcal{M}[k](m-1,\dots,m-1).$$

Рассмотрим $\mathcal{H}[k]$ при $k = q-1$. Легко видеть, что если $(r_0,\dots,r_{t-1}) \in \mathcal{H}[q-1]$ и $r_j = m-1$ для некоторого j, то $(r_0,\dots,r_{t-1}) = (m-1,\dots,m-1)$. Кроме того, полагая

$$\mathcal{W} = \Big\langle 1 - (1-x_0^{q-1}) \cdots (1-x_{m-1}^{q-1}) \Big\rangle_{\mathbb{F}_q} = \Big\langle \sum_{v \neq 0} X^v \Big\rangle_{\mathbb{F}_q},$$

мы видим, что

$$\mathcal{F}^{q-1} = \mathcal{W} \oplus \mathcal{M}[q-1](m-2,\dots,m-2)$$

как прямая сумма $GL_m(q)$-подмодулей. Следовательно, имеем следующее разложение в прямую сумму $GL_m(q)$-подмодулей:

$$\mathcal{F} = \mathcal{W} \oplus \mathcal{M}[q-1](m-2,\dots,m-2) \oplus \bigoplus_{k=0}^{q-2} \mathcal{F}^k. \tag{3}$$

Все слагаемые (и композиционные факторы) не изоморфны за исключением $\mathcal{W} \cong \mathcal{F}^0$. Следующая теорема следует из результатов работы [11], определений модулей $\mathcal{M}(\bar\lambda)$ и $\mathcal{M}[k](\bar r)$, леммы 2.2 и теоремы 2.3.

Теорема 2.4. *Справедливы следующие утверждения.*

(i) *При $k \neq q-1$ любой неразложимый $GL_m(q)$-модуль в $\mathcal{F}^k$ равен некоторому модулю $\mathcal{M}[k](\bar r)$.*

(ii) *При $k = q-1$ любой неразложимый $GL_m(q)$-модуль в $\mathcal{M}[k](m-2,\dots,m-2)$ равен некоторому модулю $\mathcal{M}[k](\bar r)$, $\bar r \neq (m-1,\dots,m-1)$.*

(iii) *Любой $GL_m(q)$-подмодуль в $\mathcal{F}^k$ равен сумме некоторых модулей $\mathcal{M}[k](\bar r)$ и, возможно, $\mathcal{W}$.*

(iv) *$\mathcal{M}[k](\bar r) \subseteq \mathcal{M}[k](\bar r')$ если $\bar r \leqslant \bar r'$.*

(v) *Подмодуль $\mathcal{M}[k](\bar r)$ неразложим как $GL_m(q)$-модуль, максимальный полупростой фактор-модуль которого изоморфен $S(k_0 + r_1p - r_0, \dots k_{t-1} + r_0p - r_{t-1})$.*

(vi) *Если $\bar r \in \mathcal{H}(k)$, то $G_m\mathcal{M}[k](\bar r) = \mathcal{M}(k_0 + r_1p - r_0, \dots, k_{t-1} + r_0p - r_{t-1})$.*

(vii) *Модуль $\mathcal{M}(\lambda_0, \dots \lambda_{t-1}) \neq \mathcal{M}(0,\dots,0)$ равен $G_m\mathcal{M}[k](\bar r)$, где*

$$k > 0, \quad k \equiv \lambda_0 + \dots + \lambda_{t-1}p^{t-1} \pmod{q-1},$$

$$k = k_0 + k_1p + \dots + k_{t-1}p^{t-1}, \quad 0 \leqslant k_i \leqslant p-1,$$

$$r_j = \frac{1}{q-1}\left(\sum_{i=0}^{t-1} \lambda_{j+i}p^i - \sum_{i=0}^{t-1} k_{j+i}p^i\right).$$

Предыдущая теорема описывает $GL_m(q)$-инвариантные подмодули в $\mathcal{F}$. Теперь мы выясним, когда эти модули инвариантны также относительно группы V.

Теорема 2.5. *Подмодуль $\mathcal{M}$ модуля $\mathcal{F}$ инвариантен относительно $AGL_m(q)$ тогда и только тогда, когда он равен сумме нескольких модулей вида $\mathcal{M}[k](\bar{r})$ таких, что*

$$\mathcal{M}[k](\bar{r}) \subseteq \mathcal{M}, \quad \mathcal{M}[k](\bar{r}) \neq 0, \quad k_j > 0 \quad \Rightarrow \quad \mathcal{M}[\dots, k_{j-1}, k_j - 1, k_{j+1}, \dots](\bar{r}) \subseteq \mathcal{M}$$

и

$$\mathcal{M}[k](\bar{r}) \subseteq \mathcal{M}, \quad \mathcal{M}[k](\bar{r}) \neq 0, \quad k_j = k_{j+1} = \dots = k_{j+a-1} = 0, \quad k_{j+a} > 0, \quad a > 0 \quad \Rightarrow$$
$$\mathcal{M}[\dots, k_{j-1}, p-1, \dots, p-1, k_{j+a} - 1, k_{j+a+1}, \dots](\dots, r_j, r_{j+1} - 1, \dots, r_{j+a} - 1, r_{j+a+1}, \dots) \subseteq \mathcal{M}.$$

Доказательство. Необходимость. Пусть модуль $\mathcal{M}$ инвариантен относительно $AGL_m(q)$. Если $\mathcal{M}$ содержит моном $x_0^{q-1} \cdots x_{m-1}^{q-1}$, то $\mathcal{M} = \mathcal{F}$. Предположим, что $x_0^{q-1} \cdots x_{m-1}^{q-1} \notin \mathcal{M}$. Тогда

$$\mathcal{M} \subseteq \mathcal{M}[q-1](m-2, \dots, m-2) \oplus \bigoplus_{k=0}^{q-2} \mathcal{F}^k.$$

Но композиционные факторы $GL_m(q)$-модуля $\mathcal{M}[q-1](m-2, \dots, m-2) \oplus \bigoplus\limits_{k=0}^{q-2} \mathcal{F}^k$ не изоморфны, следовательно, согласно теореме 2.4, модуль $\mathcal{M}$ равен сумме нескольких модулей $\mathcal{M}[k](\bar{r})$. Если $\mathcal{M}[k](\bar{r}) \subseteq \mathcal{M}$, то

$$G_m \mathcal{M}[k](\bar{r}) = \mathcal{M}(k_0 + r_1 p - r_0, \dots, k_{t-1} + r_0 p - r_{t-1}) \subseteq \mathcal{M}.$$

Без потери общности можно предположить, что $j = 0$. Пусть $k_0 + pr_1 - r_0 > 0$. Если $k_0 > 0$, то

$$\mathcal{M}[k_0 - 1, k_1, \dots, k_{t-1}](\bar{r}) \subseteq \mathcal{M}(k_0 - 1 + pr_1 - r_0, \dots, k_{t-1} + pr_0 - r_{t-1}) \subseteq \mathcal{M}.$$

Если $k_0 = 0$, $k_1 > 0$, то $\mathcal{M}[p-1, k_1 - 1, k_2, \dots, k_{t-1}](r_0, r_1 - 1, r_2, \dots)$ — множество элементов вида

$$x_0^{i_{00} + i_{01} p + \dots + i_{0,t-1} p^{t-1}} x_1^{i_{10} + i_{11} p + \dots + i_{1,t-1} p^{t-1}} \cdots x_{m-1}^{i_{m-1,0} + i_{m-1,1} p + \dots + i_{m-1,t-1} p^{t-1}}$$

со свойством

$$\begin{gathered} i_{00} + i_{10} + \dots + i_{m-1,0} \leqslant (p-1) + p(r_1 - 1) - r_0, \\ i_{01} + i_{11} + \dots + i_{m-1,1} \leqslant (k_1 - 1) + pr_2 - (r_1 - 1), \\ \dots \\ i_{0,t-1} + i_{1,t-1} + \dots + i_{m-1,t-1} \leqslant k_{t-1} + pr_0 - r_{t-1}. \end{gathered}$$

Поэтому

$$\mathcal{M}[p-1, k_1 - 1, k_2, \dots, k_{t-1}](r_0, r_1 - 1, r_2, \dots) \subseteq$$
$$\subseteq \mathcal{M}((p-1) + p(r_1 - 1) - r_0, k_1 - 1 + pr_2 - (r_1 - 1), k_2 + pr_3 - r_2, \dots) \subseteq \mathcal{M}.$$

Если $k_0 + pr_1 - r_0 = 0$, то модули

$$\mathcal{M}[k_0 - 1, k_1, \dots, k_{t-1}](\bar{r}), \quad \mathcal{M}[p-1, k_1 - 1, k_2, \dots, k_{t-1}](r_0, r_1 - 1, r_2, \dots)$$

при $k_0 = 0, \dots$ равны нулю по определению.

Другие случаи могут быть рассмотрены аналогично.

Достаточность следует из следующих фактов:

$$G_m \mathcal{M}[k](\bar{r}) = \mathcal{M}[k](\bar{r}) + \sum_{j=0}^{t-1} \mathcal{M}(\dots, k_j + pr_{j+1} - r_j - 1, \dots) +$$
$$+ \sum_{j=0}^{t-1} \mathcal{M}(\dots, k_j + pr_{j+1} - r_j - p, k_{j+1} + pr_{j+2} - r_{j+1} + 1, \dots),$$

где

$$\mathcal{M}(\dots, k_j + pr_{j+1} - r_j - 1, \dots) =$$
$$= G_m\mathcal{M}[\dots, k_{j-1}, p-1, \dots, p-1, k_{j+a} - 1, \dots](\dots, r_{j+1} - 1, \dots, r_{j+a} - 1, \dots),$$
$$\mathcal{M}(\dots, k_j + pr_{j+1} - r_j - p, k_{j+1} + pr_{j+2} - r_{j+1} + 1, \dots) = G_m\mathcal{M}[k](\dots, r_j, r_{j+1} - 1, r_{j+2}, \dots).$$

Теорема доказана. □

3. Перестановочный модуль

В этом разделе мы изучим структуру $\mathcal{A}$ как $GL_m(q)$- и $AGL_m(q)$-модуля. Прежде всего, найдем разложение модуля $\mathcal{A}$ в прямую сумму $GL_m(q)$-подмодулей, которое может рассматриваться как поднятие разложения (3).

Группа $R_p^* = R_p \setminus pR_p$ обратимых элементов кольца R_p имеет единственную подгруппу, изоморфную $\mathbb{F}_q^*$. Эта подгруппа называется группой мультипликативных представителей и является множеством всех решений уравнения $x^{q-1} = 1$. Также она является множеством всех обратимых элементов кольца R_p конечного порядка. Представитель Тейхмюллера $\tilde{\alpha} \in R_p$ элемента $\alpha \in \mathbb{F}_q$ определен следующим образом: он равен нулю, если $\alpha = 0$, и при $\alpha \neq 0$ равен корню $(q-1)$-й степени из единицы в R_p, чей класс вычетов по модулю p равен α.

Определим

$$w = \sum_{v \in V} X^v - p^n X^0, \qquad \mathcal{N}[0] = R_p w,$$
$$\mathcal{N}[q-1] = \left\{ a = \sum_{v \neq 0} a_v X^v \in \mathcal{A} \;\middle|\; g(a) = a,\ g = \operatorname{diag}(\alpha, \dots, \alpha) \in GL_m(q) \right\},$$
$$\mathcal{N}[k] = \left\{ a \in \mathcal{A} \;\middle|\; g(a) = \tilde{\alpha}^{-k} a,\ g = \operatorname{diag}(\alpha, \dots, \alpha) \in GL_m(q) \right\}, \quad 0 < k < q-1.$$

Тогда имеем следующее разложение в прямую сумму $GL_m(q)$-подмодулей:

$$\mathcal{A} = \bigoplus_{k=0}^{q-1} \mathcal{N}[k].$$

Заметим, что

$$\mathcal{N}[0] + \mathcal{N}[q-1] = \left\{ a \in \mathcal{A} \;\middle|\; g(a) = a,\ g = \operatorname{diag}(\alpha, \dots, \alpha) \in GL_m(q) \right\}.$$

Далее, полагая

$$\mathcal{A}^0 = \left\{ \sum_{v \in V} a_v X^v \;\middle|\; a_v \in R_p,\ \sum_{v \in V} a_v = 0 \right\}, \qquad \mathcal{W} = R_p \sum_{v \neq 0} X^v, \qquad \mathcal{N}' = \mathcal{N}[q-1] \cap \mathcal{A}^0,$$

имеем

$$\mathcal{N}[q-1] = \mathcal{W} + \mathcal{N}';$$

поэтому можем записать

$$\mathcal{A} = \bigoplus_{k=0}^{q-1} \mathcal{N}[k] = \mathcal{W} \oplus \mathcal{N}' \oplus \bigoplus_{k=0}^{q-2} \mathcal{N}[k], \qquad \mathcal{A}^0 = \mathcal{N}' \oplus \bigoplus_{k=0}^{q-2} \mathcal{N}[k].$$

Следовательно, мы построили требуемое поднятие разложения (3). Отметим, что мы используем одинаковую букву $\mathcal{W}$ для модулей, порожденных элементом $\sum_{v \neq 0} X^v$ над $\mathbb{F}_q$ и над R_p, но это не должно привести к недоразумению. Значение $\mathcal{W}$ может быть определено единственным образом из контекста.

Пусть K — расширение степени t поля p-адических чисел такое, что $K \supset R_p$. Тогда $AGL_m(q)$-модуль $K\mathcal{A}$ разлагается в прямую сумму тривиального модуля K и модуля $K\mathcal{A}^0$. Поэтому мы можем ограничиться описанием G_m-инвариантных подмодулей в $\mathcal{A}^0$.

Лемма 3.1 ([9]). *Пусть $\mathcal{L}$ — G_m-инвариантный подмодуль в $\mathcal{A}^0$, $\mathcal{L} \not\subseteq p\mathcal{A}^0$. Тогда $\mathcal{L} \ni w$ и $\mathcal{L} \supset p^{mt}\mathcal{A}^0$. В частности, существует конечное число классов подобия G_m-инвариантных подмодулей в $\mathcal{A}^0$.*

Следующие две теоремы дают главный результат нашей работы.

Теорема 3.2. *Справедливы следующие утверждения.*

(i) *Для любого $\mathbb{F}_q GL_m(q)$-модуля $\mathcal{M}[\bar{k}](\bar{r}) \neq 0$ существует (единственный) минимальный $R_p GL_m(q)$-модуль*

$$\mathcal{N}[\bar{k}](\bar{r}) = \mathcal{N}[k](\bar{r}) \subseteq \mathcal{N}[k]$$

такой, что

$$(\mathcal{N}[k](\bar{r}) + p\mathcal{A})/p\mathcal{A} \cong (\mathcal{N}[k](\bar{r}) + p\mathcal{N}[k])/p\mathcal{N}[k] \cong \mathcal{M}[k](\bar{r}).$$

(ii) *Для этого модуля имеем*

$$\mathcal{N}[k](\bar{r}) \supseteq p^{d_0+\dots+d_{t-1}}\mathcal{N}[k](r_0+d_0,\dots,r_{t-1}+d_{t-1}),$$
$$(\mathcal{N}[k](\bar{r}) \cap p^d\mathcal{N}[k] + p^{d+1}\mathcal{N}[k])/p^{d+1}\mathcal{N}[k] \cong \sum_{d_0+\dots+d_{t-1}\leqslant d} \mathcal{M}[k](r_0+d_0,\dots,r_{t-1}+d_{t-1}).$$

(iii) *$R_p GL_m(q)$-модуль $\mathcal{N}[k](\bar{r})$ неразложим.*

(iv) $\widehat{\sigma}(\mathcal{N}[k_0,\dots,k_{t-1}](r_0,\dots,r_{t-1})) = \mathcal{N}[k_{t-1},k_0,\dots,k_{t-2}](r_{t-1},r_0,\dots,r_{t-2})$.

(v) *Любой $GL_m(q)$-инвариантный подмодуль в $\mathcal{A}^0$ равен сумме нескольких модулей вида $p^{l(k,\bar{r})}\mathcal{N}[k](\bar{r})$.*

В случае $\mathcal{M}[k](\bar{r}) = 0$ (что означает $\bar{r} \notin \mathcal{H}(k)$) положим $\mathcal{N}[k](\bar{r}) = 0$.

Теорема 3.3. *Подмодуль $\mathcal{N}$ в $\mathcal{A}^0$, $\mathcal{N} \not\subseteq p\mathcal{A}^0$, инвариантен относительно $AGL_m(q)$ тогда и только тогда, когда*

$$\mathcal{N} = \mathcal{N}[0] + \sum_{(k,\bar{r})\in D} p^{l(k,\bar{r})}\mathcal{N}[k](\bar{r}) + p^{mt}\mathcal{A}^0,$$

с условием, что

$$p^l\mathcal{N}[k](\bar{r}) \subseteq \mathcal{N}, \quad \mathcal{N}[k](\bar{r}) \neq 0, \quad k_j > 0 \quad \Rightarrow \quad p^l\mathcal{N}[\dots,k_{j-1},k_j-1,k_{j+1},\dots](\bar{r}) \subseteq \mathcal{N},$$
$$p^l\mathcal{N}[k](\bar{r}) \subseteq \mathcal{N}, \quad \mathcal{N}[k](\bar{r}) \neq 0, \quad k_j = k_{j+1} = \dots = k_{j+a-1} = 0, \quad k_{j+a} > 0, \quad a > 0 \quad \Rightarrow$$
$$\Rightarrow \quad p^{l+b}\mathcal{N}[\dots,k_{j-1},p-1,\dots,p-1,k_{j+a}-1,k_{j+a+1},\dots](\bar{r}') \subseteq \mathcal{N},$$

где

$$(\bar{r}') = (\dots,r_j,\max(r_{j+1}-1,0),\dots,\max(r_{j+a}-1,0),r_{j+a+1},\dots),$$
$$b = |\{r_i = 0 \mid i = j+1,\dots,j+a\}|.$$

Запишем предыдущие результаты для частного случая $m = 1$. В теории кодирования этот случай соответствует аффинно инвариантным расширенным циклическим кодам. Имеем $\mathcal{N}[k](\bar{r}) = \mathcal{N}[k]$ для всех $\bar{r}$, поскольку $(\bar{r}) = (0,\dots,0)$.

Следствие 3.4. *Пусть $m = 1$. Тогда справедливы следующие утверждения.*

(i) *$\mathcal{N}[k]$ является свободным модулем ранга 1 над R_p и*

$$\mathcal{N}[k]/p\mathcal{N}[k] \cong \mathcal{M}[k](0,\dots,0).$$

(ii) $\widehat{\sigma}(\mathcal{N}[k_0,\dots,k_{t-1}]) = \mathcal{N}[k_{t-1},k_0,\dots,k_{t-2}]$.

(iii) *Подмодуль $\mathcal{N}$ в $\mathcal{A}^0$, $\mathcal{N} \not\subseteq p\mathcal{A}^0$, инвариантен относительно $AGL_1(q)$ тогда и только тогда, когда*

$$\mathcal{N} = \mathcal{N}[0] + \sum_{\bar{k}\in D} p^{l(\bar{k})}\mathcal{N}[\bar{k}] + p^t\mathcal{A}^0,$$

с условием, что

$$p^l\mathcal{N}[k]\subseteq\mathcal{N},\quad \mathcal{N}[k]\neq 0,\quad k_j>0\quad\Rightarrow\quad p^l\mathcal{N}[\dots,k_{j-1},k_j-1,k_{j+1},\dots]\subseteq\mathcal{N},$$
$$p^l\mathcal{N}[k]\subseteq\mathcal{N},\quad \mathcal{N}[k]\neq 0,\quad k_j=k_{j+1}=\dots=k_{j+a-1}=0,\quad k_{j+a}>0,\quad a>0\quad\Rightarrow$$
$$\Rightarrow\quad p^{l+a}\mathcal{N}[\dots,k_{j-1},p-1,\dots,p-1,k_{j+a}-1,k_{j+a+1},\dots]\subseteq\mathcal{N}.$$

4. Доказательства

В этом разделе мы докажем теоремы 3.2 и 3.3. Мы будем использовать некоторые результаты из [9].

4.1. Структура групповой алгебры $\mathcal{F}$ над аффинной группой. В этом разделе мы напомним другую формулировку [9] результатов из раздела 2.1, используя тот факт, что элементы модуля $\mathcal{F}$ могут рассматриваться как элементы групповой алгебры.

Пусть $\mathcal{F}^{(j)}$ — идеал в кольце $\mathcal{F}$, порожденный элементами $(1-X^{v_1})\cdots(1-X^{v_j})$, $v_i\in V$. Имеем $AGL_m(q)$-инвариантную фильтрацию

$$\mathcal{F}=\mathcal{F}^{(0)}\supset\mathcal{F}^{(1)}\supset\mathcal{F}^{(2)}\supset\cdots\supset\{0\}.$$

Заметим, что $\mathcal{F}^{(1)}$ — единственный максимальный идеал алгебры $\mathcal{F}$. При $0\leqslant s\leqslant m-1$, $0\leqslant d\leqslant t-1$ введем элементы

$$Y_{sd}=\sum_{\alpha\in\mathbb{F}_q^*}\alpha^{-p^d}X^{\alpha e_s},\qquad q>2,$$
$$Y_{sd}=Y_s=X^{e_s}-1,\qquad q=2.$$

Лемма 4.1 ([9]). *Справедливы следующие утверждения*:

(i) $Y_{sd}\in\mathcal{F}^{(1)}$;

(ii) *элементы* $\prod\limits_{s=0}^{m-1}\prod\limits_{d=0}^{t-1}Y_{sd}^{i_{sd}}$, $0\leqslant i_{sd}\leqslant p-1$, *образуют* $\mathbb{F}_q$*-базис модуля* $\mathcal{F}$;

(iii) $(Y_{sd})^p=0$;

(iv) *подпространство* $\mathbb{F}_q\prod\limits_{s=0}^{m-1}\prod\limits_{d=0}^{t-1}Y_{sd}^{i_{sd}}$ *инвариантно относительно диагональной подгруппы группы* $GL_m(q)$ *и* $\operatorname{diag}(\alpha_1,\dots,\alpha_m)(Y_{sd})=\alpha_s^{p^d}Y_{sd}$;

(v) $\widehat{g}(Y_{sd})\equiv\sum\limits_{i=0}^{m-1}g_{is}^{p^d}Y_{id}\pmod{\mathcal{F}^{(2)}}$ *для* $g=(g_{ij})\in GL_m(q)$;

(vi) $\widehat{\sigma}^i(Y_{sd})=Y_{s,d+i}$ (*второй индекс по модулю* t).

Преимуществом базиса $\left\{\prod\limits_{s=0}^{m-1}\prod\limits_{d=0}^{t-1}Y_{sd}^{i_{sd}}\right\}$ является то, что он более подходит для изучения идеалов в $\mathcal{F}$. Подмодуль $\mathcal{M}\subseteq\mathcal{F}$ является идеалом тогда и только тогда, когда он инвариантен относительно умножений на элементы Y_{sd}. Отметим, что произведение $\prod\limits_{s=0}^{m-1}\prod\limits_{d=0}^{t-1}Y_{sd}^{i_{sd}}$ рассматривается как произведение в групповой алгебре $\mathcal{F}$. В частности, элемент Y_{sd}, рассматриваемый как функция, равен $x_s^{q-1-p^d}$ при $q>2$. Однако $Y_{sd}\cdot Y_{sd}=Y_{sd}^2\neq x_s^{q-1-2p^d}$.

Определим модули

$$\mathcal{R}(\lambda_0,\dots,\lambda_{t-1})=\Big\langle Y_{00}^{i_{00}}Y_{01}^{i_{01}}\cdots Y_{0,t-1}^{i_{0,t-1}}\cdots Y_{m-1,0}^{i_{m-1,0}}Y_{m-1,1}^{i_{m-1,1}}\cdots Y_{m-1,t-1}^{i_{m-1,t-1}}\;\Big|$$
$$\prod_{s=0}^{m-1}x_s^{(p-1-i_{s0})+\dots+(p-1-i_{s,t-1})p^{t-1}}\in\mathcal{M}(m(p-1)-\lambda_0,\dots,m(p-1)-\lambda_{t-1})\Big\rangle,$$

где $0 \leqslant \lambda_j \leqslant m(p-1)$, $0 \leqslant i_{sj} \leqslant p-1$. В частности,

$$\mathcal{R}(0,\dots,0) = \mathcal{F}, \quad \mathcal{R}(m(p-1),\dots,m(p-1)) = \left\langle \sum_{v\in V} X^v \right\rangle.$$

Имеем

$$\mathcal{R}(\lambda_0,\dots,\lambda_{t-1}) \supseteq \mathcal{R}(\dots,\lambda_{j-1},\lambda_j+1,\lambda_{j+1},\dots), \qquad \lambda_j < m(p-1),$$
$$\mathcal{R}(\lambda_0,\dots,\lambda_{t-1}) \supseteq \mathcal{R}(\dots,\lambda_j+p,\lambda_{j+1}-1,\dots), \qquad \lambda_{j+1} > 0.$$

Определим $GL_m(q)$-модули $\widehat{\mathcal{F}}$, $\widehat{\mathcal{F}}^k$, $\widehat{\mathcal{M}}(\bar\lambda)$, $\widehat{\mathcal{W}}$, где они соответственно равны $\mathcal{F}$, $\mathcal{F}^k$, $\mathcal{M}(\bar\lambda)$, $\mathcal{W}$ как множества и действие задано следующим образом:

$$g \circ f(x) = f({}^t g x).$$

Аналогично модулям $\bar S$ и $S(\lambda_0,\dots,\lambda_{t-1})$ из п. 2.1 определим модули

$$\tilde S = S(V)/(V^{(p)}), \quad \widehat S(\lambda_0,\dots,\lambda_{t-1}) = \bigotimes_{j=0}^{t-1} (\tilde S^{\lambda_j})^{(p^j)},$$

рассматривая V вместо V^*. Ясно, что подмодуль $\widehat{\mathcal{M}}(\lambda_0,\dots,\lambda_{t-1})$ неразложим как $AGL_m(q)$-модуль, максимальный полупростой фактормодуль которого изоморфен $\widehat S(\lambda_0,\dots,\lambda_{t-1})$.

Поскольку модуль $\mathcal{R}(m(p-1),\dots,m(p-1))$ имеет размерность 1, можно определить $GL_m(q)$-инвариантное спаривание

$$\mathcal{F}\times\mathcal{F} \to \mathbb{F}_q, \quad \widehat{\mathcal{F}}\times\widehat{\mathcal{F}} \to \mathbb{F}_q;$$

поэтому существуют следующие изоморфизмы $GL_m(p^t)$-модулей:

$$\widehat S(m(p-1)-\lambda_0,\dots,m(p-1)-\lambda_{t-1})^* \cong \widehat S(\lambda_0,\dots,\lambda_{t-1}) \cong$$
$$\cong S(\lambda_0,\dots,\lambda_{t-1})^* \cong S(m(p-1)-\lambda_0,\dots,m(p-1)-\lambda_{t-1}).$$

Теорема 4.2 (см. [9]). *Справедливы следующие утверждения.*

(i) *Подмодуль $\mathcal{R}(\lambda_0,\dots,\lambda_{t-1})$ неразложим как $AGL_m(q)$-модуль, максимальный полупростой фактормодуль которого изоморфен $\widehat S(\lambda_0,\dots,\lambda_{t-1}) \cong S(m(p-1)-\lambda_0,\dots,m(p-1)-\lambda_{t-1})$.*

(ii) *Для $AGL_m(q)$-инвариантного подмодуля $\mathcal{M}\subseteq\mathcal{F}$ имеем $\mathcal{M} = \mathcal{R}(\lambda_0,\dots,\lambda_{t-1})$ тогда и только тогда, когда $\mathcal{M} = \mathcal{M}(m(p-1)-\lambda_0,\dots,m(p-1)-\lambda_{t-1})$.*

(iii) *Любой $AGL_m(q)$-инвариантный подмодуль в $\mathcal{F}$ равен сумме некоторых модулей вида $\mathcal{R}(\lambda_0,\dots,\lambda_{t-1})$.*

(iv) *Для $AGL_m(q)$-инвариантного подмодуля $\mathcal{M}\subseteq\mathcal{F}$ имеем*

$$\mathcal{R} = \sum_{\bar\lambda\in D} \mathcal{M}(\bar\lambda)$$

тогда и только тогда, когда

$$\mathcal{M} = \sum_{\bar\lambda\in D} \mathcal{M}(m(p-1)-\lambda_0,\dots,m(p-1)-\lambda_{t-1}).$$

4.2. Структура группового кольца $\mathcal{A}$. В этом пункте мы опишем структуру кольца $\mathcal{A}$ с помощью специального базиса, который является поднятием базиса из леммы 4.1.

Пусть $\mathcal{A}^{(j)}$ — идеал кольца $\mathcal{A}$, порожденный элементами $(1-X^{v_1})\cdots(1-X^{v_j})$, $v_i\in V$. Следующая лемма описывает конструкцию нашего специального базиса (ср. с леммой 4.1).

Лемма 4.3 (см. [9]). *Существуют элементы $Z_{sd}\in\mathcal{A}$, $0\leqslant s\leqslant m-1$, $0\leqslant d\leqslant t-1$ со следующими свойствами*:

(i) $Z_{sd}\in\mathcal{A}^{(1)}$ *и* $Z_{sd}\equiv Y_{sd} \pmod{\mathcal{A}^{(2)}}$;

(ii) *элементы* $\prod_{s=0}^{m-1}\prod_{d=0}^{t-1} Z_{sd}^{i_{sd}}$, $0\leqslant i_{sd}\leqslant p-1$, *образуют R_p-базис модуля $\mathcal{A}$*;

(iii) $(Z_{sd})^p = -pZ_{s,d+1}$;

(iv) *подпространство* $R_p \prod_{s=0}^{m-1} \prod_{d=0}^{t-1} Z_{sd}^{i_{sd}}$ *инвариантно относительно диагональной подгруппы группы* $GL_m(q)$ *и*

$$\operatorname{diag}(\alpha_1, \dots, \alpha_m)(Z_{sd}) = \tilde{\alpha_s}^{p^d} Z_{sd};$$

(v) $\widehat{g}(Z_{sd}) \equiv \sum_{i=0}^{m-1} \tilde{g}_{is}^{p^d} Z_{id} \pmod{\mathcal{A}^{(2)}}$ *для* $g = (g_{ij}) \in GL_m(q)$;

(vi) $\widehat{\sigma}^i(Z_{sd}) = Z_{s,d+i}$ (*второй индекс по модулю* t).

Напомним, что модуль $\mathcal{L} \subseteq \mathcal{A}$ инвариантен относительно группы V тогда и только тогда, когда $\mathcal{L}$ — идеал кольца $\mathcal{A}$. Следовательно, согласно предыдущей лемме, $\mathcal{L}$ инвариантен относительно V тогда и только тогда, когда он инвариантен относительно умножений на элементы Z_{sd}.

Определим идеалы

$$\mathcal{L}(\lambda_0, \dots, \lambda_{t-1}) = \Big\langle Z_{00}^{i_{00}} Z_{01}^{i_{01}} \cdots Z_{0,t-1}^{i_{0,t-1}} \cdots Z_{m-1,0}^{i_{m-1,0}} Z_{m-1,1}^{i_{m-1,1}} \cdots Z_{m-1,t-1}^{i_{m-1,t-1}} \;\Big|\; i_{0j} + i_{1j} + \cdots + i_{m-1,j} \geqslant \mu_j,\ j = 0, 1, \dots, t-1;\ \mathcal{R}(\bar{\mu}) \subseteq \mathcal{R}(\bar{\lambda}) \Big\rangle.$$

С другой стороны, они могут быть определены индуктивно: если

$$\mathcal{L}'(\lambda_0, \dots, \lambda_{t-1}) = \Big\langle Z_{00}^{i_{00}} Z_{01}^{i_{01}} \cdots Z_{0,t-1}^{i_{0,t-1}} \cdots Z_{m-1,0}^{i_{m-1,0}} Z_{m-1,1}^{i_{m-1,1}} \cdots Z_{m-1,t-1}^{i_{m-1,t-1}} \;\Big|\; i_{0j} + i_{1j} + \cdots + i_{m-1,j} \geqslant \lambda_j,\ j = 0, 1, \dots, t-1 \Big\rangle,$$

то

$$\mathcal{L}(\lambda_0, \dots, \lambda_{t-1}) = \mathcal{L}'(\lambda_0, \dots, \lambda_{t-1}) + \sum_{i=0}^{t-1} \mathcal{L}(\dots, \lambda_i + p, \lambda_{i+1} - 1, \dots).$$

В частности,

$$\mathcal{L}(0, \dots, 0) = \mathcal{A}.$$

Заметим, что

$$\widehat{\sigma}(\mathcal{L}(\lambda_0, \dots, \lambda_{t-1})) = \mathcal{L}(\lambda_{t-1}, \lambda_0, \dots, \lambda_{t-2}).$$

Модули $\mathcal{L}(\bar{\lambda})$ могут рассматриваться как поднятия и как аналоги модулей $\mathcal{R}(\bar{\lambda})$. Ясно, что

$$\mathcal{L}(\bar{\lambda}) \supseteq \sum_{j=0}^{t-1} \mathcal{L}(\lambda_0, \dots, \lambda_j + 1, \dots, \lambda_{t-1}) + \sum_{j=0}^{t-1} \mathcal{L}(\lambda_0, \dots, \lambda_j + p, \lambda_{j+1} - 1, \dots, \lambda_{t-1}).$$

Если $i_{sj} > p - 1$, то $Z_{sj}^{i_{sj}} = -pZ_{sj}^{i_{sj}-p} Z_{s,j+1}^1$ по лемме 4.3(iii), поэтому

$$\mathcal{L}(\bar{\lambda}) \supseteq p\mathcal{L}(\lambda_0, \dots, \lambda_j - p, \lambda_{j+1} + 1, \dots),$$

где мы полагаем

$$\mathcal{L}(\lambda_0, \dots, m(p-1) + 1, \lambda_{j+2}, \dots) = p\mathcal{L}(\lambda_0, \dots, m(p-1) + 1 - p, \lambda_{j+2} + 1, \dots).$$

В частности, для $\bar{\lambda} = (m(p-1), \dots, m(p-1))$ имеем

$$\begin{aligned}\mathcal{L}(\bar{\lambda}) &\supseteq p\mathcal{L}(m(p-1) - p, m(p-1) + 1, m(p-1) \dots, m(p-1)) = \\ &= p^2\mathcal{L}(m(p-1) - p, m(p-1) + 1 - p, m(p-1) + 1 \dots, m(p-1)) = \cdots = \\ &= p^t\mathcal{L}((m-1)(p-1), \dots, (m-1)(p-1)).\end{aligned}$$

Лемма 4.4 (см. [9]). *Модуль* $\mathcal{L}(\bar{\lambda})$ *инвариантен относительно* $AGL_m(q)$.

Положим $\mathcal{L} = \mathcal{L}(\lambda_0, \dots, \lambda_{t-1})$ и определим

$$\mathcal{L}_i = p\mathcal{L}(\lambda_0, \dots, \lambda_i - p, \lambda_{i+1} + 1, \dots)$$

если $\lambda_i \geqslant p$ и $\mathcal{L}_i = 0$ в других случаях. Напомним, что $\mathcal{L}_i \subset \mathcal{L}$. Положим

$$\tilde{\mathcal{L}} = \sum_{j=0}^{t-1} \mathcal{L}(\lambda_0, \dots, \lambda_j + 1, \dots, \lambda_{t-1}) + \sum_{j=0}^{t-1} \mathcal{L}(\dots, \lambda_j + p, \lambda_{j+1} - 1, \dots).$$

Композиционными факторами модуля $(\mathcal{L}+p^2\mathcal{A})/(\tilde{\mathcal{L}}+p^2\mathcal{A})$ являются $\widehat{S}(\lambda_0,\dots,\lambda_{t-1})$ (он получается из максимального полупростого фактормодуля модуля $\mathcal{L}$) и $\widehat{S}(\lambda_0,\dots,\lambda_i-p,\lambda_{i+1}+1,\dots,\lambda_{t-1})$, $i=0,\dots,t-1$ (они получаются из максимального полупростого фактормодуля модуля $\mathcal{L}_i$). Следовательно, существует расширение модуля $\widehat{S}(\lambda_0,\dots,\lambda_{t-1})$ при помощи модуля $\widehat{S}(\lambda_0,\dots,\lambda_i-p,\lambda_{i+1}+1,\dots,\lambda_{t-1})$, и мы хотим показать, что это расширение не расщепляемо. Для этого положим

$$\mathcal{L}^i=\tilde{\mathcal{L}}+\sum_{j\neq i}\mathcal{L}_j+p^2\mathcal{A},\quad \bar{\mathcal{L}}=(\mathcal{L}+\mathcal{L}^i)/\mathcal{L}^i,\quad \bar{\mathcal{L}}_i=(\mathcal{L}_i+\mathcal{L}^i)/\mathcal{L}^i.$$

Заметим, что

$$(\mathcal{L}+p^2\mathcal{A})/(\tilde{\mathcal{L}}+\sum\mathcal{L}_i+p^2\mathcal{A})\cong\widehat{S}(\lambda_0,\dots,\lambda_{t-1}),$$
$$\bar{\mathcal{L}}_i\cong\widehat{S}(\lambda_0,\dots,\lambda_i-p,\lambda_{i+1}+1,\dots,\lambda_{t-1}).$$

Лемма 4.5 (см. [9]). *Пусть* $\mathcal{L}=\mathcal{L}(\lambda_0,\dots,\lambda_{t-1})$.

(i) *Если* $\lambda_i\geqslant p$, $\lambda_{i+1}<m(p-1)$, *то последовательность*

$$0\to\bar{\mathcal{L}}_i\to\bar{\mathcal{L}}\to(\mathcal{L}+p^2\mathcal{A})/\left(\tilde{\mathcal{L}}+\sum\mathcal{L}_i+p^2\mathcal{A}\right)\to 0$$

$GL_m(q)$-*модулей, которая может быть записана как*

$$0\to\widehat{S}(\lambda_0,\dots,\lambda_i-p,\lambda_{i+1}+1,\dots,\lambda_{t-1})\to\bar{\mathcal{L}}\to\widehat{S}(\lambda_0,\dots,\lambda_{t-1})\to 0,$$

не расщепляема.

(ii) *Если* $\bar{\lambda}=(m(p-1),\dots,m(p-1))$, *то*

$$\mathcal{L}/\tilde{\mathcal{L}}=\langle\bar{w}\rangle\oplus\big(q\mathcal{L}((m-1)(p-1),\dots,(m-1)(p-1))+\tilde{\mathcal{L}}\big)/\tilde{\mathcal{L}},$$

где $\bar{w}$ — *образ* w *в* $\mathcal{L}/\tilde{\mathcal{L}}$.

4.3. Доказательства теорем. Определим решетку

$$\mathcal{L}=\mathcal{L}((m-1)(p-1),\dots,(m-1)(p-1))=$$
$$=\left\langle\prod Z_{sj}^{i_{sj}}\;\middle|\;(m-1)(p-1)\leqslant i_{0,j}+\dots+i_{m-1,j},\ 0\leqslant j\leqslant t-1\right\rangle_{R_p}.$$

Покажем, что

$$(\mathcal{L}\cap p^r\mathcal{N}[k]+p^{r+1}\mathcal{N}[k])/p^{r+1}\mathcal{N}[k]\cong\sum_{r_0+\dots+r_{t-1}\leqslant r}\mathcal{M}[k](r_0,\dots,r_{t-1}).$$

Сначала заметим, что

$$\mathcal{L}=\left\langle\prod Z_{sj}^{i_{sj}}\;\middle|\;(m-1)(p-1)\leqslant i_{0,j}+\dots+i_{m-1,j}\leqslant m(p-1),\ 0\leqslant j\leqslant t-1\right\rangle_{R_p}.$$

В самом деле, если мы имеем моном $\prod Z_{sj}^{i_{sj}}\in\mathcal{L}$ с $i_{0,j}+\dots+i_{m-1,j}>m(p-1)$ для некоторого j, то $i_{sj}\geqslant p$ для некоторого s и $Z_{sj}^{i_{sj}}=-pZ_{sj}^{i_{sj}-p}Z_{s,j+1}$. Поэтому степень может быть редуцирована.

Далее,

$$\mathcal{L}=\sum_{0\leqslant k\leqslant q-1}\left\langle\prod Z_{sj}^{i_{sj}}\;\middle|\;i_{0,j}+\dots+i_{m-1,j}=m(p-1)-k_j,\ 0\leqslant j\leqslant t-1\right\rangle_{R_p}.$$

Из определения модуля $\mathcal{N}[k]$ легко видеть, что

$$\mathcal{L}\cap\mathcal{N}[k]=\left\langle\prod Z_{sj}^{i_{sj}}\;\middle|\;i_{0,j}+\dots+i_{m-1,j}=m(p-1)-k_j,\ 0\leqslant j\leqslant t-1\right\rangle_{R_p},\quad k>0.$$

В случае $k=0$ имеем

$$\prod Z_{sj}^{p-1}\in\mathcal{N}[0]+\mathcal{N}[q-1].$$

Теперь выясним, какие мономы порождают (над R_p) модуль $\mathcal{L} \cap p^r\mathcal{N}[k]$. Эти порождающие мономы получены из мономов

$$\prod Z_{sj}^{i_{sj}}, \qquad i_{0,j} + \cdots + i_{m-1,j} = m(p-1) - k_j, \quad 0 \leqslant j \leqslant t-1,$$

умножениями на p и с помощью соотношения

$$Z_{s,j}^p = -pZ_{s,j+1}. \tag{4}$$

Если мы используем это соотношение r_{j+1} раз для каждого j ($j = 0, \ldots, t-1$), то получим моном

$$\pm p^r \prod Z_{sj}^{i_{sj}}, \quad i_{0,j} + \cdots + i_{m-1,j} = m(p-1) - k_j - pr_{j+1} + r_j,$$

где $r_0 + \cdots + r_{t-1} = r$. Следовательно,

$$(\mathcal{L} \cap p^r\mathcal{N}[k] + p^{r+1}\mathcal{N}[k])/p^{r+1}\mathcal{N}[k] \cong \sum_{r_0+\cdots+r_{t-1}\leqslant r} \mathcal{M}[k](\bar{r}), \tag{5}$$

поскольку

$$\begin{aligned}\mathcal{M}[k](\bar{r}) &= \mathcal{F}^k \cap \mathcal{M}(k_0 + pr_1 - r_0, \ldots, k_{t-1} + pr_0 - r_{t-1}) = \\ &= \mathcal{F}^k \cap \mathcal{R}(m(p-1) - (k_0 + pr_1 - r_0), \ldots, m(p-1) - (k_{t-1} + pr_0 - r_{t-1})).\end{aligned}$$

Предыдущие рассмотрения дают нам основание положить

$$\mathcal{N}[k](\bar{r}) = \sum_{\bar{r}' \leqslant \bar{r}} \left\langle \prod Z_{sj}^{i_{sj}} \;\middle|\; i_{0,j} + \cdots + i_{m-1,j} = m(p-1) - (k_j + pr'_{j+1} - r'_j) \right\rangle_{R_p}$$

для $k > 0$ и

$$\mathcal{N}[0](0, \ldots, 0) = \mathcal{N}[0].$$

Найдем $\mathcal{N}[k](\bar{r}) \cap p^d\mathcal{N}[k]$, $k > 0$. Мономы этого модуля получены из порождающих мономов модуля $\mathcal{N}[k](\bar{r})$ умножениями на p и с помощью соотношения (4). Если мы используем это соотношение d_{j+1} раз для каждого j ($j = 0, \ldots, t-1$), то получим моном

$$\pm p^d \prod Z_{sj}^{i_{sj}}, \quad i_{0,j} + \cdots + i_{m-1,j} = m(p-1) - k_j - p(r_{j+1} + d_{j+1}) + r_j + d_j,$$

где $d_0 + \cdots + d_{t-1} = d$. Следовательно, утверждение (ii) доказано.

Докажем, что $\mathcal{N}[k](\bar{r})$ инвариантен относительно $GL_m(q)$. Пусть $g \in GL_m(q)$. Элемент $a = g(Z_{0,t-1})$ обладает свойством

$$\operatorname{diag}(\alpha, \ldots, \alpha)(a) = \tilde{\alpha}^{p^{t-1}} a;$$

поэтому $g(Z_{0,t-1})$ равен линейной комбинации элементов

$$Z_{s,t-1}, \quad Z_{s_1,t-2}Z_{s_2,t-2}\cdots Z_{s_p,t-2}, \quad Z_{s_1,t-3}\cdots Z_{s_{bp},t-3}Z_{t_1,t-2}\cdots Z_{t_{p-b},t-2}, \quad \ldots.$$

Достаточно доказать, что для любого монома $f \in \mathcal{N}[k](\bar{r})$, заменяя одну переменную $Z_{0,t-1}$ в мономе f элементами

$$Z_{s,t-1}, \quad Z_{s_1,t-2}Z_{s_2,t-2}\cdots Z_{s_p,t-2}, \quad Z_{s_1,t-3}\cdots Z_{s_{bp},t-3}Z_{t_1,t-2}\cdots Z_{t_{p-b},t-2}, \quad \ldots,$$

мы получим снова элемент из модуля $\mathcal{N}[k](\bar{r})$. Все эти подстановки могут быть получены как комбинации следующих элементарных подстановок:

$$Z_{0,t-1} \to Z_{s,t-1}, \quad Z_{s,t-1} \to Z_{s_1,t-2}\cdots Z_{s_p,t-2}, \quad Z_{s,t-2} \to Z_{s_1,t-3}\cdots Z_{s_p,t-3}, \quad \ldots.$$

Легко видеть, что после этих элементарных подстановок мы получим снова моном из $\mathcal{N}[k](\bar{r})$. Например, применяя подстановку $Z_{s,t-1} \to Z_{s_1,t-2}\cdots Z_{s_p,t-2}$, получим моном $\prod Z_{dj}^{i_{dj}}$, где

$$\begin{gathered}i_{00} + i_{10} + \cdots + i_{m-1,0} = m(p-1) - (k_0 + pr_1 - r_0), \quad \ldots \\ i_{0,t-2} + i_{1,t-2} + \cdots + i_{m-1,t-2} = m(p-1) - (k_{t-1} + p(r_{t-1} - 1) - r_{t-2}), \\ i_{0,t-1} + i_{1,t-1} + \cdots + i_{m-1,t-1} = m(p-1) - (k_{t-1} + pr_0 - (r_{t-1} - 1)),\end{gathered}$$

т.е. моном из $\mathcal{N}[k](r_0, \ldots, r_{t-2}, r_{t-1} - 1)$.

Определим решетку

$$\widehat{\Lambda} = R_p G_m u \subset \mathcal{A}^0,$$

где

$$u = X^{e_0}\Big(\sum_{\alpha\in\mathbb{F}_q} X^{\alpha e_1}\Big)\cdots\Big(\sum_{\alpha\in\mathbb{F}_q} X^{\alpha e_{m-1}}\Big) - q^{m-1}X^0.$$

Из [5, предложение 9(x)] известно, что

$$Z_{s,0}^{p-1}Z_{s,1}^{p-1}\cdots Z_{s,t-1}^{p-1} = (-1)^{t-1}\Big(\sum_{\alpha\in\mathbb{F}_q} X^{\alpha e_s} - qX^0\Big). \tag{6}$$

Лемма 4.5 и соотношение (6) влекут $\widehat{\Lambda} = \mathcal{L}$.

Пусть $G = GL_m(q)$ и $H = \big\{(a_{ij}) \in G \;\big|\; a_{0j} = 0$ для всех $j = 1,\dots,m-1,\ a_{00} = 1\big\}$. Тогда

$$\widehat{\Lambda}/p\widehat{\Lambda} \cong \mathrm{Ind}_H^G(u).$$

С другой стороны, для $\widehat{\mathcal{F}}_0 = \bigoplus_{k=1}^{q-1}\widehat{\mathcal{F}}^k = \{f \mid f(0) = 0\}$ имеем

$$\widehat{\mathcal{F}}_0 \cong \mathrm{Ind}_H^G(X^{e_0}).$$

Следовательно,

$$\mathcal{L}/p\mathcal{L} \cong \widehat{\Lambda}/p\widehat{\Lambda} \cong \widehat{\mathcal{F}}_0.$$

Заметим, что любой подмодуль и фактормодуль модуля $\widehat{\mathcal{F}}_0$ однозначно определен множеством композиционных факторов и любой неразложимый подмодуль модуля $\widehat{\mathcal{F}}_0$ однозначно определен его максимальным полупростым фактормодулем. Композиционные факторы модуля $\widehat{\mathcal{F}}_0$ неизоморфны.

Согласно (5) имеем

$$(\mathcal{N}[k](0,\dots,0) + p\mathcal{A})/p\mathcal{A} \cong \mathcal{M}[k](0,\dots,0).$$

Следовательно, $\mathcal{N}[k](0,\dots,0)/p\mathcal{N}[k](0,\dots,0)$ — модуль, изоморфный слагаемому модуля $\widehat{\mathcal{F}}_0$, а его максимальный полупростой фактормодуль изоморфен модулю

$$\mathcal{M}[k](0,\dots,0) \cong S(\bar{k}) \cong \widehat{S}(m(p-1) - k_0,\dots,m(p-1) - k_{t-1}).$$

Последний модуль изоморфен максимальному полупростому фактормодулю модуля

$$\widehat{\mathcal{M}}[p-1-k_0,\dots,p-1-k_{t-1}](m-1,\dots,m-1)$$

при $0 < k < q-1$ и изоморфен максимальному полупростому фактормодулю модуля

$$\widehat{\mathcal{M}}[q-1](m-2,\dots,m-2)$$

при $k = q-1$. Следовательно, имеем

$$\mathcal{N}[k](0,\dots,0)/p\mathcal{N}[k](0,\dots,0) \cong \widehat{\mathcal{F}}^{q-1-k}, \quad 0 < k < q-1,$$
$$\mathcal{N}[q-1](0,\dots,0)/p\mathcal{N}[q-1](0,\dots,0) \cong \widehat{\mathcal{M}}[q-1](m-2,\dots,m-2).$$

Рассмотрим структуру модуля $\widehat{\mathcal{F}}^{q-1-k}$, $0 < k < q-1$. Любой неразложимый подмодуль модуля $\widehat{\mathcal{F}}^{q-1-k}$ равен одному из модулей $\widehat{\mathcal{M}}[q-1-k](\dots,m-1-r_j,\dots,)$, максимальный полупростой фактормодуль которого изоморфен

$$\widehat{S}(\dots,p-1-k_j+p(m-1-r_{j+1})-(m-1-r_j),\dots) =$$
$$= \widehat{S}(\dots,m(p-1)-k_j-pr_{j+1}+r_j,\dots) \cong S(\dots,k_j+pr_{j+1}-r_j,\dots).$$

Аналогично, при $k = q-1$ любой неразложимый подмодуль модуля $\widehat{\mathcal{M}}[q-1](m-2,\dots,m-2)$ равен одному из модулей $\widehat{\mathcal{M}}[q-1](\dots,m-2-r_j,\dots)$, максимальный полупростой фактормодуль которого изоморфен

$$\widehat{S}(\dots,p-1+p(m-2-r_{j+1})-(m-2-r_j),\dots) =$$
$$= \widehat{S}(\dots,(m-1)(p-1)-pr_{j+1}+r_j,\dots) \cong S(\dots,k_j+pr_{j+1}-r_j,\dots).$$

Следовательно, если $r = \sum r_i$, то $\mathcal{N} = p^r\mathcal{N}[k](\bar{r}) \subseteq p^r\mathcal{N}[k]$ является единственным минимальным подмодулем в $\mathcal{N}[k](0,\dots,0)$ со свойством

$$(\mathcal{N}+p^{r+1}\mathcal{N}[k])/p^{r+1}\mathcal{N}[k] \cong \mathcal{M}[k](\bar{r}).$$

Поскольку максимальный полупростой фактормодуль модуля $\mathcal{M}[k](\bar{r})$ изоморфен модулю $S(\dots,k_j+pr_{j+1}-r_j,\dots)$, получаем, что

$$(\mathcal{N}+p\mathcal{N}[k](0,\dots,0))/p\mathcal{N}[k](0,\dots,0) \cong \widehat{M}[q-1-k](\dots,m-1-r_j,\dots)$$

при $0<k<q-1$ и

$$(\mathcal{N}+p\mathcal{N}[k](0,\dots,0))/p\mathcal{N}[k](0,\dots,0) \cong \widehat{M}[q-1](\dots,m-2-r_j,\dots)$$

при $k=q-1$.

Модуль $\mathcal{N}[k](\bar{r})$ неразложим согласно лемме 4.5 и согласно структуре модуля $\widehat{\mathcal{F}}^{q-1-k}$. Фактически, имеем следующие изоморфизмы $GL_m(q)$-модулей:

$$\mathcal{N}[k](\bar{r})/\sum_{\bar{s}<\bar{r}}\mathcal{N}[k](\bar{s}) \cong (p^r\mathcal{N}[k](\bar{r})+p\mathcal{N}[k](0,\dots,0))/p\mathcal{N}[k](0,\dots,0) \cong$$
$$\cong \widehat{M}[q-1-k](\dots,m-1-r_j,\dots), \qquad 0<k<q-1,$$
$$\mathcal{N}[k](\bar{r})/\sum_{\bar{s}<\bar{r}}\mathcal{N}[k](\bar{s}) \cong (p^r\mathcal{N}[k](\bar{r})+p\mathcal{N}[k](0,\dots,0))/p\mathcal{N}[k](0,\dots,0) \cong$$
$$\cong \widehat{M}[q-1](\dots,m-2-r_j,\dots), \qquad k=q-1.$$

Нам осталось изучить поведение модуля $\mathcal{N}[k](\bar{r})$ относительно умножений на элементы Z_{ab}. Положим для простоты $a=b=0$. Используем некоторые условные соглашения. Из определения модуля $\mathcal{N}[k](\bar{r})$ легко видеть, что

$$GL_m(q)(Z_{00}\cdot\mathcal{N}[k](\bar{r})) = \mathcal{N}[k_0-1,k_1,\dots](\bar{r}),$$

где мы предполагаем, что

$$\mathcal{N}[\dots,-1,k_{j+1},\dots](\bar{r}) = \mathcal{N}[\dots,p-1,k_{j+1}-1,\dots](r_j,r_{j+1}-1,r_{j+2},\dots), \tag{7}$$
$$\mathcal{N}[k](\dots,r_j,-1,r_{j+2},\dots) = p\mathcal{N}[k](\dots,r_j,0,r_{j+2},\dots), \tag{8}$$
$$\mathcal{N}[k](\bar{r}) = p\mathcal{N}[k](\dots,r_j,r_{j+1}+1,r_{j+2},\dots) \quad \text{if } k_j+pr_{j+1}-r_j=-1. \tag{9}$$

Эти равенства немедленно влекут доказательство теоремы 3.3 в одну сторону. Докажем достаточность. Нам нужно доказать, что при условиях теоремы утверждение $p^l\mathcal{N}[k](\bar{r}) \subseteq \mathcal{N}$, $\mathcal{N}$ инвариантен относительно $AGL_m(q)$, влечет $p^l\mathcal{N}[\dots,k_{j-1},k_j-1,k_{j+1},\dots](\bar{r}) \subseteq \mathcal{N}$ (мы можем предполагать $j=0$ и мы подразумеваем соглашения (7)–(9)). Это ясно, если $k_0+pr_1-r_0>0$. Предположим, что $k_0+pr_1-r_0=0$. Тогда мы должны доказать, что

$$p^l\mathcal{N}[k_0-1,k_1,\dots](\bar{r}) = p^{l+1}\mathcal{N}[k_0-1,k_1,\dots](r_0,r_1+1,r_2\dots) \subseteq \mathcal{N}.$$

Но это следует из факта

$$p^{l+1}\mathcal{N}[k_0,k_1,\dots](r_0,r_1+1,r_2\dots) \subseteq p^l\mathcal{N}[k](\bar{r}) \subseteq \mathcal{N},$$

если $k_1+pr_2-(r_1+1) \geqslant 0$. Если $k_1+pr_2-(r_1+1)=-1$, то мы рассмотрим

$$p^l\mathcal{N}[k_0-1,k_1,\dots](\bar{r}) = p^{l+2}\mathcal{N}[k_0-1,k_1,\dots](r_0,r_1+1,r_2+1,\dots),$$

и т. д.

СПИСОК ЛИТЕРАТУРЫ

1. *Абдухаликов К. С.* Инвариантные целочисленные решетки в алгебрах Ли типа A_{p^m-1}// Мат. сб. — 1993. — *184*, № 4. — С. 61–104.
2. *Абдухаликов К. С.* Целочисленные решетки, ассоциированные с конечной аффинной группой// Мат. сб. — 1994. — *185*, № 12. — С. 3–18.
3. *Бондал А. И. Кострикин А. И., Фам Хю Тьеп*. Инвариантные решетки, решетка Лича и его четные унимодулярные аналоги в алгебрах A_{p-1}// Мат. сб. — 1986. — *172*, № 8. — С. 435–464.
4. *Abdukhalikov K. S.* Defining sets of cyclic codes invariant under the affine group// International Workshop on Coding and Cryptography. Paris, January 8–12, 2001. — Amsterdam: Elsevier, 2001.
5. *Abdukhalikov K. S.* Affine invariant and cyclic codes over p-adic numbers and finite rings// Designs, Codes, and Cryptography. — 2001. — *23*, № 3. — С. 343–370.
6. *Abdukhalikov K. S.* Codes over p-adic numbers and finite rings invariant under the full affine group// Finite Fields Their Appl. — 2001. — *7*, № 4. — С. 449–467.
7. *Abdukhalikov K. S.* Defining sets of extended cyclic codes invariant under the affine group// (в печати).
8. *Abdukhalikov K. S.* Doubly transitive groups and lattices// J. Math. Sci. — 1999. — *93*, № 6. — С. 809–823.
9. *Abdukhalikov K. S.* Lattices invariant under the affine general linear group// J. Algebra (принято к публикации).
10. *Assmus E. F., Key J. D.* Polynomial codes and finite geometries// Handbook of Coding Theory, Vol. 2 (Pless V. S., Huffman W. C., eds.). — Elsevier, 1998. — Chap. 16, С. 1269–1343.
11. *Bardoe M., Sin P.* The permutation modules for $GL(n+1,\mathbb{F}_q)$ acting on $\mathbb{P}^n(\mathbb{F}_q)$ and $\mathbb{F}_q^{n+1}$// J. London Math. Soc. (2). — 2000. — *61*, № 1. — С. 58–80.
12. *Barnes E. S., Sloane N. J. A.* New lattice packings of spheres// Can. J. Math. — 1983. — *35*. — С. 117–130.
13. *Berger T., Charpin P.* The permutation group of affine-invariant extended cyclic codes// IEEE Trans. Inform. Theory. — 1996. — *42*, № 6. — С. 2194–2209.
14. *Berger T. P.* Automorphism groups and permutation groups of affine-invariant codes// Finite Fields and Applications/ Proc. 3rd Int. Conf. Glasgow, UK, July 11–14, 1995. — Cambridge: Cambridge Univ. Press, 1996. — Lond. Math. Soc. Lect. Note Ser. *233*. — С. 31–45.
15. *Charpin P.* Codes cycliques étendus invariants sous le groupe affine/ Thèse de Doctorat d'État. — Université Paris VII, 1987.
16. *Delsarte P.* On cyclic codes that are invariant under the general linear group// IEEE Trans. Inform. Theory. — 1970. — *16*. — С. 760–769.
17. *Hammons R., Kumar P. V., Calderbank A. R., Sloane N. J. A., Solé P.* The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes// IEEE Trans. Inform. Theory. — 1994. — *40*, № 2. — С. 301–319.
18. *Kasami T., Lin S., Peterson W. W.* Some results on cyclic codes which are invariant under the affine group and their applications// Inform. Control. — 1967. — *11*. — С. 475–496.
19. *Kostrikin A. I., Pham Huu Tiep.* Orthogonal decompositions and integral lattices. — Berlin: Walter de Gruyter, 1994.
20. *Sastry N. S. N., Sin P.* On the double transitive permutation representations of $Sp(2n,\mathbb{F}_2)$// J. Algebra. — 2002. — *257*. — С. 509–527.
21. *Sin P.* The permutation representations of $Sp(2m,\mathbb{F}_2)$ acting on the vectors of its standard module// J. Algebra. — 2001. — *241*. — С. 578–591.

К. Абдухаликов
Институт математики, Казахстан, Алматы
E-mail: abdukhalikov@math.kz

Современная математика и ее приложения. Том 13 (2004). С. 24–39

УДК 512.55

КОЛЬЦА МНОГОЧЛЕНОВ ORE ОДНОЙ ПЕРЕМЕННОЙ В КОМПЬЮТЕРНОЙ АЛГЕБРЕ

© 2004 г. **С. А. АБРАМОВ, Х. К. ЛЕ, З. ЛИ**

Аннотация. Мы описываем несколько алгоритмов, относящихся к кольцам многочленов Ore (кольцам Ore), и Maple-пакет, реализующий основные операции в произвольном кольце Ore. Этот пакет можно использовать в качестве базового для многих алгоритмов в кольцах Ore, в частности, в дифференциальных кольцах, кольцах со сдвигом и кольцах с q-сдвигом.

СОДЕРЖАНИЕ

1. Введение

Теория колец Ore (или, то же самое, колец многочленов Ore) дает возможность рассматривать обыкновенные линейные дифференциальные, разностные, q-разностные и другие операторы с общей точки зрения. Эти кольца были предложены Ore [25–27] как основа единой теории факторизации операторов, обобщающей теорию, разработанную ранее Ландау и Леви для дифференциального случая [18, 22, 23]. Способ интерпретации абстрактных многочленов Ore как линейных операторов на векторном пространстве был предложен Джекобсоном [17].

Теория колец Ore хороша не только тем, что позволяет единообразно доказывать утверждения об операторах разного вида, но также и открываемой ею возможностью создания многоцелевых алгоритмов и соответствующих программ, которые можно настраивать на конкретный вид операторов и уравнений. Стоит упомянуть, что идея привлечения колец Ore в компьютерной алгебре впервые была высказана и использована Бронштейном и Петковшеком [10], где описан алгоритм факторизации в произвольном кольце Ore.

В данной работе мы описываем некоторые (но далеко не все) алгоритмы компьютерной алгебры, относящиеся к кольцам Ore. Раздел 2 содержит обзор колец многочленов Ore одной переменной. В разделе 3, посвященном сопряженным операторам, материал изложен в более общем виде, чем ранее [6]; материал раздела 4 об эффективном вычислении наибольших общих делителей (gcd) и наименьших общих кратных (lcm) излагается впервые. В разделе 5 дается обзор пакета `OreTools`, который позволяет работать с многочленами Ore от одной переменной в системе компьютерной алгебры Maple [24]. Этот пакет можно использовать в качестве базы для многих алгоритмов в кольцах Ore, в частности, в дифференциальных кольцах, кольцах со сдвигом E и кольцах с q-сдвигом Q.

Сравнение этого пакета с другими подобными пакетами проводится в разделах 4 и 6. Информация о доступе к пакету приведена в разделе 7.

ISSN 1512–1712

2. Кольца многочленов Оре одной переменной

В разделах 2.1, 2.4 дается краткий обзор общей теории многочленов Оре одной переменной и соответствующих линейных операторов. Детальное обсуждение и доказательства соответствующих утверждений см. в [10,17,25]. В разделе 2.2 мы рассматриваем идею гильбертова упрощения, следуя описанию из [10,13]. В разделе 2.3 приводятся определение и основные свойства сопряженных многочленов (детали см. в [13, гл. 1, 8 (разд. 3)]).

2.1. Многочлены Оре. Пусть k — поле характеристики 0, $\sigma : k \to k$ — автоморфизм k.

Определение 2.1. Дифференцирование относительно σ — это любое отображение $\delta : k \to k$, для которого

$$\delta(a+b) = \delta a + \delta b \quad \text{и} \quad \delta(ab) = \sigma(a)\delta b + \delta a\, b \quad \text{для любых} \quad a, b \in k. \tag{1}$$

Определение 2.2. Множество констант (относительно σ и δ) — это

$$\mathrm{Const}_{\sigma,\delta}(k) = \{a \in k : \sigma(a) = a,\ \delta a = 0\}.$$

Можно показать, что $\mathrm{Const}_{\sigma,\delta}(k)$ — подполе поля k.

Следующая лемма описывает связь между σ и δ. Если не возникает путаницы, мы обозначаем символом 1 тождественное отображение на k.

Лемма 2.1. *Пусть δ — дифференцирование k относительно σ.*

(i) *Если $\sigma \neq 1$, то существует элемент $\alpha \in k$, для которого $\delta = \alpha(\sigma - 1)$.*
(ii) *Если $\delta \neq 0$, то существует элемент $\beta \in k$, для которого $\sigma = \beta\,\delta + 1$.*

Пример 2.1. Пусть $k = \mathbb{F}(t)$ в случаях 1–4 и $k = \mathbb{F}(q,t)$ в случаях 5–7, где $\mathbb{F}$ — любое подполе $\mathbb{C}$.

	Случай	σ	δ
1	дифференциальный	1	$\frac{d}{dt}$
2	эйлеров дифференциальный	1	$t\frac{d}{dt}$
3	рекуррентный	E	0
4	разностный	E	$E-1$
5	q-рекуррентный	Q	0
6	q-разностный	Q	$Q-1$
7	q-дифференциальный	Q	$\frac{Q-1}{t(q-1)}$

Определение 2.3. Кольцо Оре (многочленов одной переменной) над k, заданное посредством σ и δ и обозначаемое $k[x;\sigma,\delta]$, — это кольцо многочленов от x над k с обычным сложением многочленов и умножением, заданным формулой

$$xa = \sigma(a)x + \delta a \quad \text{для любого} \quad a \in k. \tag{2}$$

Элементы кольца $k[x;\sigma,\delta]$ называются многочленами Оре. Заметим, что в качестве k можно рассматривать некоторое кольцо (мы будем рассматривать многочлены Оре над кольцами в разделах 2.4, 3 и 4).

Пусть $p(x) \in k[x;\sigma,\delta]$ и $p(x) = p_m x^m + \cdots + p_1 x + p_0$, $p_m \neq 0$; тогда $m = \deg p(x)$, $p_m = \mathrm{lc}\, p(x)$. Положим $\deg 0 = -\infty$, $\mathrm{lc}\, 0 = 0$. Если $\mathrm{lc}\, p(x) = 1$, то многочлен $p(x)$ называется *унитарным*. Можно показать, что в $k[x;\sigma,\delta]$ имеются алгоритмы правого и левого деления. Пусть $a, b \in k[x;\sigma,\delta] \setminus \{0\}$. Применяя алгоритм правого деления, мы получаем

$$a = q_1 b + r_1, \quad q_1, r_1 \in k[x;\sigma,\delta], \quad \deg r_1 < \deg b;$$

r_1, q_1 называются соответственно *правым остатком* и *правым частным* при делении a на b. Аналогично, применяя алгоритм левого деления, мы получаем

$$a = b q_2 + r_2, \quad q_2, r_2 \in k[x;\sigma,\delta], \quad \deg r_2 < \deg b;$$

r_2, q_2 называются соответственно *левым остатком* и *левым частным* при делении a на b.

Для данных $a, b \in k[x;\sigma,\delta]$ можно найти *наибольший общий правый делитель* (gcrd) правым алгоритмом Евклида и *наименьшее общее левое кратное* (lclm) *расширенным* правым алгоритмом

Евклида. Вычисление *наибольшего общего левого делителя* (gcld) и, соответственно, *наименьшего общего правого кратного* (lcrm) можно свести к вычислению gcrd и, соответственно, lclm использованием сопряжения.

2.2. Гильбертово упрощение. Гильбертово упрощение — это изоморфизм колец, который отображает произвольное кольцо Оре в кольцо Оре с с тривиальным дифференцированием при условии, что σ нетривиален.

Предложение 2.2. *Если существует $\alpha \in k$, для которого $\alpha \neq \sigma(\alpha)$, то биекция*

$$H_\alpha : k[x;\sigma,\delta] \to k[y;\sigma,0], \quad H_\alpha\left(\sum_i a_i x^i\right) = \sum_i a_i \left(\frac{y+\delta\alpha}{\alpha-\sigma(\alpha)}\right)^i,$$

является изоморфизмом колец.

2.3. Сопряженные многочлены.

Определение 2.4. Пусть $k[x;\sigma,\delta]$ — кольцо Оре. Сопряженное к $k[x;\sigma,\delta]$ кольцо Оре — это кольцо $k[x;\sigma^*,\delta^*]$, где

$$\sigma^* = \sigma^{-1}, \quad \delta^* = -\delta\,\sigma^{-1}. \tag{3}$$

Пусть $a = a_n x^n + \cdots + a_1 x + a_0 \in k[x;\sigma,\delta]$. Сопряженный многочлен a^* определяется соотношением

$$a^* = x^n a_n + \cdots + x a_1 + a_0 \in k[x;\sigma^*,\delta^*].$$

Отметим, что произведение $x^i a_i$ надо вычислять в кольце Оре $k[x;\sigma^*,\delta^*]$. Легко показать, что $\mathrm{Const}_{\sigma,\delta}(k) = \mathrm{Const}_{\sigma^*,\delta^*}(k)$ и $(\sigma^*)^* = \sigma$, $(\delta^*)^* = \delta$. Также можно проверить, что сопряжение — линейное (над $\mathrm{Const}_{\sigma,\delta}$) биективное отображение и $(a^*)^* = a$, $(ab)^* = b^* a^*$. Кроме того,

$$\mathrm{gcld}(a,b) = (\mathrm{gcrd}(a^*,b^*))^*, \quad \mathrm{lcrm}(a,b) = (\mathrm{lclm}(a^*,b^*))^*.$$

Пример 2.2. Из примера 2.1 и определения 2.4 получаем следующую таблицу.

	Случай	σ^*	δ^*
1	дифференциальный	1	$-\frac{d}{dt}$
2	эйлеров дифференциальный	1	$-t\frac{d}{dt}$
3	рекуррентный	E^{-1}	0
4	разностный	E^{-1}	$E^{-1}-1$
5	q-рекуррентный	Q^{-1}	0
6	q-разностный	Q^{-1}	$Q^{-1}-1$
7	q-дифференциальный	Q^{-1}	$\frac{Q^{-1}-1}{t(q-1)}$

2.4. Многочлены Оре как линейные операторы.

Определение 2.5. Пусть V — векторное пространство над k. Отображение $\theta : V \to V$ псевдолинейно относительно σ и δ, если

$$\theta(u+v) = \theta(u) + \theta(v), \quad \theta(a\,u) = \sigma(a)\theta(u) + \delta a\,u \tag{4}$$

для любых $a \in k$, $u, v \in V$.

Предположим, что K — σ,δ-согласованное надкольцо k, т.е. σ и δ продолжаются соответственно до автоморфизма кольца K и его дифференцирования относительно σ. Мы также предположим, что $\mathrm{Const}_{\sigma,\delta}(K) = \mathrm{Const}_{\sigma,\delta}(k)$ и будем использовать обозначение C для этого поля. Заметим, что K — векторное пространство над k и, следовательно, может играть роль V. Мы будем рассматривать псевдолинейные отображения из K в K, предполагая, что соотношения (4) выполнены для любых $a, u, v \in K$.

Лемма 2.3. *Для любого $c \in K$ отображение $\theta_c : K \to K$, заданное формулой*

$$\theta_c(a) = c\sigma(a) + \delta a, \tag{5}$$

K-псевдолинейно относительно σ и δ, и $\theta_c(1) = c$. Наоборот, для любого K-псевдолинейного отображения θ элемент $c = \theta(1)$ таков, что отображение θ совпадает с θ_c, определенным в (5).

Рассмотрим кольцо $k[\theta]$ C-линейных операторов $L : K \to K$ вида $L = p(\theta)$, $p(x) \in k[x; \sigma, \delta]$. Соответствие $p(x) \to p(\theta)$ дает гомоморфизм колец $\Theta : k[x; \sigma, \delta] \to k[\theta]$ благодаря псевдолинейности θ. Мы предположим, что

$$p(\theta) \text{ — нулевой оператор на } K \iff p(x) \text{ — нулевой многочлен Оре} \tag{6}$$

и, как следствие, соответствие $p(x) \to p(\theta)$ задает изоморфизм колец. Если $L = p(\theta)$, то положим $\operatorname{ord} L = \deg p$.

Иногда удобно рассматривать также кольца $K[x; \sigma, \delta]$ и $K[\theta]$. Мы предположим, что для них выполнено (6).

Легко привести пример, который показывает, что (6) не выполнено в общем случае (скажем, $K = k = \mathbb{C}$, $\sigma(z) = \bar{z}$, $\delta = 0$, $\theta = \sigma$). В предложении 3.2 мы сформулируем простое и естественное достаточное условие выполнения (6).

Как следствие лемм 2.1 и 2.3 мы получаем следующее утверждение.

Предложение 2.4. *Отображение θ, K-псевдолинейное относительно σ и δ, равно $\delta + \theta(1)$, если $\sigma = 1$, и $(\theta(1) + \alpha)\sigma - \alpha$, если $\sigma \neq 1$, при этом α определено в лемме* 2.1(i).

Условие (6) не выполнено в случае $\theta(1) + \alpha = 0$ (иначе $\theta + \alpha = 0$), так что мы заключаем, что если $\sigma \neq 1$, то $\theta(1) + \alpha \neq 0$. Мы дополнительно предположим, что $\theta(1) + \alpha$ не есть делитель нуля в K (это выполнено, например, если $\theta(1) \in k$ и, как следствие, $\theta(1) + \alpha \in k$).

Пример 2.3. Псевдолинейные отображения θ и константы $c = \theta(1)$:

	Случай	θ	c
1	дифференциальный	$\frac{d}{dt}$	0
2	эйлеров дифференциальный	$t\frac{d}{dt}$	0
3	рекуррентный	E	1
4	разностный	$E - 1$	0
5	q-рекуррентный	Q	1
6	q-разностный	$Q - 1$	0
7	q-дифференциальный	$\frac{Q-1}{t(q-1)}$	0

3. Сопряженные операторы

3.1. Оператор ∇. Пусть θ — псевдолинейное отображение из K в K относительно σ, δ. Положим $\nabla = \theta - \theta(1)$, $\nabla \in K[\theta]$. Согласно предложению 2.4,

$$\nabla = \begin{cases} \delta, & \text{если } \sigma = 1, \\ (\theta(1) + \alpha)(\sigma - 1), & \text{если } \sigma \neq 1. \end{cases}$$

Согласно лемме 2.1 и тому факту, что $\theta(1) + \alpha$ не есть делитель нуля, для любого $f \in K$ имеем

$$\nabla(f) = 0 \text{ если и только если } f \in C. \tag{7}$$

Отсюда легко вывести, что при $L \in K[\theta]$ выполнено соотношение $L(1) = 0$, если и только если существует $M \in K[\theta]$, для которого $L = M\nabla$. Учитывая тот факт, что $L(f) = (Lf)(1)$, и условие (6), получаем следующее утверждение.

Предложение 3.1. *Пусть $p \in K[x; \sigma, \delta]$, $L = p(\theta)$, $f \in K$. Тогда $L(f) = 0$, если и только если существует $M \in K[\theta]$, для которого $Lf = M\nabla$, т.е. если и только если pf делится справа на $x - \theta(1)$.*

Пусть $c = \theta(1)$ и $p \in K[x;\sigma,\delta] \setminus \{0\}$, $\deg p = d$; тогда существует неотрицательное целое n, для которого

$$p = (b_{d-n}(x-c)^{d-n} + \cdots + b_1(x-c) + b_0)(x-c)^n,$$

где $b_0, \ldots, b_{d-n} \in K$, $b_0 \neq 0$. Отсюда вытекает следующее утверждение.

Предложение 3.2. *Предположим, что для любого неотрицательного целого n существует $f \in K$, для которого $\nabla^n(f) \in C \setminus \{0\}$. Тогда* (6) *выполнено для любого $p \in K[x;\sigma,\delta]$.*

Пример 3.1. Продолжение примера 2.3:

	Случай	∇
1	дифференциальный	$\frac{d}{dt}$
2	эйлеров дифференциальный	$t\frac{d}{dt}$
3	рекуррентный	$E-1$
4	разностный	$E-1$
5	q-рекуррентный	$Q-1$
6	q-разностный	$Q-1$
7	q-дифференциальный	$\frac{Q-1}{t(q-1)}$

3.2. Сопряженные операторы и интегрирующие множители. Согласно лемме 2.3, $\theta = \theta_c = c\sigma + \delta$, где $c = \theta(1)$. Положим $\theta^* = c\sigma^* + \delta^*$, где σ^*, δ^* такие же, как в (3). Заметим, что $\theta(1) = c = \theta^*(1)$.

Определение 3.1. Пусть $k[x;\sigma,\delta]$ — кольцо Оре, θ — псевдолинейное отображение относительно σ,δ. Сопряженное к $k[\theta]$ кольцо определяется как кольцо операторов $k[\theta^*]$. Если $p \in k[x;\sigma,\delta]$ и $L = p(\theta)$, то сопряженный к L оператор определяется как $L^* = p^*(\theta^*) \in k[\theta^*]$.

Имеем $(LM)^* = M^*L^*$ для любых $L, M \in k[\theta]$. Если мы предположим, что (6) выполнено для $K[x;\sigma^*,\delta^*]$ и $K[\theta^*]$, то вдобавок $(L^*)^* = L$ для любого $L \in k[\theta]$.

Рассмотрим оператор $\nabla^* = \theta^* - \theta(1) = \theta^* - \theta^*(1)$. Согласно предложению 3.1, $L^*(f) = 0$, если и только если существует $M \in K[\theta^*]$, для которого $L^*f = M\nabla^*$, т.е. $fL = \nabla M^*$. Отсюда вытекает следующее утверждение.

Предложение 3.3. *Пусть $p \in K[x;\sigma,\delta]$, $L = p(\theta)$, $f \in K$. Тогда $L^*(f) = 0$, если и только если существует $N \in K[\theta]$, для которого $fL = \nabla N$, т.е. если и только если fp делится слева на $x - \theta(1)$.*

Предложения 3.1 и 3.3 представляют собой аналог теоремы Безу для алгебраических уравнений с одним неизвестным.

Пример 3.2. Продолжение примеров 2.2 и 2.3:

	Случай	θ^*	∇^*
1	дифференциальный	$-\frac{d}{dt}$	$-\frac{d}{dt}$
2	эйлеров дифференциальный	$-t\frac{d}{dt}$	$-t\frac{d}{dt}$
3	рекуррентный	E^{-1}	$E^{-1}-1$
4	разностный	$E^{-1}-1$	$E^{-1}-1$
5	q-рекуррентный	Q^{-1}	$Q^{-1}-1$
6	q-разностный	$Q^{-1}-1$	$Q^{-1}-1$
7	q-дифференциальный	$\frac{Q^{-1}-1}{t(q-1)}$	$\frac{Q^{-1}-1}{t(q-1)}$

Естественно назвать *интегрирующим множителем* для L любой $f \in K$, для которого $fL = \nabla N$, $N \in K[\theta]$. Предложение 3.3 — аналог классической теоремы из теории обыкновенных дифференциальных уравнений, но формулировка этого предложения дана в общей «форме Оре».

Пример 3.3. Пусть $k = \mathbb{C}(n)$, $\sigma = \theta = E$, $\delta = 0$, $\nabla = E - 1$, K — кольцо последовательностей с элементами из $\mathbb{C}$. Рассмотрим оператор

$$L = (n+4)E^2 + E - (n+1) \in k[\theta].$$

Соответствующее сопряженное уравнение $L^*(f) = 0$ имеет вид

$$L^*(f) = -(n+1)f(n) + f(n-1) + (n+2)f(n-2) = 0. \tag{8}$$

Если интегрирующий множитель f для L является гипергеометрическим термом, то его можно найти, применяя алгоритм Hyper [28] к (8); это применение проходит успешно и дает $f = (-1)^n$. Как следствие,

$$(-1)^n L = (E-1)((-1)^{n-1}(n+3)E + (-1)^n(n+1)).$$

3.3. Аккуратное интегрирование. Элемент $g \in K$ называется *первообразным* для $f \in K$, если $\nabla(g) = f$. Предположим, что $\theta(1) \in k$ (т.е. $\nabla \in k[\theta]$) и рассмотрим следующую задачу: пусть заданы $f \in K$ и минимальный аннулирующий оператор $L \in k[\theta]$ для f (значение $n = \operatorname{ord} L$ — минимальное с тем свойством, что $L \in k[\theta]$ и $L(f) = 0$). Определить, существует ли такой первообразный элемент g элемента f, для которого минимальный аннулирующий оператор $\tilde{L}$ имеет порядок n. Если это так, то построить такой элемент g и его минимальный аннулирующий оператор.

Эта задача (задача *аккуратного интегрирования*) была решена в [6]. Сопряженные операторы играют ключевую роль в решении. Мы приводим ниже краткое описание алгоритма. Заметим, что в [6] описание дано в двух (главных) случаях: $\sigma = 1$, $\theta = \delta$ и $\theta = \sigma - 1$, $\delta = 0$. Если задача имеет положительное решение (существует оператор $\tilde{L}$ порядка n), то алгоритм строит $r \in k[\theta]$, $\operatorname{ord} r = n - 1$, для которого $g = r(f)$, вместе с $\tilde{L}$.

В [6] было показано, что оператор $\tilde{L}$, для которого $\operatorname{ord} \tilde{L} = n$, существует, если и только если уравнение $L^*(y) = 1$ имеет решение l в k. В этом случае r таково, что $1 - lL = \nabla r$ (так что r можно найти левым делением) и $\tilde{L} = 1 - r\nabla$. Если такого l не существует, то интегрирующий оператор r также не существует, в то время как минимальный аннулирующий оператор $\tilde{L}$ для g равен $L\nabla$, $\operatorname{ord} \tilde{L} = n + 1$.

Как замечено в [6], этот алгоритм обобщает алгоритм Госпера для неопределенного гипергеометрического суммирования [15] в двух смыслах: (а) он решает аналогичную задачу для более широкого класса уравнений, (б) он работает для любого порядка n, а не только для $n = 1$.

Пример 3.4. Продемонстрируем использование аккуратного интегрирования в вычислении первообразных для выражений, включающих в себя присоединенные функции Лежандра первого и второго рода:

$$p_1 = (27t^2+4)^{5/4}\mathcal{P}^{5/2}_{2/3\sqrt{7}-1/2}\left(-\frac{3}{2}\sqrt{3}i\,t\right),$$
$$p_2 = (27t^2+4)^{5/4}\mathcal{Q}^{5/2}_{2/3\sqrt{7}-1/2}\left(-\frac{3}{2}\sqrt{3}i\,t\right).$$

Как p_1, так и p_2 аннулируются дифференциальным оператором

$$L = (27t^2+4)D^2 - 81tD + 24.$$

Соответствующее сопряженное уравнение $L^*(y) = 1$ имеет вид

$$(27t^2+4)\frac{d^2}{dt^2}y(t) + 189\,t\frac{d}{dt}y(t) + 159\,y(t) = 1;$$

оно имеет рациональное решение $l = 1/159$ (решения, имеющие вид рациональных функций, могут быть найдены алгоритмом из [1]). Следовательно, оператор $r \in k[\theta]$, для которого $\int p_1 dt = r(p_1)$ и $\int p_2 dt = r(p_2)$, — это левое частное от деления $1 - lL$ на ∇, которое равно

$$\left(-\frac{9}{53}t^2 - \frac{4}{159}\right)D + \frac{45}{53}t.$$

Заметим, что ни Maple 8, ни Mathematica 4 не могут вычислить два этих неопределенных интеграла.

4. Новые модулярные методы вычисления gcd и lcm

Обычное коммутативное кольцо многочленов $k[x]$ — это частный случай колец многочленов Оре. Многие эффективные методы для коммутативного случая были обобщены на некоммутативные $k[x;\sigma,\delta]$ (см. [12,16,20,21]). В этом разделе мы предлагаем новые модулярные методы вычисления gcrd и lclm многочленов Оре. Для применения модулярных методов требуются небольшие ограничения на поле коэффициентов. Пусть $\mathbb{D}$ — либо кольцо целых чисел $\mathbb{Z}$, либо кольцо многочленов от нескольких переменных над $\mathbb{Z}$. Пусть t — новая переменная над $\mathbb{D}$, а $\mathbb{D}[t]$ — кольцо обычных коммутативных многочленов от t над $\mathbb{D}$. Мы будем работать в кольце Оре $\mathbb{D}[t][x;\sigma,\delta]$, у которого кольцо констант содержит $\mathbb{D}$. Заметим, что σ — автоморфизм $\mathbb{D}[t]$.

4.1. Вычисление gcrd. Пусть p — простое. Гомоморфизм колец ϕ_p из $\mathbb{D}[t]$ в $\mathbb{Z}_p[t]$ называется *модулярным относительно* σ, если

$$\phi_p(\mathbb{D}) = \mathbb{Z}_p, \quad \phi_p(t) = t, \quad \deg_t(\sigma(t)) = \deg_t \phi_p(\sigma(t)).$$

Определим автоморфизм σ_p на $\mathbb{Z}_p[t]$ как переводящий t в $\phi_p(\sigma(t))$, а любой элемент $\mathbb{Z}_p$ — в себя. Далее, определим аддитивное отображение δ_p из $\mathbb{Z}_p[t]$ в себя как переводящее t^n в $\phi_p(\delta(t^n))$ при $n \in \mathbb{N}$. Непосредственно проверяется, что диаграммы

$$\begin{array}{ccc} \mathbb{D}[t] & \xrightarrow{\sigma} & \mathbb{D}[t] \\ {\scriptstyle\phi_p}\downarrow & & \downarrow{\scriptstyle\phi_p} \\ \mathbb{Z}_p[t] & \xrightarrow{\sigma_p} & \mathbb{Z}_p[t] \end{array} \qquad \begin{array}{ccc} \mathbb{D}[t] & \xrightarrow{\delta} & \mathbb{D}[t] \\ {\scriptstyle\phi_p}\downarrow & & \downarrow{\scriptstyle\phi_p} \\ \mathbb{Z}_p[t] & \xrightarrow{\delta_p} & \mathbb{Z}_p[t] \end{array}$$

коммутативны и что $\mathbb{Z}_p[t][x,\sigma_p,\delta_p]$ — кольцо Оре. Модулярный гомоморфизм ϕ_p можно продолжить до отображения из $\mathbb{D}[t][x,\sigma,\delta]$ в $\mathbb{Z}_p[t][x,\sigma_p,\delta_p]$, переводящего $\sum\limits_i a_i x^i$ в $\sum\limits_i \phi_p(a_i)x^i$, где $a_i \in \mathbb{D}[t]$. Это продолженное отображение также будет обозначаться ϕ_p; тот факт, что оно является гомоморфизмом колец, устанавливается прямой проверкой.

Пусть e — элемент $\mathbb{Z}_p$. Под отображением вычисления ψ_e из $\mathbb{Z}_p[t]$ в $\mathbb{Z}_p$ мы понимаем отображение, которое переводит $\sum\limits_i m_i t^i$ в $\sum\limits_i m_i e^i$, где $m_i \in \mathbb{Z}_p$. Такое отображение вычисления можно продолжить до отображения из $\mathbb{Z}_p[t][x,\sigma_p,\delta_p]$ в $\mathbb{Z}_p[x]$, переводящего $\sum\limits_i a_i x^i$ в $\sum\limits_i \psi_e(a_i)x^i$, где $a_i \in \mathbb{Z}_p[t]$. Это продолженное отображение снова обозначается ψ_e.

Пример 4.1. Рассмотрим дифференциальное кольцо $D = \mathbb{Z}_p[t][x;1,\frac{d}{dt}]$ и отображение вычисления ψ_e. Если ψ_e — гомоморфизм колец из D в$\mathbb{Z}_p[x]$ с как-либо определенным умножением, то $\psi_e(xt) = \psi_e(tx+1) = ex+1$ и, с другой стороны,

$$\psi_e(xt) = \psi_e(x)\psi_e(t) = xe = x(\underbrace{1+\cdots+1}_{e \text{ раз}}) = ex.$$

Это приводит к противоречию.

Итак, как бы мы ни определили умножение в $\mathbb{Z}_p[x]$, ψ_e обычно не является гомоморфизмом колец. Это лишь гомоморфизм модулей (гомоморфизм левого модуля $\mathbb{Z}_p[t][x]$ над $\mathbb{Z}_p[t]$ в $\mathbb{Z}_p[t]$ над $\mathbb{Z}_p$).

Ключевая задача в модулярных gcrd-методах формулируется следующим образом.

Задача E. По данным P_1, P_2 в $\mathbb{Z}_p[t][x,\delta_p,\sigma_p]$ и отображению вычисления ψ_e вычислить образ $\operatorname{gcrd}(P_1,P_2)$ под действием ϕ_e.

Алгоритм GCRD_e, описанный в [21], решает задачу E. Пусть $\deg P_i = n_i$, $i = 1,2, n = \max(n_1,n_2)$, $n_t = \max(\deg_t P_1, \deg_t P_2)$ и $G = \operatorname{gcrd}(P_1,P_2)$ имеет степень g. Число тех отображений ψ_e, для которых GRCD_e выдает неправильные образы или ошибку, не превосходит $(n_1+n_2)n_t$. Следовательно, GCRD_e выдает достаточно много правильных образов для процесса комбинирования, когда простое число p достаточно велико. Сложность GCRD_e близка к $\left(n_t n^2 + n^3\right)$ в дифференциальном случае. Слагаемое n^3 происходит из редукции строк в матрице Сильвестра

для P_1 и P_2, содержащей (n_1+n_2) строк и (n_1+n_2) столбцов. Мы изложим улучшенный вариант алгоритма GCRD_e, сложность которого ограничена сверху величиной $\big(n_t(n-g)^2+(n-g)^3\big)$. Это улучшение позволяет нашему модулярному методу для gcrd эффективно работать, когда g велико. В общих чертах, улучшенный алгоритм — это тщательно спланированный процесс редукции строк в матрице, ассоциированной с $\operatorname{sres}_{g-1}(P_1,P_2)$ и содержащей $n_1+n_2-2(g-1)$ строк и n_1+n_2-g+2 столбцов.

Чтобы описать улучшение, условимся о терминологии. Мы отсылаем читателя к [20] за определением субрезультантов P_1 и P_2 и связанными с этим обозначениями. Напомним, что m-й субрезультант P_1 и P_2 обозначается S_m для $m=n_2,n_2-1,\dots,0$. Пара последовательных субрезультантов S_m и S_{m+1} называется gcrd-*парой* P_1 и P_2 *с индексом* m, если $\deg S_m=m$ и $S_{m+1}=0$. Непосредственно из [20, теорема 4.2] и структуры пропусков в цепочке субрезультантов вытекает следующее утверждение.

Предложение 4.1. *Пусть P_1,P_2 в $\mathbb{Z}_p[t][x,\delta_p,\sigma_p]$ имеют степени n_1 и n_2 соответственно, где $n_1\geqslant n_2>0$. Тогда P_1 и P_2 имеют* gcrd-*пару, если и только если* gcrd P_1 *и P_2 имеет положительную степень. Если* gcrd-*пара существует, то она единственна.*

При заданной последовательности

$$x^{n_2-1}P_1,\ \dots,\ xP_1,\ P_1,\ x^{n_1-1}P_2,\ \dots,\ xP_2,\ P_2, \tag{9}$$

отображение вычисления ψ_e называется *собственным* относительно P_1 и P_2, если

$$\deg\psi_e(x^iP_1)=(n_1+i)\qquad\text{при } i=0,\dots,(n_2-1),$$
$$\deg\psi_e(x^jP_2)=(n_2+j)\qquad\text{при } j=0,\dots,(n_1-1).$$

Собственное относительно P_1 и P_2 отображение ψ_e называется *неудачным*, если $\deg\psi_e(S_m)<\deg S_m$ для некоторого ненулевого S_m. Заметим, что это определение менее ограничительно, чем определение неудачных отображений вычисления в [21]. Пара образов последовательных субрезультантов S_m и S_{m+1} под действием ψ_e называется *псевдо*-gcrd-*парой с индексом* m, если $\deg\psi_e(S_m)=m$ и $\psi_e(S_{m+1})=0$.

Предложение 4.2. *Пусть P_1,P_2 в $\mathbb{Z}_p[t][x,\delta_p,\sigma_p]$ имеют степени n_1 и n_2 соответственно, $n_1\geqslant n_2>0$. Пусть G — унитарный* gcrd *для P_1 и P_2 степени g. Пусть ψ_e — собственное относительно P_1 и P_2 отображение вычисления. Тогда справедливы следующие утверждения.*

1) *Если ψ_e не неудачно и g положительно, то $(\psi_e(S_g),\psi_e(S_{g-1}))$ — единственная псевдо-*gcrd-*пара для P_1 и P_2 под действием ψ_e и $\psi_e(G)$ — унитарный многочлен, ассоциированный с $\psi_e(S_g)$.*
2) *Если ψ_e не неудачно, а g — нулевое, то у P_1 и P_2 нет псевдо-*gcrd-*пар и $\phi_e(S_0)$ — ненулевой.*
3) *Если ψ_e неудачно и у P_1, P_2 есть псевдо-*gcrd-*пара $(\psi_e(S_m),\psi_e(S_{m+1}))$, то $m\geqslant g$. В этом случае $m=g$, $\psi_e(G)$ — по-прежнему унитарный многочлен, ассоциированный с $\psi_e(S_g)$.*

Доказательство. Первое и второе утверждения следуют из предложения 4.1 и того факта, что ψ_e отображает цепочку субрезультантов P_1 и P_2 с сохранением степени. Последнее же следует из того, что $\operatorname{sres}_{g-1}(P_1,P_2)=\operatorname{sres}_{g-2}(P_1,P_2)=\ldots=\operatorname{sres}_0(P_1,P_2)=0$. □

Для данных последовательности (9) и собственного относительно P_1 и P_2 отображения вычисления ψ_e мы ищем псевдо-grcd-пару в последовательности $\psi_e(P_2)$, $\psi_e(S_{n_2-1})$, $\psi_e(S_{n_2-2})$, $\psi_e(S_0)$. Пусть M_{n_2-1} — ассоциированная с S_{n_2-1} матрица. Вычисляем $H_{n_2-1}=\psi_e(S_{n_2-1})$ гауссовым исключением в строках $\psi_e(M_{n_2-1})$. Если $H_{n_2-1}=0$, то мы получаем псевдо-gcrd-пару $(\psi_e(P_2),H_{n_2-1})$ и возвращаем унитарный многочлен, ассоциированный с $\psi_e(P_2)$. В противном случае полагаем $d=\deg H_{n_2-1}$.

Согласно [20, теорема 4.2], нам нужно вычислить только $H_d=\psi_e(S_d)$. Если степень H_d меньше d, то ψ_e неудачно, выдаем сообщение об ошибке. Иначе вычисляем $H_{d-1}=\psi_e(S_{d-1})$ гауссовым исключением в строках матрицы, ассоциированной с $\psi_e(S_{d-1})$. Если $H_{d-1}=0$, получаем псевдо-gcrd-пару (H_d,H_{d-1}) и возвращаем унитарный многочлен, ассоциированный с H_d. Иначе заменяем

d на $\deg H_{d-1}$ и повторяем процесс. Если псевдо-gcrd-пар не найдено, мы в конце концов вычислим $H_0 = \psi_e(S_0)$. Если $H_0 \neq 0$, то возвращаем 1 (в этом случае P_1 и P_2 имеют тривиальный gcrd). Иначе сообщаем об ошибке (в этом случае значение e — неудачное).

Описанный выше процесс может выдать либо унитарный многочлен H положительной степени из $\mathbb{Z}_p[x]$, либо 1, либо сообщение об ошибке. В первом случае H — либо образ G под действием ψ_e, либо $\deg H > g$, что означает, что ψ_e неудачно, согласно предложению 4.2. Во втором случае G тривиален. В последнем случае ψ_e неудачно. Имеется не более $n_2^2(n_1+n_2)n_t$ неудачных отображений вычисления. Так как матрица M_i, ассоциированная с S_i, является подматрицей в матрице M_j, ассоциированной с S_j при $i > j$, результаты, полученные при гауссовом исключении в M_i, можно повторно использовать при гауссовом исключении в M_j. Таким образом, сложность вычисления $\psi_e(S_{n_2-1})$, $\psi_e(S_{n_2-2})$, …, $\psi_e(S_{g-1})$ та же, что и сложность вычисления $\psi_e(S_{g-1})$ гауссовым исключением. Последняя сложность ограничена выражением $(n_t(n-g)^2+(n-g)^3)$, в котором $n_t(n-g)^2$ — сложность вычисления $\psi_e(M_{g-1})$, а $(n-g)^3$ — сложность гауссовых исключений в M_{g-1} для дифференциального случая. Использование описанного выше метода вместо GCRD_e дает нам общее улучшение модулярного метода поиска gcrd при g, близком к n_2.

Эксперимент 1. Для вычисления gcrd двух данных многочленов Оре p_1 и p_2 реализованы три разных метода: Евклида, без использования дробей и модулярный. Эвристически выбирается один из этих трех методов на основании догадок о степени $\gcrd(p_1, p_2)$.

Таблица 1 показывает сравнительное время работы в эксперименте[1]. Случайно порождается 10 пар многочленов в дифференциальном кольце. На каждую пару многочленов p_1 и p_2 наложены следующие ограничения:

$$\deg p_1, \deg p_2 \leqslant 17, \quad \deg \gcrd(p_1, p_2) \geqslant 2.$$

В таблицу также включено время, потраченное функцией `DEtools[GCRD]`.

Таблица 1. Вычисление gcrd: время (в секундах) для разных методов.

	Евклида	Без дробей	Модулярный	Эвристический	DEtools
1	65.72	27.09	16.57	16.94	33.30
2	184.96	56.11	28.64	29.44	49.85
3	168.88	103.03	31.87	32.10	55.60
4	221.47	166.94	43.09	43.89	70.11
5	25.06	22.58	21.43	22.14	14.94
6	65.61	53.16	33.70	31.92	30.27
7	123.79	79.32	40.87	41.96	37.97
8	148.57	68.68	33.89	35.05	52.83
9	28.71	14.76	15.42	15.63	15.79
10	120.57	85.44	27.54	28.65	59.24

Если $\gcrd(p_1, p_2)$ тривиален, то модулярный метод заметно быстрее, чем любой немодулярный метод, поскольку модулярный метод может обнаружить, что p_1 и p_2 взаимно просты, удачным модулярным гомоморфизмом и удачным отображением вычисления. Если $\gcrd(p_1, p_2)$ нетривиален, экспериментальные результаты показывают, что эффективность модулярного метода зависит от следующих факторов:

а) сколько делений требуется для вычисления $\gcrd(p_1, p_2)$ в правом алгоритме Евклида;

б) насколько «прост» $\gcrd(p_1, p_2)$.

Под «простотой» мы подразумеваем, что коэффициенты имеют низкие степени и короткие целые коэффициенты. Чем больше требуется делений, тем больше работы проделают немодулярные методы. Чем проще $\gcrd(p_1, p_2)$, тем меньше образов требуется для восстановления настоящего gcrd в модулярном методе. При любых входных данных модулярный метод не приводит к разбуханию каких-либо промежуточных выражений.

[1]Все приведенные времена были получены на 400MHz SUN SPARC SOLARIS с 1Gb RAM.

4.2. Вычисление lclm. Применим модулярную технику к вычислению lclm. Пусть $P_1, \dots, P_m$ из $\mathbb{D}[t][x;\sigma,\delta]$ имеют соответственно положительные степени $d_1, \dots, d_m$. Пусть $L = \operatorname{lclm}(P_1, \dots, P_m)$. Чтобы вычислить L, можно сначала вычислить $L_{12} = \operatorname{lclm}(P_1, P_2)$, а затем вычислить $\operatorname{lclm}(L_{12}, P_3, \dots, P_m)$ рекурсивно (по m). Этот «многошаговый» алгоритм не очень хорошо работает на практике, отчасти потому, что коэффициенты промежуточных lclm обычно гораздо сложнее, чем у P_i.

Процедура *LCLM* в Maple-пакете `DEtools`, написанная ван Хоие, дает прямой метод вычисления lclm нескольких многочленов Оре. Этот метод работает следующим образом. Пусть

$$d = d_1 + \cdots + d_m, \quad Q_d = q_d x^d + \cdots + q_0,$$

где $q_0, \dots, q_d$ — произвольные коэффициенты. Для $i = 1, \dots, m$ вычисляется правый остаток R_i от деления Q_d на P_i. Ясно, что Q_d — общее левое кратное $P_1, \dots, P_m$ степени не выше d, если и только если $R_1 = \cdots = R_m = 0$. Это приводит к линейной однородной алгебраической системе

$$(q_0, \dots, q_d) M_d = 0, \tag{10}$$

где M — $((d+1) \times d)$-матрица над k. Для удобства мы будем говорить, что $\tilde{Q}_d = \tilde{q}_d x^d + \cdots + \tilde{q}_0$ из $\mathbb{D}[t][x;\sigma,\delta]$ — решение (10), если $(\tilde{q}_0, \dots, \tilde{q}_d)$ — решение системы (10); таким образом, L — ненулевое решение (10) наименьшей степени.

Итак, чтобы найти L, надо найти решение (10) наименьшей степени ($\deg L$ может быть меньше d).

Предложение 4.3. *Значение* $\deg L$ *равно рангу* M_d *из* (10).

Доказательство. Пусть $\deg L = l$. Поскольку $l \leqslant d$, все $L, xL, \dots, x^{d-l}L$ являются решениями (10). Итак, пространство решений системы (10) имеет размерность не меньше $(d+1-l)$. С другой стороны, любое ненулевое решение $\tilde{Q}_d$ уравнения (10) — общее левое кратное $P_1, \dots, P_m$ степени не выше d, так что правый остаток от деления $\tilde{Q}_d$ на L равен нулю, т.е. $\tilde{Q}$ — k-линейная комбинация $L, xL, \dots, x^{d-l}L$. Таким обрзом, пространство решений (10) имеет размерность $(d+1-l)$. Следовательно, ранг M_d равен d. □

Для вычисления L мы, во-первых, строим матрицу M_d, заданную (10). Во-вторых, применяем модулярное отображение и отображение вычисления к элементам M_d, чтобы получить матрицу M'_d над $\mathbb{Z}_p$. В-третьих, вычисляем ранг r для M'_d. В-четвертых, полагаем $Q_r = q_r x^r + \cdots + q_0$, где $q_0, \dots, q_r$ — неопределенные коэффициенты. Для $i = 1, \dots, m$ вычисляем правый остаток R_i от деления Q_r на P_i. Условие $R_1 = \cdots = R_m = 0$ дает линейную однородную алгебраическую систему

$$(q_0, \dots, q_r) M_r = 0. \tag{11}$$

Любое нетривиальное решение (11) соответствует $\operatorname{lclm}(P_1, \dots, P_m)$, потому что $r \leqslant \deg L$ согласно предложению 4.3. Если система (11) имеет только тривиальное решение, то заменяем r на $(r+1)$ и повторяем четвертый шаг. Так как r почти всегда равно рангу M_d, то на практике, скорее всего, не возникнет необходимости повторения четвертого шага. Мы будем ссылаться на этот метод как на «одношаговый» метод.

Эксперимент 2. Множество испытаний, связанных с вычислением lclm, состоит из 10 троек многочленов в дифференциальном кольце. На каждую тройку многочленов p_1, p_2 и p_3 мы накладываем следующие ограничения:

$$\deg p_1 = \deg p_2 = 5, \quad \deg \operatorname{gcrd}(p_1, p_2) = 2, \quad \deg p_3 = 3.$$

Таблица 2 показывает сравнение времени работы многошагового и одношагового метода. Мы также включаем время для функции `DEtools[LCLM]`. Заметим, что если $\deg \operatorname{lclm}(p_1, p_2, p_3) = \deg p_1 + \deg p_2 + \deg p_3$, то время для одношагового метода и `DEtools[LCLM]` примерно одинаково.

Таблица 2. Вычисление lclm: время (в секундах) для разных методов.

	Многошаговый	Одношаговый	DEtools
1	114.53	25.99	87.48
2	147.36	24.28	107.60
3	111.95	33.36	105.33
4	124.15	30.41	84.41
5	128.65	30.76	102.63
6	144.56	29.35	103.03
7	96.84	18.60	61.73
8	115.08	28.36	92.74
9	140.59	21.18	122.81
10	123.97	16.13	62.31

Мы завершаем этот раздел рассмотрением вычислений lclm в прямом алгоритме вычисления минимального телескопирующего оператора для рациональной функции [19]. Рассмотрим рациональную функцию $R(n,k) = R_1 + R_2 + R_3$, где

$$R_1 = \frac{n+1}{(2n+5k+3)^2} + \frac{n}{(2n+5k+5)^2},$$
$$R_2 = \frac{n+2}{3n+4k+4} - \frac{3}{3n+4k-2},$$
$$R_3 = \frac{(n-3)^2}{n-7k+5} + \frac{1}{n-7k+6}.$$

Вычисленные минимальные телескопирующие операторы L_1 для R_1, L_2 для R_2 и L_3 для R_3 равны

$$\begin{aligned}
L_1 = \mathrm{OrePoly}\Big(&(n+5)(n+4)(n+3)(n+2)(2n+7),\ 5(n+5)(n+4)(n+3),\\
&-5(n+5)(n+4)(n+1),\ 5(n+5)(n+2)(n+1),\\
&-5(n+3)(n+2)(n+1),\ -(2n+5)(n+4)(n+3)(n+2)(n+1)\Big),\\
L_2 = \mathrm{OrePoly}\Big(&-n^2-10n-15,\ 0,\ -12,\ 0,\ n^2+6n-1\Big),\\
L_3 = \mathrm{OrePoly}\Big(&n^{14}+14n^{13}+63n^{12}+28n^{11}-553n^{10}-1218n^9+929n^8+\\
&+4984n^7+1848n^6-6496n^5-4592n^4+2688n^3+2304n^2+1,\\
&-7(2n+1)(n-1)^2(n+3)^2(n+2)^2(n+1)^2n^2,\\
&7(2n+1)(n+3)^2(n+2)^2(n+1)^2n^2,\ -7(2n+1)(n+3)^2(n+2)^2(n+1)^2,\\
&7(2n+1)(n+3)^2(n+2)^2,\ -7(2n+1)(n+3)^2,\ 14n+7,\\
&-n^{14}+28n^{12}-294n^{10}+1444n^8-3409n^6+3528n^4-1296n^2-1\Big)
\end{aligned}$$

(о представлении многочленов Оре см. раздел 5.2). Минимальный телескопирующий оператор L для рациональной функции R равен $\mathrm{lclm}(L_1, L_2, L_3)$. Если воспользоваться одношаговым методом, то это вычисление L займет 6.28 с, использование многошагового метода потребует 273.90 с.

5. Пакет `OreTools`

Основная цель пакета `OreTools` — предоставить простейшие операции в заданном кольце Оре и упростить дальнейшую разработку алгоритмов различных вычислений в кольцах Оре. Пакет интегрирован в Maple. В частности, он используется (a) как основа пакета `LinearOperators`, включающего функции вычисления минимальных полностью факторизуемых аннуляторов [9], и для вычисления даламберовых решений неоднородных линейных функциональных уравнений [7];

(б) в пакете `SumTools` [4] для эффективного прямого вычисления минимальных Z-пар рациональных функций [19], для вычисления бесконечных сумм методом аккуратного интегрирования и (в) в пакете `Slode` [3] для нахождения формальных решений линейных однородных дифференциальных уравнений в виде рядов с даламберовыми коэффициентами.

В этом разделе мы даем обзор пакета `OreTools`. Детальное обсуждение предлагаемых возможностей и детали реализации см. в [5]. Ранняя версия пакета `OreTools` описывалась в [9, § 6]. Код этой версии был разработан Е. В. Зимой.

5.1. Определение кольца Оре и сопряженного к нему; работа с параметрами этих колец. На рисунке 1 представлено множество функций, которые помогают определить кольцо Оре и кольцо, сопряженное к данному кольцу Оре (которое само является кольцом Оре), а также функции для работы с параметрами кольца Оре.

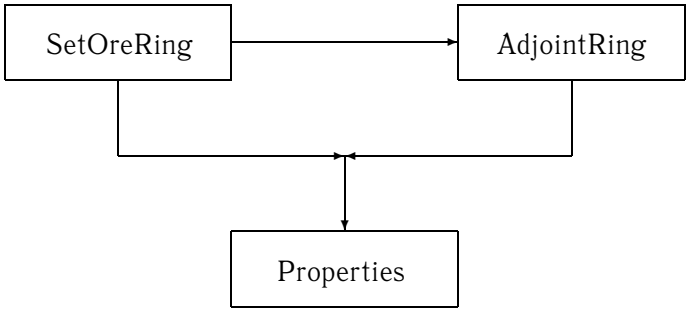


Рис. 1. Определение кольца Оре и работа с его параметрами

Кольцо Оре от одной переменной определяется посредством функции *SetOreRing*. Предопределены *дифференциальное* кольцо, кольцо со *сдвигом* и с *q-сдвигом*. Чтобы определить другие кольца, нужно задать процедуры вычисления σ, δ, $\theta(1)$ и σ^{-1}.

Сопряженное к данному кольцу Оре определяется функцией *AdjointRing*. Ее вход — кольцо Оре, а выход — сопряженное к нему.

Со свойствами данного кольца Оре, напр., σ, σ^{-1}, $\theta(1)$, δ, можно работать в подмодуле `Properties`.

5.2. Средства работы с многочленами Оре. Многочлен Оре представляется структурой OrePoly. Она состоит из ключевого слова OrePoly с последовательностью коэффициентов, начинающейся со степени нуль. Например, в дифференциальном случае с дифференциальным оператором D $\mathrm{OrePoly}(2/t, t, t+1, 1)$ представляет оператор $2/t + tD + (t+1)D^2 + D^3$.

На рис. 2 представлены основные средства работы с многочленами Оре. Их можно разделить на четыре группы: утилиты, арифметические операции, функции преобразования и математические операции.

Утилиты включают функции для таких действий с многочленами Оре, как, например, нахождение старшего и младшего коэффициентов или степени данного многочлена Оре.

Основные арифметические операции над многочленами Оре включают:

1) линейные операции: сложение, вычитание, умножение на скаляр;
2) операции по нормализации: вычисление содержания, примитивной части, левого и правого унитарных ассоциированных;
3) умножение, деления (левые и правые остатки и частные);
4) левые и правые gcd, lcm, расширенные gcd и gcrd, зависящие от параметра [2].

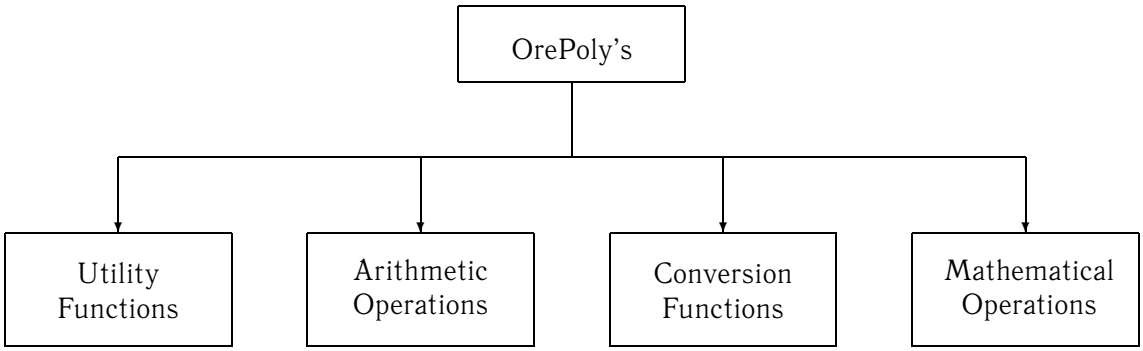


Рис. 2. Средства работы с многочленами Оре

Функции преобразования играют роль интерфейса между пакетом `OreTools` и системой Maple. Они включают в себя функции прямого и обратного преобразования между данным многочленом Оре и соответствующим линейным функциональным уравнением.

Пакет поддерживает некоторые математические операции. Они включают в себя функции аккуратного интегрирования (раздел 3.3) и вычисления интегрирующего множителя (раздел 3.2).

Подмодуль `Modular` предоставляет пользователю основные операции над многочленами Оре, коэффициенты которых — рациональные функции над $\mathbb{Z}_p$; а подмодуль `FractionFree` предоставляет операции без использования дробей над многочленами Оре, коэффициенты которых — многочлены над $\mathbb{Z}$.

5.3. Примеры. В кольце A со сдвигом

```
> A := SetOreRing(n,'shift');
```

$$A := \mathrm{UnivariateOreRing}(n, \mathit{shift})$$

рассмотрим два многочлена Оре p_1 и p_2:

```
> p_1 := \OrePoly((n-3)*n^2,n^4+n^3-4*n^2-n-2,
  n^4+3*n^3+2*n^2+n-4,n^3+6*n^2+10*n+2,n^2+6*n+6):
> p_2 := \OrePoly((n-3)*n^3,n^5+n^4-6*n^3+4*n^2-3*n-2,
  n^5+n^4-n^3+7*n^2-2*n-3,n^4+5*n^3+7*n^2+5*n+1,(n^2+6*n+6)*n):
```

Вычислим gcrd p_1 и p_2:

```
> GCD['right'](p_1,p_2,A);
```

$$\mathrm{OrePoly}\left(\frac{n-3}{n^2-3}, 1\right).$$

Вычислим gcld p_1 и p_2:

```
> GCD['left'](p_1,p_2,A);
```

$$\mathrm{OrePoly}\left(n^2, n+1, 1\right).$$

Для двух многочленов Оре p_3 и p_4

```
> p_3 := \OrePoly(1,1,0,(a+2)*n):
> p_4 := \OrePoly(0,(a+2)*(a+1)*n):
```

предположим заранее, что значение параметра a удовлетворяет уравнению $a(a+1)(a+2) = 0$, и

вычислим gcrd p_3 и p_4 в зависимости от параметра a:

```
> ParametricGCRD(p_3, p_4, (a+1)*(a+2)*a, a, A);
```

$$\begin{cases} \mathrm{OrePoly}\,(-1) & a = 0, \\ \mathrm{OrePoly}\,(1,1,0,n) & a+1 = 0, \\ \mathrm{OrePoly}\,(1,1) & a+2 = 0. \end{cases}$$

6. Сравнение

Существуют и другие Maple-пакеты, которые предоставляют средства для работы с общими кольцами Оре или с конкретным кольцом Оре. Среди них пакет `Ore_algebra` [11] для колец Оре от нескольких переменных, пакет `DEtools` для дифференциального случая, пакет `LREtools` для случая сдвига и пакет `QDifferenceEquations` для случая q-сдвига. Хотя основное внимание `LREtools` и `QDifferenceEquations` сосредоточено на поиске решений специального вида (напр., полиномиальных, рациональных) для линейных рекуррентных (q-рекуррентных) соотношений с полиномиальными коэффициентами, пакеты `Ore_algebra` и `DEtools` предоставляют, хотя и в меньшей степени по сравнению с пакетом `OreTools`, поддержку основных операций в кольцах Оре.

Сравнение `DEtools` с `OreTools` проведено в двух экспериментах, описанных в разделе 4. В настоящем разделе мы сравниваем `Ore_algebra` с `OreTools`.

Единственная функциональность пакетов, которая позволяет провести прямое сравнение между `Ore_algebra` и `OreTools`, — это расширенный правый алгоритм Евклида: *skew_gcdex* в `Ore_algebra` и *ExtendedGCD* в `OreTools`. Использование *skew_gcdex* является единственным способом вычислить gcrd в пакете `Ore_algebra` (неизбежное построение двух дополнительных многочленов иногда оказывается избыточным).

В этом эксперименте использованы два набора тестов. Каждый набор состоит из 10 пар многочленов p_1 и p_2. Пары первого набора порождались в кольце со сдвигом, а второго — в дифференциальном кольце.

На каждую пару p_1, p_2 наложены следующие ограничения:

$$7 \leqslant \deg p_1, \deg p_2 \leqslant 10, \quad \deg \operatorname{gcrd}(p_1, p_2) \geqslant 2.$$

Каждый коэффициент p_1 и p_2 — многочлен степени не более 5 и состоит не более чем из 2 членов.

Таблицы 3 и 4 отражают затраты *ExtendedGCD* и *skew_gcdex* по времени (в секундах) и памяти (в килобайтах).

Таблица 3. OreTools и Ore_algebra: рекуррентный случай.

	ExtendedGCD		skew_gcdex	
	время	память	время	память
1	123	703,329	1,691	4,669,006
2	55	276,828	487	1,555,668
3	183	830,378	1,269	3,420,360
4	44	230,488	648	1,977,186
5	145	654,363	364	1,219,685
6	113	511,026	268	979,230
7	47	236,447	470	1,549,453
8	179	780,795	656	1,984,256
9	49	241,977	128	490,365
10	89	417,157	177	635,439

Стоит отметить, что все кольца Оре, объявленные в пакете `Ore_algebra`, по умолчанию имеют целые коэффициенты, а любой другой тип коэффициентов надо явно объявлять. Поэтому простейшие операции могут потребовать от пользователей нетривиальных усилий и знаний.

Таблица 4. OreTools и Ore_algebra: дифференциальный случай.

	ExtendedGCD		skew_gcdex	
	время	память	время	память
1	24	245,039	765	2,828,435
2	20	169,934	189	976,940
3	38	340,290	437	1,968,124
4	20	167,486	300	1,324,531
5	11	81,216	151	861,778
6	23	206,490	53	360,019
7	17	159,388	216	1,030,755
8	23	201,707	333	1,370,342
9	13	113,148	47	319,017
10	13	117,665	61	418,924

7. Доступ

Информация о доступе к библиотечному архиву пакета `OreTools`, образцам рабочих распечаток Maple, а также об установке пакета находится по следующему адресу:

`http://www.scg.math.uwaterloo.ca/~hqle/code/OreTools/OreTools.html`

СПИСОК ЛИТЕРАТУРЫ

1. *Абрамов С. А.* Рациональные решения линейных обыкновенных дифференциальных и разностных уравнений с полиномиальными коэффициентами// Ж. вычисл. мат. и мат. физ. — 1989. — *11*. — С. 1611–1620.
2. *Глотов П. Е.* Алгоритм поиска наибольшего общего делителя полиномов Оре с полиномиальными коэффициентами, зависящими от параметра// Программирование. — 1998. — *6*. С. 14–21.
3. *Рябенко А. А.* Maple-пакет символьного построения решений линейных обыкновенных дифференциальных уравнений в виде степенных рядов// Программирование. — 1999. — *5*. — С. 71–80.
4. *Abramov S. A., Carette J. C., Geddes K. O., Le H. Q.* Symbolic Summation in Maple/ Technical Report CS-2002-32. — Ontario: School of Computer Science, University of Waterloo, 2002.
5. *Abramov S. A., Le H. Q., Li Z.* `OreTools`: a computer algebra library for univariate Ore polynomial rings/ Technical Report CS-2003-12. — Ontario: School of Computer Science, University of Waterloo, 2003.
6. *Abramov S. A., van Hoeij M.* Integration of solutions of linear functional equations// Integral Transform. Special Functions. — 1999. — *8*, №. 1–2. — С. 3–12.
7. *Abramov S. A., Zima E. V.* D'Alembertian solutions of inhomogeneous linear equations (differential, difference, and some other)// в сб.: Proc. 1996 Int. Symp. on Symbolic and Algebraic Computation (ed. Lakshman Y. N.). — ACM Press, 1996. — С. 232–240.
8. *Abramov S. A., Zima E. V.* A universal program to uncouple linear systems// в сб.: Proc. Int. Conf. on Computational Modeling and Computing in Physics. — Dubna, 1996. С. 16–26.
9. *Abramov S. A., Zima E. V.* Minimal completely factorable annihilators// в сб.: Proc. 1997 Int. Symp. on Symbolic and Algebraic Computation (ed. Küchlin W.). — ACM Press, 1997. — С. 290–297.
10. *Bronstein M., Petkovšek M.* An introduction to pseudolinear algebra/ Theoretical Computer Science. — 1996. № 157. — С. 3–33.
11. *Chyzak F., Salvy B.* Non-commutative elimination in Ore algebras proves multivariate identities// J. Symb. Comput. — 1998. — *26*, № 2. — С. 187–227.
12. *Giesbrecht M., Zhang Y.* Factoring and decomposing Ore polynomials over $\mathbb{F}_p(t)$// Proc 2003 Int. Symp. on Symbolic and Algebraic Computation (в печати).
13. *Cohn P. M.* Free Rings and Their Relations. — Academic Press, 1971.
14. *Cohn P. M.* Skew Fields. Theory of General Division Rings/ Encycl. Mathematics Its Appl. — Cambridge Univ. Press, 1995. — *57*.
15. *Gosper R. W.* Decision procedure for indefinite hypergeometric summation// Proc. Natl. Acad. Sci. USA. — 1978. — *75*. — С. 40–42.
16. *van der Hoeven J.* FFT-like multiplication of linear differential operators// J. Symb. Comput. — 2002. — *33*, № 1. — С. 123–127.

17. *Jacobson N.* Pseudo-linear transformations// Ann. Math. — 1937. — *38*, № 2. — С. 484–507.
18. *Landau E.* Über irreduzible Differentialgleichungen// J. reine angew. Math. — 1902. — *124*. — С. 115–120.
19. *Le H. Q.* A direct algorithm to construct the minimal Z-pairs for rational functions// Adv. Appl. Math. — 2003. — *30*. — С. 137–159.
20. *Li Z.* A subresultant theory for ore polynomials with applications// в сб.: Proc. 1998 Int. Symp. on Symbolic and Algebraic Computation (ed. Gloor O.). — ACM Press, 1998. — С. 132–139.
21. *Li Z., Nemes I.* A modular algorithm for computing greatest common right divisors of Ore polynomials// в сб.: Proc. 1997 Int. Symp. on Symbolic and Algebraic Computation (ed. Küchlin W.). — ACM Press, 1997. — С. 282–289.
22. *Loewy A.* Über reduzible lineare homogene Differentialgleichungen// Math. Ann. — 1903. — *56*. — С. 549–584.
23. *Loewy A.* Über vollstandig reduzible lineare homogene Differentialgleichungen// Math. Ann. — 1906. — *62*. — С. 89–117.
24. *Monagan M. B., Geddes K. O., Heal K. M., Labahn G., Vorkoetter S. M., McCarron J., DeMarco P.* Maple 8. Introductory Programming Guide. — Waterloo Maple Inc., Waterloo, Ontario, Canada, 2002.
25. *Ore O.* Theory of non-commutative polynomials// Ann. Math. — 1933. — *34*. — С. 480–508.
26. *Ore O.* Formale Theorie der linearen Differentialgleichungen, I// J. reine angew. Math. — 1932. — *167*. — С. 221–234.
27. *Ore O.* Formale Theorie der linearen Differentialgleichungen, II// J. reine angew. Math. — 1932. — *167*. — С. 235–252.
28. *Petkovšek M.* Hypergeometric solutions of linear recurrences with polynomial coefficients// J. Symb. Comput. — 1992. — *14*. — С. 243–264.
29. *Poole E. G. C.* Introduction to the theory of linear ordinary differential equations. — New York: Dover Publications Inc., 1936.
30. *Wedderburn J. H. M.* Non-commutative domains of integrity// J. reine angew. Math. — 1932. — *167*. — С. 129–141.

С. А. Абрамов
Вычислительный центр им. Дородницына РАН, Москва
E-mail: abramov@ccas.ru

H. Q. Le
Symbolic Computation Group, University of Waterloo, Canada
E-mail: hqle.@scg.math.uwaterloo.ca

Z. Li
Symbolic Computation Group, University of Waterloo, Canada
E-mail: z6li@scg.math.uwaterloo.ca

Современная математика и ее приложения. Том 13 (2004). С. 40–52

УДК 512.55

ОБОБЩЕННЫЕ ДИФФЕРЕНЦИРОВАНИЯ КВАНТОВОЙ ПЛОСКОСТИ

© 2004 г. **В. А. АРТАМОНОВ**

Аннотация. В работе описываются обобщенные дифференцирования квантовой плоскости.

СОДЕРЖАНИЕ

1. Введение

Пусть k — основное поле с фиксированной квадратной матрицей $\mathbf{q} = (q_{ij}) \in \mathrm{Mat}(n,k)$ размера $n \geqslant 2$, элементы $q_{ij} \in k^*$ которой удовлетворяют условиям $q_{ii} = q_{ij}q_{ji} = 1$ для всех i, j. Кроме того, фиксируем целое число r так, что $0 \leqslant r \leqslant n$. Обозначим через

$$\mathcal{O}_{\mathbf{q}} = k_{\mathbf{q}}[X_1^{\pm 1}, \ldots, X_r^{\pm 1}, X_{r+1}, \ldots, X_n]$$

ассоциативную k-алгебру с единицей, порождаемую элементами

$$X_1, \ldots, X_n, X_1^{-1}, \ldots, X_r^{-1}$$

с определяющими соотношениями

$$\begin{aligned} X_i X_j &= q_{ij} X_j X_i, \quad 1 \leqslant i, j \leqslant r, \\ X_i X_i^{-1} &= X_i^{-1} X_i = 1, \quad 1 \leqslant i \leqslant r. \end{aligned} \tag{1.1}$$

Алгебра $\mathcal{O}_{\mathbf{q}}$ называется *алгеброй квантовых многочленов*, а элементы q_{ij} — *мультипараметрами*. В случае $n = 2$, $r = 0$ алгебра $\mathcal{O}_{\mathbf{q}} = \mathcal{O}_q$ называется *квантовой плоскостью*. При этом $q = q_{12}$.

Алгебра $\mathcal{O}_{\mathbf{q}}$ является координатной алгеброй квантового аффинного пространства $\mathbb{A}^n_{\mathbf{q}}$, если $r = 0$ и координатной алгеброй квантового тора $\mathbb{T}^n_{\mathbf{q}}$ при $r = n$ [11]. Объединяя оба случая, мы можем рассмотреть случай произвольного r, $0 \leqslant r \leqslant n$. Тогда алгебру $\mathcal{O}_{\mathbf{q}}$ можно рассматривать как координатную алгебру $\mathbb{T}^r_{\mathbf{q}} \times \mathbb{A}^{n-r}_{\mathbf{q}}$ [11, с. 15].

Алгебры $\mathcal{O}_{\mathbf{q}}$ при $r = n$ были введены в [14]. Один из основных результатов [14] состоит в описании алгоритма вычисления размерности Крулля алгебры $\mathcal{O}_{\mathbf{q}}$ в терминах мультипараметров. Следующая теорема Брукса [10] решает проблему, поставленную в [14].

Теорема 1.1. *Пусть d — размерность Крулля алгебры $\mathcal{O}_{\mathbf{q}}$ при $r = n$. Тогда d равно глобальной размерности алгебры $\mathcal{O}_{\mathbf{q}}$ и равно максимальному числу коммутирующих одночленов от $X_1, \ldots, X_n$, мультииндексы которых независимы в $\mathbb{Z}^n$.*

Работа выполнена при поддержке Российского фонда фундаментальных исследований (проект № 03-01-00167) и грантов INTAS-00-566 и НШ-1910.2003.1.

Алгебра $\mathcal{O}_{\mathbf{q}}$ является левой и правой нетеровой областью с телом частных F. При лексикографическом порядке на множестве мультииндексов А. И. Мальцев и Б. Нейман построили тело косых (квантовых) лорановских рядов $\mathcal{F}$, которое содержит F в качестве подтела [1]. Тело $\mathcal{F}$ определяется как множество всех отображений $f : \mathbb{Z}^n \to k$, для которых $\operatorname{supp} f = \{m \in \mathbb{Z}^n \mid f(m) \neq 0\}$ является артиновым множеством по отношению к лексикографическому порядку в $\mathbb{Z}^n$. Элемент $f \in \mathcal{F}$ можно рассматривать как ряд $f = \sum\limits_{m\in\mathbb{Z}^n} f(m)X^m$. Основными объектами исследования в настоящей работе будут алгебры $\mathcal{O}_{\mathbf{q}}$ и тела F, $\mathcal{F}$.

В разделе 2 излагаются недавние результаты по автоморфизмам и дифференцированиям общих квантовых многочленов. В разделах 3 и 4 доказываются новые результаты о скобках Пуассона и обобщенных дифференцированиях квантовой плоскости $k_q[X, Y] = \mathcal{O}_q$ и квантового тора $k_q[X^{\pm1}, Y^{\pm1}]$. В теоремах 4.1, 4.2 излагается описание обобщенных дифференцирований алгебр $k_q[X, Y]$, $k_q[X^{\pm1}, Y^{\pm1}]$. Далее в теоремах 4.4, 4.11 показано, что если D — ненулевое алгебраическое γ-дифференцирование, то γ является торическим автоморфизмом. В случае нулевой характеристики любое алгебраическое γ-дифференцирование с торическим автоморфизмом γ является нулевым. В случае положительной характеристики всегда существует ненулевое алгебраическое дифференцирование. Аналогичные результаты для случая не менее трех переменных рассмотрены в [7].

2. Автоморфизмы и дифференцирования

Автоморфизмы и дифференцирования алгебры $\mathcal{O}_{\mathbf{q}}$ рассматривались в [3] (случай $r = 0$) и в [16] (случай $r = n$). Мы рассмотрим уточнение этих результатов в специальном «общем» случае. До конца работы мы будем предполагать, что алгебра $\mathcal{O}_{\mathbf{q}}$ является *общей алгеброй квантовых многочленов*. Это означает, что мультипараметры q_{ij}, $1 \leqslant i < j \leqslant n$, независимы в мультипликативной группе k^* поля k. Если $n = 2$, то это означает, что $q = q_{12}$ не является корнем из 1.

Из (1.1) следует, что алгебра $\mathcal{O}_{\mathbf{q}}$ имеет *торические* автоморфизмы γ вида

$$\gamma(X_i) = \gamma_i X_i, \quad \gamma_i \in k^*, \quad 1 \leqslant i \leqslant n. \tag{2.1}$$

Все торические автоморфизмы образуют подгруппу $\operatorname{Aut}^+ \mathcal{O}_{\mathbf{q}}$ в группе $\operatorname{Aut} \mathcal{O}_{\mathbf{q}}$ всех автоморфизмов. Если $r = n$, то дополнительно имеются *зеркальные* автоморфизмы τ, где

$$\tau(X_i) = \tau_i X_i^{-1}, \quad \tau_i \in k^*, \quad 1 \leqslant i \leqslant n.$$

Легко видеть, что любой зеркальный автоморфизм имеет порядок 2 и все зеркальные автоморфизмы образуют смежный класс по подгруппу торических автоморфизмов.

Для дальнейшего нам потребуется один из результатов работы [16].

Теорема 2.1. *Пусть γ — эндоморфизм алгебры $\mathcal{O}_q$ такой, что $n = 2$. Если $r = n = 2$, то существуют такие целые числа l, s, t, v и ненулевые коэффициенты $\beta, \xi \in k$, что*

$$\gamma(X) = \beta X^l Y^s, \quad \gamma(Y) = \xi X^t Y^v, \quad lv - st = 1. \tag{2.2}$$

В частности, γ является автоморфизмом.

Если $r = 1$ и γ — автоморфизм алгебры $\mathcal{O}_q$, то существует такое целое число t и коэффициенты $\beta, \delta \in k^*$, что

$$\gamma(X) = \beta X, \quad \gamma(Y) = \delta X^s Y. \tag{2.3}$$

Если $r = 0$, то любой автоморфизм алгебры $\mathcal{O}_q$ является торическим.

Следствие 2.2. $\operatorname{Aut} k_q[X, Y] \subset \operatorname{Aut} k_q[X^{\pm1}, Y] \subset \operatorname{Aut} k_q[X^{\pm1}, Y^{\pm1}]$.

Следствие 2.3. *Пусть $0 \leqslant r < n = 2$. Тогда каждый автоморфизм алгебры $\mathcal{O}_q$ является торическим.*

Следствие 2.4. *Пусть $r = n = 2$ и γ — автоморфизм конечного порядка алгебры $\mathcal{O}_q$, причем порядок γ не делится ни на 4, ни на 3. Тогда γ — либо торический, либо зеркальный автоморфизм.*

Теорема 2.5. *Пусть G — конечная группа автоморфизмов алгебры $\mathcal{O}_q = k_q[X^{\pm 1}, Y^{\pm 1}]$ (т.е. $r = n = 2$). Если G^+ — подгруппа торических автоморфизмов из G, то $G^+ \lhd G$ и группа G является полупрямым произведением $G = G^+ \leftthreetimes \langle\tau\rangle$, где $\langle\tau\rangle$ — циклическая группа одного из порядков 1, 2, 3, 4, 6.*

Если h — рациональная функция от одной переменной, то отображения

$$X \mapsto h(Y)X, \quad Y \mapsto Y, \quad X \mapsto X, \quad Y \mapsto h(X)Y \tag{2.4}$$

определяют автоморфизм тела F. Кроме того, имеются торические и зеркальные автоморфизмы F.

Гипотеза 2.6 (Ж. Алев)**.** Группа автоморфизмов тела F порождается торическими, зеркальными автоморфизмами, автоморфизмами вида (2.4) и сопряжениями.

Частичное решение гипотезы 2.6 получено в [8].

Напомним некоторые результаты об автоморфизмах алгебры $\mathcal{O}_{\mathbf{q}}$, $n \geqslant 2$, и тела частных F из работ [1, 3, 4, 8, 9, 16]. В статье [3] рассматривается группа автоморфизмов $\operatorname{Aut}\mathcal{O}_{\mathbf{q}}$ и алгебра Ли дифференцирований $\operatorname{Der}\mathcal{O}_{\mathbf{q}}$ в случае $r = 0$. В статье [9] дается полное описание группы $\operatorname{Aut}\mathcal{O}_{\mathbf{q}}$ при $0 \leqslant r \leqslant n$ и $n \geqslant 3$. Необходимо отметить, что случай $r = n$ был также рассмотрен в [16] даже без предположения о том, что алгебра $\mathcal{O}_{\mathbf{q}}$ общая.

Теорема 2.7 (см. [9,16])**.** *Пусть γ — инъективный автоморфизм общей алгебры квантовых многочленов $\mathcal{O}_{\mathbf{q}}$, причем $n \geqslant 3$. Тогда γ является либо торическим, либо (при $r = n$) зеркальным автоморфизмом. В частности, группа $\operatorname{Aut}\mathcal{O}_{\mathbf{q}}$ является полупрямым произведением нормальной подгруппы торических автоморфизмов и циклической группы порядка 2. Если $r < n$, то $\operatorname{Aut}\mathcal{O}_{\mathbf{q}}$ состоит из торических автоморфизмов и потому является абелевой группой. Если G — конечная подгруппа в $\operatorname{Aut}\mathcal{O}_{\mathbf{q}}$, то подалгебра инвариантов $\mathcal{O}_{\mathbf{q}}^G$ является нетеровой слева и справа алгеброй, $\mathcal{O}_{\mathbf{q}}$ является конечно порожденным левым и правым $\mathcal{O}_{\mathbf{q}}^G$-модулем. Кроме того, F^G является телом частных алгебры $\mathcal{O}_{\mathbf{q}}^G$.*

Гипотеза 2.8. Пусть $n \geqslant 3$. Доказать, что группа автоморфизмов тела F порождается торическими, зеркальными автоморфизмами и сопряжениями.

Теорема 2.9 (см. [18])**.** *Пусть $\mathcal{O}_{\mathbf{q}}$ при $r = n$ является простой алгеброй (не обязательно общей). Тогда любой эндоморфизм алгебры $\mathcal{O}_{\mathbf{q}}$ является автоморфизмом.*

Гипотеза 2.10. Доказать, что каждый эндоморфизм тела F является автоморфизмом.

Эндоморфизм γ тела лорановских рядов $\mathcal{F}$ *непрерывен*, если он определяется образами $\gamma(X_1), \ldots, \gamma(X_n)$. Частичное решение гипотезы 2.8 получено в следующей теореме.

Теорема 2.11 (см. [2])**.** *Пусть $\mathcal{O}_{\mathbf{q}}$ — общая алгебра квантовых многочленов и γ — непрерывный автоморфизм тела $\mathcal{F}$. Предположим, что если $n = 2$, то γ имеет конечный порядок. Тогда существует такой элемент $z \in \mathcal{F}$ и торический автоморфизм γ', что γ является произведением $(\operatorname{Ad} z)\gamma'$, где $(\operatorname{Ad} z)x = zxz^{-1}$.*

Теорема 2.12 (см. [2])**.** *Пусть $\mathcal{O}_{\mathbf{q}}$ — общая алгебра квантовых многочленов и G — конечная группа непрерывных автоморфизмов тела $\mathcal{F}$. Тогда существует такой элемент $w \in \mathcal{F}$, что $(\operatorname{Ad} w)G(\operatorname{Ad} w)^{-1}$ состоит из торических автоморфизмов.*

Алгебра $\mathcal{O}_{\mathbf{q}}$ имеет *частные* производные ∂_i, $1 \leqslant i \leqslant n$, где $\partial_i(X_j) = \delta_{ij}X_j$. Заметим, что $[\partial_i, \partial_j] = 0$, $[\partial_i, \operatorname{ad}_u] = \operatorname{ad}_{\partial_i u}$. Если $\operatorname{char} k = p > 0$, то $\partial_i^p = \partial_i$. Поэтому линейная оболочка L операторов $\partial_1, \ldots, \partial_n$ является абелевой алгеброй Ли размерности n. Следующая теорема следует из [3] в случае $r = 0$ из [16] в случае $r = n$.

Теорема 2.13 (см. [2,7])**.** *Пусть $\mathcal{O}_{\mathbf{q}}$ — общая алгебра квантовых многочленов. Тогда имеется прямое разложение векторных пространств*

$$\operatorname{Der}\mathcal{O}_{\mathbf{q}} = \operatorname{Derint}\mathcal{O}_{\mathbf{q}} \oplus L.$$

Любая конечномерная подалгебра Ли в $\operatorname{Der}\mathcal{O}_{\mathbf{q}}$ является абелевой.

Аналогичный результат верен и для алгебры Ли $\operatorname{Der}\mathcal{F}$ непрерывных дифференцирований тела $\mathcal{F}$. Как и выше, дифференцирование ∂ тела $\mathcal{F}$ *непрерывно*, если оно задается значениями $\partial(X_1),\dots,\partial(X_n)$.

Если $r=n$, то алгебра $\mathcal{O}_{\mathbf{q}}$ проста [14]. Поэтому (см. [12]) $\operatorname{Derint}\mathcal{O}_{\mathbf{q}}\simeq\mathcal{O}_{\mathbf{q}}/k$ является простой алгеброй Ли. Аналогично [12], специальная йорданова алгебра $\mathcal{O}_{\mathbf{q}}^{+}$ с новым умножением $a\circ b=\dfrac{1}{2}[ab+ba]$ является простой йордановой алгеброй.

Предложение 2.14. *Пусть* $\operatorname{char}k=0$ *и* ∂ *— либо дифференцирование алгебры* $\mathcal{O}_{\mathbf{q}}$*, либо непрерывное дифференцирование тела* $\mathcal{F}$*. Предположим, что существует такой ненулевой многочлен* $f(T)\in k[T]$*, что* $f(\partial)=0$*. Тогда* $\partial=0$*.*

В настоящей работе мы распространим этот результат на обобщенные дифференцирования.

3. Пуассоновы структуры

Пуассоновой структурой на k-алгебре A называется такое k-билинейное умножение $\{x,y\}$ на A, называемое *скобкой Пуассона*, что

1) A является алгеброй Ли относительно умножения $\{x,y\}$;
2) $\{xy,z\}=\{x,z\}y+x\{y,z\}$ для всех $x,y,z\in A$.

Алгебра A с пуассоновой скобкой называется *пуассоновой алгеброй*.

Пуассоновы алгебры рассматривались в [13]. В [15] при некоторых предположениях на множество мультипараметров показано, что для алгебры $\mathcal{O}_{\mathbf{q}}$ при $r=0,n$ найдется такая пауссонова алгебра $\mathcal{O}_{\mathbf{q}'}$, что топологическое пространство примитивных (первичных) идеалов в $\mathcal{O}_{\mathbf{q}}$ и симплектических (первичных пуассоновых) идеалов в $\mathcal{O}_{\mathbf{q}'}$ гомеоморфны.

В этом разделе мы опишем все пуассоновы структуры на общей алгебре квантовых многочленов $\mathcal{O}_{\mathbf{q}}$. Согласно свойству 2) отображение $x\mapsto\{y,x\}$ является дифференцированием алгебры $\mathcal{O}_{\mathbf{q}}$. Из теоремы 2.13 следует, что

$$\{b,a\}=\sum_{i=1}^{n}\alpha_i(b)\partial_i(a)+[\operatorname{ad}w(b)]a, \tag{3.1}$$

где $\alpha_1,\dots,\alpha_n$ — линейные формы на $\mathcal{O}_{\mathbf{q}}$ и $w(b)\in\mathcal{O}_{\mathbf{q}}$. Можно также предполагать, что постоянный член в $w(y)$ нулевой. Так как скобка Пуассона антикоммутативна, имеем

$$0=\{a,a\}=\sum_{i}\alpha_i(x)\partial_i(a)+[\operatorname{ad}w(b)]a.$$

Полагая $a=X_i$, получаем

$$\alpha_i(X_i)X_i+[\operatorname{ad}w(X_i)]X_i=0. \tag{3.2}$$

Пусть

$$w(X_i)=\sum_{m_1,\dots,m_n\in\mathbb{Z}}\eta_{m_1,\dots,m_n}X_1^{m_1}\cdots X_n^{m_n},$$

где $\eta_{m_1,\dots,m_n}\in k$. Согласно [7, предложение 1.5], в (3.2) получаем

$$\begin{aligned}0&=\alpha_i(X_i)X_i+[\operatorname{ad}w(X_i)]\,X_i=\\&=\alpha_i(X_i)X_i+\sum_{m_1,\dots,m_n\in\mathbb{Z}}\eta_{m_1,\dots,m_n}\left[\prod_{t>i}q_{ti}^{m_t}-\prod_{i>t}q_{it}^{m_t}\right]X_1^{m_1}\cdots X_{i-1}^{m_{i-1}}X_i^{m_i+1}X_{i+1}^{m_{i+1}}\cdots X_n^{m_n}.\end{aligned} \tag{3.3}$$

Поскольку мультипараметры независимы, то

$$\prod_{t>i}q_{ti}^{m_t}-\prod_{i>t}q_{it}^{m_t}\neq 0$$

за исключением случая $m_1=\dots=m_{i-1}=m_{i+1}=\dots=m_n=0$. Следовательно, (3.3) влечет $w(x_i)\in k[X_i^{\pm1}]$ и поэтому $\alpha_i(X_i)=0$.

Предположим, что $1 \leqslant i < j \leqslant n$ и $w(X_i) = \sum\limits_{m\in\mathbb{Z}\setminus 0} \xi_{im} X_i^m$. Из антикоммутативности скобки Пуассона в (3.1) имеем

$$\begin{aligned} 0 &= \{X_i, X_j\} + \{X_j, X_i\} = \\ &= \alpha_i(X_j)X_i + \alpha_j(X_i)X_j + [\operatorname{ad} w(X_j)]X_i + [\operatorname{ad} w(X_i)]X_j = \\ &= \alpha_i(X_j)X_i + \alpha_j(X_i)X_j + \sum_m \xi_{im}(q_{ji}^m - 1)X_i X_j^m + \sum_m \xi_{jm}(1 - q_{ji}^m)X_i^m X_j. \end{aligned} \tag{3.4}$$

Следовательно, $\xi_{im} = \xi_{jm} = 0$ если $m \neq 1$ и $\alpha_j(X_i) = \alpha_i(X_j) = 0$. Кроме того, $\xi_{i1} = \xi_{j1} = \xi \in k$. Отсюда $w(X_i) = \xi X_i$, где $\xi \in k$.

Для любого одночлена $a \in \mathcal{O}_{\mathbf{q}}$ и любого индекса $1 \leqslant i \leqslant n$ получаем

$$\begin{aligned} 0 &= \{X_i, a\} + \{a, X_i\} = \\ &= \xi(\operatorname{ad} X_i)a + \sum_{j=1}^{n} \alpha_j(a)\partial_j X_i + (\operatorname{ad} w(a))X_i = \\ &= \alpha_i(a)X_i + [\operatorname{ad}(w(a) - \xi a)]\, X_i. \end{aligned}$$

Следовательно, $\alpha_i(a) = 0$ и $w(a) - \xi a \in k[X_i^{\pm 1}]$ для любого i. Поэтому $w(a) = \xi a$.

Теорема 3.1. *Пусть в общей алгебре квантовых многочленов $\mathcal{O}_{\mathbf{q}}$ задана скобка Пуассона. Тогда существует такой элемент $\xi \in k$, что $\{a, b\} = \xi[a, b]$.*

Доказательство. Мы уже показали, что $\{a, b\} = \xi[\operatorname{ad} w(a)]b = \xi[a, b]$ для любого одночлена a. Следовательно, это равенство можно продолжить на любой элемент из $\mathcal{O}_{\mathbf{q}}$. □

Скобка Пуассона $\mathcal{F}$ *непрерывна*, если она однозначно определяется своими значениями $\{X_i, X_j\}$, $1 \leqslant i < j \leqslant n$. Как и выше, мы можем доказать следующее утверждение.

Теорема 3.2. *Пусть на теле $\mathcal{F}$ общих лорановских квантовых рядах задана непрерывная пуассонова структура. Тогда существует такой элемент $\xi \in k$, что $\{a, b\} = \xi[a, b]$.*

4. Обобщенные дифференцирования

Пусть γ — автоморфизм квантового тора $\mathcal{O}_q = k_q[X^{\pm 1}, Y^{\pm 1}]$, причем q не является корнем из 1. Согласно теореме 2.1, найдутся такие целые числа l, s, t, v и элементы $\beta, \xi \in k$, что выполнено равенство (2.2). Линейный оператор D на $\mathcal{O}_q$ называется γ-*дифференцированием*, если

$$D(ab) = D(a)b + \gamma(a)D(b) \quad \forall a, b \in \mathcal{O}_q.$$

Следовательно,

$$\begin{aligned} 0 &= D(XY - qYX) = \\ &= D(X)Y - q\gamma(Y)D(X) + \gamma(X)D(Y) - qD(Y)X = \\ &= D(X)Y - q\xi X^t Y^v D(X) + \beta X^l Y^s D(Y) - qD(Y)X. \end{aligned} \tag{4.1}$$

Для любого элемента $w \in \mathcal{O}_q$ t имеется *внутреннее* γ-дифференцирование

$$\operatorname{ad}_\gamma(a) = wa - \gamma(a)w.$$

В частности,

$$(\operatorname{ad}_\gamma)X = wX - \beta X^l Y^s w.$$

Если $\lambda \in k$, то $\operatorname{ad}_\gamma \lambda = 0$. Поэтому всюду в дальнейшем, рассматривая внутреннее γ-дифференцирование $\operatorname{ad}_\gamma w$, мы всегда будем предполагать, что постоянный член w равен нулю.

Предположим, что $l \neq 1$. Тогда найдется элемент $w \in \mathcal{O}_q$ такой, что

$$D(X) - (\operatorname{ad}_\gamma)X = \sum_{l=1}^{|l-1|} X^i f_i(Y), \quad f_i(Y) \in k[Y^{\pm 1}].$$

Заметим, что оператор $D - \mathrm{ad}_\gamma w$ снова является γ-дифференцированием $\mathcal{O}_q$. Следовательно, без ограничения общности можно считать, что

$$D(X) = \sum_{l=1}^{|l-1|} X^i f_i(Y).$$

Тогда в (4.1) получаем

$$0 = \sum_{l=1}^{|l-1|} X^i f_i(Y)Y - q\xi X^t Y^v \sum_{l=1}^{|l-1|} X^i f_i(Y) + \beta X^l Y^s D(Y) - qD(Y)X. \tag{4.2}$$

Пусть

$$D(Y) = \sum_{a \leqslant j \leqslant b} X^j g_j(Y), \quad g_j(Y) \in k[Y^{\pm 1}].$$

Если $l > 1$, то, сравнивая в (4.2) старшие члены из X, получаем, что $l + b \leqslant l - 1$ и поэтому $b \leqslant -1$. Таким образом, $a \leqslant b \leqslant -1$. С другой стороны, сравнивая в (4.2) младшие члены из X, мы получаем $a + 1 \geqslant 1$, откуда $a \geqslant 0$, что приводит к противоречию.

Предположим, что $l < 1$. Тогда $b + 1 \leqslant |l - 1| = 1 - l$ и $b + l \leqslant 0$. С другой стороны, $1 \leqslant a + l \leqslant b + l \leqslant 0$, что снова приводит к противоречию.

Аналогично, заменяя X на Y, рассматривается случай $v \neq 1$. Следовательно, доказана следующая теорема.

Теорема 4.1. *Пусть D является γ-дифференцированием , где γ — такое же, как в* (2.2). *Если либо $l \neq 1$, либо $v \neq 1$, то D является внутренним γ-дифференцированием.*

Рассмотрим теперь случай $l = v = 1$. Так как $lv - ts = 1$, то получаем, что $ts = 0$. Пусть $t \neq 0$ и $s = 0$. Для любого одночлена $X^a Y^b$ имеем

$$[\mathrm{ad}_\gamma X^a Y^b]X = X^a Y^b X - \beta X \cdot X^a Y^b = (q^b - \beta)X^{a+1} Y^b. \tag{4.3}$$

Так как q не является корнем из 1, то существует по крайней мере одно такое целое число b, что $q^{-b} = \beta$. Заменяя D на $D - \mathrm{ad}_\gamma w$ для некоторого $w \in \mathcal{O}_q$ как и в [7, § 1] можно считать, что $D(X) = f(X)Y^b$, где $f(X) \in k[X^{\pm 1}]$ и $\beta = q^{-b}$. Отметим, что по (4.3) для любого $h(X) \in k[X^{\pm 1}]$ имеем

$$\left[\mathrm{ad}_\gamma(h(X)Y^b)\right] X = 0.$$

Следовательно, можно

$$D(Y) = \sum_i g_i(X)Y^i, \quad g_i(X) \in k[X^{\pm 1}], \tag{4.4}$$

заменить на

$$D(Y) - \left[\mathrm{ad}_\gamma(h(X)Y^b)\right] Y = \sum_{i \neq b+1} g_i(X)Y^i + \left[g_{b+1}(X) - h(X) + \xi X^t h(q^{-1}X)\right] Y^{b+1}. \tag{4.5}$$

Поэтому, если $t \neq 0$, то найдется такое $h(X)$, что

$$g_{b+1}(X) = \sum_{i=0}^{|t|-1} a_i X_i, \quad a_i \in k. \tag{4.6}$$

Согласно (4.4), получаем в (4.1)

$$\begin{aligned} 0 &= f(X)Y^{b+1} - q\xi X^t Y f(X)Y^b + \beta X \sum_i g_i(X)Y^i - q \sum_i g_i(X)Y^i X = \\ &= \left[f(X) - q\xi X^t f(q^{-1}X)\right] Y^{b+1} + \sum_i [\beta - q^{1-i}] X g_i(X) Y^i. \end{aligned}$$

Значит, если $1 - i \neq -b$, то $\beta - q^{1-i} \neq 0$ и $g_i(X) = 0$. Поэтому

$$f(X) = q\xi X^t f(q^{-1}X), \quad D(Y) = g(X)_{b+1} Y^{b+1}, \quad \beta = q^{-b}. \tag{4.7}$$

Если $t \neq 0$, то из (4.7) вытекает, что $f(X) = 0$.

Предположим, что $t = 0$ и

$$f(X) = \sum_j \theta_j X^j, \quad \theta_j \in k.$$

В силу (4.7) получаем, что $\theta_j = q^{1-j}\xi\theta_j$. Если $q^d = \xi$, то $\theta_j = 0$ при условии, что $1 - j \neq -d$. Таким образом, $f(X) = \theta X^{d+1}$. Пусть

$$g(X) = \sum_j \tau_j X^j, \quad h(X) = \sum_j \omega_j X^j, \quad \tau_j, \omega_i \in k.$$

Тогда в (4.5) получаем

$$g_{b+1}(X) + h(X) - \xi h(q^{-1}X) = \sum_j \left(\tau_j + \omega_j - \xi\omega_j q^{-j}\right) X^j.$$

Предположим, что $j \neq d$. Тогда $1 - \xi q^{-j} \neq 0$. Поэтому существуют такие $\omega_j \in k$, что $\tau_j + \omega_j - \xi\omega_j q^{-j} = 0$. Значить, мы можем считать, что

$$g(X) = \tau X^d, \quad \tau \in k, \quad \xi = q^d.$$

Таким образом, мы уточнили теорему 4.1.

Теорема 4.2. *Предположим, что γ-дифференцирование D алгебры $\mathcal{O}_q$ имеет вид*

$$\gamma(X) = \beta X, \quad \gamma(Y) = \xi X^t Y.$$

Если $t \neq 0$, то найдется такой элемент $w \in \mathcal{O}_q$, что

$$D(X) = (\mathrm{ad}_\gamma\, w)X, \quad D(Y) = (\mathrm{ad}_\gamma\, w)Y + g(X)Y^{b+1}, \tag{4.8}$$

где $g(X) = g_{b+1}(X) \in k[X^{\pm 1}]$ — такой же, как в (4.4)*, причем $\beta = q^{-b}$. Если $t = 0$, то найдется такой элемент $w \in \mathcal{O}_q$, что*

$$\begin{aligned} D(X) &= (\mathrm{ad}_\gamma\, w)X + \theta X^{d+1}, && \theta \in k, \quad \xi = q^d, \\ D(Y) &= (\mathrm{ad}_\gamma\, w)Y + \tau X^d Y^{b+1}, && \tau \in k, \quad \beta = q^{-b}. \end{aligned} \tag{4.9}$$

Аналогично рассматривается случай такого автоморфизма γ, что

$$\gamma(X) = \beta X Y^s, \quad \gamma(Y) = \xi Y.$$

Следующее следствие обобщает [7, следствия 1.10 и 1.14].

Следствие 4.3. *Предположим, что автоморфизм γ имеет конечный порядок. Тогда либо D является внутренним γ-дифференцированием, либо γ является торическим автоморфизмом и существует такой элемент $w \in \mathcal{O}_q$, что*

$$D(X) = (\mathrm{ad}_\gamma\, w)X + \theta X, \quad D(Y) = (\mathrm{ad}_\gamma\, w)Y + \tau Y,$$

где $(\beta - 1)\tau = (\xi - 1)\theta = 0$.

Доказательство. Поскольку γ имеет конечный порядок, мы можем вывести из теоремы 4.2, что $t = 0$. Согласно теоремам 4.1 и 4.2, можно предположить, что

$$\gamma(X) = \beta X, \quad \gamma(Y) = \xi Y,$$

где $\beta, \xi \in k^*$ — корни из 1. Тогда в (4.9) мы получаем, что $b = d = 0$. Следовательно, по модулю внутреннего дифференцирования $\mathrm{ad}_\gamma\, w$ получаем, что $D(X) = \theta X$, $D(Y) = \tau Y$. Тогда

$$\begin{aligned} 0 &= D(X)Y + \beta X D(Y) - qD(Y)X - q\xi Y D(X) = \\ &= \theta XY + \beta X\tau Y - q\tau YX - q\xi Y\theta X = \\ &= (\theta + \beta\tau - \tau - \xi\theta)XY. \end{aligned}$$

Следствие доказано. □

Далее мы опишем *алгебраические* γ-дифференцирования D, т.е. операторы D, которые удовлетворяют алгебраическому уравнению

$$D^n + a_{n-1}D + \cdots + a_1 D + a_0 E = 0, \tag{4.10}$$

где $a_i \in k$ и E — тождественный оператор. Без ограничения общности можно считать, что основное поле k алгебраически замкнуто.

Возьмем элемент $h \in k_q[X^{\pm 1}, Y^{\pm 1}] \setminus 0$. Тогда линейная оболочка

$$\langle D^{n-1}h, \ldots, Dh, h\rangle$$

является D-инвариантной. Легко видеть, что найдется такое натуральное число M, что если $h = X^m Y^r$, то

$$\langle D^{n-1}h, \ldots, Dh, h\rangle \subseteq \langle X^i Y^j \mid |m-i|, |r-j| < M\rangle.$$

Следовательно, для любого натурального числа L существует собственный вектор

$$f = \sum_{j>L} f_j(X)^i Y^j, \quad f_j(X) \in k[X]X^L, \tag{4.11}$$

оператора D с собственным значением $\lambda \in k$. Но каждое собственное значение является корнем многочлена (4.10). Поэтому имеется только конечное множество собственным значений оператора D.

Рассмотрим сначала случай внутреннего γ-дифференцирования $D = \mathrm{ad}_\gamma w$. Тогда

$$(w - \lambda)f = \gamma(f)w. \tag{4.12}$$

Предположим, что $w \neq 0$ и $\zeta X^a Y^b$ — старший (младший) член w в смысле лексикографического порядка на свободной абелевой группе мультииндексов $\mathbb{Z}^2$, $(a,b) \in \mathbb{Z}^2$. Если $(a,b) \neq (0,0)$, то $\zeta X^a Y^b$ является старшим (младшим) членом $w - \lambda$. Сравнивая в (4.12) старшие (младшие) члены, получаем, что старший член f инвариантен относительно γ с точностью до скалярного множителя. Это означает, что если матрица

$$\begin{pmatrix} l & s \\ t & v \end{pmatrix}$$

— такая же, как в (2.2), то

$$\begin{pmatrix} l & t \\ s & v \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}.$$

Таким образом, мы можем сделать замену переменных вида

$$X \mapsto X' = X^{a_{11}}Y^{a_{12}}, \quad Y \mapsto Y' = X^{a_{21}}Y^{a_{22}},$$

где

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}),$$

таким образом, чтобы $\gamma(X') = \beta X'$, $\gamma(Y') = \xi(X')^t Y'$. Следовательно, без ограничения общности можно считать, что $X' = X$, $Y' = Y$, γ такие же, как в теореме 4.2, и старший (младший) член f является степенью X. Но мы могли взять f из (4.11) при $L > 0$ для новой системы переменных X, Y. Поэтому изложенные выше рассуждения показывают, что γ является торическим автоморфизмом. Итак, нами доказана следующая теорема.

Теорема 4.4. *Пусть D — обобщенное алгебраическое дифференцирование из теоремы* 4.1. *Тогда $D = 0$.*

Пусть теперь D, γ, w из теоремы 4.2 и D удовлетворяет уравнению (4.10). Предположим , что L — натуральное число и f из (4.11), $Df = \lambda f$. Пусть $t \neq 0$ и D, $g(X)$, b из (4.8). Положим $D' = D - \mathrm{ad}_\gamma w$. Тогда $D'(X) = 0$, $D'(Y) = g(X)Y^{b+1}$, где $q^{-b} = \beta$. Таким образом, $D'(f(X)) = 0$ для любого $f(X) \in k[X^{\pm 1}]$.

Лемма 4.5. *Если $m > 0$, то*

$$(X^t Y)^m = q^{-t\frac{m(m-1)}{2}} X^{tm} Y^m.$$

Доказательство. Случай $m=1$ очевиден. По индукции

$$(X^tY)^{m+1} = X^tY\left(q^{-t\frac{m(m-1)}{2}}X^{tm}Y^m\right) = \\ = q^{-t\frac{m(m-1)}{2}-t}X^{t(m+1)}Y^{m+1} = q^{-t\frac{m(m+1)}{2}}X^{t(m+1)}Y^{m+1}.$$

Лемма доказана. □

Если $j>0$, то

$$\begin{aligned} D'\left(f(X)Y^j\right) &= D'\left(f(X)\right)Y^j + f\left(\gamma(X)\right)D'(Y^j) = f(\beta X)D'(Y^j) = \\ &= f(\beta X)\sum_{m=0}^{j-1}\gamma(Y)^m D'(Y)Y^{j-m-1} = \\ &= f(\beta X)\sum_{m=0}^{j-1}(\xi X^tY)^m g(X)Y^{b+1}Y^{j-m-1} = \\ &= f(\beta X)\sum_{m=0}^{j-1}\xi^m q^{-t\frac{m(m-1)}{2}}X^{tm}Y^m g(X)Y^{b+j-m} = \\ &= \sum_{m=0}^{j-1}\xi^m q^{-t\frac{m(m-1)}{2}}f(\beta X)X^{tm}g(q^{-m}X)Y^{b+j}. \end{aligned} \tag{4.13}$$

Таким образом, $Df = [\mathrm{ad}_\gamma w]f + \lambda f$, где f — такое же, как в (4.11). Пусть

$$\deg_Y f = m, \quad \deg_Y w = i_1, \quad w = \sum_{i_0\leqslant i\leqslant i_1} w_i(X)Y^i,$$

где $w_i(X)\in k[X^{\pm 1}]$. Применяя (4.13) мы получаем

$$\sum_{j>L}\lambda f_j(X)Y^j = \tag{4.14}$$

$$\begin{aligned} &= w\sum_{j>L}f_j(X)Y^j - \sum_{j>L}f_j(\beta X)\gamma(Y)^j w + \sum_{j>L}D'\left(f_j(X)Y^j\right) = \\ &= w\sum_{j>L}f_j(X)Y^j - \sum_{j>L}f_j(\beta X)\xi^j q^{-t\frac{j(j-1)}{2}}X^{tj}Y^j w + \\ &\quad + \sum_{j>L}f_j(\beta X)\left[\sum_{r=0}^{j-1}\xi^r q^{-t\frac{r(r-1)}{2}}X^{tr}g(q^{-r}X)\right]Y^{b+j} = \\ &= \sum_{\substack{L<j\leqslant m\\ i_0\leqslant i\leqslant i_1}}\left[w_i(X)f_j(q^{-i}X) - f_j(\beta X)\xi^j q^{-t\frac{j(j-1)}{2}}X^{tj}w_i(q^{-j}X)\right]Y^{i+j} + \\ &\quad + \sum_{j>L}f_j(\beta X)\left[\sum_{r=0}^{j-1}\xi^r q^{-t\frac{r(r-1)}{2}}X^{tr}g(q^{-r}X)\right]Y^{b+j}. \end{aligned} \tag{4.15}$$

Лемма 4.6. *Если $w=0$, то $g=D=0$.*

Доказательство. По предположению в (4.14) и в (4.15) получаем

$$\sum_{j>L}\lambda f_j(X)Y^j = \sum_{j>L}f_j(\beta X)\left[\sum_{r=0}^{j-1}\xi^r q^{-t\frac{r(r-1)}{2}}X^{tr}g(q^{-r}X)\right]Y^{b+j}$$

и поэтому

$$\delta_{b,0}\lambda f_m(X) = f_m(\beta X)\left[\sum_{r=0}^{j-1}\xi^r q^{-t\frac{r(r-1)}{2}}X^{tr}g(q^{-r}X)\right], \tag{4.16}$$

если $b \geqslant 0$. Если $b < 0$, то

$$\lambda f_m(X) = 0 \tag{4.17}$$

и поэтому $\lambda = 0$. Снова получаем равенство (4.16). Сравнивая степени по X в (4.16), мы получаем $g = 0$ в (4.4). Отсюда $D = 0$. □

Лемма 4.7. *Если $g = 0$, то $w = D = 0$.*

Доказательство. Согласно предположениям в (4.14) и (4.15), получаем

$$\sum_{j>L} \lambda f_j(X) Y^j = \sum_{\substack{L<j\leqslant m \\ i_0\leqslant i\leqslant i_1}} \left[w_i(X) f_j(q^{-i}X) - f_j(\beta X)\xi^j q^{-t\frac{j(j-1)}{2}} X^{tj} w_i(q^{-j}X) \right] Y^{i+j}.$$

Если $i_1 \leqslant 0$, то (4.17) выполнено и $\lambda = 0$. Поэтому

$$w_{i_1}(X) f_m(q^{-i_1}X) = f_m(\beta X)\xi^m q^{-t\frac{m(m-1)}{2}} X^{tm} w_{i_1}(q^{-m}X). \tag{4.18}$$

Сравнивая степени по X, мы получаем, что $w_{i_1} = 0$, поскольку $t \neq 0$. Следовательно, $w = 0$.

В случае $i_1 > 0$ мы снова получаем (4.18). □

Лемма 4.8. *Если $b > i_1$, то $w = g = D = 0$.*

Доказательство. Пусть $b \geqslant 0$. Сравнивая члены в (4.14), (4.15), содержащие Y^{b+m}, получаем

$$\lambda \delta_{0,b} f_b(X) = f_b(\beta X) \left[\sum_{r=0}^{m-1} \xi^r q^{-t\frac{r(r-1)}{2}} X^{tr} g(q^{-r}X) \right] Y^{b+m}, \tag{4.19}$$

Это означает, что $g = 0$, поскольку выполнено (4.4).

Если $b < 0$, то, сравнивая члены из (4.15), содержащие Y^m, получаем (4.17), откуда $\lambda = 0$. В этом случае сравним в (4.15) члены, содержащие Y^{b+m}. Получаем снова равенство (4.19). Остается применить лемму 4.7. □

Лемма 4.9. *Если $i_1 > b$, то $w = g = D = 0$.*

Доказательство. Пусть $i_1 \geqslant 0$ Сравнивая в (4.15) члены, содержащие Y^{i_1+m}, получаем

$$\delta_{i_1,0} \lambda f_m(X) = w_{i_1}(X) f_m(q^{-i_1}X) - f_m(\beta X)\xi^m q^{-t\frac{m(m-1)}{2}} X^{tm} w_b(q^{-m}X), \tag{4.20}$$

что невозможно, если $w \neq 0$, поскольку отличаются степени по X в левой и правой частях в (4.20).

Пусть $i_1 < 0$. Тогда (4.17) выполнено и поэтому $\lambda = 0$. Снова получаем (4.20). Таким образом, во всех случаях $w = 0$ и $g = D = 0$ согласно лемме 4.6. □

Лемма 4.10. *Пусть $i_1 = b$. Тогда $g = w = D = 0$.*

Доказательство. Если $i_1 = b < 0$, то, сравнивая в (4.15), (4.14) коэффициенты при Y^m, получаем, что $\lambda = 0$. Поэтому либо $i_1 = b \geqslant 0$, либо $i_1 = b < 0$ и $\lambda = 0$.

Напомним, что $\beta = q^{-b}$. Сравнивая в (4.15) коэффициенты при Y^{m+b} получаем, что

$$\lambda \delta_{0,b} f_m(X) = w_b(X) f_m(q^{-b}X) - f_m(q^{-b}X)\xi^m q^{-t\frac{m(m-1)}{2}} X^{tm} w_b(q^{-m}X) + \\ + f_m(q^{-b}X) \left[\sum_{r=0}^{m-1} \xi^r q^{-t\frac{r(r-1)}{2}} X^{tr} g(q^{-r}X) \right]$$

и поэтому

$$\lambda \delta_{b,0} = w_b(X) - \xi^m q^{-t\frac{m(m-1)}{2}} X^{tm} w_b(q^{-m}X) + \sum_{r=0}^{m-1} \xi^r q^{-t\frac{r(r-1)}{2}} X^{tr} g(q^{-r}X). \tag{4.21}$$

Возьмем теперь такое L чтобы $L > |t|$ и L было бы больше, чем разность между наибольшей и наименьшей степенью X в $w_b(X)$. Тогда разрыв длин в ряду экспонент X не меньше $|t| + 1$ в $w_b(X)$ и $w_b(X)\xi^j q^{-t\frac{r(r-1)}{2}} X^{tj} w_b(q^{-j}X)$. Поэтому $\xi^r q^{-t\frac{r(r-1)}{2}} X^{tr} g(q^{-r}X)$ обращается в нуль для некоторого r в силу (4.4). Следовательно, (4.21) влечет $g = 0$. Остается применить лемму 4.7. □

Теорема 4.11. *Пусть D — алгебраическое γ-дифференцирование, где либо $\gamma(X)=\beta X$, $\gamma(Y)=\xi X^tY$, либо симметрично $\gamma(X)=XY^s$, $\gamma(Y)=\beta Y$. Если $t,s\neq 0$, то $D=0$.*

Доказательство. Применить леммы 4.8–4.10. □

Предположим теперь, что γ — торический автоморфизм вида

$$\gamma(X)=\beta X,\quad \gamma(Y)=\xi Y,\quad \beta,\xi\in k^*.$$

Согласно теореме 4.2, обобщенное γ-дифференцирование D имеет вид (4.9). Положим $D'=D-\mathrm{ad}_\gamma w$. Тогда

$$\begin{aligned} D'(X)&=\theta X^{d+1}, && \theta\in k,\quad \xi=q^d,\\ D'(Y)&=\tau X^dY^{b+1}, && \tau\in k,\quad \beta=q^{-b}. \end{aligned}$$

Для любых натуральных чисел u,v получаем

$$\begin{aligned} D'(X^uY^v)&=D'(X^u)Y^v+\gamma(X)^uD'(Y^v)=\\ &=\left[\sum_{i=0}^{u-1}\gamma(X)^iD'(X)X^{u-i-1}\right]Y^v+\gamma(X)^u\left[\sum_{i=0}^{v-1}\gamma(Y)^iD'(Y)Y^{v-i-1}\right]=\\ &=\left[\sum_{i=0}^{u-1}\beta^iX^i\theta X^{d+1}X^{v-i-1}\right]Y^v+\beta^uX^u\left[\sum_{i=0}^{v-1}\xi^iY^i\tau X^dY^{b+1}Y^{v-i-1}\right]=\\ &=\theta(1+\beta+\cdots+b^{u-1})X^{u+d}Y^v+\beta^u\tau X^{u+d}\left[\sum_{i=0}^{v-1}\xi^iq^{-id}\right]Y^{b+v}=\\ &=\theta(1+q^{-b}+\cdots+q^{-b(u-1)})X^{d+u}Y^v+q^{-bu}\tau X^{u+d}\left[\sum_{i=0}^{v-1}q^{di}q^{-id}\right]Y^{b+v}=\\ &=\theta(1+q^{-b}+\cdots+q^{-b(u-1)})X^{d+u}Y^v+vq^{-bu}\tau X^{u+d}Y^{v+b}. \end{aligned}\tag{4.22}$$

Предложение 4.12. *Пусть ζX^rY^s, ηX^uY^v — два таких одночлена, что*

$$(\zeta X^rY^s)(\eta X^uY^v)=\left[\eta(q^{-b}X)^u(q^dY)^v\right](\zeta X^rY^s).$$

Тогда

$$(s-b)u+(d-r)v=0.\tag{4.23}$$

Доказательство. Имеем

$$\begin{gathered}(\zeta X^rY^s)(\eta X^uY^v)=\zeta\eta q^{-su}X^{u+r}Y^{v+s},\\ \left[\eta(q^{-b}X)^u(q^dY)^v\right](\zeta X^rY^s)=\zeta\eta q^{-bv+dv-vr}X^{u+r}Y^{v+s}.\end{gathered}$$

Поэтому

$$q^{-su}=q^{-bv+dv-vr}$$

и (4.23) доказано, поскольку q не является корнем из 1. □

Следствие 4.13. *Пусть ζX^rY^s — старший член $w\neq 0$ относительно лексикографического порядка. Предположим, что*

$$(r,s)>(d,\max(b,0))\tag{4.24}$$

в $\mathbb{Z}^2$ в смысле лексикографического порядка. Пусть ηX^uY^v — старший член f. Если (4.23) *не выполнено, то старший член $D(f)$ равен $\theta X^{u+r}Y^{v+s}$.*

Следствие 4.14. *Пусть ζX^rY^s — старший член $w\neq 0$ относительно лексикографического порядка и выполнено* (4.24). *Тогда оператор D не является алгебраическим.*

Доказательство. Пусть для D выполнено условие (4.10). Предположим сначала, что $r > d$. Возьмем такое $v > 0$, что

$$(r-d)v > n|sd - br|.$$

Утверждается, что старший член $D^j(Y^v)$, $1 \leqslant j \leqslant n$, имеет вид $\theta_j X^{jr} Y^{v+js}$. Случай $j = 1$ вытекает из следствия 4.13, поскольку $(s-b)\cdot 0 + (d-r)v < 0$. Предположим, что наша гипотеза справедливо для некоторого $j \leqslant n$. Тогда

$$(s-b)jr + (d-r)(v+js) = j(-br+ds) + (d-r)v > 0.$$

Пусть теперь $r = d$ и $s > b$. В этом случае возьмем такое $u > 0$, что $(s-b)u > n(s-b)r$. □

Предположим теперь, что $(r,s) \leqslant (d, \max(b,0))$. С этого момента предположим также, что основное поле k имеет нулевую характеристику. Пусть $r < d$ и $\eta X^u Y^v$ — старший член f. Если $b > 0$, то, согласно (4.22), старший член $D(f)$ равен $\eta v q^{-nb} X^{u+d} Y^{b+v}$. Поэтому старший член $D^j(f)$, $1 \leqslant j \leqslant n$, равен

$$\eta q^M v(v+b)\cdots[v+(j-1)b]\, X^{u+jd} Y^{v+jb}$$

для некоторого целого M, при условии, что

$$v(v+b)\cdots[v+(j-1)b] \neq 0. \tag{4.25}$$

Так как поле k имеет нулевую характеристику, то существует такое целое число v, что выполнено (4.25). Поэтому в этом случае утверждение выполнено.

Аналогично рассматривается случай $b < 0$.

Пусть теперь $b = 0$. Тогда старший член $D(f)$ по (4.22) равен $(\theta u + \tau v) X^{u+d} Y^m$. Мы всегда можем выбрать такое $\theta \in k^*$, что

$$(\theta u + \tau v)(\theta(u+d) + \tau v)\cdots(\theta(u+(n-1)d) + \tau v) \neq 0;$$

снова D не является алгебраическим оператором. Таким образом, мы доказали следующее утверждение.

Предложение 4.15. *Пусть k имеет нулевую характеристику. Если D — алгебраический оператор, то $r = d$ и $s = \max(b,0)$.*

Предположим теперь, что $s = b > 0$. Согласно (4.22), старший член $D(X^u Y^v)$ равен

$$\zeta X^d Y^b \cdots X^u Y^v - \zeta (q^{-b}X)^u (q^q Y)^v X^d Y^b + \tau u q^{-bv} X^{u+d} Y^{v+b} =$$
$$= \left(\zeta q^{-bu} - \zeta q^{-b} + \tau u q^{-bv}\right) X^{u+d} Y^{v+b}.$$

Взяв достаточно большое u, мы можем получить

$$\zeta q^{-bu} - \zeta q^{-b} + \tau u q^{-bv} \neq 0.$$

Как и выше, отсюда следует, что D не алгебраично.

Предположим, что $b \leqslant 0$ и $s = 0$. Тогда

$$\zeta X^d \cdot X^u Y^v - \zeta (q^{-b}X)^u (q^q Y)^v X^d + \theta u X^{u+d} Y^v + \delta_{b,0} v q^{-bv} X^{u+d} Y^v =$$
$$= \left(\zeta - \zeta q^{-bu} + \theta u + \delta_{b,0} v q^{-bv}\right) X^{u+d} Y^v.$$

Снова взяв достаточно большое u такое, чтобы

$$\zeta - \zeta q^{-bu} + \theta u + \delta_{b,0} v q^{-bv} \neq 0,$$

получаем, что D снова не алгебраично. Итак, доказано первое утверждение в следующей теореме.

Теорема 4.16. *Пусть поле k имеет нулевую характеристику и D — алгебраическое γ-дифференцирование, где γ — торический автоморфизм. Тогда $D = 0$.*

Доказательство. Мы уже знаем, что $D = D'$. Из (4.22) получаем, что

$$D(X^u) = \left(1 + q^{-b} + \cdots + q^{-b(u-1)}\right) X^{u+d}.$$

Так как q не является корнем из 1 и $\operatorname{char} k = 0$, то

$$1 + q^{-b} + \cdots + q^{-b(u-1)} \neq 0.$$

Следовательно, индукцией по j проверяем, что $D^m(X^u) = \lambda X^{u+md}$. Это означает, что ненулевой оператор D не является алгебраическим. Аналогично получаем, что $b = 0$.

Согласно (4.22), для любых $u, v > 0$ имеем

$$D(X^u Y^v) = (\theta u + \tau v) X^u Y^v.$$

Если $F(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0$ — многочлен из (4.10), то $\theta u + \tau v$ — корень $F(T)$ для любой пары чисел $u, v > 0$. Следовательно, $\theta = \tau = 0$ и $D = 0$. □

Напомним, что если $\operatorname{char} k = p > 0$, то $\partial_i^p = \partial_i$ для $i = 1, 2$. Здесь ∂_i — дифференцирование $\mathcal{O}_q$, причем $\partial_i(X) = \delta_{i1}X$, $\partial_i(Y) = \delta_{i2}Y$.

СПИСОК ЛИТЕРАТУРЫ

1. *Артамонов В. А.* Автоморфизмы тел квантовых рациональных функций// Мат. сб. — 2000. — *191*, № 12. — С. 3–26.
2. *Артамонов В. А.* Действия квантовых групп на квантовых пространствах// Вестн. МГУ. Сер. 1, мат., мех. — 2003. — *3*. — С. 13–17.
3. *Alev J., Chamarie M.* Dérivations et automorphismes de quelques algèbres quantiques// Commun. Algebra. — 1992. — *20*, № 6. — С. 1787–1802.
4. *Alev J., Dumas F.* Invariants du corps de Weyl sous l'action de groupes finis// Commun. Algebra. — 1997. — *25*, № 5. — С. 1655–1673.
5. *Artamonov V. A.* Valuations on quantum fields// Commun. Algebra. — 2001. — *29*, № 9. — С. 3889–3904.
6. *Artamonov V. A.* Actions of Hopf algebras on quantum polynomials// в кн.: Representation of algebras. — New York: Marcel Dekker, 2001. — С. 11–20.
7. *Artamonov V. A.* Pointed Hopf algebras acting on quantum polynomials// J. Algebra. — 2003. — *259*, № 2. — С. 323–352.
8. *Artamonov V. A., Cohn P. M.* The skew field of rational functions on the quantum plane// J. Math. Sci. — 1999. — *93*, № 6. — С. 824–829.
9. *Artamonov V. A., Wisbauer R.* Homological properties of quantum polynomials// Algebras and representation theory. — 2001. — *4*, № 3. — С. 219–247.
10. *Brookes C. J. B.* Crossed products and finitely presented groups// J. Group Theory. — 2000. — *3*. — С. 433–444.
11. *Brown K. A., Goodearl K. R.* Lecture on algebraic quantum groups. — Basel–Boston: Birkhäuser, 2002.
12. *Herstein I. N.* On the Lie and Jordan rings of a simple associative ring// Amer. J. Math. — 1955. — *77*. — С. 279–285.
13. *Korogodski L. I., Soibelman Ya. I.* Algebra of functions on quantum groups. Part 1. — Providence: Amer. Math. Soc., 1998.
14. *McConnell J. C., Pettit J. J.* Crossed products and multiplicative analogues of Weyl algebras// J. London Math. Soc. — 1988. — *38*, № 1. — С. 47–55.
15. *Sei-Qwon O., Chun-Gil P., Shin Youg-Yeon.* Quantum n-space and Poisson n-space// Commun. Algebra. — 2002. — *30*, № 9. — С. 4197–4209.
16. *Osborn J. P., Passman D.* Derivations of skew polynomial rings// J. Algebra. — 1995. — *176*, № 2. — С. 417–448.
17. *van Oystaeyen F.* Algebraic geometry for associative algebras. — New York: Marcel Dekker, 2000.
18. *Richard L.* Sur les endomorphismes des tores quantiques// Commun. Algebra. — 2002. — *30*, № 11. — С. 5282–5306.

В. А. Артамонов
Московский государственный университет
E-mail: artamon@mech.math.msu.su

Современная математика и ее приложения. Том 13 (2004). С. 53–70

УДК 512.55

LP-ПРОБЛЕМЫ ДЛЯ РАНГОВЫХ НЕРАВЕНСТВ НАД ПОЛУКОЛЬЦАМИ: ФАКТОРИЗАЦИОННЫЙ РАНГ

© 2004 г. **Л. Б. БИСЛИ, А. Э. ГУТЕРМАН**

Аннотация. Получена характеризация линейных отображений матриц над полукольцами, сохраняющих множество упорядоченных наборов матриц и удовлетворяющих экстремальным ранговым свойствам относительно факторизационного ранга.

СОДЕРЖАНИЕ

1. Введение

Определение 1.1. *Полукольцом* $\mathcal{S}$ называется алгебраическая система, состоящая из множества $\mathcal{S}$ и двух бинарных операций, сложения и умножения, удовлетворяющих следующим аксиомам:

- $\mathcal{S}$ является коммутативным моноидом по сложению (нейтральный элемент обозначается 0);
- $\mathcal{S}$ является полугруппой по умножению (если существует нейтральный элемент, то он обозначается 1);
- умножение дистрибутивно относительно сложения с двух сторон;
- $s0 = 0s = 0$ для всех $s \in \mathcal{S}$.

В этой статье мы предполагаем существование в полукольце $\mathcal{S}$ единицы 1, отличной от 0.

Определение 1.2. Полукольцо называется *антинегативным*, если в нем только нулевой элемент имеет аддитивный обратный.

Определение 1.3. Полукольцо $\mathcal{S}$ называется *булевым*, если $\mathcal{S}$ реализуется как множество подмножеств данного множества M. В этом случае суммой двух подмножеств является их объединение, а произведением — пересечение. Нулевой элемент — пустое множество, а единица — все множество M.

Тривиальная проверка показывает, что булево полукольцо коммутативно и антинегативно. Если $\mathcal{S}$ состоит только из пустого множества и множества M, то оно называется бинарным булевым полукольцом (или $\{0,1\}$-полукольцом) и обозначается $\mathbf{B}$.

Работа выполнена при частичной поддержке Российского фонда фундаментальных исследований (проект № 02-01-00218) и гранта НШ-1910.2003.01.

Определение 1.4. Полукольцо называется *цепным*, если множество $\mathcal{S}$ является вполне упорядоченным с универсальными максимальным и минимальным элементами и операциями, заданными по правилам $a+b=\max\{a,b\}$ и $a\cdot b=\min\{a,b\}$.

Легко доказать, что любое цепное полукольцо $\mathcal{S}$ является булевым полукольцом на подходящем семействе подмножеств в $\mathcal{S}$. Для этого достаточно рассмотреть в качестве M множество всех элементов $\mathcal{S}$ и выбрать все его подмножества, состоящие из элементов, строго меньших данного.

Пусть $\mathcal{M}_{m,n}(\mathcal{S})$ — множество всех $(m\times n)$-матриц с коэффициентами из полукольца $\mathcal{S}$. Теория матриц над полукольцами является предметом интенсивных исследований в последние пятьдесят лет (см., например, работы [8, 12] и библиографию в них). В частности, многие авторы изучали различные ранговые функции для матриц над полукольцами и их свойства (см. [5, 7, 9, 11, 18]). Среди ранговых функций, имеющих интересные свойства и приложения, наиболее известен факторизационный ранг.

Определение 1.5. Матрица $A\in\mathcal{M}_{m,n}(\mathcal{S})$ имеет *факторизационный ранг* k, $\operatorname{rank}(A)=k$, если существуют такие матрицы $B\in\mathcal{M}_{m,k}(\mathcal{S})$ и $C\in\mathcal{M}_{k,n}(\mathcal{S})$, что $A=BC$ и k является наименьшим положительным целым числом, для которого это разложение существует. По определению считается, что нулевой факторизационный ранг имеет только нулевая матрица.

Пусть $\mathcal{S}$ — подполукольцо некоторого поля. Тогда определена обычная функция матричного ранга $\rho(A)$ для любой матрицы $A\in\mathcal{M}_{m,n}(\mathcal{S})$. Простые примеры показывают, что над полукольцами эти функции, вообще говоря, не совпадают. Однако неравенство $\operatorname{rank}(A)\geqslant\rho(A)$ выполняется всегда.

Поведение функции ρ относительно матричного сложения и умножения устанавливается следующими классическими неравенствами:

- *неравенства для суммы матриц*:
$$|\rho(A)-\rho(B)|\leqslant\rho(A+B)\leqslant\rho(A)+\rho(B),$$
- *неравенства Сильвестра*:
$$\rho(A)+\rho(B)-n\leqslant\rho(AB)\leqslant\min\{\rho(A),\rho(B)\},$$
- *неравенство Фробениуса*:
$$\rho(AB)+\rho(BC)\leqslant\rho(ABC)+\rho(B),$$

где A, B, C — матрицы подходящих размеров с коэффициентами из поля.

Арифметические свойства факторизационного ранга существенно зависят от структуры полукольца коэффициентов и ограничиваются следующими неравенствами, установленными в [2].

Для произвольного антинегативного полукольца:

(1) $\operatorname{rank}(A+B)\leqslant\operatorname{rank}(A)+\operatorname{rank}(B)$;
(2) $\operatorname{rank}(AB)\leqslant\min\{\operatorname{rank}(A),\operatorname{rank}(B)\}$.

Для полукольца с булевой арифметикой:

(3) $\operatorname{rank}(A+B)\geqslant\begin{cases}\operatorname{rank}(A), & \text{если } B=O,\\ \operatorname{rank}(B), & \text{если } A=O,\\ 1, & \text{если } A\neq O \text{ и } B\neq O;\end{cases}$

(4) $\operatorname{rank}(AB)\geqslant\begin{cases}0, & \text{если } \operatorname{rank}(A)+\operatorname{rank}(B)\leqslant n,\\ 1, & \text{если } \operatorname{rank}(A)+\operatorname{rank}(B)>n.\end{cases}$

Для подполуколец в $\mathbb{R}^+$, справедливо следующее:

(5) $\operatorname{rank}(A+B)\geqslant|\rho(A)-\rho(B)|$;

(6) $\operatorname{rank}(AB)\geqslant\begin{cases}0, & \text{если } \rho(A)+\rho(B)\leqslant n,\\ \rho(A)+\rho(B)-n, & \text{если } \rho(A)+\rho(B)>n;\end{cases}$

(7) $\rho(AB)+\rho(BC)\leqslant\operatorname{rank}(ABC)+\operatorname{rank}(B)$.

Как было доказано в [2], неравенства (1)–(7) точны и неулучшаемы.

Естественный вопрос состоит в характеризации случаев равенства в рассматриваемых неравенствах. Даже для матриц над полями это открытый вопрос (см. [13,14,16,17]). Структура матричных многообразий, возникающих в качестве экстремальных случаев в этих неравенствах, не известна ни над полями, ни над полукольцами. Стандартный способ выбора элементов таких многообразий состоит в применении линейных преобразований, сохраняющих данное многообразие, к семействам матриц, заведомо ему принадлежащих. Цель настоящей работы состоит в характеризации всех таких преобразований матриц над полукольцами. Полная классификация аналогичных преобразований матриц над полями была получена в [1,3,4,10]. Подробный обзор по теории операторов, сохраняющих матричные инварианты, дается в [15].

Авторы благодарны профессору В. Н. Латышеву за постоянное внимание к данной работе.

2. Общие результаты

Мы будем использовать следующие обозначения для семейств матриц, возникающих в качестве экстремальных случаев в вышеперечисленных неравенствах:

$$\mathcal{F}_1(\mathcal{S}) = \{(X,Y) \in \mathcal{M}_{m,n}(\mathcal{S})^2 \mid \operatorname{rank}(X+Y) = \operatorname{rank}(X) + \operatorname{rank}(Y)\},$$
$$\mathcal{F}_{2B}(\mathcal{S}) = \{(X,Y) \in \mathcal{M}_{m,n}(\mathcal{S})^2 \mid \operatorname{rank}(X+Y) = 1\},$$
$$\mathcal{F}_{2R}(\mathcal{S}) = \{(X,Y) \in \mathcal{M}_{m,n}(\mathcal{S})^2 \mid \operatorname{rank}(X+Y) = |\rho(X) - \rho(Y)|\},$$
$$\mathcal{F}_3(\mathcal{S}) = \{(X,Y) \in \mathcal{M}_n(\mathcal{S})^2 \mid \operatorname{rank}(XY) = \min\{\operatorname{rank}(X), \operatorname{rank}(Y)\}\},$$
$$\mathcal{F}_{4N}(\mathcal{S}) = \{(X,Y) \in \mathcal{M}_n(\mathcal{S})^2 \mid \operatorname{rank}(XY) = 0\},$$
$$\mathcal{F}_{4B}(\mathcal{S}) = \{(X,Y) \in \mathcal{M}_n(\mathcal{S})^2 \mid \operatorname{rank}(XY) = 1\},$$
$$\mathcal{F}_{4R}(\mathcal{S}) = \{(X,Y) \in \mathcal{M}_n(\mathcal{S})^2 \mid \operatorname{rank}(XY) = \rho(X) + \rho(Y) - n\},$$
$$\mathcal{F}_5(\mathcal{S}) = \{(X,Y,Z) \in \mathcal{M}_n(\mathcal{S})^3 \mid \operatorname{rank}(XYZ) + \operatorname{rank}(Y) = \rho(XY) + \rho(YZ)\}.$$

Определение 2.1. Преобразование T *сохраняет* множество $\mathcal{P}$, если из $X \in \mathcal{P}$ следует, что $T(X) \in \mathcal{P}$. Если $\mathcal{P}$ является множеством упорядоченных пар (троек), то предполагается, что из условия $(X,Y) \in \mathcal{P}$ (соответственно, $(X,Y,Z) \in \mathcal{P}$) следует, что $(T(X),T(Y)) \in \mathcal{P}$ (соответственно, $(T(X),T(Y),T(Z)) \in \mathcal{P}$).

Определение 2.2. Преобразование T *строго сохраняет* множество $\mathcal{P}$, если $X \in \mathcal{P}$ тогда и только тогда, когда $T(X) \in \mathcal{P}$. Если $\mathcal{P}$ является множеством упорядоченных пар (троек), то $(X,Y) \in \mathcal{P}$ (соответственно, $(X,Y,Z) \in \mathcal{P}$) эквивалентно $(T(X),T(Y)) \in \mathcal{P}$ (соответственно, $(T(X),T(Y),T(Z)) \in \mathcal{P}$).

Определение 2.3. Преобразование $T : \mathcal{M}_{m,n}(\mathcal{S}) \to \mathcal{M}_{m,n}(\mathcal{S})$ называется (U,V)-*оператором*, если существуют такие обратимые матрицы U и V подходящих размеров, что $T(X) = UXV$ для всех $X \in \mathcal{M}_{m,n}(\mathcal{S})$, или, при $m = n$, $T(X) = UX^tV$ для всех $X \in \mathcal{M}_{m,n}(\mathcal{F})$, где X^t обозначает транспонированную матрицу к матрице X.

Определение 2.4. Преобразование T называется (P,Q,B)-*оператором*, если существуют перестановочные матрицы P и Q и матрица B без нулевых коэффициентов такие, что $T(X) = P(X \circ B)Q$ для всех $X \in \mathcal{M}_{m,n}(\mathcal{S})$, или, при $m = n$, $T(X) = P(X \circ B)^tQ$ для всех $X \in \mathcal{M}_{m,n}(\mathcal{F})$. (P,Q,B)-оператор называется (P,Q)-*оператором*, если $B = J$ — матрица, все коэффициенты которой равны единице.

Определение 2.5. Пусть $\mathcal{S}$ — полукольцо (не обязательно коммутативное). Преобразование $T : \mathcal{M}_{m,n}(\mathcal{S}) \to \mathcal{M}_{m,n}(\mathcal{S})$ называется *линейным*, если оно аддитивно, $T(\alpha X) = \alpha T(X)$ и $T(X\alpha) = T(X)\alpha$ для всех $X \in \mathcal{M}_{m,n}(\mathcal{S})$, $\alpha \in \mathcal{S}$.

Определение 2.6. Матрица $A \in \mathcal{M}_{m,n}(\mathcal{S})$ называется *мономиальной*, если она имеет в точности один ненулевой элемент в каждой строке и каждом столбце.

Определение 2.7. *Линией* в матрице A называется строка или столбец матрицы A.

Определение 2.8. Матрица A *мажорирует* матрицу B если из $b_{i,j} \neq 0$ следует, что $a_{i,j} \neq 0$, что обозначается $A \geqslant B$ или $B \leqslant A$.

Определение 2.9. Если A и B — матрицы, причем $A \geqslant B$, то $A \backslash B$ обозначает матрицу C, где

$$c_{i,j} = \begin{cases} 0, & \text{если } b_{i,j} \neq 0, \\ a_{i,j} & \text{в противном случае.} \end{cases}$$

Определение 2.10. Матрица $X \circ Y$ обозначает произведение Адамара, т.е. (i,j)-й коэффициент матрицы $X \circ Y$ равен $x_{i,j}y_{i,j}$.

Пусть $\mathcal{Z}(\mathcal{S})$ — центр полукольца $\mathcal{S}$. Будем предполагать, что $m \leqslant n$, I_n — тождественная $(n \times n)$-матрица, $J_{m,n}$ — $(m \times n)$-матрица, все коэффициенты которой единичны, $O_{m,n}$ — нулевая $(m \times n)$-матрица. Мы будем опускать нижние индексы для обозначения размеров матриц, когда это не приводит к недоразумениям, и писать I, J, O соответственно. Символом $E_{i,j}$ обозначается матрица, у которой на (i,j)-м месте стоит единица, а все остальные коэффициенты нулевые; такая матрица называется *клеткой*. Пусть R_i — матрица, у которой i-я строка целиком состоит из единиц и все остальные элементы нулевые, C_j — матрица, у которой j-й столбец целиком состоит из единиц и все остальные элементы нулевые. Мы обозначаем через $|A|$ число ненулевых коэффициентов в матрице A. Пусть $A[i,j|k,l]$ обозначает (2×2)-подматрицу A, которая лежит на пересечении i-й и j-й строк с k-м и l-м столбцами.

Лемма 2.11. *Пусть $\mathcal{S}$ — полукольцо, $B = (b_{i,j}) \in \mathcal{M}_{m,n}(\mathcal{S})$, $m,n \geqslant 2$, и элементы $b_{i,j}$ обратимы для всех $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant m$. Рассмотрим произвольную пару целых чисел (k,l), для которой $2 \leqslant k \leqslant n$, $2 \leqslant l \leqslant m$. Предположим, что факторизационный ранг любой $(l \times k)$-подматрицы матрицы B равен* 1. *Тогда факторизационный ранг любой $((l+1) \times k)$-подматрицы* (*если такая существует*) *равен* 1 *и факторизационный ранг любой $(l \times (k+1))$-подматрицы* (*если такая существует*) *равен* 1.

Доказательство. Рассмотрим произвольную $(l \times (k+1))$-подматрицу матрицы B. Применяя перестановку строк и столбцов, если это необходимо, мы можем предполагать, что эта подматрица имеет вид $C = (b_{i,j})$, где $1 \leqslant i \leqslant l$, $1 \leqslant j \leqslant k+1$. Введем обозначения

$$B_1 = (b_{i,j}), \quad 1 \leqslant i \leqslant l, \quad 1 \leqslant j \leqslant k,$$
$$B_2 = (b_{i,j}), \quad 1 \leqslant i \leqslant l, \quad 2 \leqslant j \leqslant k+1.$$

По условию существуют четыре вектора

$$\mathbf{s} = (s_1, \ldots, s_l) \in \mathcal{S}^l, \quad \mathbf{t} = (t_1, \ldots, t_k) \in \mathcal{S}^k, \quad \mathbf{u} = (u_1, \ldots, u_l) \in \mathcal{S}^l, \quad \mathbf{v} = (v_1, \ldots, v_k) \in \mathcal{S}^k$$

такие, что

$$B_1 = \mathbf{s}^t\mathbf{t}, \quad B_2 = \mathbf{u}^t\mathbf{v}.$$

Обозначим через s'_i правый обратный элемента $s_i \in \mathcal{S}$ (он существует, поскольку $s_it_j = b_{i,j}$ — обратимый элемент) и через v''_j — левый обратный элемента $v_j \in \mathcal{S}$ (он существует, поскольку $u_iv_j = b_{i,j+1}$). Рассмотрим подматрицу

$$D = (d_{i,j}) = \mathbf{s}^t(t_1, t_2, \ldots, t_k, s'_1u_1v_k).$$

Проверим, что $C = D$. Первые k столбцов этих матриц совпадают согласно определению векторов $\mathbf{s}$ и $\mathbf{t}$. Рассмотрим последний столбец. Имеем

$$d_{1,k+1} = s_1 \cdot s'_1u_1v_k = u_1v_k = b_{1,k+1};$$

последнее равенство следует из разложения для B_2. Согласно определению векторов $\mathbf{u}$, $\mathbf{v}$ из разложений для матриц B_1 и B_2 следует, что

$$s_it_j = b_{i,j} = u_iv_{j-1} \quad \text{для всех} \quad i = 1, \ldots, l, \quad j = 2, \ldots, k.$$

Следовательно,

$$s'_iu_i = t_jv''_{j-1} \quad \text{для всех} \quad i = 1, \ldots, l.$$

Отсюда $s'_1u_1 = \ldots = s'_lu_l$. Поэтому для всех $i = 2, \ldots, l$ имеем

$$d_{i,k+1} = s_i \cdot s'_1u_1v_k = s_i \cdot s'_iu_iv_k = u_iv_k = b_{i,k+1},$$

т.е. $C = D$. Следовательно, $\mathrm{rank}(C) = 1$. Аналогичные рассуждения для $((l+1) \times k)$-матриц завершают доказательство. □

Следующие два утверждения вытекают из леммы 2.11.

Следствие 2.12. *Пусть $\mathcal{S}$ — полукольцо, $B = (b_{i,j}) \in \mathcal{M}_{m,n}(\mathcal{S})$, $m, n \geqslant 2$. Предположим, что $b_{i,j}$ обратимы для всех $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant m$ и $\mathrm{rank}(B') = 1$ для любой (2×2)-подматрицы B' матрицы B. Тогда $\mathrm{rank}(B) = 1$.*

Следствие 2.13. *Пусть $\mathcal{S}$ — полукольцо, $B = (b_{i,j}) \in \mathcal{M}_{m,n}(\mathcal{S})$, $m, n \geqslant 2$. Предположим, что $b_{i,j}$ обратимы для всех $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant m$. Допустим, что $\mathrm{rank}(B) > 1$. Тогда существует (2×2)-подматрица матрицы B факторизационного ранга 2.*

Следующая теорема имеет принципиальное значение для дальнейших рассмотрений.

Теорема 2.14. *Пусть $\mathcal{S}$ — антинегативное полукольцо без делителей нуля и $T : \mathcal{M}_{m,n}(\mathcal{S}) \to \mathcal{M}_{m,n}(\mathcal{S})$ — линейный оператор. Тогда следующие утверждения эквивалентны*:

1) *T биективен*;
2) *T сюръективен*;
3) *существуют перестановка σ множества индексов $\{(i,j) \mid i = 1, 2, \ldots, m;\ j = 1, 2, \ldots, n\}$ и обратимые элементы $b_{i,j} \in \mathcal{Z}(\mathcal{S})$, $i = 1, 2, \ldots, m$, $j = 1, 2, \ldots, n$, такие, что*

$$T(E_{i,j}) = b_{i,j}E_{\sigma(i,j)}$$

для всех $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant m$.

Доказательство. Импликации 1) ⇒ 2) и 3) ⇒ 1) очевидны. Коэффициенты $b_{i,j} \in \mathcal{Z}(\mathcal{S})$, поскольку T — линейное отображение. Докажем импликацию 2) ⇒ 3).

Предположим, что отображение T сюръективно. Тогда для любой пары (i,j) существует матрица X такая, что $T(X) = E_{i,j}$. Очевидно, что $X \neq O$ в силу линейности T. Следовательно, существует пара индексов (r,s) такая, что $X = x_{r,s}E_{r,s} + X'$, где (r,s)-й коэффициент матрицы X' является нулевым и выполняются следующие два условия: $x_{r,s} \neq 0$ и $T(E_{r,s}) \neq O$. В противном случае для всех пар (r,s) или $x_{r,s} = 0$, или $T(E_{r,s}) = O$. Тогда $T(X) = 0$, что противоречит предположению $T(X) = E_{i,j}$. Так как $\mathcal{S}$ — антинегативное полукольцо без делителей нуля, имеем

$$T(x_{r,s}E_{r,s}) \leqslant T(x_{r,s}E_{r,s}) + T(X \setminus (x_{r,s}E_{r,s})) = T(X) = E_{i,j}.$$

Следовательно, $x_{r,s}T(E_{r,s}) = T(x_{r,s}E_{r,s}) \leqslant E_{i,j}$ и $T(E_{r,s}) \neq O$. Поэтому $T(E_{r,s}) \leqslant E_{i,j}$. В противном случае $T(E_{r,s})$ является линейной комбинацией клеток. Тогда $x_{r,s}T(E_{r,s})$ также является линейной комбинацией клеток, поскольку $\mathcal{S}$ антинегативно и не имеет делителей нуля.

Пусть $P_{i,j} = \{E_{r,s} \mid T(E_{r,s}) \leqslant E_{i,j}\}$. Согласно доказанному, $P_{i,j} \neq \emptyset$ для всех (i,j). По своему определению, $P_{i,j} \cap P_{u,v} = \emptyset$, как только $(i,j) \neq (u,v)$. Это означает, что $\{P_{i,j}\}$ является семейством mn непустых множеств, определяющих разбиение множества клеток. Согласно принципу Дирихле получаем $|P_{i,j}| = 1$ для всех (i,j). Отсюда следует, что для каждой пары (r,s) существует единственная такая пара (i,j), что $T(E_{r,s}) = b_{r,s}E_{i,j}$. Таким образом, существует такая перестановка σ на множестве $\{(i,j) \mid i = 1, 2, \ldots, m;\ j = 1, 2, \ldots, n\}$, что для некоторых скаляров $b_{i,j}$ имеем $T(E_{i,j}) = b_{i,j}E_{\sigma(i,j)}$. Нам осталось показать, что все элементы $b_{i,j}$ обратимы. Поскольку отображение T сюръективно и $T(E_{r,s}) \not\leqslant E_{\sigma(i,j)}$ для всех $(r,s) \neq (i,j)$, существует такой элемент α, что $T(\alpha E_{i,j}) = E_{\sigma(i,j)}$. Тогда в силу линейности отображения T имеем

$$T(\alpha E_{i,j}) = \alpha T(E_{i,j}) = \alpha b_{i,j}E_{\sigma(i,j)} = E_{\sigma(i,j)},$$

т.е., $\alpha b_{i,j} = 1$. Аналогично проверяется, что $b_{i,j}$ обратимы справа. Поэтому элемент $b_{i,j}$ обратим. □

Замечание 2.15. Непосредственно проверяется, что при $m = 1$ или $n = 1$ все рассматриваемые линейные преобразования являются (P, Q, B)-операторами, а если $m = n = 1$ — то (P, P^t, B)-операторами.

Далее мы будем предполагать, что $m, n \geqslant 2$.

Лемма 2.16. *Пусть $\mathcal{S}$ — антинегативное полукольцо, $T : \mathcal{M}_{m,n}(\mathcal{S}) \to \mathcal{M}_{m,n}(\mathcal{S})$ — линейное преобразование, отображающее линии в линии и задаваемое формулой $T(E_{i,j}) = b_{i,j}E_{\sigma(i,j)}$, где σ является перестановкой на множестве $\{(i,j) \mid i = 1,2,\ldots,m;\ j = 1,2,\ldots,n\}$, и $b_{i,j} \in \mathcal{S}$ — некоторые ненулевые элементы, $i = 1,2,\ldots,m$, $j = 1,2,\ldots,n$. Тогда T является (P,Q,B)-оператором.*

Доказательство. Так как при $a + b = m$ линейная комбинация a строк и b столбцов может мажорировать J лишь в случае $b = 0$ (или $a = 0$, если $m = n$) получаем, что или образ любой строки есть строка, а образ любого столбца есть столбец, или, при $m = n$, образ любой строки есть столбец, а образ любого столбца есть строка. Следовательно, существуют перестановочные матрицы P и Q такие, что

$$T(R_i) \leqslant PR_iQ, \quad T(C_j) \leqslant PC_jQ$$

или, при $m = n$,

$$T(R_i) \leqslant P(R_i)^tQ, \quad T(C_j) \leqslant P(C_j)^tQ.$$

Так как любая клетка лежит на пересечениии строки и столбца и T отображает ненулевые клетки в ненулевые клетки с весами, получаем, что

$$T(E_{i,j}) = Pb_{i,j}E_{i,j}Q = P(E_{i,j} \circ B)Q$$

или, при $m = n$,

$$T(E_{i,j}) = Pb_{i,j}E_{j,i}Q = P(E_{i,j} \circ B)^tQ,$$

где $B = (b_{i,j})$ определяется действием T на клетках. □

Лемма 2.17. *Пусть $\mathcal{S}$ — коммутативное полукольцо. Если $T(X) = X \circ B$ для всех $X \in \mathcal{M}_{m,n}(\mathcal{S})$ и $\operatorname{rank}(B) = 1$, то существуют диагональные матрицы D и E, такие что $T(X) = DXE$ для всех $X \in \mathcal{M}_{m,n}(\mathcal{S})$.*

Доказательство. Если $\operatorname{rank}(B) = 1$, то существуют векторы $\mathbf{d} = [d_1, d_2, \ldots, d_m]$ и $\mathbf{e} = [e_1, e_2, \ldots, e_n]$ такие, что $B = \mathbf{d}\mathbf{e}^t$, или $b_{i,j} = d_ie_j$. Пусть $D = \operatorname{diag}\{d_1, d_2, \ldots, d_m\}$ и $E = \operatorname{diag}\{e_1, e_2, \ldots, e_n\}$. Так как (i,j)-й коэффициент $T(X)$ — это $b_{i,j}x_{i,j}$ и (i,j)-й коэффициент матрицы DXE — это $d_ix_{i,j}e_j = b_{i,j}x_{i,j}$, то лемма доказана. □

Если умножение в полукольце не является коммутативным, то простая характеризация оператора T отсутствует, однако можно доказать следующую лемму.

Лемма 2.18. *Пусть $\mathcal{S}$ — полукольцо. Рассмотрим линейное преобразование $T : \mathcal{M}_{m,n}(\mathcal{S}) \to \mathcal{M}_{m,n}(\mathcal{S})$, определенное как $T(X) = X \circ B$ для всех $X \in \mathcal{M}_{m,n}(\mathcal{S})$, где $\operatorname{rank}(B) = 1$ и все коэффициенты $b_{i,j} \in \mathcal{Z}(\mathcal{S})$ обратимы. Тогда T сохраняет факторизационный ранг.*

Доказательство. Рассмотрим матрицу $X \in \mathcal{M}_{m,n}(\mathcal{S})$, $\operatorname{rank}(X) = k$. По определению, существуют такие матрицы $Y \in \mathcal{M}_{m,k}(\mathcal{S})$ и $Z \in \mathcal{M}_{k,n}(\mathcal{S})$, что $X = YZ$, т.е. $x_{i,j} = \sum\limits_{l=1}^{k} y_{i,k}z_{k,j}$ для всех i, j. Так как $\operatorname{rank}(B) = 1$, получаем, что существуют такие векторы $\mathbf{d} = [d_1, d_2, \ldots, d_m]$ и $\mathbf{e} = [e_1, e_2, \ldots, e_n]$, что $B = \mathbf{d}\mathbf{e}^t$ или $b_{i,j} = d_ie_j$. Рассмотрим такие матрицы $D = (d_{i,j}) \in \mathcal{M}_{m,k}(\mathcal{S})$ и $E = (e_{i,j}) \in \mathcal{M}_{m,k}(\mathcal{S})$, что $d_{i,j} = d_i$ для всех $i = 1,\ldots,m$, $j = 1,\ldots,k$ и $e_{i,j} = e_j$ для всех $i = 1,\ldots,k$, $j = 1,\ldots,n$. Так как $b_{i,j} \in \mathcal{Z}(\mathcal{S})$, то

$$T(X) = (Y \circ D)(E \circ Z).$$

Следовательно, $\operatorname{rank}(T(X)) \leqslant \operatorname{rank}(X)$. В силу того, что $b_{i,j}$ обратимы, получаем, что T — биекция. Применение аналогичных рассуждений для T^{-1} завершает доказательство. □

3. LP-проблема для $\mathcal{F}_1$

Напомним, что

$$\mathcal{F}_1(\mathcal{S}) = \{(X,Y) \in \mathcal{M}_{m,n}(\mathcal{S})^2 \mid \operatorname{rank}(X+Y) = \operatorname{rank}(X) + \operatorname{rank}(Y)\}.$$

Лемма 3.1. *Пусть $\mathcal{S}$ — антинегативное полукольцо, σ — перестановка на множестве пар $\{(i,j) \mid 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant n\}$, линейное отображение $T : \mathcal{M}_{m,n}(\mathcal{S}) \to \mathcal{M}_{m,n}(\mathcal{S})$ определяется на образующих по формуле $T(E_{i,j}) = b_{i,j}E_{\sigma(i,j)}$ для некоторых скаляров $b_{i,j}$, $i = 1,\dots,m$, $j = 1,\dots,n$, которые не являются делителями нуля. Тогда если T сохраняет $\mathcal{F}_1$, то T является (P,Q,B)-оператором.*

Доказательство. Исследуем действие T на строках и столбцах матриц. Пусть образы двух клеток лежат в одной линии, а клетки — нет. Обозначим через E, F пару таких клеток, что $\operatorname{rank}(E+F) = 2$ и $\operatorname{rank}(T(E+F)) = 1$. Тогда $(E,F) \in \mathcal{F}_1$, но $(T(E),T(F)) \notin \mathcal{F}_1$, противоречие. Следовательно, T отображает линии в линии. Результат следует из леммы 2.16. □

Лемма 3.2. *Если $\mathcal{S}$ — антинегативное полукольцо и для некоторого $B = (b_{i,j})$, где $b_{i,j}$ — обратимые, $i = 1,\dots,m$, $j = 1,\dots,n$, отображение $T(X) = X \circ B$ сохраняет $\mathcal{F}_1$, то* $\operatorname{rank}(B) = 1$. *Если полукольцо $\mathcal{S}$ коммутативно, то $T(X) = DXE$ для диагональных матриц D и E подходящих размеров.*

Доказательство. Если $\operatorname{rank}(B) \geqslant 2$, то согласно следствию 2.13 существует такая (2×2)-подматрица $B[i,j|k,l]$, что

$$\operatorname{rank}(B[i,j|k,l]) = 2.$$

Пусть

$$J' = E_{i,k} + E_{j,k} + E_{i,l} + E_{j,l}.$$

Тогда

$$T(J') = b_{i,k}E_{i,k} + b_{j,k}E_{j,k} + b_{i,l}E_{i,l} + b_{j,l}E_{j,l} = B'.$$

В таком случае для $q \neq k,l$ имеем

$$\operatorname{rank}(E_{i,q} + J') = 2 = \operatorname{rank}(E_{i,q}) + \operatorname{rank}(J'),$$

т.е. $(E_{i,q}, J') \in \mathcal{F}_1$, тогда как

$$\operatorname{rank}(T(E_{i,q} + J')) = \operatorname{rank}(b_{i,q}E_{i,q} + B') = 2 \neq \operatorname{rank}(b_{i,q}E_{i,q}) + \operatorname{rank}(B') = 1 + 2 = 3;$$

противоречие. Следовательно, $\operatorname{rank}(B) = 1$.

Если $\mathcal{S}$ — коммутативное полукольцо, то согласно лемме 2.17 существуют такие диагональные матрицы D и E, что $T(X) = DXE$. □

Теорема 3.3. *Пусть $\mathcal{S}$ — антинегативное полукольцо без делителей нуля, $T : \mathcal{M}_{m,n}(\mathcal{S}) \to \mathcal{M}_{m,n}(\mathcal{S})$ — сюръективный линейный оператор. Если T сохраняет $\mathcal{F}_1$, то T является (P,Q,B)-оператором, где $B = (b_{i,j}) \in \mathcal{M}_{m,n}(\mathcal{Z}(\mathcal{S}))$, коэффициенты $b_{i,j}$ обратимы для всех $i = 1,\dots,m$, $j = 1,\dots,n$, и* $\operatorname{rank}(B) = 1$.

Доказательство. Если отображение T сюръективно и $\mathcal{S}$ — антинегативное полукольцо без делителей нуля, то из теоремы 2.14 следует, что T определяется перестановкой σ на множестве $\{(i,j) \mid 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant n\}$, т.е. $T(E_{i,j}) = b_{i,j}E_{\sigma(i,j)}$ для некоторых обратимых скаляров $b_{i,j} \in \mathcal{Z}(\mathcal{S})$.

Согласно лемме 3.1 получаем, что T является (P,Q,B)-оператором. Согласно лемме 3.2 имеем $\operatorname{rank}(B) = 1$. □

Следствие 3.4. *Пусть $\mathcal{S}$ — коммутативное антинегативное полукольцо без делителей нуля, $T : \mathcal{M}_{m,n}(\mathcal{S}) \to \mathcal{M}_{m,n}(\mathcal{S})$ — сюръективный линейный оператор. Отображение T сохраняет множество $\mathcal{F}_1$ тогда и только тогда, когда T является (U,V)-оператором, где U и V — обратимые мономиальные матрицы.*

Доказательство. Легко проверяется, что умножение на обратимые матрицы не меняет факторизационного ранга. Кроме того, над коммутативным полукольцом операция транспонирования не меняет факторизационного ранга. Следовательно, эти операции сохраняют $\mathcal{F}_1$.

Последовательное применение теоремы 3.3 и леммы 3.2 позволяет получить, что T имеет вид $T(X) = PDXEQ$ для всех $X \in \mathcal{M}_{m,n}(\mathcal{S})$, или, при $m = n$, $T(X) = PDX^tEQ$ для всех $X \in \mathcal{M}_{m,n}(\mathcal{S})$, где D и E — диагональные матрицы подходящих размеров. Так как T сюръективно, то коэффициенты диагональных матриц D и E обратимы, что доказывает следствие. □

Над конечным или цепным полукольцом предположение сюръективности из предыдущей теоремы можно заменить на предположение, что T строго сохраняет множество $\mathcal{F}_1$.

Теорема 3.5. *Пусть $\mathcal{S}$ — конечное антинегативное или произвольное цепное полукольцо, $T : \mathcal{M}_{m,n}(\mathcal{S}) \to \mathcal{M}_{m,n}(\mathcal{S})$ — линейный оператор, строго сохраняющий $\mathcal{F}_1$. Тогда T является (P, Q, B)-оператором, где $B \in \mathcal{M}_{m,n}(\mathcal{Z}(\mathcal{S}))$ — матрица с ненулевыми коэффициентами.*

Доказательство. Непосредственная проверка показывает, что для цепного или конечного полукольца $\mathcal{S}$ существуют такие положительные целые $\alpha > \beta$, что $\alpha \cdot 1_{\mathcal{S}} = \beta \cdot 1_{\mathcal{S}}$. В [6] доказано, что в конечном полукольце существует степень T, являющаяся идемпотентом. Аналогичное справедливо для цепных полуколец. В самом деле, согласно определениям умножения и сложения в цепном полукольце, коэффициенты каждой степени данной матрицы A содержатся в множестве коэффициентов A. Поэтому множество различных матриц среди степеней A является конечным. Следовательно, существуют положительные целые s и t такие, что для всех $p, q > s$, $p \equiv q (\mathrm{mod}\, t)$ справедливо, что $A^p = A^q$. В частности, $A^{st} = A^{2st}$. Следовательно, у каждого оператора над цепным полукольцом найдется идемпотентная степень. В обоих случаях положим $L = T^d$ и $L^2 = L$. Легко проверяется, что L строго сохраняет $\mathcal{F}_1$.

Если $X \in \mathcal{M}_{m,n}(\mathcal{S})$ и $(X, X) \in \mathcal{F}_1$, то $X = O$. Следовательно, если $A \neq O$, то $L(A) \neq O$, так как L строго сохраняет $\mathcal{F}_1$.

Исследуем действие L на строках и столбцах. Предположим, что $L(R_i)$ не мажорируется R_i. Тогда существуют (r, s) такие, что $E_{r,s} \leqslant L(R_i)$, тогда как $E_{r,s} \not\leqslant R_i$. Легко видеть, что $(R_i, E_{r,s}) \in \mathcal{F}_1$ и существует матрица $X = (x_{i,j}) \in \mathcal{M}_{m,n}(\mathcal{S})$, $x_{r,s} = 0$, такая, что $L(R_i) = aE_{r,s} + X$ для некоторого $0 \neq a \in \mathcal{S}$.

Предположим, что

$$\begin{gathered}
L(\beta R_i + (\alpha - \beta)aE_{r,s}) = L(\beta R_i) + L((\alpha - \beta)aE_{r,s}) = \\
= L^2(\beta R_i) + L((\alpha - \beta)aE_{r,s}) = L(\beta L(R_i)) + L((\alpha - \beta)aE_{r,s}) = \\
= L(\beta(aE_{r,s} + X)) + L((\alpha - \beta)aE_{r,s}) = L(\beta aE_{r,s} + \beta X) + L((\alpha - \beta)aE_{r,s}) = \\
= L(\beta X) + L(\beta aE_{r,s}) + L((\alpha - \beta)aE_{r,s}) = L(\beta X) + L(\beta aE_{r,s} + (\alpha - \beta)aE_{r,s}) = \\
= L(\beta X) + L(\alpha aE_{r,s}) = L(\alpha X) + L(\alpha aE_{r,s}) = L(\alpha(X + aE_{r,s})) = \\
= L(\alpha L(R_i)) = L^2(\alpha R_i) = L(\alpha R_i) = L(\beta R_i).
\end{gathered}$$

Теперь $(\beta R_i, (\alpha - \beta)aE_{r,s}) \in \mathcal{F}_1$, однако

$$L(\beta R_i) + L((\alpha - \beta)aE_{r,s}) = L(\beta R_i + (\alpha - \beta)aE_{r,s}) = L(\beta R_i);$$

следовательно, $(L(\beta R_i), L((\alpha - \beta)aE_{r,s})) \notin \mathcal{F}_1$, противоречие.

Мы установили, что $L(R_i) \leqslant R_i$ для всех i. Аналогично, $L(C_j) \leqslant C_j$ для всех j. Рассматривая матрицу $E_{i,j}$, которая мажорируется как R_i, так и C_j имеем$L(E_{i,j}) \leqslant E_{i,j}$. В силу антинегативности $\mathcal{S}$ получаем, что T отображает клетки в клетки с весами или $|T(E_{i,j})| = 1$ для всех i, j и все коэффициенты $T(J)$ ненулевые.

Следовательно, T индуцирует перестановку σ на множестве индексов $\{1, 2, \ldots, m\} \times \{1, 2, \ldots, n\}$, т.е. $T(E_{i,j}) = b_{i,j}E_{\sigma(i,j)}$ для некоторых скаляров $b_{i,j}$. Из линейности T следует, что $b_{i,j} \in \mathcal{Z}(\mathcal{S})$.

Согласно лемме 3.1 T является (P, Q, B)-оператором. □

Следствие 3.6. *Пусть $\mathcal{S}$ — цепное полукольцо. Тогда линейный оператор $T : \mathcal{M}_{m,n}(\mathcal{S}) \to \mathcal{M}_{m,n}(\mathcal{S})$ строго сохраняет $\mathcal{F}_1$ тогда и только тогда, когда T является (P, Q)-оператором (т.е. $B = J$).*

Доказательство. Как проверено в начале доказательства следствия 3.4, (P,Q)-операторы сохраняют множество $\mathcal{F}_1$.

Согласно теореме 3.5 получаем, что $T-(P,Q,B)$-оператор. Пусть $\alpha = b_{i,j}$ — наименьший ненулевой коэффициент матрицы B. Тогда в силу того, что $\mathcal{S}$ — цепное полукольцо, имеем $(E_{i,j}, \alpha J) \in \mathcal{F}_1$, тогда как $T(E_{i,j}+\alpha J) = T(\alpha J)$. Следовательно, $(T(E_{i,j}), T(\alpha J)) \notin \mathcal{F}_1$; противоречие. □

4. LP-проблема для $\mathcal{F}_{2B}$

Напомним, что

$$\mathcal{F}_{2B}(\mathcal{S}) = \{(X,Y) \in \mathcal{M}_{m,n}(\mathcal{S})^2 \mid \operatorname{rank}(X+Y) = 1\}.$$

Теорема 4.1. *Пусть $\mathcal{S}$ — антинегативное полукольцо без делителей нуля и $T : \mathcal{M}_{m,n}(\mathcal{S}) \to \mathcal{M}_{m,n}(\mathcal{S})$ — сюръективное линейное отображение. Если T сохраняет $\mathcal{F}_{2B}$, то T является (P,Q,B)-оператором, где $B = (b_{i,j}) \in \mathcal{M}_{m,n}(\mathcal{Z}(\mathcal{S}))$, коэффициенты $b_{i,j}$ обратимы для всех $i = 1,\dots,m$, $j = 1,\dots,n$ и $\operatorname{rank}(B) = 1$.*

Доказательство. Если отображение T сюръективно и $\mathcal{S}$ — антинегативное полукольцо без делителей нуля, то согласно теореме 2.14 имеем, что $T(E_{i,j}) = b_{i,j}E_{\sigma(i,j)}$ для обратимых скаляров $b_{i,j} \in \mathcal{Z}(\mathcal{S})$. Легко проверяется, что клетки с весами $\alpha E_{i,j}$ и $\beta E_{r,s}$ лежат на одной линии в том и только том случае, когда $\operatorname{rank}(\alpha E_{i,j} + \beta E_{r,s}) = 1$, что эквивалентно $(\alpha E_{i,j}, \beta E_{r,s}) \in \mathcal{F}_{2B}$. Следовательно, линии отображаются в линии, а T является (P,Q,B)-оператором согласно лемме 2.16.

Предположим, что $\operatorname{rank}(B) > 1$. Тогда согласно следствию 2.13 существует такая (2×2)-подматрица $B[i,j|k,l]$, что $\operatorname{rank}(B[i,j|k,l]) = 2$. Пусть

$$A = E_{j,k} + E_{i,l} + E_{j,l}, \quad B = E_{i,k}.$$

Следовательно,

$$\operatorname{rank}(A+B) = \operatorname{rank}(E_{j,k} + E_{i,l} + E_{j,l} + E_{i,k}) = 1,$$

т.е. $(A,B) \in \mathcal{F}_{2B}$, тогда как

$$\operatorname{rank}(T(A) + T(B)) = \operatorname{rank}(b_{i,k}E_{i,k} + b_{j,k}E_{j,k} + b_{i,l}E_{i,l} + b_{j,l}E_{j,l}) = 2,$$

т.е. $(T(A), T(B)) \notin \mathcal{F}_{2B}$. Это противоречие показывает, что $\operatorname{rank}(B) = 1$. □

Легко видеть, что для коммутативных полуколец операция транспонирования сохраняет множество $\mathcal{F}_{2B}$. Следовательно, все (P,Q,B)-операторы, где все элементы B обратимы, сохраняют множество $\mathcal{F}_{2B}$. Это позволяет усилить теорему 4.1 следующим образом.

Следствие 4.2. *Пусть $\mathcal{S}$ — коммутативное антинегативное полукольцо без делителей нуля и $T : \mathcal{M}_{m,n}(\mathcal{S}) \to \mathcal{M}_{m,n}(\mathcal{S})$ — сюръективный линейный оператор. Тогда T сохраняет множество $\mathcal{F}_{2B}$ в том и только том случае, когда T является (P,Q,B)-оператором, где $B = (b_{i,j}) \in \mathcal{M}_{m,n}(\mathcal{Z}(\mathcal{S}))$, коэффициенты $b_{i,j}$ обратимы для всех $i = 1,\dots,m$ и $j = 1,\dots,m$ и* $\operatorname{rank}(B) =$.

Над цепными полукольцами эта теорема может быть усилена.

Теорема 4.3. *Пусть $\mathcal{S}$ — цепное полукольцо и $T : \mathcal{M}_{m,n}(\mathcal{S}) \to \mathcal{M}_{m,n}(\mathcal{S})$ — линейное отображение, сохраняющее $\mathcal{F}_{2B}$. В этом случае T сюръективно тогда и только тогда, когда T строго сохраняет $\mathcal{F}_{2B}$, тогда и только тогда, когда T является (P,Q)-оператором.*

Доказательство. Любой (P,Q)-оператор сюръективен и строго сохраняет множество $\mathcal{F}_{2B}$.

Пусть T — сюръективное отображение. Согласно теореме 4.1 получаем, что T является (P,Q)-оператором ($B = J$, так как единственный обратимый элемент цепного кольца — это 1).

Предположим, что T строго сохраняет $\mathcal{F}_{2B}$. Покажем, что существует такой элемент $\beta \in \mathcal{S}$, что отображение βT сюръективно на множестве $\mathcal{M}_{m,n}(\beta\mathcal{S})$. Для этого достаточно проверить, что для любой пары индексов (i,j) существуют $Y \in \mathcal{M}_{m,n}(\mathcal{S})$ и $a \in \mathcal{S}$ такие, что $T(Y) = aE_{i,j}$. Если это не выполняется или если существует клетка, образ которой не мажорируется клеткой, то существуют

$(0,1)$-матрица $N=(n_{i,j})$ и пара индексов (r,s) такие, что $n_{r,s}=0$ и $T(N)\geqslant T(J)$. Покажем, что существует такой элемент $\alpha\in\mathcal{S}$, что $T(\alpha J\backslash E_{r,s})=T(\alpha J)$.

Пусть $G=T(N)$, $\alpha=\min\{g_{i,j}\mid g_{i,j}\neq 0\}$, $H=T(J)$. Так как $N-(0,1)$-матрица, то существует такая $(0,1)$-матрица M, что $J=N+M$. Следовательно,

$$H=T(J)=T(N)+T(M)=G+T(M).$$

Тогда $h_{i,j}\geqslant g_{i,j}$ для всех (i,j), так как $\mathcal{S}$ — цепное полукольцо. Согласно выбору N, $T(N)\geqslant T(J)$, т.е. $g_{i,j}=0$ влечет $h_{i,j}=0$. Тогда $\alpha h_{i,j}=\alpha=\alpha g_{i,j}$ по определению α и умножения в цепном полукольце. Следовательно,

$$T(\alpha N)=\alpha T(N)=\alpha T(J)=T(\alpha J).$$

Аналогично можно проверить, что если K — произвольная $(0,1)$-матрица такая, что $N\leqslant K\leqslant J$ и $T(K)=R=(r_{i,j})$, то $\alpha r_{i,j}=\alpha g_{i,j}$. Следовательно, $T(\alpha K)=T(\alpha J)$, а значит, поскольку $N\leqslant J\backslash E_{r,s}\leqslant J$, получаем, что $T(\alpha J\backslash E_{r,s})=T(\alpha J)$.

Непосредственно проверяется, что $(\alpha J\backslash E_{r,s},\alpha J\backslash E_{r,s})\notin\mathcal{F}_{2B}$, так как $\operatorname{rank}(\alpha J\backslash E_{r,s})\neq 1$. Вместе с тем $(\alpha J,\alpha J)\in\mathcal{F}_{2B}$. Следовательно, $(T(\alpha J\backslash E_{r,s}),T(\alpha J\backslash E_{r,s}))\notin\mathcal{F}_{2B}$, тогда как $(T(\alpha J),T(\alpha J))\in\mathcal{F}_{2B}$, что противоречит $T(\alpha J)=T(\alpha J\backslash E_{r,s})$. Следовательно, не существует матрицы N, обладающей хотя бы одним нулевым коэффициентом и такой, что $T(N)\geqslant T(J)$. Следовательно, образ клетки мажорирует только одну клетку. Тогда для $\beta=\min\{h_{i,j}\mid H=T(J)\}$ отображение βT является сюръективным на $\mathcal{M}_{m,n}(\beta\mathcal{S})$ и, как было показано ранее, является (P,Q)-оператором, т.е. $T-(P,Q,B)$-оператор на $\mathcal{M}_{m,n}(\mathcal{S})$. Далее, если $b_{i,j}\neq 1$, то $(E_{i,j}+b_{i,j}J,E_{i,j}+b_{i,j}J)\notin\mathcal{F}_{2B}$, но

$$T(E_{i,j}+b_{i,j}J)=T(E_{i,j})+T(b_{i,j}J)=b_{i,j}T(E_{i,j})+T(b_{i,j}J)=T(b_{i,j}E_{i,j}+b_{i,j}J)=T(b_{i,j}J)$$

по определению сложения и умножения в цепном полукольце, и $(b_{i,j}J,b_{i,j}J)\in\mathcal{F}_{2B}$. Получаем противоречие. Следовательно, $B=J$, и теорема доказана. □

5. LP-проблема для $\mathcal{F}_{2R}$

Напомним, что для $\mathcal{S}\subseteq\mathbb{R}_+$

$$\mathcal{F}_{2R}(\mathcal{S})=\{(X,Y)\in\mathcal{M}_{m,n}(\mathcal{S})^2\mid\operatorname{rank}(X+Y)=|\rho(X)-\rho(Y)|\}.$$

Лемма 5.1. *Пусть E_1, E_2, E_3 и E_4 — различные клетки с весами. Предположим, что $\operatorname{rank}(E_1+E_2)=2$ и $\operatorname{rank}(E_1+E_2+E_3+E_4)=1$. Тогда ненулевые коэффициенты матрицы $E_1+E_2+E_3+E_4$ лежат в пересечении двух строк и столбцов (т.е. ненулевые коэффициенты лежат в ее (2×2)-подматрице).*

Доказательство. Пусть $\operatorname{rank}(E_1+E_2)=2$. Тогда не все ненулевые коэффициенты матрицы $E_1+E_2+E_3+E_4$ лежат в одной строке или одном столбце. Матрица ранга 1 с четырьмя ненулевыми коэффициентами, не лежащими в одной линии, содержит эти коэффициенты в некоторой своей (2×2)-подматрице. □

Теорема 5.2. *Пусть $\mathcal{S}\subseteq\mathbb{R}_+$ — полукольцо и $T:\mathcal{M}_{m,n}(\mathcal{S})\to\mathcal{M}_{m,n}(\mathcal{S})$ — сюръективный линейный оператор. Тогда T сохраняет $\mathcal{F}_{2R}$ в том и только в том случае, когда $T(X)=PDXEQ$ для всех $X\in\mathcal{M}_{m,n}(\mathcal{S})$, или, при $m=n$, $T(X)=PDX^tEQ$ для всех $X\in\mathcal{M}_{m,n}(\mathcal{S})$, где D и E — диагональные матрицы, P и Q — перестановочные матрицы подходящего размера.*

Доказательство. Легко проверить, что данные операторы сохраняют $\mathcal{F}_{2R}$.

Согласно теореме 2.14 получаем, что $T(E_{i,j})=b_{i,j}E_{\sigma(i,j)}$ для некоторой перестановки σ множества $\{(i,j)\mid 1\leqslant i\leqslant m,1\leqslant j\leqslant n\}$ и $b_{i,j}$ обратимы для всех (i,j). Проверим, что T переводит линии в линии.

Если $m=n=2$, умножая на перестановочные матрицы слева и справа, можно предполагать, что $T(E_{1,1})=b_{1,1}E_{1,1}$. Следовательно, если T не переводит линии в линии, то без ограничения общности можно считать, что $T(E_{1,2})=b_{1,2}E_{2,2}$ (случай, когда $T(E_{2,1})=b_{2,1}E_{2,2}$, рассматривается аналогично). Кроме того, без ограничения общности можно предполагать, что $T(E_{2,1})=b_{2,1}E_{2,1}$ и $T(E_{2,2})=b_{2,2}E_{1,2}$ (случай $T(E_{2,1})=b_{2,1}E_{1,2}$ и $T(E_{2,2})=b_{2,2}E_{2,1}$ рассматривается аналогично). Так как $1\in\mathcal{S}$ по определению и $\mathcal{S}\subseteq\mathbb{R}_+$, элементы $2,3\in\mathcal{S}$. Рассмотрим пару матриц $(A,B)\in\mathcal{F}_{2R}$,

где $A = E_{1,1} + E_{1,2} + 2E_{2,1} + E_{2,2}$, $B = E_{2,2}$. Так как $\rho(T(B)) = 1$, $T(A+B) \neq 0$ и T сохраняет множество $\mathcal{F}_{2R}$, получаем, что $\operatorname{rank}(T(A+B)) = 1$ и $\rho(T(A)) = 2$. Следовательно, $\rho(T(A+B)) = 1$. Применяя T к паре $(T(A), T(B)) \in \mathcal{F}_{2R}$, получаем аналогично, что

$$\rho(T^2(A+B)) = \rho(b_{1,1}^2 E_{1,1} + b_{1,2}b_{2,2}E_{1,2} + 2b_{2,1}^2 E_{2,1} + 2b_{1,2}b_{2,2}E_{2,2}) = 1.$$

Следовательно, $b_{1,1} = b_{2,1}$ и, поскольку $\rho(T(A+B)) = 1$, то $b_{1,2} = 4b_{2,2}$. Рассмотрим пару матриц $(C, D) \in \mathcal{F}_{2R}$, где $C = E_{1,1} + E_{1,2} + 3E_{2,1} + E_{2,2}$, $D = 2E_{2,2}$. Легко проверить, что $\rho(T(C+D)) = 2$; это противоречит предположению о том, что $(T(C), T(D)) \in \mathcal{F}_{2R}$.

Предположим, что $m+n \geqslant 5$. Допустим, что существует некоторая строка R_i такая, что $T(R_i)$ не мажорируется никакой строкой или столбцом. Следовательно, в строке R_i существуют две клетки, образы которых не лежат в одной линии, т.е. для некоторых k, l имеем $\operatorname{rank}(T(E_{i,k} + E_{i,l})) = 2$. Отсюда $T(E_{i,k} + E_{i,l}) = b_{i,k}E_{r,s} + b_{i,l}E_{p,q}$ для некоторых $p \neq r$ и $q \neq s$. Для произвольных фиксированных $j \neq i$ имеем $(E_{i,k}+E_{i,l}+E_{j,k}, E_{j,l}) \in \mathcal{F}_{2R}$, откуда $(T(E_{i,k}+E_{i,l}+E_{j,k}), T(E_{j,l})) \in \mathcal{F}_{2R}$. Согласно лемме 5.1 получаем

$$T(E_{i,k} + E_{i,l} + E_{j,k}) + T(E_{j,l}) = b_{i,k}E_{r,s} + b_{i,l}E_{p,q} + \alpha E_{r,q} + \beta E_{p,s},$$

где $\alpha = b_{j,k}$ или $b_{j,l}$ и $\beta = b_{j,l}$ или $b_{j,k}$ соответственно. Так как σ является перестановкой, получаем $m \leqslant 2$. Аналогично, $n \leqslant 2$. Это противоречит предположению о том, что $m + n \geqslant 5$; следовательно, образ каждой строки мажорируется некоторой строкой или столбцом. Согласно лемме 2.16 получаем, что T является (P, Q, B)-оператором, где $b_{i,j}$ обратимы для любых индексов (i, j).

Если $\operatorname{rank}(B) \neq 1$, то согласно следствию 2.13 существует (2×2)-подматрица B ранга 2, т.е. найдутся такие клетки $E_{i,k}$, $E_{i,l}$, $E_{j,k}$, $E_{j,l}$, что $\operatorname{rank}(T(E_{i,k} + E_{i,l} + E_{j,k} + E_{j,l})) = 2$. Однако $(E_{i,k} + E_{i,l} + E_{j,k}, E_{j,l}) \in \mathcal{F}_{2R}$, тогда как $(T(E_{i,k}+E_{i,l}+E_{j,k}), T(E_{j,l})) \notin \mathcal{F}_{2R}$, противоречие. Следовательно, $\operatorname{rank}(B) = 1$. Лемма 2.17 завершает доказательство. □

6. LP-проблема для $\mathcal{F}_3$

Напомним, что

$$\mathcal{F}_3(\mathcal{S}) = \{(X, Y) \in \mathcal{M}_n(\mathcal{S})^2 \mid \operatorname{rank}(XY) = \min\{\operatorname{rank}(X), \operatorname{rank}(Y)\}\}.$$

Теорема 6.1. *Пусть $\mathcal{S}$ — антинегативное полукольцо без делителей нуля, $T : \mathcal{M}_n(\mathcal{S}) \to \mathcal{M}_n(\mathcal{S})$ — сюръективный линейный оператор, сохраняющий $\mathcal{F}_3$. Тогда существует перестановочная матрица P такая, что $T(X) = P(X \circ B)P^t$ для всех $X \in \mathcal{M}_n(\mathcal{S})$, где все коэффициенты $B \in \mathcal{M}_n(\mathcal{Z}(\mathcal{S}))$ являются обратимыми и* $\operatorname{rank}(B) = 1$.

Доказательство. Согласно теореме 2.14 имеем $T(E_{i,j}) = b_{i,j}E_{\sigma(i,j)}$ для некоторых обратимых скаляров $b_{i,j} \in \mathcal{Z}(\mathcal{S})$ и перестановки σ на $\{(i, j) \mid 1 \leqslant i, j \leqslant n\}$.

Рассмотрим $(E_{i,j}, E_{j,k}) \in \mathcal{F}_3$ для всех k. Тогда

$$\operatorname{rank}(T(E_{i,j})T(E_{j,k})) = \min\{\operatorname{rank}(T(E_{i,j})), \operatorname{rank}(T(E_{j,k}))\} = 1,$$

но $T(E_{i,j})T(E_{j,k}) = b_{i,j}b_{j,k}E_{\sigma(i,j)}E_{\sigma(j,k)}$. Отсюда следует, что $E_{\sigma(j,k)}$ лежит в той же строке, что и $E_{\sigma(j,1)}$ для всех $k = 1, \ldots, n$, т.е. T отображает строки в строки; аналогично T отображает столбцы в столбцы. Из леммы 2.16 следует, что $T(X) = P(X \circ B)Q$ для некоторых перестановок P и Q.

Покажем, что $Q = P^t$. В самом деле, $T(E_{i,j}) = b_{i,j}E_{\sigma(i),\tau(j)}$, где σ — перестановка, соответствующая P, и τ — перестановка, соответствующая Q^t. Однако $(E_{1,i}, E_{i,1}) \in \mathcal{F}_3$; следовательно, $(E_{\sigma(1),\tau(i)}, E_{\sigma(i),\tau(1)}) \in \mathcal{F}_3$, и поэтому $\sigma \equiv \tau$. Таким образом, $Q = P^t$.

Осталось показать, что $\operatorname{rank}(B) = 1$. Предположим, что $\operatorname{rank}(B) \geqslant 2$. Тогда согласно следствию 2.13 существуют индексы i, j, k, l такие, что $\operatorname{rank}(B[i, j|k, l]) = 2$. Пусть $A = E_{1,i} + E_{2,q}$ и $J' = E_{i,k}+E_{i,l}+E_{j,k}+E_{j,l}$, где $q \neq i, j$. Тогда $\operatorname{rank}(AJ') = 1 = \min\{\operatorname{rank}(A), \operatorname{rank}(J')\}$. Следовательно, $(A, J') \in \mathcal{F}_3$. Однако, как следует из условия $J' \circ B = B[i, j|k, l] = 2$ и неизменности факторизационного ранга при умножении на перестановочные матрицы, $\operatorname{rank}(T(J') = \operatorname{rank}(B[i, j|k, l]) = 2$. Кроме того, $\operatorname{rank}(T(A)) = 2$, так как T переводит линии в линии. Однако

$$\operatorname{rank}(T(A)T(J')) = \operatorname{rank}(P(A \circ B)P^tP(J' \circ B)P^t) =$$
$$= \operatorname{rank}(P(b_{1,i}b_{i,k}E_{1,k} + b_{1,i}b_{i,l}E_{1,l})P^t) = 1.$$

Тогда $(T(A), T(J')) \notin \mathcal{F}_3$, противоречие. Следовательно, $\operatorname{rank}(B) = 1$. □

Лемма 6.2. *Пусть $\mathcal{S}$ — антинегативное полукольцо, удовлетворяющее условию $1+1 \neq 1$ в $\mathcal{S}$. Предположим, что отображение $T : \mathcal{M}_n(\mathcal{S}) \to \mathcal{M}_n(\mathcal{S})$ определено формулой $T(X) = DXE$ для всех $X \in \mathcal{M}_n(\mathcal{S})$, где $D, E \in \mathcal{M}_n(\mathcal{S})$ — обратимые диагональные матрицы, $n > 4$. Тогда T сохраняет $\mathcal{F}_3$ в том и только том случае, когда $E = \alpha D^{-1}$ для всех обратимых $\alpha \in \mathcal{S}$.*

Доказательство. Если $E = \alpha D^{-1}$, то, как легко показать, отображение T сохраняет множество $\mathcal{F}_3$. Теперь предположим, что $E \neq \alpha D^{-1}$ для любого обратимого α. Пусть $L(X) = ET(X)E^{-1} = EDX$. Пусть, кроме того, $G = ED$. Матрица G является диагональной, но не скалярной. Обозначим $G = \operatorname{diag}\{g_1, g_2, \ldots, g_n\}$. Предположим, что $g_3 \neq g_4$. Пусть

$$A = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 4 \\ 1 & 1 & 4 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}.$$

Пусть $X = A \oplus O_{n-4}$ и $Y = G^{-1}(B \oplus O_{n-4})$. Тогда

$$XY = \begin{bmatrix} g_2^{-1} & g_2^{-1} & g_3^{-1} + g_4^{-1} & g_3^{-1} + g_4^{-1} \\ g_1^{-1} & g_1^{-1} & g_3^{-1} + g_4^{-1} & g_3^{-1} + g_4^{-1} \\ g_1^{-1} + g_2^{-1} & g_1^{-1} + g_2^{-1} & 4g_4^{-1} & 4g_4^{-1} \\ g_1^{-1} + g_2^{-1} & g_1^{-1} + g_2^{-1} & 4g_3^{-1} & 4g_3^{-1} \end{bmatrix} \oplus O_{n-4}.$$

Тогда $\operatorname{rank}(XY) = 2$ (так как $g_3 \neq g_4$), $\operatorname{rank}(X) = 4$, $\operatorname{rank}(Y) = 2$. Таким образом $(A, B) \in \mathcal{F}_3$. Однако

$$L(X)L(Y) = G\left(\begin{bmatrix} 1 & 1 & 2 & 2 \\ 1 & 1 & 2 & 2 \\ 2 & 2 & 4 & 4 \\ 2 & 2 & 4 & 4 \end{bmatrix} \oplus O_{n-4}\right),$$

откуда $\operatorname{rank}(L(X)L(Y)) = 1$, $\operatorname{rank}(L(X)) = 4$, $\operatorname{rank}(L(Y)) = 2$, т.е. $(L(X), L(Y)) \notin \mathcal{F}_3$. Следовательно, L не сохраняет $\mathcal{F}_3$.

В случае $g_3 = g_4$, но $g_1 \neq g_2$ рассмотрим вместо A матрицу

$$A' = \begin{bmatrix} 0 & 4 & 1 & 1 \\ 4 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix},$$

во всех других случаях $n \geqslant 5$, т.е. можно разбить нулевой блок на две части и рассмотреть $X' = O_r \oplus A \oplus O_{n-r-4}$ или $X' = O_r \oplus A' \oplus O_{n-r-4}$ для подходящего r. Лемма доказана. □

При некоторых дополнительных условиях на $\mathcal{S}$ мы можем в точности охарактеризовать линейные отображения, сохраняющие $\mathcal{F}_3$.

Следствие 6.3. *Пусть $\mathcal{S}$ — коммутативное антинегативное полукольцо без делителей нуля с условием $1+1 \neq 1$. Предположим, что $T : \mathcal{M}_n(\mathcal{S}) \to \mathcal{M}_n(\mathcal{S})$ — сюръективный линейный оператор, $n > 4$. Тогда T сохраняет $\mathcal{F}_3$ в том и только том случае, когда $T(X) = \alpha PDXD^{-1}P^t$ для всех $X \in \mathcal{M}_n(\mathcal{S})$, где $D \in \mathcal{M}_n(\mathcal{S})$ — обратимая диагональная матрица, α обратим в $\mathcal{S}$ и $P \in \mathcal{M}_n(\mathcal{S})$ — перестановочная матрица.*

Доказательство. Легко проверить, что операторы вида $T(X) = \alpha PDXD^{-1}P^t$ сохраняют $\mathcal{F}_3$.

Предположим, что T сохраняет $\mathcal{F}_3$. Тогда, применяя теорему 6.1 и лемму 2.17, получаем, что $T(X) = PDXEP^t$ для обратимых диагональных матриц D и E. Лемма 6.2 завершает доказательство. □

Для цепных полуколец справедливо следующее утверждение.

Теорема 6.4. *Пусть $\mathcal{S}$ — цепное полукольцо и $T : \mathcal{M}_n(\mathcal{S}) \to \mathcal{M}_n(\mathcal{S})$ — линейное отображение. Отображение T строго сохраняет $\mathcal{F}_3$ тогда и только тогда, когда существует перестановочная матрица P такая, что $T(X) = PXP^t$ для всех $X \in \mathcal{M}_n(\mathcal{S})$.*

Доказательство. Все операторы вида $T(X) = PXP^t$, $X \in \mathcal{M}_n(\mathcal{S})$, строго сохраняют $\mathcal{F}_3$.

Предположим, что T строго сохраняет $\mathcal{F}_3$. Пусть существует $(0,1)$-матрица M и пара (r,s) такая, что $m_{r,s} = 0$ и $T(M) \geqslant T(J)$. Обозначим $G = T(M) = (g_{i,j})$. Тогда, как и в доказательстве теоремы 4.3, для $A = J \setminus E_{r,s}$ и $\alpha = \min\{g_{i,j} \mid g_{i,j} \neq 0\}$ получаем, что $T(\alpha A) = T(\alpha J)$. Однако $(\alpha A, \alpha A) \notin \mathcal{F}_3$, так как $\operatorname{rank}(\alpha A) = 2$ и $\operatorname{rank}((\alpha A)^2) = 1$, тогда как $\operatorname{rank}((\alpha J)^2) = \operatorname{rank}(\alpha J)$, а значит, $(\alpha J, \alpha J) \in \mathcal{F}_3$. Получено противоречие, так как $(T(\alpha J), T(\alpha J)) = (T(\alpha A), T(\alpha A))$. Следовательно, для $\beta = \min\{h_{i,j} \mid H = T(J)\}$, как и при доказательстве теоремы 4.3, получаем, что отображение βT сюръективно и согласно теореме 6.3 $\beta T(X) = PXP^t$ для всех $X \in \mathcal{M}_n(\beta\mathcal{S})$. Таким образом, для данной матрицы $B \in \mathcal{M}_{m,n}(\mathcal{S})$ справедливо, что $T(X) = P(X \circ B)P^t$ для всех $X \in \mathcal{M}_n(\mathcal{S})$.

Покажем, что $B = J$. Предположим, что $b_{i,j} < 1$ для некоторой пары (i,j). Пусть $A = J \setminus E_{i,j} + b_{i,j}E_{i,j}$. Тогда $T(A) = T(J)$, однако поскольку $\operatorname{rank}(A) = 2$, $(A, A) \notin \mathcal{F}_3$. Вместе с тем $(T(A), T(A)) = (T(J), T(J)) \in \mathcal{F}_3$, противоречие. Следовательно, $B = J$, и теорема доказана. □

7. LP-проблема для $\mathcal{F}_{4N}$

Напомним, что

$$\mathcal{F}_{4N}(\mathcal{S}) = \{(X,Y) \in \mathcal{M}_n(\mathcal{S})^2 \mid \operatorname{rank}(XY) = 0\}.$$

Теорема 7.1. *Пусть $\mathcal{S}$ — антинегативное полукольцо без делителей нуля и $T : \mathcal{M}_n(\mathcal{S}) \to \mathcal{M}_n(\mathcal{S})$ — невырожденный $(T(X) = O \Longrightarrow X = O)$ аддитивный оператор. Предположим, что $T(J)$ имеет ненулевой коэффициент в каждой строке и столбце. Тогда T сохраняет $\mathcal{F}_{4N}$ в том и только том случае, когда $T(X) = P(X \circ B)P^t$, $X \in \mathcal{M}_n(\mathcal{S})$, и все коэффициенты матрицы B не являются делителями нуля.*

Доказательство. Необходимость проверяется непосредственно.

Так как $T(J)$ имеет ненулевой коэффициент в любой строке и любом столбце, то существуют n различных клеток, образы которых имеют ненулевые коэффициенты в любой строке. Предположим, что эти клетки могут быть выбраны таким образом, что их ненулевые коэффициенты занимают менее чем n столбцов. Пусть $X = E_1 + E_2 + \cdots + E_n$ есть сумма n таких клеток и X не имеет ненулевых коэффициентов в столбце k. Тогда $(X, R_k) \in \mathcal{F}_{4N}$, и, следовательно, $(T(X), T(R_k)) \in \mathcal{F}_{4N}$. Однако $T(X)T(R_k) \neq O$, противоречие.

Следовательно, T переводит столбцы в столбцы и, кроме того, T индуцирует перестановку на множестве столбцов. Аналогично, T индуцирует перестановку на множестве строк, т.е. $T(X) = P(X \circ B)Q$ для всех $X \in \mathcal{M}_n(\mathcal{S})$ и некоторых перестановочных матриц P и Q. Покажем, что $Q = P^t$. В самом деле, имеем $T(E_{i,j}) = b_{i,j}E_{\pi(i),\tau(j)}$. Если $Q \neq P^t$, то $\pi \neq \tau$. Следовательно, для некоторого i имеем $\pi(i) \neq \tau(i)$, а значит, для некоторого $j \neq i$ имеем $\pi(j) = \tau(i)$. Здесь $(E_{i,i}, E_{j,i}) \in \mathcal{F}_{4N}$, но $T(E_{i,i})T(E_{j,i}) = b_{i,i}b_{j,i}E_{\pi(i),\tau(i)}E_{\pi(j),\tau(i)} = b_{i,i}b_{j,i}E_{\pi(i),\tau(i)} \neq O$, противоречие. Следовательно, $\pi = \tau$ и $T(X) = P(X \circ B)P^t$ для всех $X \in \mathcal{M}_n(\mathcal{S})$. Так как отображение T невырождено, то все коэффициенты матрицы B не являются делителями нуля. □

Следствие 7.2. *Пусть $\mathcal{S}$ — антинегативное полукольцо без делителей нуля и $T : \mathcal{M}_n(\mathcal{S}) \to \mathcal{M}_n(\mathcal{S})$ — сюръективный линейный оператор. Тогда T сохраняет $\mathcal{F}_{4N}$ в том и только том случае, когда существуют такие перестановочная матрица P и $b_{i,j} \in \mathcal{Z}(\mathcal{S})$, обратимые для всех i,j, что $T(X) = P(X \circ B)P^t$ для всех $X \in \mathcal{M}_n(\mathcal{S})$.*

Доказательство. Доказывается последовательным применением теорем 2.14 и 7.1, соответственно. □

Следствие 7.3. *Пусть $\mathcal{S}$ — антинегативное полукольцо, $T : \mathcal{M}_n(\mathcal{S}) \to \mathcal{M}_n(\mathcal{S})$ — линейный оператор. Тогда T строго сохраняет $\mathcal{F}_{4N}$ в том и только том случае, когда существуют такие перестановочная матрица P и $b_{i,j} \in \mathcal{Z}(\mathcal{S})$, не являющиеся делителями нуля для всех i,j, что $T(X) = P(X \circ B)P^t$ для всех $X \in \mathcal{M}_n(\mathcal{S})$.*

Доказательство. Легко видеть, что операторы вида $T(X) = P(X \circ B)P^t$, $X \in \mathcal{M}_n(\mathcal{S})$, где $b_{i,j}$ не являются делителями нуля для всех i, j, строго сохраняют $\mathcal{F}_{4N}$. Предположим, что T строго сохраняет $\mathcal{F}_{4N}$.

Покажем, что $T(J)$ имеет ненулевой элемент в любой строке и любом столбце. Предположим, что, напротив, $T(J)$ имеет нулевой столбец (случай нулевой строки полностью аналогичен). Умножая, если это необходимо, на перестановочную матрицу, можно предположить, что все ненулевые элементы находятся в столбцах $1, 2, \ldots, t$ матрицы $T(J)$ и все элементы столбцов $(t+1), \ldots, n$ нулевые. Тогда существуют матрицы-столбцы C_{j_1}, C_{j_2}, $\ldots$, C_{j_s}, образы которых имеют ненулевые элементы в столбцах с 1-го по t-й. Пусть $l \neq j_k$ для всех k, $1 \leqslant k \leqslant s$. Тогда $(C_{j_1}+C_{j_2}+\cdots+C_{j_s})R_l = O$. Так как T сохраняет $\mathcal{F}_{4N}$, получаем, что $T(C_{j_1} + C_{j_2} + \cdots + C_{j_s})T(R_l) = O$. Тогда $T(R_l)$ не имеет ненулевых элементов в строках с 1-й по t-ю, так как в любой из первых t столбцов $T(C_{j_1} + C_{j_2} + \cdots + C_{j_s})$ существует ненулевой элемент. Следовательно, $T(E_{l,l})$ имеет ненулевые элементы только в строках с номерами $t+1, \ldots, n$ и столбцах с номерами $1, \ldots, t$. Отсюда $T(E_{l,l})^2 = O$, т.е. $(T(E_{l,l}), T(E_{l,l})) \in \mathcal{F}_{4N}$, противоречие с тем, что T строго сохраняет $\mathcal{F}_{4N}$ и $(E_{l,l}, E_{l,l}) \notin \mathcal{F}_{4N}$.

Следовательно, матрица $T(J)$ не имеет нулевых строк и столбцов. Проверим, что T — невырожденное отображение. Предположим, что существует $X \neq O$ такой, что $T(X) = O$. Следовательно, $(T(X), T(I)) \in \mathcal{F}_{4N}$, в то время как $(X, I) \notin \mathcal{F}_{4N}$, противоречие с условиями на T. Таким образом, применима теорема 7.1, согласно которой $T(X) = P(X \circ B)P^t$ для всех $X \in \mathcal{M}_n(\mathcal{S})$ для некоторой перестановочной матрицы P и матрицы B, элементы которой не являются делителями нуля. Следствие доказано. □

8. LP-проблема для $\mathcal{F}_{4B}$

Напомним, что

$$\mathcal{F}_{4B}(\mathcal{S}) = \{(X, Y) \in \mathcal{M}_n(\mathcal{S})^2 \mid \operatorname{rank}(XY) = 1\}.$$

Лемма 8.1. *Пусть $\mathcal{S}$ — цепное полукольцо, $T(E_{i,j}) = b_{i,j}E_{\sigma(i,j)}$, где σ — некоторая перестановка на множестве $\{(i, j) \mid 1 \leqslant i, j \leqslant n\}$ и $b_{i,j} \in \mathcal{S}$ — ненулевые элементы. Тогда T сохраняет $\mathcal{F}_{4B}$ в том и только том случае, когда существует матрица перестановки $P \in \mathcal{M}_n(\mathcal{S})$ такая, что $T(X) = PXP^t$ для всех $X \in \mathcal{M}_n(\mathcal{S})$.*

Доказательство. Очевидно, что отображение $T(X) = PXP^t$ сохраняет $\mathcal{F}_{4B}$. Предположим, что T сохраняет $\mathcal{F}_{4B}$. Рассмотрим $(E_{i,i}, E_{i,k}) \in \mathcal{F}_{4B}$ для всех k. Если $T(E_{i,i}) = b_{i,i}E_{r,s}$ для некоторых r, s, то $T(E_{i,k}) = b_{i,k}E_{s,\tau(k)}$, где τ — некоторая перестановка. Отсюда $T(R_i) \leqslant R_s$. Следовательно, T индуцирует перестановку строк. Аналогично, T индуцирует перестановку столбцов. Следовательно, для некоторых перестановок π и τ имеем $T(E_{i,j}) = b_{i,j}E_{\pi(i),\tau(j)}$. Таким образом, $\operatorname{rank}(T(E_{i,i})T(E_{i,j}))$ должен быть равен 1, а значит, $\pi(i) = \tau(i)$, т.е. $\pi = \tau$, откуда получаем, что $T(X) = P(X \circ B)P^t$ для всех $X \in \mathcal{M}_n(\mathcal{S})$, где P — перестановка, соответствующая π.

Если $B \neq J$, то $b_{p,q} < 1$ для некоторых (p, q). Следовательно,

$$(E_{i,i} + E_{i,q} + E_{p,i} + b_{p,q}E_{p,q}, I) \notin \mathcal{F}_{4B},$$

тогда как $(E_{i,i} + E_{i,q} + E_{p,i} + E_{p,q}, I) \in \mathcal{F}_{4B}$. Однако

$$T(E_{i,i} + E_{i,q} + E_{p,i} + b_{p,q}E_{p,q}) = T(E_{i,i} + E_{i,q} + E_{p,i} + E_{p,q}),$$

что противоречит условиям на T. Следовательно, $B = J$, а значит, $T(X) = PXP^t$ для всех $X \in \mathcal{M}_n(\mathcal{S})$. □

Теорема 8.2. *Пусть $\mathcal{S}$ — цепное полукольцо, $T : \mathcal{M}_n(\mathcal{S}) \to \mathcal{M}_n(\mathcal{S})$ — сюръективный линейный оператор. Отображение T сохраняет $\mathcal{F}_{4B}$ тогда и только тогда, когда существует перестановочная матрица $P \in \mathcal{M}_n(\mathcal{S})$ такая, что $T(X) = PXP^t$ для всех $X \in \mathcal{M}_n(\mathcal{S})$.*

Доказательство. Согласно теореме 2.14 получаем, что для всех i, j, $1 \leqslant i, j \leqslant n$, имеет место равенство $T(E_{i,j}) = b_{i,j}E_{\sigma(i,j)}$ для некоторых обратимых скаляров $b_{i,j}$. Лемма 8.1 завершает доказательство. □

Теорема 8.3. *Пусть $\mathcal{S}$ — цепное полукольцо, $T : \mathcal{M}_n(\mathcal{S}) \to \mathcal{M}_n(\mathcal{S})$ — линейное отображение. Тогда T строго сохраняет $\mathcal{F}_{4B}$ в том и только том случае, когда существует перестановочная матрица $P \in \mathcal{M}_n(\mathcal{S})$ такая, что $T(X) = PXP^t$ для всех $X \in \mathcal{M}_n(\mathcal{S})$.*

Доказательство. Поскольку операторы вида $T(X) = PXP^t$ сохраняют $\mathcal{F}_{4B}$, предположим, что T строго сохраняет $\mathcal{F}_{4B}$ и покажем, что T имеет вид $T(X) = PXP^t$. Пусть M — такая $(0,1)$-матрица, что

$$|T(M)| = |T(J)| \quad \text{и, если} \quad |T(N)| = |T(J)|, \quad \text{то} \quad |M| \leqslant |N| \tag{8.1}$$

(т.е. M — минимальная матрица относительно свойства (8.1)). Пусть α — наименьший ненулевой коэффициент матрицы $T(M)$. Тогда $T(\alpha M) = T(\alpha J)$.

Предположим, что существует такой индекс j, что j-й столбец матрицы M является нулевым. Тогда $\alpha M \alpha E_{j,k} = O$, т.е. $(\alpha M, \alpha E_{j,k}) \notin \mathcal{F}_{4B}$. Следовательно,

$$(T(\alpha M), T(\alpha E_{j,k})) = (T(\alpha J), T(\alpha E_{j,k})) \notin \mathcal{F}_{4B}.$$

Поскольку T строго сохраняет $\mathcal{F}_{4B}$, отсюда следует, что $(\alpha J, \alpha E_{j,k}) \notin \mathcal{F}_{4B}$, противоречие. Следовательно, матрица M не содержит нулевых столбцов. Аналогично, матрица M не содержит нулевых строк.

Поскольку $(\alpha J, I) \in \mathcal{F}_{4B}$, имеем $(T(\alpha M), I) \in \mathcal{F}_{4B}$, следовательно, $(\alpha M, I) \in \mathcal{F}_{4B}$. Отсюда следует, что $\operatorname{rank}(M) = 1$. Тогда $\alpha M = \alpha J$. Так как матрица M выбрана в соответствии с условием (8.1), отображение T индуцирует биекцию на множестве клеток, т.е. $T(E_{i,j}) = b_{i,j} E_{\sigma(i,j)}$ для некоторой перестановки σ множества $\{(i,j) \mid 1 \leqslant i,j \leqslant n\}$ и ненулевых $b_{i,j} \in \mathcal{S}$. Применение леммы 8.1 завершает доказательство теоремы. □

9. LP-проблема для $\mathcal{F}_{4R}$

Напомним, что для $\mathcal{S} \subseteq \mathbb{R}_+$

$$\mathcal{F}_{4R}(\mathcal{S}) = \{(X,Y) \in \mathcal{M}_n(\mathcal{S})^2 \mid \operatorname{rank}(XY) = \rho(X) + \rho(Y) - n\}.$$

Лемма 9.1. *Пусть $\mathcal{S} \subseteq \mathbb{R}_+$ — некоторое полукольцо, отображение $T : \mathcal{M}_n(\mathcal{S}) \to \mathcal{M}_n(\mathcal{S})$ определено формулой $T(X) = DXE$ для всех $X \in \mathcal{M}_n(\mathcal{S})$, где $D, E \in \mathcal{M}_n(\mathcal{S})$ — обратимые диагональные матрицы, $n > 4$. Тогда отображение T сохраняет множество $\mathcal{F}_{4R}$ в том и только том случае, когда $E = \alpha D^{-1}$ для некоторого обратимого элемента $\alpha \in \mathcal{S}$.*

Доказательство. Если $E = \alpha D^{-1}$, непосредственная проверка показывает, что T сохраняет $\mathcal{F}_{4R}$. Допустим, что для любого обратимого элемента α справедливо $E \neq \alpha D^{-1}$. Обозначим $L(X) = ET(X)E^{-1} = EDX$ и пусть $G = ED$. Согласно предположению матрица G не является скалярной. Так же, как и в лемме 6.2, без ограничения общности можно предположить, что $G = \operatorname{diag}\{g_1, g_2, \ldots, g_n\}$, где $g_3 \neq g_4$. Рассмотрим матрицы A и B, выбранные в доказательстве леммы 6.2, $X = A \oplus I_{n-4}$ и $Y = B \oplus I_{n-4}$. Тогда

$$XY = \begin{bmatrix} 1 & 1 & 2 & 2 \\ 1 & 1 & 2 & 2 \\ 2 & 2 & 4 & 4 \\ 2 & 2 & 4 & 4 \end{bmatrix} \oplus I_{n-4},$$

т.е. $\rho(L(X)) = \rho(X) = n-1$, $\rho(L(Y)) = \rho(Y) = n-2$, $\operatorname{rank}(XY) = n-3$. Тогда $(X,Y) \in \mathcal{F}_{4R}$. Однако

$$L(X)L(Y) = G \left(\begin{bmatrix} g_2 & g_2 & g_3+g_4 & g_3+g_4 \\ g_1 & g_1 & g_3+g_4 & g_3+g_4 \\ g_1+g_2 & g_1+g_2 & 4g_4 & 4g_4 \\ g_1+g_2 & g_1+g_2 & 4g_3 & 4g_3 \end{bmatrix} \oplus I_{n-4} \right),$$

так что $\operatorname{rank}(L(X)L(Y)) = n-2$, поскольку $g_3 \neq g_4$. Следовательно, $(L(X), L(Y)) \notin \mathcal{F}_{4R}$. Таким образом, отображение L не сохраняет множество $\mathcal{F}_{4R}$. Полученное противоречие завершает доказательство. □

Теорема 9.2. *Пусть $\mathcal{S} \subseteq \mathbb{R}_+$ — некоторое полукольцо, $T : \mathcal{M}_n(\mathcal{S}) \to \mathcal{M}_n(\mathcal{S})$ — сюръективное линейное отображение, $n > 4$. Тогда T сохраняет множество $\mathcal{F}_{4R}$ в том и только том случае, когда существуют такие перестановочная матрица $P \in \mathcal{M}_n(\mathcal{S})$, обратимый элемент $\alpha \in \mathcal{S}$ и обратимая диагональная матрица $D \in \mathcal{M}_n(\mathcal{S})$, что $T(X) = \alpha PDXD^{-1}P^t$ для всех $X \in \mathcal{M}_n(\mathcal{S})$.*

Доказательство. Легко видеть, что операторы вида $T(X) = \alpha PDXD^{-1}P^t$, $X \in \mathcal{M}_n(\mathcal{S})$, где $P \in \mathcal{M}_n(\mathcal{S})$ — некоторая перестановочная матрица, $\alpha \in \mathcal{S}$ — обратимый элемент, $D \in \mathcal{M}_n(\mathcal{S})$ — обратимая диагональная матрица, сохраняют множество $\mathcal{F}_{4R}$. Предположим теперь, что отображение T сохраняет множество $\mathcal{F}_{4R}$, и покажем, что T имеет требуемый вид.

Поскольку T сюръективно, из теоремы 2.14 следует, что $T(E_{i,j}) = b_{i,j}E_{\sigma(i,j)}$ для некоторой перестановки σ и матрицы B с обратимыми коэффициентами. Если $\operatorname{rank}(A) = n$, то $(E_{i,j}, A) \in \mathcal{F}_{4R}$. Так как $\operatorname{rank}(T(E_{i,j})) = 1$ и T сохраняет множество $\mathcal{F}_{4R}$, то отсюда следует, что $\operatorname{rank}(T(A)) = n$. Таким образом, T сохраняет множество матриц ранга n.

Если прообраз строчки не доминируется ни одной линией, то существуют такие клетки $E_{i,k}$ и $E_{i,l}$, что $T(E_{i,k} + E_{i,l}) \leqslant E_{r,s} + E_{p,q}$, причем $p \neq r$, $q \neq s$. Дополним матрицу $E_{r,s} + E_{p,q}$ до перестановочной матрицы, добавив к ней подходящие $n-2$ клетки. Таким образом, мы найдем матрицу, которая является образом перестановочной матрицы, но доминируется $n-1$ линией, противоречие с тем, что T сохраняет матрицы ранга n. Следовательно, прообразом каждой строки является строка или столбец. Аналогично, прообразом каждого столбца является строка или столбец, т.е. T отображает линии в линии. Согласно лемме 2.16 T является (P, Q, B)-оператором. Поскольку $(E_{1,1}, E_{2,1} + E_{3,2} + \cdots + E_{n,n-1}) \in \mathcal{F}_{4R}$, тогда как $(E_{1,1}, E_{1,2} + E_{2,3} + \cdots + E_{n-1,n}) \notin \mathcal{F}_{4R}$, получаем, что транспонирование не сохраняет $\mathcal{F}_{4R}$. Следовательно, существуют такие матрицы перестановки P и Q, что $T(X) = P(X \circ B)Q$ для некоторой матрицы B с обратимыми коэффициентами.

Без ограничения общности можно считать, что $P = I$. Если $Q \neq I$, пусть Q соответствует перестановке π и $\pi(1) \neq 1$. Без ограничения общности, $T(E_{1,1}) = b_{1,1}E_{1,2}$. Тогда $(E_{1,1}, E_{2,2} + E_{3,3} + \cdots + E_{n,n}) \in \mathcal{F}_{4R}$, хотя $(T(E_{1,1}), T(E_{2,2} + E_{3,3} + \cdots + E_{n,n})) \notin \mathcal{F}_{4R}$, поскольку

$$(b_{1,1}E_{1,1}), (b_{2,2}E_{2,\pi(2)} + E_{3,\pi(3)} + \cdots + E_{n,\pi(n)}) = b_{1,1}E_{1,2}b_{2,2}E_{2,\pi(2)} \neq O.$$

Полученное противоречие показывает, что $Q = P^t$ и без ограничения общности можно считать далее, что $T(X) = X \circ B$.

Предположим, что $\operatorname{rank}(B) > 1$. Тогда согласно следствию 2.13 существуют такие индексы i, j, k, l, что $\operatorname{rank}(B[i, j|k, l]) = 2$. Пусть

$$X = b_{i,k}^{-1}E_{i,k} + b_{i,l}^{-1}E_{i,l} + b_{j,k}^{-1}E_{j,k} + b_{j,l}^{-1}E_{j,l} + E_3 + E_4 + \cdots + E_n,$$

где E_3, E_4, …, E_n выбраны таким образом, что $\operatorname{rank}(X) = n$. Однако $\operatorname{rank}(T(X)) \leqslant n - 1$, противоречие с тем, что T сохраняет множество матриц ранга n. Следовательно $\operatorname{rank}(B) = 1$. Поледовательное применение лемм 3.2 и 9.1 завершает доказательство. □

10. LP-проблема для $\mathcal{F}_5$

Напомним, что для $\mathcal{S} \subseteq \mathbb{R}_+$

$$\mathcal{F}_5(\mathcal{S}) = \{(X, Y, Z) \in \mathcal{M}_n(\mathcal{S})^3 \mid \operatorname{rank}(XYZ) + \operatorname{rank}(Y) = \rho(XY) + \rho(YZ)\}.$$

Лемма 10.1. *Пусть $\mathcal{S} \subseteq \mathbb{R}_+$ — полукольцо и линейное биективное отображение $T : \mathcal{M}_n(\mathcal{S}) \to \mathcal{M}_n(\mathcal{S})$ сохраняет множество $\mathcal{F}_5$. Тогда существуют такие перестановочная матрица $P \in \mathcal{M}_n(\mathcal{S})$ и матрица $B \in \mathcal{M}_n(\mathcal{Z}(\mathcal{S}))$ с обратимыми коэффициентами, что $T(X) = P(X \circ B)P^t$ для всех $X \in \mathcal{M}_n(\mathcal{S})$.*

Доказательство. Согласно теореме 2.14 $T(E_{i,j}) = b_{i,j}E_{\sigma(i,j)}$ для некоторой перестановки σ на множестве $\{(i, j) \mid 1 \leqslant i, j \leqslant n\}$ и обратимых элементов $b_{i,j} \in \mathcal{S}$.

Легко видеть, что $(E_{i,j}, E_{j,k}, E_{k,l}) \in \mathcal{F}_5$ для всех l и произвольных фиксированных i, j, k. Тогда

$$\begin{gathered}\rho(T(E_{i,j})T(E_{j,k})) + \rho(T(E_{j,k})T(E_{k,l})) = \\ = \operatorname{rank}(T(E_{i,j})T(E_{j,k})T(E_{k,l})) + \operatorname{rank} T(E_{j,k}).\end{gathered} \tag{10.1}$$

Согласно теореме 2.14 отсюда следует, что $T(E_{i,j}) = b_{i,j}E_{p,q}$, $T(E_{j,k}) = b_{j,k}E_{r,s}$, $T(E_{k,l}) = b_{k,l}E_{u,v}$ для некоторых скаляров $b_{i,j}, b_{j,k}, b_{k,l}$ и индексов p, q, r, s, u, v.

Так как $\operatorname{rank}(b_{j,k}E_{r,s}) = 1 \neq 0$, из равенства (10.1) следует, что или $r = q$, или $s = u$, или верно и то, и другое.

Если для всех $l = 1, \ldots, n$ справедливы оба равенства, то для фиксированных i, j, k ненулевые элементы всех матриц $T(E_{k,l})$, $l = 1, \ldots, n$, лежат в одной строке. Следовательно, T отображает строки в строки. Аналогично, легко видеть, что T отображает столбцы в столбцы.

Допустим теперь, что существует такой индекс l, что для тройки $(E_{i,j}, E_{j,k}, E_{k,l})$ выполняется только одно из написанных равенств. Без потери общности можно предположить, что $s = u$ и $r \neq q$. Тогда для произвольного m, $1 \leqslant m \leqslant n$, справедливо $(E_{i,j}, E_{j,k}, E_{k,m}) \in \mathcal{F}_5$. Согласно теореме 2.14 $T(E_{k,m}) = b_{k,m}E_{w,z}$ для подходящих w, z, зависящих от k, m. Во введенных обозначениях имеем $(E_{p,q}, E_{r,s}, E_{w,z}) \in \mathcal{F}_5$. Поскольку $r \neq q$, отсюда следует, что $w = s$ для всех w. Следовательно, в этом случае мы также получили, что строки переходят в строки. Аналогичные рассуждения, проводимые с первой матрицей, показывают, что столбцы переходят в столбцы. Легко видеть, что в случае $s \neq u$ и $r = q$ также строки переходят в строки и столбцы в столбцы.

Согласно лемме 2.16 отсюда следует, что существуют такие перестановочные матрицы P и Q, что $T(X) = P(X \circ B)Q$ для всех $X \in \mathcal{M}_n(\mathcal{S})$, причем все коэффициенты матрицы B обратимы.

Чтобы показать, что $Q = P^t$, достаточно заметить, что $(E_{i,j}, E_{j,j}, E_{j,i}) \in \mathcal{F}_5$. Следовательно, $(E_{\sigma(i),\tau(j)}, E_{\sigma(j),\tau(j)}, E_{\sigma(j),\tau(i)}) \in \mathcal{F}_5$, откуда $\sigma \equiv \tau$. □

Лемма 10.2. *Пусть $\mathcal{S} \subseteq \mathbb{R}_+$ — полукольцо, отображение $T : \mathcal{M}_n(\mathcal{S}) \to \mathcal{M}_n(\mathcal{S})$ определяется формулой $T(X) = DXE$ для всех $X \in \mathcal{M}_n(\mathcal{S})$, где $D, E \in \mathcal{M}_n(\mathcal{S})$ — обратимые диагональные матрицы, $n > 4$. Тогда T сохраняет $\mathcal{F}_5$ в том и только том случае, когда $E = \alpha D^{-1}$ для некоторого обратимого элемента $\alpha \in \mathcal{S}$.*

Доказательство. Если $E = \alpha D^{-1}$, легко видеть, что T сохраняет $\mathcal{F}_5$. Допустим, что $E \neq \alpha D^{-1}$ ни для какого обратимого элемента $\alpha \in \mathcal{S}$. Пусть $L(X) = ET(X)E^{-1} = EDX$, $G = ED$. Согласно предположению G не является скалярной матрицей. Так же, как и в лемме 6.2, без ограничения общности можно предполагать, что $G = \operatorname{diag}\{g_1, g_2, \ldots, g_n\}$ и $g_3 \neq g_4$. Рассмотрим матрицы A и B, выбранные в доказательстве леммы 6.2, $X = A \oplus O_{n-4}$, $Y = I_4 \oplus O_{n-4}$, $Z = B \oplus O_{n-4}$. Тогда

$$XYZ = \begin{bmatrix} 1 & 1 & 2 & 2 \\ 1 & 1 & 2 & 2 \\ 2 & 2 & 4 & 4 \\ 2 & 2 & 4 & 4 \end{bmatrix} \oplus O_{n-4},$$

т.е. $\rho(L(X)L(Y)) = \rho(XY) = 3$, $\rho(L(Y)L(Z)) = \rho(YZ) = 2$, $\operatorname{rank}(L(Y)) = \operatorname{rank}(Y) = 4$, $\operatorname{rank}(XYZ) = 1$. Тогда $(X, Y, Z) \in \mathcal{F}_5$. Однако

$$L(X)L(Y)L(Z) = G\left(\begin{bmatrix} g_2^2 & g_2^2 & g_3^2+g_4^2 & g_3^2+g_4^2 \\ g_1^2 & g_1^2 & g_3^2+g_4^2 & g_3^2+g_4^2 \\ g_1^2+g_2^2 & g_1^2+g_2^2 & 4g_4^2 & 4g_4^2 \\ g_1^2+g_2^2 & g_1^2+g_2^2 & 4g_3^2 & 4g_3^2 \end{bmatrix} \oplus O_{n-4}\right),$$

т.е. $\operatorname{rank}(L(X)L(Y)L(Z)) = 2$, поскольку $g_3 \neq g_4$. Тогда $(L(X), L(Y), L(Z)) \notin \mathcal{F}_5$. Таким образом, L не сохраняет $\mathcal{F}_5$. Лемма доказана. □

Теорема 10.3. *Пусть $\mathcal{S} \subseteq \mathbb{R}_+$ — полукольцо, $T : \mathcal{M}_n(\mathcal{S}) \to \mathcal{M}_n(\mathcal{S})$ — сюръективное линейное отображение, $n > 4$. Тогда T сохраняет $\mathcal{F}_5$ в том и только том случае, когда $T(X) = \alpha PDXD^{-1}P^t$ для всех $X \in \mathcal{M}_n(\mathcal{S})$, где $D \in \mathcal{M}_n(\mathcal{S})$ — обратимая диагональная матрица, $\alpha \in \mathcal{S}$ — обратимый элемент, $P \in \mathcal{M}_n(\mathcal{S})$ — перестановочная матрица.*

Доказательство. Непосредственной проверкой легко убедиться, что отображения вида $T(X) = \alpha PDXD^{-1}P^t$ сохраняют множество $\mathcal{F}_5$.

Допустим, что T сохраняет $\mathcal{F}_5$. Тогда согласно лемме 10.1 $T(X) = P(X \circ B)P^t$, где все коэффициенты матрицы B обратимы.

Проверим, что $\operatorname{rank}(B) = 1$. Допустим, что $\operatorname{rank}(B) \geqslant 2$. Тогда согласно следствию 2.13 существуют такие индексы i, j, k, l, что $\operatorname{rank}(B[i,j|k,l]) = 2$. Пусть $X = 0$, $Y = E_{i,k} + E_{i,l} + E_{j,k} + E_{j,l}$, $Z = E_{k,1}$. Тогда

$$\rho(XY) + \rho(YZ) = 0 + 1 = \operatorname{rank}(XYZ) + \operatorname{rank}(Y),$$

т.е. $(X, Y, Z) \in \mathcal{F}_5$. С другой стороны, $\operatorname{rank}(Y \circ B) = 2$, так как $\operatorname{rank}(B[i,j|k,l]) = 2$ и $\rho(Y \circ B \cdot Z \circ B) = 1$, поскольку Z — клетка. Следовательно, $(T(X), T(Y), T(Z)) \notin \mathcal{F}_5$, противоречие. Последовательное применение лемм 3.2 и 10.2 завершает доказательство теоремы. □

СПИСОК ЛИТЕРАТУРЫ

1. *Beasley L. B.* Linear operators which preserve pairs on which the rank is additive// J. Korean SIAM. — 1998. — *2*. — С. 27–30.
2. *Beasley L. B., Guterman A. E.* Rank inequalities over semirings/ Preprint.
3. *Beasley L. B., Guterman A. E., Neal C. L.* Linear preservers for Sylvester and Frobenius bounds on matrix rank// Rocky Mount. J. Math. (в печати).
4. *Beasley L. B., Lee S.-G., Song S.-Z.* Linear operators that preserve pairs of matrices which satisfy extreme rank properties// Linear Algebra Appl. — 2002. — *350*. — С. 263–272.
5. *Beasley L. B., Lee S.-G., Song S.-Z.* Linear operators that preserve zero-term rank of Boolean matrices// J. Korean Math. Soc. — 1999. — *36*, № 6. — С. 1181–1190.
6. *Beasley L. B., Pullman N. J.* Operators that preserve semiring matrix functions// Linear Algebra Appl. — 1988. — *99*. — С. 199–216.
7. *Beasley L. B., Pullman N. J.* Semiring rank versus column rank// Linear Algebra Appl. — 1988. — *101*. — С. 33–48.
8. *Glazek K.* A Guide to the Literature on Semirings and their Applications in Mathematics and Information Sciences. — Kluwer Academic, 2002.
9. *Gregory D. A., Pullman N. J.* Semiring rank: Boolean rank and nonnegative rank factorization// J. Combin. Inform. System Sci. — 1983. — *8*. — С. 223–233.
10. *Guterman A. E.* Linear preservers for matrix inequalities and partial orderings// Linear Algebra Appl. — 2001. — *331*. — С. 75–87.
11. *Huang S.-G., Song S.-Z.* Spanning column ranks and there preservers of nonnegative matrices// Linear Algebra Appl. — 1997. — *254*. — С. 485–495.
12. *Kim K. H.* Boolean Matrix Theory and Applications/ Pure Appl. Math. — New York: Marcel Dekker, 1982. — *70*.
13. *Marsaglia G., Styan P.* When does $\operatorname{rk}(A+B) = \operatorname{rk}(A) + \operatorname{rk}(B)$?// Can. Math. Bull. — 1972. — *15*, № 3. — С. 451–452.
14. *Marsaglia G., Styan P.* Equalities and inequalities for ranks of matrices// Linear Multilin. Algebra. — 1974. — *2*. — С. 269–292.
15. *Pierce P. et al.* A survey of linear preserver problems// Linear Multilin. Algebra. — 1992. — *33*. — С. 1–119.
16. *Tian Y.* Rank equalities related to outer inverses of matrices and applications// Linear Multilin. Algebra. — 2002. — *49*. — С. 269–288.
17. *Tian Y.* Upper and lower bounds for ranks of matrix expressions using generalized inverses// Linear Algebra Appl. — 2002. — *355*. — С. 187–214.
18. *Watts V. L.* Boolean rank of Kronecker products// Linear Algebra Appl. — 2001. — *336*. — С. 261–264.

L. B. Beasley
Department of Mathematics and Statistics,
Utah State University
E-mail: lbeasley@math.usu.edu

А. Э. Гутерман
Московский государственный университет им. М. В. Ломоносова,
механико-математический факультет
E-mail: guterman@mmascience.ru

Современная математика и ее приложения. Том 13 (2004). С. 71–78

УДК 512.55

О НЕКОТОРЫХ ЛИ-ДОПУСТИМЫХ ПОДАЛГЕБРАХ МАТРИЧНЫХ АЛГЕБР

© 2004 г. **К. И. БЕЙДАР, М. А. ЧЕБОТАРЬ, Ю. ФОНГ, В.-Ф. КЕ**

Аннотация. Пусть $M_n(F)$ — алгебра матриц над полем F и A — подалгебра Ли алгебры $M_n(F)$. Пусть $*$ — операция, определенная на алгебре A, такая, что $(x*x)*x = x*(x*x)$ для всех $x \in A$ и $x*y-y*x = xy-yx$ для всех $x, y \in A$, где xy — обычное умножение алгебры $M_n(F)$. Используя теорию функциональных тождеств, мы дадим описание операции $*$ в случае, когда A является алгеброй матриц, нецентральным лиевым идеалом, односторонним идеалом, алгеброй Ли кососимметрических элементов или алгеброй верхнетреугольных матриц.

С тех пор как в 1948 г. А. Альберт инициировал изучение ли-допустимых алгебр [1], эта область стала популярна как среди математиков, так и среди физиков. С детальной историей вопроса, многими интересными результатами и их приложениями к физике читатель может ознакомиться в книгах С. Окубо [17] и Х. Мыюнга [15].

Для любой (не обязательно ассоциативной) алгебры $A = (A, +, *)$ над полем F определим антикоммутативную алгебру $A^- = (A, +, [\![\,,]\!])$ как векторное пространство A с умножением $[\![x, y]\!] = x*y - y*x$. Алгебра A называется *ли-допустимой*, если A^- является алгеброй Ли; A называется *гибкой*, если $(x*y)*x = x*(y*x)$ для всех $x, y \in A$.

В обычной (ассоциативной) квантовой механике эволюция оператора x во времени задается уравнением Гейзенберга с гамильтонианом H:

$$\frac{d}{dt}x = i(Hx - xH).$$

Каким свойством должна обладать неассоциативная алгебра, чтобы быть совместимой с этим уравнением? Оказалось, что все такие алгебры в точности являются гибкими ли-допустимыми алгебрами [17, Sec. 7.2].

Классификация гибких ли-допустимых алгебр A таких, что A^- — полупростая алгебра Ли, в течение длительного времени оставалась открытым вопросом, поставленным А. Альбертом [1].

Частичное решение проблемы Альберта было получено в 1962 г. Ф. Лауфером и М. Томбером [13]. Они классифицировали конечномерные гибкие ли-допустимые алгебры A, в которых операция взятия степени ассоциативна, над алгебраически замкнутыми полями характеристики 0. Х. Мыюнг [14, 15] получил описание конечномерных гибких ли-допустимых алгебр A над алгебраически замкнутыми полями положительной характеристики таких, что операция возведения в степень ассоциативна и A^- — это либо классические алгебры Ли, либо обобщенные алгебры Витта.

В 1981 г. Г. Бенкарт и Дж. Осборн [8] и С. Окубо и Х. Мыюнг [18] независимо получили классификацию конечномерных гибких ли-допустимых алгебр A над алгебраически замкнутым полем нулевой характеристики таких, что алгебры Ли A^- полупросты, решив тем самым проблему Альберта.

Напомним, что алгебра $(A, +, *)$ называется

(i) *ассоциативной относительно возведения в степень*, если любая подалгебра алгебры A, порожденная одним элементом, является ассоциативной;

(ii) *ассоциативной относительно возведения в третью степень*, если $(x*x)*x = x*(x*x)$ для всех $x \in A$;

(iii) *ассоциативной относительно возведения в четвертую степень*, если

$$((x*x)*x)*x = (x*(x*x))*x = (x*x)*(x*x) = x*((x*x)*x) = x*(x*(x*x))$$

для всех $x \in A$.

ISSN 1512–1712

Понятно, что гибкая алгебра является ассоциативной относительно возведения в третью степень, и известно (см., например, [1] или [15, Lemma 1.11]), что алгебра A над полем характеристики 0 является ассоциативной относительно возведения в степень тогда и только тогда, когда она ассоциативна относительно возведения в третью степень и четвертую степень.

В [9] описаны все умножения $*$ алгебры матриц, являющиеся ассоциативными относительно возведения в степень. В [7] классифицированы такие ли-допустимые алгебры A, что операция возведения в третью степень ассоциативна и алгебры A^- полупросты. В [16] описаны ли-допустимые алгебры A, для которых операция возведения в третью степень ассоциативна и алгебры A^- являются алгебрами Вирасоро. В [12] классифицированы ли-допустимые алгебры A, для которых операция возведения в третью степень ассоциативна и алгебры A^- являются алгебрами Каца—Муди.

Работая с такими ли-допустимыми алгебрами A, что A^- — подалгебры Ли некоторых ассоциативных алгебр, приходится иметь дело с несколькими умножениями, включая обычное (ассоциативное) умножение. Например, ли-допустимые умножения $*$ на алгебре A $(n \times n)$-матриц над полем F — это умножения, удовлетворяющие тождеству $x*y-y*x = xy-yx$ для всех $x, y \in A$, где xy обозначает ассоциативное умножение алгебры A; естественно попытаться описать $*$ в терминах ассоциативного умножения, что и было сделано в [9].

Пусть $(W, +, \cdot)$ — ассоциативная F-алгебра и A — подалгебра Ли алгебры W^-. Умножение $*$, определенное на A, называется *ли-совместимым*, если $(A, +, *)$ является F-алгеброй и существует ненулевой элемент $c \in F$ такой, что

$$[\![x, y]\!] = x * y - y * x = c[x, y] = cxy - cyx \quad \text{для всех } x, y \in A.$$

В 2000 г. К. И. Бейдар и М. А. Чеботарь [6] описали ли-совместимые умножения, ассоциативные относительно взятия третьей степени, на нецентральных лиевых идеалах первичных алгебр и на алгебрах Ли кососимметрических элементов в случае первичных алгебр с инволюцией. Заметим, что в [7, 9] была использована техника, свойственная для работы с матричными алгебрами и алгебрами Ли, а в [6] применялась техника функциональных тождеств.

Для знакомства с теорией функциональных тождеств читатель может обратиться к обзору [11]. С другой стороны, мы постараемся изложить все необходимые понятия и результаты.

Пусть W — ассоциативная алгебра с 1 над полем F и A — подалгебра Ли алгебры W^-. Будем говорить, что A удовлетворяет *условию* $\mathbf{C}$, если все отображения $B : A^2 \to A$ такие, что $[B(x, x), x] = 0$ для всех $x \in A$, могут быть представлены в виде

$$B(x, y) = \lambda_1 xy + \lambda_2 yx + \mu_1(x)y + \mu_2(y)x + \nu(x, y) \tag{1}$$

для некоторых элементов $\lambda_i \in F$, $i = 1, 2$, линейных отображений $\mu_i : A \to F$, $i = 1, 2$, и билинейного отображения $\nu : A^2 \to F$.

Нам потребуется определение квазиполиномов на алгебре A, которое дадим индуктивно. Под квазиполиномом степени 0 на A мы будем понимать произвольную константу $c \in F$. Если определены квазиполиномы степени $\leqslant n$, то квазиполином степени $\leqslant n+1$ — это функция вида

$$q(x_1, \ldots, x_{n+1}) = \sum_{i=1}^{n+1} q_i(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{n+1})x_i + \omega(x_1, \ldots, x_{n+1}),$$

где $q_1, q_2, \ldots, q_{n+1}$ — квазиполиномы степени $\leqslant n$ и $\omega : A^{n+1} \to F$ — полилинейная функция. В частности, квазиполином степени $\leqslant 1$ — это функция вида $q(x) = \lambda x + \mu(x)$, где $\lambda \in F$ и $\mu : A \to F$ — линейная функция. Далее, квазиполином степени $\leqslant 2$ — это в точности выражение, стоящее справа от знака равенства в (1). Константы λ_1, λ_2 и функции μ_1, μ_2, ν называются коэффициентами квазиполинома $B(x, y)$. Коэффициент ν называется свободным членом $B(x, y)$. Коэффициенты квазиполиномов произвольных степеней определяются аналогично.

Будем говорить, что алгебра A удовлетворяют *условию* $\mathbf{Q}_n$, если все квазиполиномные тождества степени $\leqslant n$ на A тривиальны, другими словами, если $q(u_1, \ldots, u_m)$ — квазиполином степени $\leqslant n$ и

$$q(u_1, \ldots, u_m) = 0 \quad \text{для всех } u_1, \ldots, u_m \in A,$$

то все коэффициенты q равны 0.

Условиям $\mathbf{C}$ и $\mathbf{Q}_n$ удовлетворяет довольно широкий класс алгебр. Мы ограничимся только примерами матричных подалгебр.

Примеры. (1) Алгебра $M_k(F)$ $(k \times k)$-матриц над полем F удовлетворяет условию $\mathbf{C}$, если $k \geqslant 3$, и удовлетворяет условию $\mathbf{Q}_n$, если $k \geqslant n+1$. Это следствия теорем 1.1 и 2.3 и условия (v) из [5, с. 3955] (см. также [10] и пример в [5, с. 3963]).

(2) Пусть L — нецентральный лиев идеал алгебры $M_k(F)$. Тогда L удовлетворяет условию $\mathbf{C}$, если $k \geqslant 4$, и удовлетворяет условию $\mathbf{Q}_n$, если $k \geqslant n+2$. Это следствия теорем 1.1 и 2.3 и условия (vi) из [5, с. 3955].

(3) Пусть A — собственный левый идеал алгебры $M_k(F)$. Тогда A удовлетворяет условию $\mathbf{C}$, если $k \geqslant 2$ и $\dim_F(A) \geqslant 3k$ (см. [3, Corollary 1.3]), и удовлетворяет условию $\mathbf{Q}_n$, если $\dim_F(A) \geqslant k(n+1)$ (см. [3, Corollary 2.6]).

(4) Алгебра Ли кососимметрических элементов $M_k(F)$ удовлетворяет условию $\mathbf{C}$, если $k \geqslant 10$, и удовлетворяет условию $\mathbf{Q}_n$, если $k \geqslant 2n+6$. Это следствия теорем 1.1 и 2.3 и условия (vii) из [5, с. 3955].

(5) Подалгебра верхнетреугольных матриц алгебры $M_k(F)$ удовлетворяет условию $\mathbf{C}$, если F содержит более трех элементов (см. [2, Theorem 1.1]), и удовлетворяет условию $\mathbf{Q}_n$, если $n < k$ (см. [2, Theorem 2.3]).

Сформулируем теорему, которая дает описание умножений, ассоциативных относительно взятия третьей степени, для алгебр, удовлетворяющих условиям $\mathbf{C}$ и $\mathbf{Q}_2$. Ввиду вышесказанного это даст общий подход к решению задачи для широкого класса алгебр.

Теорема 1. *Пусть F — поле характеристики, отличной от 2, W — ассоциативная F-алгебра с единицей и A — подалгебра Ли алгебры W^-. Пусть $* : A^2 \to A$ — ли-совместимое умножение. Предположим, что A удовлетворяет условиям $\mathbf{C}$ и $\mathbf{Q}_2$. Умножение $*$ ассоциативно относительно взятия третьей степени тогда и только тогда, когда существуют ненулевой элемент $t \in F$, элемент $\lambda \in F$, симметрическое F-линейное отображение $\mu : A \to F$ и симметрическое F-билинейное отображение $\tau : A^2 \to F$ такие, что*

$$x * y = \frac{1}{2}\{t[x,y] + \lambda x \circ y + \mu(x)y + \mu(y)x + \tau(x,y)\} \tag{2}$$

для всех $x, y \in A$. Здесь $x \circ y$ означает $xy + yx$. Кроме того, справедливы следующие утверждения.

(a) *Алгебра $(A, +, *)$ является гибкой тогда и только тогда, когда выполнено условие* (2) *и*

$$\mu([x,y]) = 0 = \tau(x,[x,y]) \quad \text{для всех } x, y \in A. \tag{3}$$

(b) *Предположим, что $F \subseteq A$ и A удовлетворяет условию $\mathbf{Q}_4$ и условию* (2) *с $\lambda \neq 0$.*

(b1) *Если умножение $*$ ассоциативно относительно взятия четвертой степени, то для всех $x, y \in A$ справедливо равенство*

$$\lambda\mu(x \circ y) + \mu(x)\mu(y) + \tau(x,y)\{2\lambda + \mu(1)\} = 0. \tag{4}$$

(b2) *Если $2\lambda + \mu(1) \neq 0$, то умножение $*$ ассоциативно относительно взятия четвертой степени тогда и только тогда, когда выполнено условие* (4).

(c) *Предположим, что A — (ассоциативная) подалгебра алгебры W и $A \cap F = \{0\}$. Если A удовлетворяет условию $\mathbf{Q}_4$ и условию* (2) *с $\lambda \neq 0$, то*

(c1) *$\tau(x,y) = 0$ для всех $x, y \in A$;*

(c2) *умножение $*$ ассоциативно относительно взятия четвертой степени тогда и только тогда, когда*

$$\lambda\mu(x \circ y) + \mu(x)\mu(y) = 0 \quad \text{для всех } x, y \in A. \tag{5}$$

Случай $\lambda = 0$ в теореме 1(b) был рассмотрен в [15, Theorem 2.14] для произвольного векторного пространства B над полем F характеристики $\neq 2, 3$ при условии, что $\dim_F(B) > 1$.

Отметим, что теорема 1 обобщает некоторые результаты работ [6, 7, 9], и мы получаем классификацию умножений, ассоциативных относительно взятия третьей степени, для всех важных подалгебр Ли матричных алгебр.

Доказательство теоремы 1. Определим отображение $B : A^2 \to A$ правилом $B(x, y) = x * y$ для всех $x, y \in A$. Очевидно, отображение B билинейно. Так как умножение $*$ ли-совместимо, имеем $x * y - y * x = c[x, y]$ для некоторого ненулевого элемента $c \in F$, т.е.

$$B(x, y) - B(y, x) = [\![x, y]\!] = c[x, y] \quad \text{для всех } x, y \in A. \tag{6}$$

Кроме того,

$$(x * x) * x - x * (x * x) = [\![B(x, x), x]\!] = c[B(x, x), x] \quad \text{для всех } x \in A. \tag{7}$$

Предположим, что умножение $*$ ассоциативно относительно взятия третьей степени, т.е. $(x * x) * x = x * (x * x)$ для всех $x \in A$. Из (7) имеем $[B(x, x), x] = 0$ для всех $x \in A$. Так как A удовлетворяет условию $\mathbf{C}$, то существуют $\lambda_i \in F$, $i = 1, 2$, линейные отображения $\mu_i : A \to F$, $i = 1, 2$, и билинейное отображение $\nu : A^2 \to F$ такие, что

$$B(x, y) = \lambda_1 xy + \lambda_2 yx + \mu_1(x)y + \mu_2(y)x + \nu(x, y) \quad \text{для всех } x, y \in A. \tag{8}$$

Из (6) и (8) получаем

$$\begin{aligned} 0 = B(x, y) - B(y, x) - c[x, y] = \\ = (\lambda_1 - \lambda_2 - c)(xy - yx) + (\mu_1(x) - \mu_2(x))y + (\mu_2(y) - \mu_1(y))x + \nu(x, y) - \nu(y, x) \end{aligned}$$

для всех $x, y \in A$. Таким образом, A удовлетворяет квазиполиномному тождеству степени 2. Согласно условию $\mathbf{Q}_2$ получаем $\lambda_1 - \lambda_2 = c \neq 0$, $\mu_1(x) = \mu_2(x)$ для всех $x \in A$ и $\nu(x, y) = \nu(y, x)$ для всех $x, y \in A$. Положив $t = (\lambda_1 - \lambda_2)$, $\lambda = (\lambda_1 + \lambda_2)$, $\mu(x) = 2\mu_1(x)$ и $\tau(x, y) = 2\nu(x, y)$, убеждаемся в справедливости условия (2).

Обратно, предположим, что выполнено условие (2). Тогда $x * x = \lambda x^2 + \mu(x)x + \frac{1}{2}\tau(x, x)$. Следовательно,

$$(x * x) * x - x * (x * x) = t[x * x, x] = 0,$$

так что умножение $*$ ассоциативно относительно взятия третьей степени.

(a) Заметим, что (2) влечет

$$\begin{aligned} (x * y) * x = \frac{1}{2}\Big\{ t\Big[\frac{1}{2}\{t[x, y] + \lambda x \circ y + \mu(x)y + \mu(y)x + \tau(x, y)\}, x\Big] + \\ + \frac{1}{2}\lambda\{t[x, y] + \lambda x \circ y + \mu(x)y + \mu(y)x + \tau(x, y)\} \circ x + \\ + \mu\Big(\frac{1}{2}\{t[x, y] + \lambda x \circ y + \mu(x)y + \mu(y)x + \tau(x, y)\}\Big)x + \\ + \frac{1}{2}\mu(x)\{t[x, y] + \lambda x \circ y + \mu(x)y + \mu(y)x + \tau(x, y)\} + \\ + \tau\Big(\frac{1}{2}\{t[x, y] + \lambda x \circ y + \mu(x)y + \mu(y)x + \tau(x, y)\}, x\Big)\Big\} \end{aligned}$$

и

$$\begin{aligned} x * (y * x) = \frac{1}{2}\Big\{ t\Big[x, \frac{1}{2}\{t[y, x] + \lambda y \circ x + \mu(y)x + \mu(x)y + \tau(y, x)\}\Big] + \\ + \frac{1}{2}\lambda x \circ \{t[y, x] + \lambda y \circ x + \mu(y)x + \mu(x)y + \tau(y, x)\} + \\ + \frac{1}{2}\mu(x)\{t[y, x] + \lambda y \circ x + \mu(y)x + \mu(x)y + \tau(y, x)\} + \\ + \mu\Big(\frac{1}{2}\{t[y, x] + \lambda y \circ x + \mu(y)x + \mu(x)y + \tau(y, x)\}\Big)x + \\ + \tau\Big(x, \frac{1}{2}\{t[y, x] + \lambda y \circ x + \mu(y)x + \mu(x)y + \tau(y, x)\}\Big)\Big\}. \end{aligned}$$

Отсюда получаем, что

$$(x*y)*x - x*(y*x) = \frac{1}{2}t\Big(\mu([x,y])x + \tau([x,y],x)\Big) \quad \text{для всех } x,y \in A. \tag{9}$$

Таким образом, если выполнены условия (2) и (3), то алгебра $(A,+,*)$ является гибкой.

Обратно, предположим, что $(A,+,*)$ — гибкая алгебра, т.е. $(x*y)*x = x*(y*x)$ для всех $x,y \in A$. В частности, умножение $*$ является ассоциативным относительно взятия третьей степени и выполнено условие (2). Следовательно, справедливо равенство (9), и мы имеем

$$\frac{1}{2}t\Big(\mu([x,y])x + \tau([x,y],x)\Big) = (x*y)*x - x*(y*x) = 0 \quad \text{для всех } x,y \in A. \tag{10}$$

Линеаризовав (10), получаем

$$\frac{1}{2}t\Big(\mu([x+z,y])(x+z) + \tau([(x+z),y],x+z)\Big) = \\ = \frac{1}{2}t\Big(\mu([x,y])z + \tau([x,y],z) + \mu([z,y])x + \tau([z,y],x)\Big) = 0$$

для всех $x,y,z \in A$. Фиксировав y, видим, что A удовлетворяет квазиполиномному тождеству степени 2. Заметим, что коэффициент при z равен $\frac{1}{2}t\mu([x,y])$ и свободный член равен $\frac{1}{2}t(\tau([x,y],z) + \tau([z,y],x))$. Так как A удовлетворяет условию $\mathbf{Q}_2$, то эти коэффициенты должны быть равны 0, откуда $\mu([x,y]) = 0$ и $\tau(x,[x,y]) = 0$ для всех $x,y \in A$, т.е. справедливо условие (3). Таким образом, утверждение (a) доказано.

(b) Пусть $1 \in A$, A удовлетворяет условию $\mathbf{Q}_4$, выполнено условие (2) и $\lambda \neq 0$. В частности,

$$x*x = \lambda x^2 + \mu(x)x + \frac{1}{2}\tau(x,x) \quad \text{для всех } x \in A.$$

Таким образом, $[x*x,x] = 0$ и

$$\begin{aligned}(x*x)*(x*x) &= \lambda\Big(\lambda x^2 + \mu(x)x + \frac{1}{2}\tau(x,x)\Big)\Big(\lambda x^2 + \mu(x)x + \frac{1}{2}\tau(x,x)\Big) + \\ &\quad + \mu(x*x)\Big(\lambda x^2 + \mu(x)x + \frac{1}{2}\tau(x,x)\Big) + \frac{1}{2}\tau(x*x,x*x) = \\ &= \lambda^3 x^4 + 2\lambda^2\mu(x)x^3 + \Upsilon_1(x,x)x^2 + \Phi_1(x,x,x)x + \Psi_1(x,x,x,x),\end{aligned} \tag{11}$$

где

$$\begin{aligned}\Upsilon_1 &= \lambda^2\tau(x,x) + \lambda\mu^2(x) + \lambda\mu(x*x),\\ \Phi_1 &= \lambda\mu(x)\tau(x,x) + \mu(x*x)\mu(x),\\ \Psi_1 &= \frac{1}{4}\lambda\tau^2(x,x) + \frac{1}{2}\mu(x*x)\tau(x,x) + \frac{1}{2}\tau(x*x,x*x).\end{aligned}$$

Вычислим $((x*x)*x)*x$. Прежде всего, из (2) получаем, что

$$\begin{aligned}(x*x)*x &= \frac{1}{2}\Big\{\lambda\Big(2\lambda x^2 + 2\mu(x)x + \tau(x,x)\Big)x + \mu(x*x)x + \\ &\quad + \mu(x)\Big(\lambda x^2 + \mu(x)x + \frac{1}{2}\tau(x,x)\Big) + \tau(x*x,x)\Big\} = \\ &= \lambda^2 x^3 + \frac{3}{2}\lambda\mu(x)x^2 + \frac{1}{2}\Big(\lambda\tau(x,x) + \mu(x*x) + \mu^2(x)\Big)x + \frac{1}{4}\mu(x)\tau(x,x) + \frac{1}{2}\tau(x*x,x).\end{aligned}$$

Отсюда $[(x*x)*x,x] = 0$ и

$$\begin{aligned}((x*x)*x)*x &= \frac{1}{2}\Big\{\lambda((x*x)*x)\circ x + \mu((x*x)*x)x \\ &\quad + \mu(x)((x*x)*x) + \tau((x*x)*x,x)\Big\} = \\ &= \lambda^3 x^4 + 2\lambda^2\mu(x)x^3 + \Upsilon_2(x,x)x^2 + \Phi_2(x,x,x)x + \Psi_2(x,x,x,x),\end{aligned} \tag{12}$$

где

$$\Upsilon_2 = \frac{1}{2}\Big(\lambda^2\tau(x,x) + \lambda\mu(x*x) + \frac{5}{2}\lambda\mu^2(x)\Big),$$
$$\Phi_2 = \lambda\Big(\frac{1}{4}\mu(x)\tau(x,x) + \frac{1}{2}\tau(x*x,x)\Big) + \frac{1}{2}\mu((x*x)*x)\frac{1}{4}\mu(x)\Big(\lambda\tau(x,x) + \mu(x*x) + \mu^2(x)\Big),$$
$$\Psi_2 = \mu(x)\Big(\frac{1}{8}\mu(x)\tau(x,x) + \frac{1}{4}\tau(x*x,x)\Big) + \frac{1}{2}\tau((x*x)*x,x).$$

Так как $1 \in A$, то

$$\mu(x*x) = \mu\Big(\lambda x^2 + \mu(x)x + \frac{1}{2}\tau(x,x)\Big) = \lambda\mu(x^2) + \mu^2(x) + \frac{1}{2}\tau(x,x)\mu(1),$$
$$\tau(x*x,x) = \tau\Big(\lambda x^2 + \mu(x)x + \frac{1}{2}\tau(x,x), x\Big) = \lambda\tau(x^2,x) + \mu(x)\tau(x,x) + \frac{1}{2}\tau(x,x)\tau(x,1).$$

Аналогично,

$$\mu((x*x)*x) = \lambda^2\mu(x^3) + 2\lambda\mu(x)\mu(x^2) + \frac{1}{2}\lambda\tau(x,x)\mu(x) + \mu^3(x) + \\ + \frac{5}{4}\mu(x)\tau(x,x)\mu(1) + \frac{1}{2}\lambda\tau(x^2,x)\mu(1) + \frac{1}{4}\tau(x,x)\tau(x,1)\mu(1),$$
$$\tau(x*x,x*x) = \lambda^2\tau(x^2,x^2) + 2\lambda\mu(x)\tau(x^2,x) + \lambda\tau(x,x)\tau(x^2,1) + \\ + \mu^2(x)\tau(x,x) + \mu(x)\tau(x,x)\tau(x,1) + \frac{1}{4}\tau^2(x,x)\tau(1,1),$$
$$\tau((x*x)*x,x) = \lambda^2\tau(x^3,x) + \frac{3}{2}\lambda\mu(x)\tau(x^2,x) + (\frac{1}{2}\lambda + \frac{1}{4}\mu(1))\tau^2(x,x) + \\ + \frac{1}{2}\lambda\mu(x^2)\tau(x,x) + \frac{1}{2}\mu^2(x)\tau(x,x) + \frac{1}{2}\mu^2(x)\tau(x,x) + \\ + \frac{3}{8}\mu(x)\tau(x,x)\tau(x,1) + \frac{1}{8}\lambda\tau(x^2,x)\tau(x,1) + \frac{1}{16}\tau(x,x)\tau^2(x,1).$$

Из (11) и (12) имеем

$$(x*x)*(x*x) - ((x*x)*x)*x = \Upsilon_3(x,x)x^2 + \Phi_3(x,x,x)x + \Psi_3(x,x,x,x), \tag{13}$$

где

$$\Upsilon_3 = \Upsilon_1 - \Upsilon_2 = \frac{1}{4}\lambda\Big(2\lambda\tau(x,x) + \mu^2(x) + 2\lambda\mu(x^2) + \tau(x,x)\mu(1)\Big),$$
$$\Phi_3 = \Phi_1 - \Phi_2 = -\Big(\frac{1}{4}\lambda\mu(x)\tau(x,x) + \frac{1}{4}\lambda\mu(x^2)\mu(x) + \frac{1}{8}\mu(x)\tau(x,x)\mu(1) + \\ + \frac{1}{2}\lambda^2\tau(x^2,x) + \frac{1}{4}\lambda\tau(x,x)\tau(x,1) + \frac{1}{2}\lambda^2\mu(x^3) + \\ + \frac{1}{4}\lambda\tau(x^2,x)\mu(1) + \frac{1}{8}\tau(x,x)\tau(x,1)\mu(1)\Big),$$
$$\Psi_3 = \Psi_1 - \Psi_2 = \frac{1}{4}\lambda\mu(x^2)\tau(x,x) + \frac{1}{8}\mu^2(x)\tau(x,x) + \frac{1}{8}\tau^2(x,x)\mu(1) + \\ + \frac{1}{2}\lambda^2\tau(x^2,x^2) + \frac{1}{2}\lambda\tau(x,x)\tau(x^2,1) + \frac{1}{8}\tau^2(x,x)\tau(1,1) - \\ - \frac{1}{8}\tau(x,x)\tau^2(x,1) - \frac{1}{4}\lambda\tau(x^2,x)\tau(x,1) - \frac{1}{2}\lambda^2\tau(x^3,x).$$

(b1) Предположим, что умножение $*$ ассоциативно относительно взятия четвертой степени. Так как

$$(x*x)*(x*x) - ((x*x)*x)*x = 0,$$

то, линеаризовав (13), получаем для всех $x_1, x_2, x_3, x_4 \in A$, что

$$\sum_{\sigma\in S_4}\Big\{\Upsilon_4(x_{\sigma(1)},x_{\sigma(2)})x_{\sigma(3)}x_{\sigma(4)} + \Phi_4(x_{\sigma(1)},x_{\sigma(2)},x_{\sigma(3)})x_{\sigma(4)} + \Psi_4(x_{\sigma(1)},x_{\sigma(2)},x_{\sigma(3)},x_{\sigma(4)})\Big\} = 0,$$

где S_4 — симметрическая группа на множестве $\{1,2,3,4\}$,

$$\Upsilon_4(x_1,x_2)=\frac{1}{4}\lambda\Big(2\lambda\tau(x_1,x_2)+\mu(x_1)\mu(x_2)+2\lambda\mu(x_1x_2)+\tau(x_1,x_2)\mu(1)\Big)$$

и

$$\begin{aligned}\Phi_4(x_1,x_2,x_3)=-\Big(&\frac{1}{4}\lambda\mu(x_1)\tau(x_2,x_3)+\frac{1}{4}\lambda\mu(x_1x_2)\mu(x_3)+\\&+\frac{1}{8}\mu(x_1)\tau(x_2,x_3)\mu(1)+\frac{1}{2}\lambda^2\tau(x_1x_2,x_3)+\\&+\frac{1}{4}\lambda\tau(x_1,x_2)\tau(x_3,1)+\frac{1}{2}\lambda^2\mu(x_1x_2x_3)+\\&+\frac{1}{4}\lambda\tau(x_1x_2,x_3)\mu(1)+\frac{1}{8}\tau(x_1,x_2)\tau(x_3,1)\mu(1)\Big),\\\Psi_4(x_1,x_2,x_3,x_4)=&\frac{1}{4}\lambda\mu(x_1x_2)\tau(x_3,x_4)+\frac{1}{8}\mu(x_1)\mu(x_2)\tau(x_3,x_4)+\\&+\frac{1}{8}\tau(x_1,x_2)\tau(x_3,x_4)\mu(1)+\frac{1}{2}\lambda^2\tau(x_1x_2,x_3x_4)+\\&+\frac{1}{2}\lambda\tau(x_1,x_2)\tau(x_3x_4,1)+\frac{1}{8}\tau(x_1,x_2)\tau(x_3,x_4)\tau(1,1)-\\&-\frac{1}{8}\tau(x_1,x_2)\tau(x_3,1)\tau(x_4,1)-\frac{1}{4}\lambda\tau(x_1x_2,x_3)\tau(x_4,1)-\frac{1}{2}\lambda^2\tau(x_1x_2x_3,x_4).\end{aligned}$$

Так как A удовлетворяет условию $\mathbf{Q}_4$, то коэффициент при x_3x_4 должен быть равен 0, т.е.

$$\frac{1}{4}\lambda\Big(2\lambda\mu(x_1\circ x_2)+2\mu(x_1)\mu(x_2)+2\tau(x_1,x_2)\{2\lambda+\mu(1)\}\Big)=0$$

для всех $x_1,x_2\in A$. Поскольку $\lambda\neq 0$, то справедливо (b1).

(b2) Предположим, что $2\lambda+\mu(1)\neq 0$ и справедливо условие (4). Тогда

$$\tau(x,y)=\frac{-1}{2\lambda+\mu(1)}\Big(\lambda\mu(x\circ y)+\mu(x)\mu(y)\Big). \tag{14}$$

Подставляя (14) в выражения Υ_3, Φ_3 и Ψ_3 в тождестве (13), можно проверить, что

$$(x*x)*(x*x)-((x*x)*x)*x=0\quad\text{для всех } x\in A.$$

Так как умножение $*$ ассоциативно относительно взятия третьей степени, то ввиду [15, Lemma 1.10] оно ассоциативно и относительно взятия четвертой степени.

(c) Предположим, что $1\notin A$. Так как A — ассоциативная подалгебра W, то из условия (2) для всех $x,y\in A$ имеем $\tau(x,y)\cdot 1\in A$, откуда $\tau(x,y)=0$. Таким образом, имеет место утверждение (c1).

Используя аргументы, аналогичные (b), видим, что справедливы соотношения (11) и (12). Так как $\tau(x,y)=0$, имеем следующий аналог (13):

$$(x*x)*(x*x)-((x*x)*x)*x=\frac{1}{4}\lambda[\mu^2(x)+2\lambda\mu(x^2)]x^2-[\frac{1}{4}\lambda\mu(x^2)\mu(x)+\frac{1}{2}\lambda^2\mu(x^3)]x$$

для всех $x\in A$. Поскольку A удовлетворяет условию $\mathbf{Q}_4$ и $\lambda\neq 0$, то, как и в (b), видим, что

$$\begin{gathered}(x*x)*(x*x)-((x*x)*x)*x=0\quad\Longleftrightarrow\\\lambda\mu(x\circ y)+\mu(x)\mu(y)=0\quad\text{для всех } x,y\in A,\end{gathered}$$

т.е. справедливо утверждение (c2). Теорема доказана. □

СПИСОК ЛИТЕРАТУРЫ

1. *Albert A. A.* Power-associative rings// Trans. Amer. Math. Soc. — 1948. — *64*. — С. 318–328.
2. *Beidar K. I., Brešar M., Chebotar M. A.* Functional identities on upper triangular matrix algebras// J. Math. Sci. — 2000. — *102*. — С. 4557–4565.
3. *Beidar K. I., Chang S.-C., Chebotar M. A., Fong Y.* On functional identities in left ideals of prime rings// Commun. Algebra. — 2000. — *28*. — С. 3041–3058.

4. *Beidar K. I., Chebotar M. A.* On functional identities and d-free subsets of rings, I// Commun. Algebra. — 2000. — *28*. — С. 3925–3951.
5. *Beidar K. I., Chebotar M. A.* On functional identities and d-free subsets of rings, II// Commun. Algebra. — 2000. — *28*. — С. 3953–3972.
6. *Beidar K. I., Chebotar M. A.* On Lie-admissible algebras whose commutator Lie algebras are Lie subalgebras of prime associative algebras// J. Algebra. — 2000. — *233*. — С. 675–703.
7. *Benkart G. M.* Power-associative Lie-admissible algebras// J. Algebra. — 1984. — *90*. — С. 37–58.
8. *Benkart G. M., Osborn J. M.* Flexible Lie-admissible algebras// J. Algebra. — 1981. — *71*. — С. 11–31.
9. *Benkart G. M., Osborn J. M.* Power-associative products on matrices// Hadron. J. — 1982. — *5*. — С. 1859–1892.
10. *Brešar M.* Commuting traces of biadditive mappings, commutativity-preserving mappings, and Lie mappings// Trans. Amer. Math. Soc. — 1993. — *335*. — С. 525–546.
11. *Brešar M.* Functional identities: A survey// Algebra and Its Applications/ Contemp. Math. — Providence, RI: Amer. Math. Soc., 2000. — *259*. — С. 93–109.
12. *Jeong K., Kang S.-J., Lee H.* Lie-admissible algebras and Kac—Moody algebras// J. Algebra. — 1997. — *197*. — С. 492–505.
13. *Laufer F. J., Tomber M. L.* Some Lie-admissible algebras// Can. J. Math. — 1962. — *14*. — С. 287–292.
14. *Myung H. C.* Some classes of flexible Lie-admissible algebras// Trans. Amer. Math. Soc. — 1972. — *167*. — С. 79–88.
15. *Myung H. C.* Malcev-admissible algebras/ Progr. Math. — Birkhäuser, 1986. — *64*.
16. *Myung H. C.* Lie-admissible algebras and the Virasoro algebra// J. Korean Math. Soc. — 1996. — *33*. — С. 1123–1128.
17. *Okubo S.* Introduction to Octonion and Other Non-Associative Algebras in Physics. — New York: Cambridge University Press, 1995.
18. *Okubo S., Myung H. C.* Adjoint operators in Lie algebras and the classification of simple flexible Lie-admissible algebras// Trans. Amer. Math. Soc. — 1981. — *264*. — С. 459–472.

К. И. Бейдар
Математический факультет,
Университет им. Ченг Гуна, Тайнань, Тайвань
М. А. Чеботарь
Механико-математический факультет,
Тульский государственный университет, Тула, Россия
Ю. Фонг
Математический факультет,
Университет им. Ченг Гуна, Тайнань, Тайвань
В.-Ф. Ке
Математический факультет,
Университет им. Ченг Гуна, Тайнань, Тайвань

Современная математика и ее приложения. Том 13 (2004). С. 79–91

УДК 512.54

ДВОЙСТВЕННЫЕ СВЯЗИ МЕЖДУ ПОЧТИ ВПОЛНЕ РАЗЛОЖИМЫМИ ГРУППАМИ И ИХ КОЛЬЦАМИ ЭНДОМОРФИЗМОВ

© 2004 г. **Е. А. БЛАГОВЕЩЕНСКАЯ**

Аннотация. Доказано, что кольца эндоморфизмов почти изоморфных почти вполне разложимых абелевых групп кольцевого типа (пвр-групп) также почти изоморфны как группы по сложению. На основании этого пвр-группы можно рассматривать в двойственной связи с их кольцами эндоморфизмов.

СОДЕРЖАНИЕ

1. Введение

Класс почти вполне разложимых групп (пвр-групп) допускает множество разнообразных неизоморфных разложений в прямую сумму (см. [1–3, 7, 10–12, 15, 16, 18]). Традиционно группы Батлера (в частности, пвр-группы) и их разложения в прямую сумму классифицируются с точностью до почти изоморфизма — эквивалентности, которая слабее изоморфизма, но достаточно точно сохраняет свойства разложимости (см. [6, теорема 7.16]). Свойства разложимости пвр-групп в прямую сумму отражаются на их кольцах эндоморфизмов, изучавшихся А. Мадером и Ф. Шульцем [17] (или определяются ими). Тесная связь между пвр-группами и их кольцами эндоморфизмов была установлена в случае блочно жестких црф-групп (групп с циклической фактор-группой по регулятору, см. [9]). Для более широкого класса пвр-групп в данной статье доказан следующий факт: если две пвр-группы кольцевого типа почти изоморфны, то их кольца эндоморфизмов также почти изоморфны как абелевы группы. Это показывает, что разложения колец эндоморфизмов почти изоморфных групп в прямую сумму односторонних идеалов тесно связаны друг с другом, а также с разложениями самих групп (см. [5, гл. XV, 106]).

Следуя традициям, для группы, порожденной набором элементов, мы используем обозначение $\langle \dots \rangle$, ранг группы X обозначается $\operatorname{rk} X$. Как обычно, $V \subset X$ означает, что V — подгруппа в X, а

$$V_* = \{g \in X \mid \exists n \in \mathbb{N} : ng \in V\}$$

обозначает чистую оболочку V в X. *Тип* $\operatorname{tp}_X g$ элемента $g \in X$, $g \neq 0$, можно определить как класс изоморфизма рациональной группы τ, которая изоморфна $\langle g \rangle_*$ в X и содержит $\mathbb{Z}$. Тогда можно сказать, что элемент g имеет тип τ, $\mathbb{Z} \subset \tau \subset \mathbb{Q}$. Далее, $\operatorname{tp}_X g$ совпадает с типом $\operatorname{tp} X$ группы, если X — однородная группа. Мы будем писать $\tau(p) = \infty$ или $p\tau = \tau$, если $1/p^n$ принадлежит τ для любого натурального n (p простое). Следуя стандартным определениям, введем также $X^*(\tau) = \sum\limits_{\sigma > \tau} X(\sigma)$ и $X^\sharp(\tau)$ — чистую оболочку $X^*(\tau)$ в X. Тип τ — критический, или элемент множества $T_{\mathrm{CR}}(X)$, если $X(\tau)/X^\sharp(\tau) \neq 0$ (см. [16, с. 37, определение 2.4.6]).

Основной объект исследования — *почти вполне разложимая группа* (пвр-группа) X, т.е. абелева группа конечного ранга без кручения, содержащая вполне разложимую группу A, для которой

ISSN 1512–1712

X/A — конечная группа. Если при этом X/A — циклическая группа, то X называется *црф-группой* и является пвр-группой с циклической фактор-группой по так называемому регулятору. Мы говорим, что X — группа *кольцевого типа*, если $T_{\mathrm{CR}}(X)$ состоит только из идемпотентных типов (т.е. тех, которые представляются характеристиками, состоящими только из символов 0 и ∞; см. [16, с. 13], [5, раздел 85]). Группа A единственным с точностью до изоморфизма образом разлагается в прямую сумму своих τ-однородных компонент A_τ, т.е. прямых сумм групп ранга 1 типа τ, $\tau \in T_{\mathrm{CR}}(X)$ ($A_\tau = 0$, если $\tau \notin T_{\mathrm{CR}}(X)$). Говорят, что X — *блочно жесткая* группа, если множество $T_{\mathrm{CR}}(X)$ — антицепь (т.е. состоит из попарно несравнимых типов). Если при этом $\operatorname{rk} A_\tau = 1$ для всех $\tau \in T_{\mathrm{CR}}(X)$, то A и X называются *жесткими* группами.

Теорема Бэра—Капланского была доказана в [9] для блочно жестких црф-групп с точностью до почти изоморфизма. В [9] было показано, что две такие группы X и Y кольцевого типа почти изоморфны тогда и только тогда, когда $\mathrm{End}(X) \cong \mathrm{End}(Y)$. В частности, было доказано, что если X — жесткая группа из этого класса, то X почти изоморфна $\mathrm{End}(X)^+$ относительно операции сложения. В настоящей работе изучаются связи между пвр-группами и их кольцами эндоморфизмов в более общей ситуации.

Любая пвр-группа X содержит особую вполне разложимую подгруппу $R(X)$, изоморфную A, которая является вполне характеристической подгруппой X и называется *регулятором* X. Вместе с ней рассматриваются следующие числа: *индекс регулятора* $[X : R(X)]$ и *регуляторный показатель*, т.е. показатель $e =: \exp X/R(X)$ фактор-группы $X/R(X)$.

Наши обозначения стандартны и содержатся в [5, 9, 10, 16]. Если группа X изоморфна Y, мы пишем $X \cong Y$, почти изоморфизм обозначается $X \cong_{\mathrm{nr}} Y$. Как обычно, $\mathbb{Z}$ — это группа всех целых чисел, $\mathbb{N}$ — множество всех натуральных чисел, $\mathbb{Q}$ — группа рациональных чисел по сложению.

Если целое число q делится на целое p, будем писать $p|q$. Как обычно, $|c|$ обозначает порядок элемента группы $c \in X$, $|C|$ — мощность группы C (используется только для конечных групп и множеств).

Для использования методов линейной алгебры мы вводим *делимую оболочку* D_H абелевой группы H конечного ранга без кручения. Обозначение E^+ используется для аддитивной группы кольца E. Пишем $f \in \mathrm{Mon}(G, F)$, если $f : G \mapsto F$ — инъективный гомоморфизм.

Монография А. Мадера «Почти вполне разложимые группы» [16] вместе с классической книгой Л. Фукса «Бесконечные абелевы группы» [5] могут служить руководством по рассматриваемым вопросам, которые также связаны с проблематикой книги П. Крылова, А. Михалева, А. Туганбаева «Связи абелевых групп и их колец эндоморфизмов» [4].

2. Предварительные сведения

Рассмотрим класс $\mathcal{A}$ почти вполне разложимых групп X кольцевого типа с регулятором

$$A = \bigoplus_{\tau \in T} A_\tau \cong \bigoplus_{\tau \in T} n_\tau \tau, \quad T = T_{\mathrm{CR}}(A), \tag{2.1}$$

где n_τ — ранг τ-однородной компоненты A_τ в A, прямой сумме n_τ экземпляров τ. Пусть $P(X)$ — конечный набор различных простых чисел, и для каждого $p \in P(X)$, $C_p(X) \neq 0$ — p-примарная конечная группа из $X/A \cong \bigoplus\limits_{p \in P(X)} C_p(X)$.

Хорошо известно, что

$$X = \sum_{p \in P(X)} X_p \tag{2.2}$$

для однозначно определенных групп $X_p \in \mathcal{A}$ с p-примарными фактор-группами $X_p/A \cong C_p$. Положим

$$e_p = \exp C_p, \quad e = \prod_{p \in P(X)} e_p, \quad C = \bigoplus_{p \in P(X)} C_p.$$

Вообще говоря, мы будем рассматривать почти вполне разложимую группу X как расширение вполне разложимой группы A при помощи конечной группы $C \cong X/A$, $eC = 0$.

Предположим, что $\tau(p) \neq \infty$ для всех $\tau \in T = T_{\mathrm{CR}}(A)$, $p \in P$, и определим канонические эпиморфизмы

$$\overline{\ } : A \to \overline{A} = A/eA, \quad \overline{\ } : \mathbb{Z} \to \mathbb{Z}/e\mathbb{Z}$$

и индуцированные гомоморфизмы

$$\overline{\ } : \operatorname{End} A \to \operatorname{End} \overline{A}, \quad \overline{\ } : \operatorname{Aut} A \to \operatorname{Aut} \overline{A}.$$

Заметим, что фактор-группа A/eA изоморфна прямой сумме $n = \sum\limits_{\tau \in T} n_\tau$ экземпляров $\mathbb{Z}/e\mathbb{Z}$.

Известно (см. [15, предложения 3.2.3, 3.2.5]), что

$$\operatorname{Ext}(C, A) \cong \operatorname{Hom}(C, \overline{A}).$$

Точнее,

$$X \cong X_f, \quad f \in \operatorname{Mon}(C, \overline{A}), \tag{2.3}$$

— группа без кручения, определенная при естественном предположении, что $C = X/A$, следующими условиями:

1) $f : X/A \to A/eA = \overline{A}$: $(x + A)f = \overline{ex}$;
2) $X_f = \{(a, c) : cf = \overline{a}\} \subset A \oplus C$.

Ясно (см. [15, 3.2.4, 3.2.5]), что X_f содержит группу

$$A\epsilon = \{(ea, 0) : \ a \in A\} \cong A$$

для всех $f \in \operatorname{Mon}(C, \overline{A})$, где $\epsilon : A \to X_f$ — естественное отображение, определенное формулой $a\epsilon = (ea, 0)$. Теперь вместо группы X будем при необходимости рассматривать X_f, $f \in \operatorname{Mon}(C, \overline{A})$. В соответствии с обозначениями [15] будем писать $f \in \operatorname{Re}\operatorname{Mon}(C, \overline{A})$, когда предполагается, что A — регулятор X.

Определение 2.1 (см. [16, 2.5.9])**.** Пусть A — вполне разложимая группа, e — положительное целое число. Мультипликативная группа $\operatorname{Typ}\operatorname{Aut}\overline{A}$ — это подгруппа всех автоморфизмов ψ группы $\overline{A} = A/eA$, удовлетворяющих условию $\overline{A(\tau)}\psi \subset \overline{A(\tau)}$ для каждого критического типа $\tau \in T_{\mathrm{CR}}(A)$.

Среди различных эквивалентных определений *почти изоморфизма* мы выбираем следующее (см. [16, определение 9.1.2, теорема 9.1.4], [6, теорема 7.16]).

Определение 2.2. Пусть G и H — группы конечного ранга без кручения. Тогда G и H *почти изоморфны*, $G \cong_{\mathrm{nr}} H$, если для каждого простого q существует мономорфизм $\phi_q : G \to H$, для которого индекс $[H : G\phi_q]$ конечен и q не делит $[H : G\phi_q]$.

Для построения вложений групп будет использоваться следующее утверждение.

Предложение 2.3 (см. [15, предложение 3.2.6])**.** *Пусть $f, g \in \operatorname{Mon}(C, \overline{A})$. Если $\eta \in \operatorname{End} A$ и $\xi \in \operatorname{End} C$ удовлетворяют условию $f\overline{\eta} = \xi g$, то соотношение $(a, c)\Psi = (a\eta, c\xi)$ задает гомоморфизм из X_f в X_g, для которого $A\epsilon\Psi \subset A\epsilon$. Обратно, если $\Psi \in \operatorname{Hom}(X_f, X_g)$ и $A\epsilon\Psi \subset A\epsilon$, то существуют единственные отображения $\eta \in \operatorname{End} A$ и $\xi \in \operatorname{End} C$, для которых $f\overline{\eta} = \xi g$ и $(a, c)\Psi = (a\eta, c\xi)$ для всех $(a, c) \in X_f$.*

Нам потребуется простое следствие этого утверждения (см. [16, лемма 8.1.5, лемма 9.2.1, (9.2.2)]).

Следствие 2.4. *Пусть X и X' — пвр-группы, которые содержат вполне разложимую группу A. Пусть e — целое число, для которого $eX \subset A$ и $eX' \subset A$. Если для $\eta \in \operatorname{Mon}(A, A)$ выполнены условия $\overline{\eta} \in \operatorname{Typ}\operatorname{Aut}\overline{A}$ и $\overline{eX}\overline{\eta} = \overline{eX'}$, то существует $\psi \in \operatorname{Mon}(X, X')$, для которого $\psi = \eta$ на A. Более того,*

$$[X' : X\psi] = [A : A\eta]. \tag{2.4}$$

Почти изоморфизм для пвр-групп совпадает с эквивалентностью, которую мы будем называть *слабым изоморфизмом* (type-isomorphism, см. [16, теорема 9.2.4]); для рассматриваемых групп он описывается следующим образом.

Определение 2.5 (см. [16, 8.1.14, 9.2.3])**.** Пусть $X, X' \in \mathcal{A}$. Тогда X и X' называются *слабо изоморфными*, $X \cong_{\mathrm{tp}} X'$, если существует $\rho \in \mathrm{Typ}\,\mathrm{Aut}\,\overline{A}$, для которого $\overline{eX}\rho = \overline{eX'}$ в $\overline{A} = A/eA$ при некотором целом e, удовлетворяющем условию $eX, eX' \subset A$.

Нам потребуется следующая выдержка из [16, теорема 9.2.4].

Теорема 2.6. *Пусть X и X' — пвр-группы с одним и тем же регулятором A. $X \cong_{\mathrm{tp}} X'$ тогда и только тогда, когда $X \cong_{\mathrm{nr}} X'$. Условие $X/A \cong X'/A$ необходимо для того, чтобы группы X и X' были слабо* (*почти*) *изоморфны.*

Отсюда следует, что если $X, X' \in \mathcal{A}$ и $X \cong_{\mathrm{nr}} X'$, то X/A и X'/A изоморфны; оба множества $P(X) = P(X')$ будем обозначать P (см. (2.1)).

Известно, что любая вполне разложимая подгруппа конечного индекса в пвр-группе изоморфна ее регулятору. Традиционно определение слабо изоморфных групп X и X' (или их изоморфных копий X_f и X_g, $f, g \in \mathrm{Re}\,\mathrm{Mon}(C, \overline{A})$) включает в себя условие, что A — регулятор обеих групп (см. определение 2.5). При изучении их колец эндоморфизмов $E \cong \mathrm{End}\,X$ и $E' \cong \mathrm{End}\,X'$ как абелевых групп нам потребуется обобщение этого понятия на вполне разложимую подгруппу конечного индекса в E^+ и E'^+.

Определение 2.7. Пусть $f, g \in \mathrm{Mon}(C, \overline{E}_0)$ для вполне разложимой группы E_0, конечной группы C, $eC = 0$, и $\overline{E}_0 = E_0/eE_0$. Тогда группы $S = S_f$, $S' = S_g$ называются слабо изоморфными относительно E_0, $S_f \cong_{\mathrm{tp}\,E_0} S_g$, если существует $\rho \in \mathrm{Typ}\,\mathrm{Aut}\,\overline{E_0}$, для которого $Cf\rho = Cg$ (или, что то же самое, $\overline{eS}\rho = \overline{eS'}$). Далее, если группы E и E' определены формулами $E = eS$, $E' = eS'$ и $S \cong_{\mathrm{tp}\,E_0} S'$, то скажем в этом случае, что E и E' слабо изоморфны относительно eE_0.

Замечание 2.8. Пусть X_f, X_g, $f, g \in \mathrm{Re}\,\mathrm{Mon}(C, \overline{A})$, — почти изоморфные группы. Из канонического разложения

$$C \cong X_f/A \cong X_g/A \cong \bigoplus_{p \in P} C_p$$

на примарные слагаемые видим, что $C_p f\rho = C_p g$ для каждого $p \in P$, поскольку порядки элементов $C_p f$ и $C_p g$ в $\overline{A}$ делят $|C_p|$ и попарно взаимно просты для разных p.

Пусть $X \in \mathcal{A}$. Согласно (2.1) можем написать $T = T_{\mathrm{CR}}(A) = \{\tau_1, \dots, \tau_k\}$, где $k = |T|$, n_i — ранг τ_i-однородной компоненты A и

$$A = (\tau_1 a_1 \oplus \cdots \oplus \tau_1 a_{n_1}) \oplus (\tau_2 a_{n_1+1} \oplus \cdots \oplus \tau_2 a_{n_1+n_2}) \oplus \cdots \oplus \\ \oplus (\tau_k a_{n_1+\cdots+n_{k-1}+1} \oplus \cdots \oplus \tau_k a_n) \quad (2.5)$$

— разложение A на слагаемые ранга 1. Будем пользоваться тем, что для каждого $j = 1, \dots, n$ чистая оболочка $\langle a_j \rangle$ в A изоморфна одной из групп ранга 1, входящих в $T = T_{\mathrm{CR}}(A) = \{\tau_1, \dots, \tau_k\}$. Тогда

$$A = \bigoplus_{j=1}^{n} \langle a_j \rangle_*. \quad (2.6)$$

Ясно, что $n = \mathrm{rk}\,A = n_1 + \cdots + n_k$ и группа X вкладывается в делимую оболочку своего регулятора

$$D = \bigoplus_{j=1}^{n} \mathbb{Q} a_j, \quad (2.7)$$

которая изоморфна аддитивной группе прямой суммы $\mathbb{Q} \oplus \mathbb{Q} \oplus \cdots \oplus \mathbb{Q}$ из $n = \mathrm{rk}\,A$ слагаемых, т.е. векторному пространству размерности n над $\mathbb{Q}$. В [9] было показано, что если X — пвр-группа, то $\mathrm{End}(X)$ — также пвр-группа как аддитивная структура.

Предложение 2.9. *Пусть X — пвр-группа с регулятором $A = \bigoplus\limits_{\tau \in T} A_\tau$, регуляторным показателем e, множеством критических типов T и $n_\tau = \mathrm{rk}\,A_\tau$. Тогда справедливы следующие утверждения*:

1) *имеется цепочка колец $e\,\mathrm{End}(A) \subseteq \mathrm{End}(X) \subseteq \mathrm{End}(A)$;*

2) $\mathrm{End}(X)^+$ — *пвр-группа с множеством критических типов* T, $R(\mathrm{End}(X)^+) \cong \mathrm{End}(A)^+$ *и, для всех* $\tau \in T$, $R(\mathrm{End}(X))$ *имеет* τ*-ранг* $\sum\limits_{\sigma \leqslant \tau} n_\sigma n_\tau$.

Точнее, $\mathrm{End}(A)$ изоморфно кольцу M $(n \times n)$-матриц вида

$$F = \{f_{ij} \in \mathbb{Q} : f_{ij} \in \mathrm{Hom}(\langle a_j \rangle_*, \langle a_i \rangle_*)\}, \tag{2.8}$$

где $\mathrm{Hom}(\langle a_j \rangle_*, \langle a_i \rangle_*) \cong \langle a_i \rangle_*$, если $\mathrm{tp}_A a_j \leqslant \mathrm{tp}_A a_i$, и 0 в противном случае.

Пусть M_e обозначает мультипликативную полугруппу, состоящую из матриц $F \in M$ с целыми элементами, которые удовлетворяют условию

$$F = \{f_{ij} \in \mathbb{Z} : \det F \neq 0,\ \gcd(\det F, e) = 1\}. \tag{2.9}$$

Для каждой матрицы $F \in M_e$ рассмотрим матрицу

$$\overline{F} = \{\overline{f_{ij}} : \overline{f_{ij}} \in \mathbb{Z}/e\mathbb{Z}\}. \tag{2.10}$$

Ясно, что $\det \overline{F} \neq \overline{0}$ и все такие матрицы $\overline{F}$ образуют структуру $\overline{M_e}$, которая изоморфна подгруппе $\mathrm{Typ}\,\mathrm{Aut}\,\overline{A}$ в $\mathrm{Aut}\,\overline{A}$ (см. определение 2.1), при этом M_e вкладывается в $\mathrm{Mon}(A, A)$.

Пусть $X, X' \in \mathcal{A}$ и $X = \sum\limits_{p \in P} X_p$, $X' = \sum\limits_{p \in P} X'_p$ — разложения на слагаемые из $\mathcal{A}$ с p-примарными конечными группами X_p/A и X'_p/A (см. (2.2)). Если $X \cong_{\mathrm{tp}} X'$, то, согласно замечанию 2.8, $X_p \cong_{\mathrm{tp}} X'_p$ для каждого простого $p \in P$. Более того (см. [16, теорема 8.1.15]), это условие не только необходимо, но и достаточно для того, чтобы группы были слабо изоморфными.

Лемма 2.10. *Пусть*

$$X = \sum_{p \in P} X_p, \quad X' = \sum_{p \in P} X'_p$$

— *канонические представления с* p*-примарными конечными группами* X_p/A *и* X'_p/A. $X \cong_{\mathrm{tp}} X'$ *тогда и только тогда, когда* $X_p \cong_{\mathrm{tp}} X'_p$ *для каждого простого* $p \in P$.

Это утверждение сводит изучение условий почти изоморфизма к условиям для групп с примарным индексом регулятора. Нам потребуется известная теорема, различные версии которой были доказаны в [7, теорема 2.3], [13, лемма 3.2].

Теорема 2.11. *Пусть* A — *вполне разложимая группа,* X_p *и* X'_p — *такие пвр-группы, что для простого* p *фактор-группы* X_p/A *и* X'_p/A *являются* p*-примарными конечными группами. Группы* X_p *и* X'_p *почти изоморфны в том и только том случае, когда существует инъективное отображение* $\Psi \in \mathrm{Hom}(X_p, X'_p)$*, удовлетворяющее условию*

$$\gcd(p, [X_p : X'_p\Psi]) = 1. \tag{2.11}$$

Набросок доказательства. Пусть $e = p^k = \exp X_p/A$, $k \in \mathbb{N}$. Тогда $eX_p \subset A \subset X'_p$ — вложение $eX_p \cong X_p$ в X'_p, которое тривиально удовлетворяет q-условию для любого простого $q \neq p$ (см. определение 2.2). Поэтому существование $\Psi \in \mathrm{Hom}(X_p, X'_p)$ с p-условием достаточно для того, чтобы группы X_p и X'_p были почти изоморфны. Обратное тривиально. □

3. Кольца эндоморфизмов почти изоморфных пвр-групп

Пусть $\mathbb{Z}_p$ — кольцо рациональных чисел со знаменателями, не делящимися на простое число p, т.е. локализация $\mathbb{Z}$ в p. Для любого кольца (или группы) Y с аддитивной структурой без кручения положим $Y_p = \mathbb{Z}_p \otimes Y$. Отождествим Y с подмножеством Y_p посредством вложения $y \to 1 \otimes y$, $y \in Y$. Развивая подход Фатикони и Шульца [13, с. 234], обобщим это на конечное множество N простых чисел: введем кольцо $\mathbb{Z}_N$ рациональных чисел со знаменателями, не делящимися на все простые $p \in N$, и рассмотрим $Y_N = \mathbb{Z}_N \otimes Y$ для кольца (группы) Y.

Нас интересуют связи между кольцами эндоморфизмов почти (слабо) изоморфных пвр-групп. Будет использоваться следующая лемма.

Лемма 3.1. *Пусть* $G = \tau_1 g_1 \oplus \cdots \oplus \tau_n g_n$ *— вполне разложимая группа кольцевого типа с* $\tau_i \in T_{\mathrm{CR}}(G)$*,* $n \geqslant |T_{\mathrm{CR}}(G)|$*, и*

$$H = \langle g_1, \ldots, g_n \rangle \cong \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n = \mathrm{rk}\, G}$$

— ее подгруппа. Пусть $\mathcal{F}, \mathcal{G} \in \mathrm{Mon}(G, G)$ *удовлетворяют следующим условиям*:

1) $\mathcal{F}|_H, \mathcal{G}|_H \in \mathrm{Mon}(H, H)$;
2) $\mathcal{F}\mathcal{G} = r1_G$ *при некотором* $r \in \mathbb{N}$.

Тогда имеется цепочка $rG \subset G\mathcal{F} \subset G$.

Доказательство. Нужно доказать только первое включение. Для каждого $i \leqslant n$ образ

$$g_i' = g_i\mathcal{F} = \sum_{j=1}^{n} f_{ji} g_j$$

определяется набором целых чисел $\{f_{ji}\}$, которые образуют матрицу $\widetilde{F}$, $\det \widetilde{F} \neq 0$, представляющую $\mathcal{F}|_H$, а также $\mathcal{F}$, потому что $G \subset D_H$, где последнее — делимая оболочка H. Заметим, что $[G : G\mathcal{F}]$ конечно согласно [16, предложение 2.1.3], а тогда для каждого i выполнено условие

$$\mathrm{tp}_G(g_i) = \mathrm{tp}_G(g_i\mathcal{F}).$$

Это означает, что

$$\tau_i = \mathrm{tp}_G(g_i') = \mathrm{tp}_{G'}(g_i')$$

для $G' = G\mathcal{F}$. Итак,

$$G' = \tau_1 g_1' \oplus \cdots \oplus \tau_n g_n'.$$

Аналогично $\mathcal{G}$ определяется матрицей $\widetilde{F^*} = \{f_{ji}' : f_{ji}' \in \mathbb{Z}\}$ с $rg_i = \sum\limits_{j=1}^{n} f_{ji}' g_j'$. Отсюда следует

$$rg_i \in \langle g_1', \ldots, g_n' \rangle \subset G'$$

для любого $i \leqslant n$, и тот факт, что

$$\tau_i = \mathrm{tp}_G(rg_i) = \mathrm{tp}_{G'}(rg_i),$$

завершает доказательство. □

Линейное преобразование $\mathcal{F}$ делимой оболочки D абелевой группы конечного ранга без кручения и ограничение $\mathcal{F}$ на некоторое $D' \subset D$ будем часто обозначать одним и тем же символом $\mathcal{F}$, когда это не приводит к путанице. Аналогично, эндоморфизм η пвр-группы можно рассматривать как эндоморфизм ее регулятора или вполне разложимой подгруппы A, если $A\eta \subset A$. Во избежание громоздких обозначений мы будем, как правило, писать E, даже если рассматривается только аддитивная структура E^+ кольца E.

Теорема 3.2. *Пусть* $X_p, X_p' \in \mathcal{A}$ *и* X_p/A*,* X_p'/A *— примарные конечные группы для простого числа* p*, для которого* $\tau(p) \neq \infty$ *при каждом* $\tau \in T_{\mathrm{CR}}(A)$ *(см.* (2.1)*). Если* X_p *почти изоморфна* X_p'*, то* $\mathrm{End}(X_p)^+$ *и* $\mathrm{End}(X_p')^+$ *почти изоморфны как абелевы группы.*

Доказательство. Для упрощения обозначений в доказательстве положим $X = X_p$ и $X' = X_p'$. Как и ранее, пусть e — натуральное число, для которого $eX, eX' \subset A$. Согласно теореме 2.6 мы имеем дело со слабо изоморфными группами X и X'; согласно определению 2.5 существует $\rho \in \mathrm{Typ}\,\mathrm{Aut}\,\overline{A}$, для которого $\overline{eX}\rho = \overline{eX'}$ и ρ задается матрицей $\overline{F} \in \overline{M_e}$. Как обычно в линейной алгебре, он действует на

$$\overline{A} = A/eA = \langle \overline{a_1} \rangle \oplus \cdots \oplus \langle \overline{a_n} \rangle, \quad |\overline{a_i}| = e,$$

умножением (слева) на матрицу $\overline{F}$ из $\overline{M_e}$ (см. (2.5), (2.6), (2.9), (2.10)). Рассмотрим прообраз F матрицы $\overline{F}$ в M_e. Он представляет элемент из $\mathrm{Mon}(A, A)$, скажем, η, для которого $\overline{\eta} = \rho$. Согласно следствию 2.4 имеется мономорфизм ψ из X в X', также представляемый F, для которого $\psi = \eta$ на A. Более того, из (2.4) заключаем, что $[X' : X\psi] = [A : A\eta]$ взаимно просто с e по условию на $\det F$. Среди линейных преобразований D (см. (2.7)) рассмотрим матрицу F^{-1} с

рациональными элементами $g_{ij} = b_{ij}/\det F$, которые можно рассматривать как дроби с одним и тем же знаменателем $\det F$, $b_{ij} \in \mathbb{Z}$.

Рассмотрим матрицу $\overline{F^{-1}}$, состоящую из элементов

$$\overline{g_{ij}} = \overline{b_{ij}}\ (\overline{\det F})^{-1} \in \overline{\mathbb{Z}} = \mathbb{Z}/e\mathbb{Z},$$

которые корректно определены, так как $\gcd(\det F, e) = 1$. Обозначим через r наименьшее натуральное число, для которого $\overline{r} = (\overline{\det F})^{-1}$ в $\mathbb{Z}/e\mathbb{Z}$, и для $d = \det F$ определим матрицу $F' = rdF^{-1}$ с целыми элементами. По построению $\overline{F^{-1}} = \overline{F}^{-1} = \overline{F'}$ и представляет $\rho^{-1} \in \operatorname{Typ}\operatorname{Aut}\overline{A}$, так что F' соответствует некоторому $\eta' \in \operatorname{Mon}(A, A)$. Следствие 2.4 влечет существование мономорфизма ϕ из X' в X, представляемого F' и совпадающего с η' на A, откуда получаем, что $[X : X'\phi] = [A : A\eta']$ взаимно просто с e.

Теперь воспользуемся тем фактом, что матрицы F и F' соответствуют мономорфизмам $\psi : X \to X'$ и $\phi : X' \to X$ соответственно, для которых $\psi|_A = \eta$, $\phi|_A = \eta'$ и $\eta, \eta' \in \operatorname{Mon}(A, A)$, так что можно сказать, что матрицы F и F' представляют некоторые инъективные эндоморфизмы A.

Пусть $E \cong \operatorname{End}(X)$ и $E' \cong \operatorname{End}(X')$ — кольца матриц; согласно предложению 2.9 и (2.8) имеем

$$eM \subseteq E \subseteq M, \quad eM \subseteq E' \subseteq M \quad \text{для всех } e \text{ при условии } eX, eX' \subset A. \tag{3.1}$$

Обозначим множество всех простых делителей e символом N и введем E_N и E'_N, как указано выше. Легко видеть, что $\mathcal{F}_0$, заданное формулой $\beta\mathcal{F}_0 = F^{-1}\beta F$, $\beta \in E'_N$, — изоморфное отображение из E'_N в E_N, так как если $k\beta \in E'$ для некоторого $k \in \mathbb{Z}$, $\gcd(k, e) = 1$, и $\alpha = F^{-1}\beta F$, то $(krd)\alpha = F'(k\beta)F \in E$ и $\gcd(krd, e) = 1$, т.е. $\alpha \in E_N$. Далее, $\mathcal{F}_0$ очевидно обратимо. Тогда $E_N = F^{-1}E'_N F$. Легко видеть, что $\overline{E_N} = \overline{E}$ и $\overline{E'_N} = \overline{E'}$ в $\overline{M} = M/eM$ и, следовательно,

$$\overline{E} = \overline{F'}\ \overline{E'}\ \overline{F} = \overline{F}^{-1}\ \overline{E'}\ \overline{F}. \tag{3.2}$$

Кольцо M — вполне разложимая группа конечного ранга относительно операции сложения (см. предложение 2.9). Нам потребуется ввести подкольцо $M_Z \subset M$, состоящее из матриц из M с целыми элементами. Пусть D_M — делимая оболочка M (совпадающая с делимой оболочкой M_Z). Рассмотрим линейное преобразование $\mathcal{F}$ пространства D_M, заданное формулой

$$\gamma\mathcal{F} = F'\gamma F, \quad \gamma \in D_M, \tag{3.3}$$

которое индуцирует изоморфизм колец

$$\overline{\mathcal{F}} : \overline{E'} \to \overline{E}. \tag{3.4}$$

Ясно, что $\mathcal{F}|_{M_Z} \in \operatorname{End} M_Z$, так как матрицы F и F' состоят из целых элементов. Поскольку $M \cong \operatorname{End}(A)$ и F и F' соответствуют некоторым элементам из $\operatorname{Mon}(A, A)$, получаем, что $M\mathcal{F} = F'MF \subset M$. Аналогично, вводя $\mathcal{G}$ условием $\gamma\mathcal{G} = F\gamma F'$, заключаем, что $M\mathcal{G} = FMF' \subset M$. Далее,

$$M\mathcal{F}\mathcal{G} = FF'MFF' = F(drF^{-1})MF(drF^{-1}) = d^2r^2M.$$

Из равенств $\mathcal{F} = rd\mathcal{F}_0$ и

$$\mathcal{F} : D_M \to D_M, \quad \operatorname{Ker}\mathcal{F} = \operatorname{Ker}\mathcal{F}_0 = 0, \tag{3.5}$$

непосредственно получаем, что $\mathcal{F} \in \operatorname{Mon}(M, M)$ и $M\mathcal{F} \cong M$; кроме того, $\mathcal{G} \in \operatorname{Mon}(M, M)$. Из линейной алгебры ясно, что $d^2r^2M_Z \subset M_Z\mathcal{F} \subset M_Z$, так как $\mathcal{F}$ можно рассматривать как отображение из $\operatorname{Mon}({M_Z}^+, {M_Z}^+)$ с

$${M_Z}^+ \cong \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{\operatorname{rk} M^+}.$$

Лемма 3.1 обеспечивает включения $d^2r^2M \subset M\mathcal{F} \subset M$ и равенство

$$\gcd([M : M\mathcal{F}], e) = 1, \tag{3.6}$$

поскольку $\gcd(rd, e) = 1$ согласно построению.

Пусть e_p — делитель e, заданный формулой $e_p = \exp X/A = \exp X'/A$. По условию e_p — степень простого числа p. Следуя теории пвр-групп, мы можем рассмотреть две пвр-группы $S \cong E^+$ и

$S' \cong E'^{+}$, которые содержат M и вложены в D_M. Определим их условием $e_pS = E^+$ и $e_pS' = E'^{+}$. Из (3.1) для $e = e_p$ непосредственно получаем, что $e_pS \subset M^+$ и $e_pS' \subset M^+$.

В доказательстве формулы (3.2) мы уже использовали тот факт, что $\mathcal{F} \in \mathrm{Hom}(E', E)$, точнее, $\mathcal{F} \in \mathrm{Mon}(E', E)$ (см. (3.5)). Было показано, что $\mathcal{F}$ также принадлежит $\mathrm{Mon}(M, M)$. Из (2.4) и (3.6) выводим, что

$$[E : E'\mathcal{F}] = [S : S'\mathcal{F}] = [M : M'\mathcal{F}]$$

взаимно просто с p, так как $p|e$. На основании теоремы 2.11 приходим к заключению, что S и S' почти изоморфны; то же верно для $E^+ \cong \mathrm{End}(X)^+$ и $E'^{+} \cong \mathrm{End}(X')^+$, как и требовалось. □

Следствие 3.3. *Пусть $X_p, X'_p \in \mathcal{A}$ и X_p/A, X'_p/A — примарные конечные группы для простого p, для которых $e_p = \exp X_p/A = \exp X'_p/A$ и $\tau(p) \neq \infty$ для каждого $\tau \in T$. Если X_p слабо изоморфно X'_p, то $\mathrm{End}(X_p)^+$ и $\mathrm{End}(X'_p)^+$ слабо изоморфны как абелевы группы относительно вполне разложимой подгруппы $e_p \mathrm{End}(A)^+$ в $\mathrm{End}(X_p)^+$ и $\mathrm{End}(X'_p)^+$. Более того, для колец $\mathcal{E} = \mathrm{End}(X_p)$, $\mathcal{E}' = \mathrm{End}(X'_p)$, $E_A = \mathrm{End}(A)$ и любого целого e, делящегося на e_p, существует $\widetilde{\mathcal{F}} \in \mathrm{Typ}\,\mathrm{Aut}\,\overline{E_A}$, где $\overline{E_A} = E_A/eE_A$, для которого $\widetilde{\mathcal{F}}$: $\overline{\mathcal{E}'} \to \overline{\mathcal{E}}$ — изоморфизм колец.*

Доказательство. Из матричных представлений $E^+ \cong \mathrm{End}(X)^+$ и $E'^{+} \cong \mathrm{End}(X')^+$ видим, что требуемый $\widetilde{\mathcal{F}} \in \mathrm{Typ}\,\mathrm{Aut}\,\overline{E_A}$ можно отождествить с $\overline{\mathcal{F}} \in \mathrm{Typ}\,\mathrm{Aut}\,\overline{M}$, так как $M \cong \mathrm{End}\,A$ (см. (3.3), (3.4)). Если e совпадает с e_p, то (3.2) означает, что $\mathcal{E}^+$ и $\mathcal{E}'^{+}$ слабо изоморфны относительно e_pE_A в смысле определения 2.7. По построению $\overline{\mathcal{F}}$ сохраняет структуру кольца. □

Напомним (см. [16, предложение 5.1.5]), что если $X = \sum\limits_{p\in P} X_p$ — почти вполне разложимая группа с регулятором A и p-примарными группами X_p/A, то

$$\mathrm{End}(X) = \bigcap_{p\in P} \mathrm{End}(X_p). \tag{3.7}$$

Теперь докажем основную теорему.

Теорема 3.4. *Пусть X и X' — почти изоморфные почти вполне разложимые группы кольцевого типа с одним и тем же регулятором A. Пусть $e = \exp X/A = \exp X'/A$ и $\tau(p) \neq \infty$ для всех $\tau \in T_{\mathrm{CR}}(A)$ и простых p, $p|e$. Тогда $\mathrm{End}(X)^+$ и $\mathrm{End}(X')^+$ почти изоморфны как абелевы группы конечного ранга без кручения.*

Доказательство. По условию X и X' принадлежат классу $\mathcal{A}$, и наши обозначения согласованы с теоремой 3.2 и ее доказательством. Пусть

$$X = \sum_{p\in P} X_p, \quad X' = \sum_{p\in P} X'_p$$

— однозначно определенные разложения (2.2) с изоморфными p-примарными группами X_p/A и X'_p/A, для которых $e_p = \exp X_p/A = \exp X'_p/A$ (см. теорему 2.6). Согласно определению 2.5 существует $\rho \in \mathrm{Typ}\,\mathrm{Aut}\,\overline{A}$, для которого $\overline{eX}\rho = \overline{eX'}$ в $\overline{A} = A/eA$. Ясно, что $\overline{eX_p}\rho = \overline{eX'_p}$ согласно замечанию 2.8, и можно применить теорему 3.2 к фиксированной паре $X_p \cong_{\mathrm{tp}} X'_p$. Построим $\mathcal{F} \in \mathrm{Mon}(D_M, D_M)$ как и выше (см. (3.5)). Напомним (см. предложение 2.9), что

$$e\,\mathrm{End}\,A \subseteq \mathrm{End}\,X_p \subseteq \mathrm{End}\,A, \quad e_p\,\mathrm{End}\,A \subseteq \mathrm{End}\,X_p \subseteq \mathrm{End}\,A$$

для каждого p; то же верно для $\mathrm{End}(X'_p)$.

Пусть

$$E_p \cong \mathrm{End}\,X_p, \quad E'_p \cong \mathrm{End}\,X'_p \tag{3.8}$$

— матричные кольца, вложенные в $M \cong \mathrm{End}(A)$. Как и в доказательстве теоремы 3.2, рассмотрим $\overline{M} = M/eM$ и $\overline{\mathcal{F}} \in \mathrm{Typ}\,\mathrm{Aut}\,\overline{M}$, который отображает $\overline{E'_p}$ на $\overline{E_p}$ (см. (3.2)), а именно,

$$\overline{E_p} = \overline{E'_p}\,\overline{\mathcal{F}} = \overline{F'}\,\overline{E'_p}\,\overline{F} = \overline{F}^{-1}\,\overline{E'_p}\,\overline{F} \quad \text{для каждого } p. \tag{3.9}$$

Вернемся к группам X и X' и их кольцам эндоморфизмов. Из (3.7) видим, что

$$\operatorname{End} X = \bigcap_{p\in P} \operatorname{End} X_p, \quad \operatorname{End} X' = \bigcap_{p\in P} \operatorname{End} X'_p,$$

и как кольца эндоморфизмов пвр-групп они удовлетворяют условиям

$$e\operatorname{End} A \subseteq \operatorname{End} X \subseteq \operatorname{End} A, \quad e\operatorname{End} A \subseteq \operatorname{End} X' \subseteq \operatorname{End} A, \tag{3.10}$$

поскольку $eX, eX' \subset A$ (см. предложение 2.9).

Предположим временно, что $|P| = 2$ и множество $P = \{p_1, p_2\}$ состоит из двух различных простых чисел; тогда $e = \exp X/A = e_1e_2$, где $e_i = \exp X_{p_i}/A$ — некоторая степень p_i, $i = 1, 2$. Поскольку $X_{p_i} \cong_{\mathrm{tp}} X'_{p_i}$ для каждого i, числа e, e_1, e_2 являются соответственно показателями групп X'/A, X'_{p_1}/A, X'_{p_2}/A согласно теореме 2.6.

Обратимся к матричному представлению $M \cong \operatorname{End}(A)$. Определим матричные кольца $E_i \cong \operatorname{End}(X_{p_i})$ и $E'_i \cong \operatorname{End}(X'_{p_i})$, $i = 1, 2$. Так как числа p_1, p_2 взаимно просты и то же верно для e_1, e_2, получаем, что $M^+ = e_1M^+ + e_2M^+$. Отсюда непосредственно вытекают соотношения

$$\begin{aligned} E_1 + E_2 = M, \quad E'_1 + E'_2 = M, \\ \overline{E_1} + \overline{E_2} = \overline{M}, \quad \overline{E'_1} + \overline{E'_2} = \overline{M}, \end{aligned} \tag{3.11}$$

поскольку

$$e_1M \subset E_1, E'_1 \subset M, \quad e_2M \subset E_2, E'_2 \subset M.$$

Это влечет одно и то же включение для четырех колец:

$$e_1e_2M \subset E_1,\ E'_1,\ E_2,\ E'_2 \subset M$$

и следующие равенства в $\overline{M} = M/e_1e_2M = M/eM$:

$$\overline{E_1 \cap E_2} = \overline{E_1} \cap \overline{E_2}, \qquad \overline{E'_1 \cap E'_2} = \overline{E'_1} \cap \overline{E'_2}.$$

Так как автоморфизм $\overline{\mathcal{F}}$ группы $\overline{M}$ влечет изоморфизм $\overline{E'_i}$ на $\overline{E_i}$, $i = 1, 2$ (см. (3.9)), немедленно получаем, что

$$\overline{\mathcal{F}} : \overline{E'_1} \cap \overline{E'_2} \to \overline{E_1} \cap \overline{E_2} \quad \text{— изоморфизм (колец).} \tag{3.12}$$

Пусть $E_* \cong \operatorname{End}(X)$ и $E'_* \cong \operatorname{End}(X')$ — матричные кольца (подкольца M). Тогда $E_* = E_1 \cap E_2$ и $E'_* = E'_1 \cap E'_2$ согласно (3.7). Мы доказали соотношение

$$\overline{E'_*}\ \overline{\mathcal{F}} = \overline{E_*}. \tag{3.13}$$

Теперь сосредоточимся на кольцах, которые являются пвр-группами по сложению. Как и выше (в доказательстве теоремы 3.2), на основании следствия 2.4 заключаем, что $\mathcal{F} \in \operatorname{Mon}(M, M)$ индуцирует инъективное отображение из E'_* в E_* и $[E_* : E'_*\mathcal{F}] = [M : M\mathcal{F}]$ взаимно просто с p_1p_2. Далее, из (3.10) следуют включения $eM \subset E_*$, $E'_* \subset M$, и вложение $E'_* \cong eE'_* \subset eM \subset E_*$ удовлетворяет q-условию из определения 2.2 для любого простого $q \neq p_1, p_2$. Следовательно, ${E'_*}^+$ и ${E_*}^+$ почти изоморфны.

Тривиальная индукция по $|P|$, основанная на том, что

$$\gcd\Big(\prod_{\substack{p\in P\\ p\neq q}} p, q\Big) = 1, \quad q \in P,$$

и начинающаяся с $|P| = 2$, завершает доказательство для $E_* \cong \operatorname{End}(X)$ и $E'_* \cong \operatorname{End}(X')$ в общем случае. Утверждение доказано. □

Следующий факт не нуждается в доказательстве, так как все необходимые рассуждения приведены в доказательстве следствия 3.3.

Следствие 3.5. *Пусть X и X' — почти изоморфные почти вполне разложимые группы кольцевого типа с одним и тем же регулятором A. Пусть $e = \exp X/A = \exp X'/A$ и $\tau(p) \neq \infty$ для всех $\tau \in T_{\mathrm{CR}}(A)$ и простых p, $p|e$. Тогда $\operatorname{End}(X)^+$ и $\operatorname{End}(X')^+$ слабо изоморфны как абелевы группы относительно вполне разложимой подгруппы $e\operatorname{End}(A)^+$ в $\operatorname{End}(X)^+$ и $\operatorname{End}(X')^+$. Более*

того, для колец $\mathcal{E} = \mathrm{End}(X)$, $\mathcal{E}' = \mathrm{End}(X')$, $E_A = \mathrm{End}(A)$ *существует* $\widetilde{\mathcal{F}} \in \mathrm{Typ}\,\mathrm{Aut}\,\overline{E_A}$, *где* $\overline{E_A} = E_A/eE_A$, *для которого* $\widetilde{\mathcal{F}}\colon \overline{\mathcal{E}'} \to \overline{\mathcal{E}}$ *— изоморфизм колец.*

Замечание 3.6. Следствие 3.5 согласуется с леммой 10.1.1 из [16], в которой кольца $\overline{\mathcal{E}}$ и $\overline{\mathcal{E}'}$ обозначены $\mathrm{Typ}\,\mathrm{Aut}_X \overline{A}$ и $\mathrm{Typ}\,\mathrm{Aut}_{X'} \overline{A}$ соответственно.

4. Двойственные булевы алгебры

Предыдущие теоремы были мотивированы весьма удивительным результатом — теоремой Бэра—Капланского для блочно жестких црф-групп кольцевого типа (см. [9, теоремы 3.4, 3.6, 4.6]).

Теорема 4.1. *Пусть* X *и* X' *— блочно жесткие црф-группы кольцевого типа. Тогда* X *и* X' *почти изоморфны, если и только если* $\mathrm{End}(X) \cong \mathrm{End}(X')$. *Если* X *— жесткая группа, то* $\mathrm{End}(X)^+ \cong_{\mathrm{nr}} X$.

Это означает, что если взять любые две пары почти изоморфных блочно жестких црф-групп с регулятором A, скажем, $X_p \cong_{\mathrm{nr}} X'_p$ и $X_q \cong_{\mathrm{nr}} X'_q$, с примарными фактор-группами над A, связанными соответственно с простыми числами $p \neq q$, то согласно теореме 4.1 и (3.7) получим

$$\mathrm{End}\,X_p \cong \mathrm{End}\,X'_p, \quad \mathrm{End}\,X_q \cong \mathrm{End}\,X'_q,$$
$$\mathrm{End}\,X_p \cap \mathrm{End}\,X_q \cong \mathrm{End}\,X'_p \cap \mathrm{End}\,X'_q.$$

Грубо говоря, это происходит потому, что

$$\mathrm{End}\,X_p + \mathrm{End}\,X_q = \mathrm{End}\,X'_p + \mathrm{End}\,X'_q = \mathrm{End}\,A$$

и существует $\eta \in \mathrm{Aut}(\mathrm{End}(A))$, отображающий $\mathrm{End}\,X_p$ на $\mathrm{End}\,X'_p$ и $\mathrm{End}\,X_q$ на $\mathrm{End}\,X'_q$.

В поисках подобных результатов для пвр-групп, не ограничиваясь блочно жесткими црф-группами, мы нашли аналогичное объяснение на «более низком» уровне, а именно, $\overline{\mathrm{End}(A)}$ (см. (3.11), (3.12), (3.13)). В предположениях теоремы 3.2 для любых пар пвр-групп $X_p \cong_{\mathrm{nr}} X'_p$ и $X_q \cong_{\mathrm{nr}} X'_q$ с p- и q-примарными фактор-группами над A, $p \neq q$, можно вывести следующее заключение:

$$\mathrm{End}(X_p)^+ \cong_{\mathrm{nr}} \mathrm{End}(X'_p)^+, \quad \mathrm{End}(X_q)^+ \cong_{\mathrm{nr}} \mathrm{End}(X'_q)^+,$$
$$\mathrm{End}(X_p)^+ \cap \mathrm{End}(X_q)^+ \cong_{\mathrm{nr}} \mathrm{End}(X'_p)^+ \cap \mathrm{End}(X'_q)^+.$$

Чтобы установить двойственность между пвр-группами и их кольцами эндоморфизмов, нам понадобится следующее утверждение.

Предложение 4.2. *Пусть* P *— конечное множество простых чисел и, для каждого* $p \in P$, $X_p \in \mathcal{A}$ *— группа, для которой* X_p/A *— p-примарная конечная группа,* $\tau(p) \neq \infty$ *при всех* $\tau \in T_{\mathrm{CR}}(A)$ (*см.* (2.1)). *Пусть* P' *и* P'' *— подмножества* P *и*

$$X(P') = \sum_{p \in P'} X_p, \quad X(P'') = \sum_{p \in P''} X_p.$$

Тогда

$$\mathrm{End}(X(P') \cap X(P'')) = \mathrm{End}\,X(P') + \mathrm{End}\,X(P'').$$

Доказательство. Пусть

$$Q' = P' \setminus P'', \quad Q'' = P'' \setminus P', \quad Q = P' \cap P''.$$

По построению

$$X(P') \cap X(P'') = X(P' \cap P'') = X(Q).$$

Из (3.7) видим, что

$$\mathrm{End}\,X(P') = \mathrm{End}\,X(Q') \cap \mathrm{End}\,X(Q), \tag{4.1}$$
$$\mathrm{End}\,X(P'') = \mathrm{End}\,X(Q'') \cap \mathrm{End}\,X(Q). \tag{4.2}$$

Суммируя (4.1) и (4.2), получаем

$$\mathrm{End}\,X(P') + \mathrm{End}\,X(P'') = \mathrm{End}\,X(Q) \cap \big(\mathrm{End}\,X(Q') + \mathrm{End}\,X(Q'')\big) = \mathrm{End}\,X(Q),$$

так как

$$\operatorname{End} X(Q') + \operatorname{End} X(Q'') = \operatorname{End} A,$$

что гарантируется условием $(Q' \cap Q'') = \varnothing$ и предложением 2.9. Это означает, что

$$\operatorname{End}\big(X(P') \cap X(P'')\big) = \operatorname{End} X(P') + \operatorname{End} X(P''),$$

как и требовалось. □

Пример 4.3. Рассмотрим вполне разложимую группу $A = \langle \tau_1 a_1 \rangle \oplus \langle \tau_2 a_2 \rangle$, для которой множество $T_{\mathrm{CR}}(A) = \{\tau_1, \tau_2\}$ состоит из двух несравнимых идемпотентных типов. Пусть P — конечное множество различных простых чисел и $\tau_1(p) \neq \infty$, $\tau_2(p) \neq \infty$, если $p \in P$, а $X(p) = \langle A, b_p \rangle$ — неразложимые црф-группы ранга 2 с соотношениями с $pb_p = a_1 + a_2$. Определим группу $X = \sum\limits_{p \in P} X(p)$, которая также является црф-группой. Для любого подмножества P' в P рассмотрим группу $X(P') = \sum\limits_{p \in P'} X(p)$; тогда множество $B = \{X(P') : P' \subset P\}$ замкнуто относительно взятия произвольных сумм и пересечений этих групп. Предположим, что $X(\varnothing) = A$. Обозначим $E = \operatorname{End}(X)$, $E(P') = \operatorname{End}(X(P'))$; тогда $E(\varnothing) = \operatorname{End}(A)$. Рассмотрим $B^* = \{E(P') : P' \subset P\}$. Из (3.7) следует, что для любых $P', P'' \in P$ имеет место оотношение

$$\operatorname{End}\big(X(P') + X(P'')\big) = \operatorname{End}\big(X(P' \cup P'')\big) = \operatorname{End} X(P') \cap \operatorname{End} X(P'').$$

Из предложения 4.2 также ясно, что

$$\operatorname{End}\big(X(P') \cap X(P'')\big) = \operatorname{End}\big(X(P' \cap P'')\big) = \operatorname{End} X(P') + \operatorname{End} X(P'').$$

Введем две булевы алгебры (см. [14]): $B = (\{X(P')\}, +, \cap, \ ')$ с дополнением $X(P')' = X(P \setminus P')$, выделенными элементами $O_B = A = X(\varnothing)$, $1_B = X = X(P)$, и $B^* = (\{E(P')\}, +, \cap, \ ')$ с дополнением $E(P')' = E(P \setminus P')$, выделенными элементами $O_{B^*} = \operatorname{End}(X) = E(P)$, $1_{B^*} = \operatorname{End}(A) = E(\varnothing)$. Операции $\cap$ и $+$ понимаются в теоретико-множественном смысле.

Согласно предложению 4.2 и (3.7) отображение f из B в B^*, заданное формулой $X(P')f = E(P')$, является антиизоморфизмом булевых алгебр, поскольку для любых $P', P'' \in P$ имеем

$$(X(P') + X(P''))f = E(P') \cap E(P''),$$
$$(X(P') \cap X(P''))f = E(P') + E(P''),$$
$$O_B f = 1_{B^*}, \quad 1_B f = O_{B^*}.$$

Заметим, что соответствующие элементы B и B^* почти изоморфны как абелевы группы, являющиеся жесткими црф-группами (см. теорему 4.1).

Определим две булевы алгебры, обобщая предыдущий пример. Пусть P — конечное множество различных простых чисел и, для каждого $p \in P$, $X(p)$ — пвр-группа кольцевого типа (не обязательно црф-группа, как в примере 4.3) с регулятором A и p-примарной конечной группой X/A, $\tau(p) \neq \infty$ для каждого $\tau \in T_{\mathrm{CR}}(A)$. Как и выше, $X(P') = \sum\limits_{p \in P'} X(p)$ и $E(P') = \operatorname{End}(X(P'))$ для любого $P' \subset P$.

Введем две булевы алгебры: B, состоящую из групп $X(P')$, и B^* с элементами $E(P')$. Операции $\cap$ и $+$, выделенные элементы O_B, 1_B, O_{B^*}, 1_{B^*} и антиизоморфизм f из B в B^* определяются, как в примере 4.3. Другими словами, для любых $P', P'' \in P$ имеем

$$X(P') + X(P'') = X(P' \cup P''), \quad X(P') \cap X(P'') = X(P' \cap P''), \tag{4.3}$$
$$E(P') + E(P'') = E(P' \cap P''), \quad E(P') \cap E(P'') = E(P' \cup P''), \tag{4.4}$$
$$O_B = X(\varnothing), \quad 1_B = X(P), \quad {O_B}^* = E(P), \quad {1_B}^* = E(\varnothing), \tag{4.5}$$
$$X(P')' = X(P \setminus P'), \quad E(P')' = E(P \setminus P'), \tag{4.6}$$
$$X(P')f = E(P'), \quad \text{в частности,} \quad O_B f = 1_{B^*}, \quad 1_B f = O_{B^*}. \tag{4.7}$$

Заметим, что f переводит возрастающие цепочки элементов B в убывающие цепочки в B^*. Элементы B и B^*, связанные отображением f, имеют соответствующие разложения на неразложимые слагаемые (левые или правые идеалы для B^* и подгруппы для B; см. [16, следствие 10.1.7], [5, гл. XV, 106]).

Замечание 4.4. Пусть P — конечное множество различных простых чисел и, для каждого $p \in P$, $X(p) \cong_{\mathrm{nr}} X'(p)$ — пара пвр-групп кольцевого типа с p-примарными конечными фактор-группами $X(p)/A \cong X'(p)/A$, $\tau(p) \neq \infty$ для каждого $\tau \in T_{\mathrm{CR}}(A)$. Как и выше (см. (4.3)–(4.7)), построим булевы алгебры B и B' с атомами $X(p)$ и $X'(p)$ соответственно и двойственные алгебры B^* и B'^*, состоящие из $E(P') = \mathrm{End}(X(P'))$ и $E'(P') = \mathrm{End}(X'(P'))$ соответственно ($P' \subset P$). Согласно лемме 2.10 элементы $X(P') \in B$ и $X'(P') \in B'$, заданные одним и тем же P', почти изоморфны. Далее, из теоремы 3.4 следует, что элементы $E(P') \in B^*$ и $E'(P') \in B'^*$ также почти изоморфны как группы по сложению.

Это замечание позволяет определить две двойственные булевы алгебры $\widetilde{B}$ и $\widetilde{B}^*$, состоящие соответственно из классов почти изоморфизма элементов B и B^*.

Пусть атомы $\widetilde{B}$ — классы $\widetilde{X}(p)$ почти изоморфизма групп $X(p)$ из B и $\widetilde{X}(P')$ для $P' \subset P$ — класс почти изоморфизма группы $X(P')$ (т.е. множество всех групп из $\mathcal{A}$, почти изоморфных $X(P')$, см. (2.1)). Далее, предположим, что булева алгебра $\widetilde{B^*}$ состоит из классов почти изоморфизма $\widetilde{E}(P')$, содержащих $\mathrm{End}\, X(P')$, т.е. множеств $\{\mathrm{End}(Y) : Y \cong_{\mathrm{nr}} X(P'),\ Y \in \mathcal{A}\}$. Определение булевых операций в $\widetilde{B}$ и $\widetilde{B}^*$ можно получить из (4.3)–(4.6), поставив над символами X, E и B знак тильда.

Мы подытожим вышеизложенное в следующей таблице, в которой $B(P)$ — булева алгебра всех подмножеств конечного множества P различных простых чисел, P' и P'' — произвольные элементы $B(P)$, и элементы булевых алгебр $\widetilde{B}$ и $\widetilde{B^*}$, заданные одним и тем же подмножеством P (в левом столбце), помещены в одну и ту же строку. Любая группа из $\widetilde{X}(P')$ имеет кольцо эндоморфизмов из соответствующего класса $\widetilde{E}(P')$.

$B(P)$	$\widetilde{B}$	$\widetilde{B^*}$
P'	$\widetilde{X}(P')$	$\widetilde{E}(P')$
$P' \cup P''$	$\widetilde{X}(P') + \widetilde{X}(P'')$	$\widetilde{E}(P') \cap \widetilde{E}(P'')$
$P' \cap P''$	$\widetilde{X}(P') \cap \widetilde{X}(P'')$	$\widetilde{E}(P') + \widetilde{E}(P'')$
P	1	O
$\varnothing$	O	1

СПИСОК ЛИТЕРАТУРЫ

1. *Благовещенская Е. А.* О прямых разложениях абелевых групп без кручения конечного ранга// Зап. науч. семин. ЛОМИ. — 1983. — *132*. — С. 17–25.
2. *Благовещенская Е. А.* Разложениях абелевых групп конечного ранга без кручения в прямые суммы неразложимых групп// Алгебра и анализ. — 1992. — *4*, № 2. — С. 62–69.
3. *Благовещенская Е. А., Яковлев А. В.* Прямые разложениях абелевых групп конечного ранга без кручения// Алгебра и анализ. — 1989. — *1*, № 1. — С. 111–127.
4. *Крылов П. А., Михалев А. В., Туганбаев А. А.* Связи абелевых групп и их колец эндоморфизмов. — Томск, 2002.
5. *Фукс Л.* Бесконечные абелевы группы. Тт. 1, 2. — М.: Мир, 1974, 1977.
6. *Arnold D.* Finite rank torsion free abelian groups and rings/ Lect. Notes Math. — Springer Verlag, 1982. — *931*.
7. *Blagoveshchenskaya E.* Direct decompositions of almost completely decomposable abelian groups// Abelian Groups and Modules/ Lect. Notes Pure Appl. Math. — 1996. — *182*. — С. 163–179.
8. *Blagoveshchenskaya E.* Classification of a class of almost completely decomposable groups// in: Rings, Modules, Algebras and Abelian Groups/ Lect. Notes Pure Appl. Algebra. Proc. Int. Algebraic Conf. — Venezia 2002.
9. *Blagoveshchenskaya E., Ivanov G., Schultz P.* The Baer–Kaplansky theorem for almost completely decomposable groups// Contemp. Math. — 2001. — *273*. — С. 85–93.
10. *Blagoveshchenskaya E., Mader A.* Decompositions of almost completely decomposable abelian groups// Contemp. Math. — 1994. — *171*. — С. 21–36.
11. *Blagoveshchenskaya E., Reid J.* Classification and direct decompositions of block rigid crq groups without homogeneous subgroups of rank 1/ Preprint, 1999.

12. *Corner A. L. S.* A note on rank and decomposition of torsion-free abelian groups// Proc. Cambridge Philos. Soc. — 1961. — *57*. — С. 230–233; 1969. — *66*. — С. 239–240.
13. *Faticoni T., Schultz P.* Direct decompositions of ACD groups with primary regulating index// Abelian Groups and Modules/ Lect. Notes Pure Appl. Math. — 1996. — *182*. — С. 233–241.
14. *Koppelberg S.* Handbook on Boolean algebras. — North-Holland, 1989.
15. *Mader A.* Almost completely decomposable abelian groups/ Photocopied notes. — Montreal, 1992.
16. *Mader A.* Almost completely decomposable abelian groups/ Algebra, Logic, and Applications. — Amsterdam: Gordon and Breach, 1999. — *13*.
17. *Mader A., Schultz P.* Endomorphism rings and automorphism groups of almost completely decomposable groups// Commun. Algebra. — 2000. — *28*. — С. 51–68.
18. *Reid J.* Some matrix rings associated with ACD groups// in: Abelian Groups and Modules/ Int. Conf. Dublin. — 1998.
19. *Vinsonhaler C.* Dualities for abelian groups and modules// in: Rings, Modules, Algebras and Abelian Groups/ Lect. Notes Pure Appl. Algebra. Proc. Int. Algebraic Conf. — Venezia, 2002.

Е. А. Благовещенская
С.-Петербургский государственный технический университет
E-mail: kate@robotek.ru, kblag2002@yahoo.com

Современная математика и ее приложения. Том 13 (2004). С. 92–130

УДК 512.55

БАЗИСЫ ГРЁБНЕРА—ШИРШОВА, КОНФОРМНЫЕ АЛГЕБРЫ И ПСЕВДОАЛГЕБРЫ

© 2004 г. **Л. А. БОКУТЬ, П. С. КОЛЕСНИКОВ**

СОДЕРЖАНИЕ

1. Введение

Работа является в определенном смысле продолжением наших работ [16,17], опубликованных в томах, посвященных 60-летию А. В. Яковлева и А. В. Михалева соответственно. Мы рады, что настоящая работа публикуется в томе, посвященном 70-летию В. Н. Латышева.

Как и упомянутые предыдущие работы, эта работа явственно разбивается на две части, посвященные изучению «классических» классов алгебр и класса конформных (и псевдо) алгебр соответственно. В данной работе при изучении классических классов алгебр мы ограничиваемся случаем ассоциативных алгебр, более точно — (полу)групповыми алгебрами, а еще более точно — (полу)группами. Дело в том, что базис Грёбнера—Ширшова (БГШ) (полу)группы — это не что иное, как БГШ ее (полу)групповой алгебры (над любым полем). Нахождение БГШ (полу)группы приводит в силу CD-леммы (леммы о композиции—diamond леммы) к нормальной форме слов исходной (полу)группы, так называемой PBW-формы, восходящей на самом деле к теореме Пуанкаре—Биркгофа—Витта (см. ниже раздел 2). Эта кольцевая терминология (CD-лемма, PBW-форма), используемая в случае (полу)групп, подчеркивает то обстоятельство, что речь идет по существу о применении теоретико-кольцевого метода для изучения (полу)групп, представленных образующими и определяющими соотношениями.

Работа выполнена при поддержке Российского фонда фундаментальных исследований (проекты №№ 01–01–0063, 03–01–06048) и Совета по грантам президента РФ и государственной поддержке ведущих научных школ (проект НШ-2069.2003.1).

ISSN 1512–1712

Ярким примером такого подхода является анализ групп Новикова—Буна с неразрешимой проблемой равенства. Как известно, первые авторские анализы этих групп, сделанные П. С. Новиковым [25], а затем позднее В. В. Буном [51], основывались на изучении цепочек выводимостей в групповых исчислениях, т.е. были по существу логическими. Работа Дж. Бриттона [55] была признана как первый алгебраический теоретико-групповой анализ этих групп, точнее, группы Буна. Сейчас же мы даем чисто теоретико-кольцевой анализ групп Новикова—Буна, не использующий никаких сведений из теории групп (например, лемму Бриттона).

То же касается и анализа конструкции С. И. Адяна [2], дающей доказательство теоремы, позже названной теоремой Адяна—Рабина, о неразрешимости марковских свойств конечно определенных групп. Аналогично получается единственность нормальной формы Маркова—Ивановского—Артина в группе кос и все другие результаты первой части работы, касающиеся (полу)групп.

Во второй части мы продолжаем исследование конформных алгебр (и их обобщений — псевдоалгебр), начатое в [16,17]. Мы укажем простое соответствие между тождествами на псевдоалгебрах и многообразиями конформных алгебр. Это соответствие дает основание ввести определение многообразий псевдоалгебр.

Понятие псевдоалгебры позволяет с общих позиций рассматривать многие общие вопросы теории обычных и конформных алгебр. Именно, высокая степень сходства свойств обычных и конформных алгебр вызвана тем, что эти объекты являются частными случаями псевдоалгебр. Например, нетеровость ассоциативной обертывающей алгебры для конечномерной алгебры Ли сохраняется при переходе к конформным алгебрам, а также к псевдоалгебрам. Кроме того, для йордановых псевдоалгебр конечного типа можно построить аналог конструкции Титса—Кантора—Кёхера (ТКК) для вложения таких псевдоалгебр в лиевы. Эта конструкция приводит, в частности, к описанию простых йордановых псевдоалгебр конечного типа.

Как и в случае обычных алгебр, одним из основных приложений CD-леммы для ассоциативных конформных алгебр является исследование структуры универсальных обертывающих ассоциативных конформных алгебр для конформных алгебр Ли конечного типа. Мы также применяем CD-лемму для нахождения БГШ «минимальных» универсальных обертывающих для простых конформных супералгебр Ли серии W_N.

2. Определение и история

2.1. Краткая история. Метод, который сейчас называется методом базисов Грёбнера—Ширшова, был предложен в 1962 г. в работе А. И. Ширшова [26], посвященной алгебрам Ли (точнее, лиевским многочленам — элементам свободной алгебры Ли). Примерно в то же время аналогичные идеи для обычных (коммутативных) многочленов были открыты Б. Бухбергером в его диссертации (научный руководитель В. Грёбнер; см. [56, 57]).

Проблема, которую рассматривали А. И. Ширшов и Б. Бухбергер, состояла в описании элементов идеала I, порожденного некоторым множеством S свободной алгебры Ли или свободной коммутативной алгебры, соответственно. Идея решения этого вопроса состояла в пополнении S до некоторого специального базиса S^{comp} идеала I. (Здесь слово «базис» имеет то же значение, что и в теореме Гильберта о базисе.) Множество S^{comp} обладает следующим свойством: если $f \in I$, то $\bar{f} = a\bar{s}b$ для некоторого $s \in S^{\mathrm{comp}}$ (здесь $\bar{f}$ означает старший одночлен многочлена f относительно некоторой упорядоченности одночленов). Для нахождения искомого пополнения в [26] было введено понятие операции композиции $(f,g)_w$ многочленов f и g относительно слова (неопределенности) w. Тогда S^{comp} есть просто замыкание S относительно этой операции. Понятию композиции из [26] соответствует понятие s-многочлена из [57]. Процесс построения S^{comp} для множества лиевских многочленов S из [26] соответствует знаменитому алгоритму Бухбергера из [57]. Основная лемма из [26] (известная как лемма о композиции для лиевских многочленов) соответствует основной теореме из [57], которая известна теперь как теорема Бухбергера или основная теорема теории базисов Грёбнера.

В 1964 Х. Хиронака опубликовал фундаментальную работу [75], в которой развил по существу те же идеи, но для идеалов алгебры формальных степенных рядов, используя младшие члены

вместо старших. Он назвал свои базисы стандартными и этот термин широко используется в настоящее время.

На самом деле имеется еще один источник этих идей. Это diamond-лемма Ньюмена [99]. П. М. Кон был, возможно, первым, кто понял фундаментальное значение леммы Ньюмена в алгебре. Он использовал ее для изучения полугрупп [63,64] и алгебр [65]. В контексте универсальных алгебр П. М. Кон сформулировал общую лемму типа леммы Ньюмена еще в первом издании (1964) своей книги [66]. В частности, под влиянием П. М. Кона Л. А. Бокуть применил лемму Ньюмена для доказательства некоторых теорем о вложении полугрупп [3, 4] и групп [5]. Эти исследования, начатые Ньюменом и продолженные Коном, привели к diamond-лемме Бергмана [36], которая фактически эквивалентна аналогу леммы Ширшова о композиции для ассоциативных алгебр [14].

В контексте универсальных алгебр переписывающий алгоритм Кнута—Бендикса появился в работе [85]. Алгоритм Ширшова [26] и алгоритм Бухбергера [56,57] являются алгоритмами типа Кнута—Бендикса. Изложение этого алгоритма для полугрупп и групп, сделанное в [70], очень близко общей версии diamond-леммы Ньюмена [99] (см., например, [5]).

Другие исследования по БГШ (некоммутативным базисам Грёбнера, стандартным базисам) освещены в работах К. И. Бейдара, В. С. Мартиндейла III и А. В. Михалева [33], В. П. Гердта и В. В. Корняка [74], В. К. Харченко [83], В. Н. Латышева [23, 90–93], А. А. Михалева и Е. Васильевой [96], А. А. Михалева и А. А. Золотых [97], Т. Мора [98], В. Уфнаровского [107].

В данной работе мы изучаем БГШ для ассоциативных (групповых и полугрупповых) алгебр и для ассоциативных конформных алгебр. Напомним определения и основные результаты.

2.2. Базисы Грёбнера—Ширшова для (не конформных) алгебр и групп. Пусть $\mathcal{X}$ — линейно упорядоченное множество, $\Bbbk$ — поле, $\Bbbk\langle\mathcal{X}\rangle$ — свободная ассоциативная алгебра над $\mathcal{X}$ и $\Bbbk$. Зафиксируем на множестве слов $\mathcal{X}^*$ некоторый линейный порядок $>$ с условием минимальности, согласованный с произведением слов; таким образом, $\mathcal{X}^*$ становится вполне упорядоченной полугруппой. В этом случае любой многочлен $f \in \Bbbk\langle\mathcal{X}\rangle$, $f \neq 0$, имеет старшее слово $\bar{f}$. Скажем, что f *унитарный*, если $\bar{f}$ входит в f с коэффициентом 1. *Композицией пересечения* $(f,g)_w$ двух унитарных многочленов f и g относительно слова w такого, что $w = \bar{f}b = a\bar{g}$, $a, b \in \mathcal{X}^*$, $\deg(\bar{f}) + \deg(\bar{g}) > \deg(w)$, называется многочлен

$$(f,g)_w = fb - ag. \tag{2.2.1}$$

Композицией включения $(f,g)_w$ двух унитарных многочленов f и g, где $w = \bar{f} = a\bar{g}b$, называется многочлен

$$(f,g)_w = f - agb. \tag{2.2.2}$$

В последнем случае преобразование

$$f \mapsto (f,g)_w = f - agb \tag{2.2.3}$$

называется *исключением старшего слова* (ИСС) g в f.

В обоих случаях слово w называется *неопределенностью* для многочленов (соотношений) f и g.

Композиция $(f,g)_w$ называется *тривиальной* относительно $S \subset \Bbbk\langle\mathcal{X}\rangle$ (обозначение $(f,g)_w \equiv 0 \pmod{S,w}$), если

$$(f,g)_w = \sum \alpha_i a_i t_i b_i \quad \text{для некоторых} \quad t_i \in S, a_i, b_i \in \mathcal{X}^*, \quad a_i\bar{t}_i b_i < w.$$

В частности, если $(f,g)_w$ преобразуется в нуль с помощью ИСС S, то $(f,g)_w$ тривиальна относительно S. Для многочленов f_1 и f_2 пишем $f_1 \equiv f_2 \pmod{S,w}$, если $f_1 - f_2 \equiv 0 \pmod{S,w}$.

Определение 2.2.1. Подмножество S из $\Bbbk\langle\mathcal{X}\rangle$ называется *базисом Грёбнера—Ширшова* (БГШ), если любая композиция многочленов из S тривиальна относительно S.

Через $\Bbbk\langle\mathcal{X}|S\rangle$ обозначаем алгебру с порождающими $\mathcal{X}$ и определяющими соотношениями S, т.е. фактор-алгебру $\Bbbk\langle\mathcal{X}\rangle/(S)$, где (S) — идеал, порожденный S.

Как уже отмечалось, мы фиксируем полный полугрупповой порядок $\leqslant$ на множестве $\mathcal{X}^*$. Обычно это *deg-lex* порядок, т.е. два слова сравниваются сначала по степени, а потом лексикографически.

Используется также следующий порядок. Зафиксируем подмножество $\mathcal{Z} \subset \mathcal{X}$, $\mathcal{X} \setminus \mathcal{Z} = \mathcal{Y}$. Предположим, что $\mathcal{Y}^*$ снабжено полным полугрупповым порядком и что $\mathcal{Z}$ вполне упорядочено. Каждое слово $u \in \mathcal{X}^*$ имеет вид

$$u = u_0 z_1 \dots u_k z_k u_{k+1}, \quad u_i \in \mathcal{Y}^*, \quad z_i \in \mathcal{Z}.$$

Определим вес u по формуле

$$\operatorname{wt}(u) = (k, u_0, z_1, \dots, u_k, z_k, u_{k+1}).$$

Упорядочим веса лексикографически и положим

$$u \leqslant v \overset{\text{def}}{\iff} \operatorname{wt}(u) \leqslant \operatorname{wt}(v).$$

Легко видеть, что этот порядок является полным и полугрупповым. Мы называем его *башенным порядком*, поскольку впервые он появился в башнях HNN-расширений групп [5–8]. Башенный порядок совпадает с deg-lex порядком, если $\mathcal{Y} = \emptyset$. Мы будем использовать также «обратный» башенный порядок: разница заключается в том, что

$$u \leqslant v \overset{\text{def}}{\iff} \operatorname{inwt}(u) \leqslant \operatorname{inwt}(v),$$

где

$$\operatorname{inwt}(u) = (k, u_{k+1}, z_k, \dots, u_1, z_1, u_0).$$

Следующая лемма восходит к теореме Пуанкаре—Биркгофа—Витта (PBW), diamond-лемме Ньюмена [99], лемме о композиции Ширшова [26] (см. также [13, 14], где лемма о композиции сформулирована в современной форме для алгебр Ли и ассоциативных алгебр соответственно), теореме Бухбергера [56] (опубликована в [57]) и diamond-лемме Бергмана [36] (эта лемма была известна также П. М. Кону, см. выше).

Лемма о композиции—diamond лемма. *Множество S является базисом Грёбнера—Ширшова тогда и только тогда, когда множество*

$$\operatorname{PBW}(S) = \{u \in \mathcal{X}^* \mid u \neq a\bar{f}b \ \text{ для любого } \ f \in S\}$$

S-редуцированных слов образует линейный базис алгебры $\Bbbk\langle \mathcal{X} | S \rangle$.

Множество $\operatorname{PBW}(S)$ называется PBW-базисом рассматриваемой алгебры относительно ее БГШ S. Это отражает отмеченный выше факт, что лемма о композиции—diamond лемма (CD-лемма для краткости) восходит также к теореме Пуанкаре—Биркгофа—Витта. На самом деле теорема PBW является частным и едва ли не основным частным случаем CD-леммы, когда

$$S = \left\{ x_i x_j - x_j x_i - \sum_k \alpha_{ij}^k x_k \;\middle|\; i > j \right\},$$

где $[x_i x_j] = \sum\limits_k \alpha_{ij}^k x_k$, $i > j$, — таблица умножения некоторой алгебры Ли. В этом случае PBW-базис имеет вид

$$\operatorname{PBW}(S) = \{x_{i_1} x_{i_2} \dots x_{i_k} \mid i_1 \leqslant i_2 \dots \leqslant i_k\}.$$

Если подмножество S из $\Bbbk\langle \mathcal{X} \rangle$ не является БГШ, то можно добавить к S все нетривиальные композиции многочленов из S и продолжить этот процесс (бесконечное число раз) до тех пор пока не получится БГШ S^{comp}, содержащий S. Эта процедура называется алгоритмом Бухбергера—Ширшова [26, 56, 57].

БГШ S называется *минимальным* (или *редуцированным*), если любой $s \in S$ есть линейная комбинация $S \setminus \{s\}$-редуцированных слов. Любой идеал из $\Bbbk\langle \mathcal{X} \rangle$ имеет единственный минимальный БГШ.

Если S — множество «полугрупповых соотношений» (т.е. многочленов вида $u - v$, где $u, v \in \mathcal{X}^*$), то любая нетривиальная композиция многочленов из S имеет такой же вид. В результате множество S^{comp} также состоит из полугрупповых соотношений.

Пусть $A = \operatorname{sgr}\langle \mathcal{X} | S \rangle$ — полугруппа. Тогда S — подмножество в $\Bbbk\langle \mathcal{X} \rangle$, и можно найти БГШ S^{comp}. Последнее множество не зависит от $\Bbbk$ и состоит из полугрупповых соотношений. Мы называем S^{comp} БГШ полугруппы A. Это то же самое, что БГШ полугрупповой алгебры $\Bbbk A = \Bbbk\langle \mathcal{X} | S \rangle$.

2.3. Базисы Грёбнера—Ширшова для ассоциативных конформных алгебр. Приведем определение конформной алгебры, в целом следуя [78]. Всюду ниже $\Bbbk$ означает поле нулевой характеристики, $\Bbbk[D]$ — алгебра многочленов от одной переменной над $\Bbbk$.

Определение 2.3.1. Левый $\Bbbk[D]$-модуль C, снабженный семейством $\Bbbk$-билинейных операций

$$(\cdot\ {}_n\ \cdot) : C \otimes C \to C, \quad n \in \{0, 1, 2, \dots\},$$

называется *конформной алгеброй*, если выполнены следующие условия (аксиомы конформной алгебры):

(C1) для любых $a, b \in C$ существует $N \geqslant 0$ такое, что $a\ {}_n\ b = 0$ для $n \geqslant N$;
(C2) $Da\ {}_n\ b = -na\ {}_{n-1}\ b$, $a\ {}_n\ Db = D(a\ {}_n\ b) + na\ {}_{n-1}\ b$.

Соотношения (C1) и (C2) называются локальностью и полуторалинейностью соответственно. Функция локальности $N(a, b)$ определяется в соответствии с (C1):

$$N(a, b) := \min\{N \geqslant 0 \mid a\ {}_n\ b = 0,\ n \geqslant N\}.$$

Алгебраическим свойствам объектов, определенных аксиомами (C1), (C2), посвящено большое число работ (см, например, [67, 78–80, 100, 101, 108]).

Определение 2.3.1 является формализацией следующей конструкции. Пусть A — произвольная (не обязательно ассоциативная) алгебра. Рассмотрим формальные степенные ряды $a(z), b(z) \in A[[z, z^{-1}]]$ и определим для них операцию n-произведения [69] формулой

$$(a\ {}_n\ b)(z) = \operatorname{Res}_w a(w)b(z)(w - z)^n, \quad n \geqslant 0, \tag{2.3.1}$$

где Res_w означает коэффициент при w^{-1} формального степенного ряда от z, w. Тогда условие локальности (C1) эквивалентно равенству

$$a(w)b(z)(w - z)^N = 0,$$

соотношение (C2) выполняется для $D = d/dz$. В случае алгебр Ли семейство n-произведений $a\ {}_n\ b$ описывает сингулярную часть расширенного операторного произведения (operator product expansion, OPE) [35] двух локальных рядов $a(z)$, $b(z)$.

Для любой конформной алгебры в смысле определения 2.3.1 можно построить обычную алгебру $A = \operatorname{Coeff} C$ такую, что C содержится в $A[[z, z^{-1}]]$ как подпространство попарно локальных рядов с n-произведением (2.3.1). Такая алгебра A определена единственным образом с точностью до изоморфизма; она называется *алгеброй коэффициентов* [80, 100] конформной алгебры C. Чтобы построить $A = \operatorname{Coeff} C$, достаточно рассмотреть пространство

$$A = \Bbbk[t, t^{-1}] \otimes_H C,$$

где $H = \Bbbk[D]$ и D действует на $\Bbbk[t, t^{-1}]$ по правилу $t^n D = -nt^{n-1}$. Обозначим $t^n \otimes_H a$ через $a(n)$, $a \in C$, $n \in \mathbb{Z}$. Умножение на A определяется по формуле [100]

$$a(n)b(m) = \sum_{s \geqslant 0} \binom{n}{s} (a\ {}_s\ b)(n + m - s).$$

Поскольку любая конформная алгебра C вкладывается в $\operatorname{Coeff} C[[z, z^{-1}]]$, алгебры коэффициентов являются важным инструментом исследования конформных алгебр.

Определение 2.3.2 (см. [100])**.** Пусть Ω — некоторое многообразие алгебр. Конформная алгебра C считается принадлежащей многообразию Ω тогда и только тогда, когда $\operatorname{Coeff} C \in \Omega$.

В [43, 44] доказан аналог CD-леммы для ассоциативных конформных алгебр. Первый шаг на пути построения теории БГШ и доказательства CD-леммы состоит в том, чтобы зафиксировать некоторый подходящий базис в свободной алгебре (так, например, в [26] для свободной алгебры Ли выбран базис, состоящий из слов Линдона—Ширшова).

Рассмотрим свободную ассоциативную конформную алгебру $C(B, N)$, порожденную множеством B с функцией локальности N на B (т. е., $N(a, b) = N$ для всех $a, b \in B$) [42, 100]. Линейный базис

алгебры $C(B,N)$ состоит из так называемых нормальных слов. Здесь мы называем нормальным слово, имеющее вид

$$[u] = [a_{1\ n_1}\ a_{2\ n_2} \dots a_{k\ n_k}\ D^i a_{a_{k+1}}], \tag{2.3.2}$$

где $a_j \in B$, $0 \leqslant n_j < N$, $i = \operatorname{ind}(u) \geqslant 0$, $|u| = k+1 \geqslant 1$ [42]. Здесь и ниже $[u]$ означает *правонормированную* расстановку скобок:

$$[u] = (a_{1\ n_1}\ (a_{2\ n_2} \dots (a_{k\ n_k}\ D^i a_{k+1}) \dots)).$$

Слово без скобок

$$u = a_{1\ n_1}\ a_{2\ n_2} \dots a_{k\ n_k}\ D^i a_{k+1}$$

называется ассоциативным нормальным словом. Хотя $C(B,N)$ и называется ассоциативной, требуется сохранять расстановку скобок на $[u]$, т.е. $C(B,N)$ на самом деле «неассоциативна».

Определим вес

$$\operatorname{wt}(u) = (n_1, a_1, \dots, n_k, a_k, a_{k+1}, i).$$

Множество всех ассоциативных нормальных слов образует «тестовую Ω-полугруппу» T с нулем, в которой

$$(u\ _n\ v)\ _m\ w = u\ _n\ (v\ _m\ w), \quad u,v,w \in T, \quad m,n \in \mathbb{Z}_+,$$

где $\Omega = \{(\cdot\ _n\ \cdot) \mid n \in \mathbb{Z}_+\}$.

Далее, положим $[u] > [v]$, если $\operatorname{wt}(u) > \operatorname{wt}(v)$ в смысле порядка deg-lex. Нормальное слово $[u]$ называется *D-свободным*, если $\operatorname{ind}(u) = 0$; конформный многочлен $f \in C(B,N)$ называется *D-свободным*, если все мономы, входящие в f, являются D-свободными. Под конформными многочленами мы понимаем элементы из $C(B,N)$.

Определение 2.3.3. *Композицией* конформных многочленов f, g мы называем элемент, полученный при помощи одной из следующих операций.

1) Если g — D-свободный многочлен и $w = \bar{f} = u\ _n\ \bar{g}\ _m\ v$ для некоторых $u,v \in T$, u — D-свободное слово, то многочлен

$$(f,g)_w = f - [u\ _n\ g\ _m\ v]$$

называется *композицией включения*.

2) Если $w = \bar{f} = u\ _n\ \bar{g}D^i$ для некоторого D-свободного $u \in T$, то

$$(f,g)_w = f - [u\ _n\ D^i g]$$

называется *композицией правого включения*.

3) Если f — D-свободный многочлен и $w = \bar{f}\ _m\ v = u\ _n\ \bar{g}$ для некоторых $u,v \in T$ таких, что u — D-свободный, $|\bar{f}| + |\bar{g}| > |w|$, то

$$(f,g)_w = [f\ _m\ v] - [u\ _n\ g]$$

называется *композицией пересечения*.

4) Если $w = \bar{f}D^i = u\ _n\ \bar{g}$ для некоторого D-свободного $u \in T$, то

$$(f,g)_w = D^i f - [u\ _n\ g]$$

называется *композицией правого пересечения*.

5) Если $a \in B$ и $n \geqslant N$, то $a\ _n\ f$ называется *композицией левого умножения*.

6) Если f не D-свободное, $a \in B$, $n \geqslant 0$, то $f\ _n\ a$ называется *композицией правого умножения*.

Преобразование $f \mapsto (f,g)_w$, где $(f,g)_w$ — композиция вида 1) или 2), является аналогом ИСС в случае обычных алгебр.

Пусть S — подмножество (унитарных) многочленов из $C(B,N)$. Как и в случае обычных алгебр, положим $(f,g)_w \equiv 0 \pmod{S,w}$, если

$$(f,g)_w = \sum_{i\in I} \alpha_i [u_{i\ n_i}\ s_{i\ m_i}\ v_i] + \sum_{j\in J} \alpha_j [u_{j\ n_j}\ D^{l_j} s_j], \tag{2.3.3}$$

где $I \cap J = \emptyset$, $s_i, s_j \in S$, $[u_{i\ n_i}\ s_{i\ m_i}\ v_i]$, $[u_{j\ n_j}\ D^{l_j} s_j]$ — нормальные S-слова (т.е. $s_i, s_j \in S$, s_i $(i \in I)$ D-свободны, $u_i, v_i, u_j \in T$, u_i, u_j D-свободны, $0 \leqslant n_i, m_i, n_j < N$) и

$$u_{i\ n_i}\ \bar{s}_{i\ m_i}\ v_i < w, \quad u_{j\ n_j}\ \bar{s}_j D^{l_j} < w$$

для всех $i \in I$, $j \in J$. Кроме того, для D-свободных многочленов f и g множество J должно быть пустым.

Далее, композиция вида $h = a\ _n\ f$ или $g\ _m\ a$, тривиальна по модулю S, если h может быть представлено в виде (2.3.3) таким образом, что

$$|u_{i\ n_i}\ \bar{s}_{i\ m_i}\ v_i| \leqslant |\bar{h}|, \quad |u_{j\ n_j}\ \bar{s}_j D^{l_j}| \leqslant |\bar{h}|$$

для $i, j \in J$. Если $h = a\ _n\ f$ для D-свободного f или $h = g\ _m\ a$, то множество J должно быть пустым.

Определение 2.3.4. Подмножество $S \subset C(B, N)$ называется базисом Грёбнера—Ширшова (БГШ), если любая композиция многочленов из S тривиальна по модулю S.

CD-лемма (для ассоциативных конформных алгебр)**.** *Пусть S — базис Грёбнера—Ширшова в $C(B, N)$. Тогда* $\mathrm{PBW}(S)$ *является линейным базисом ассоциативной конформной алгебры $C(B, N|S)$, порожденной множеством B с определяющими соотношениями S относительно* (*постоянной*) *функции локальности N.*

В случае конформных алгебр множество $\mathrm{PBW}(S)$ состоит из таких $[u]$, что $u \neq v\ _n\ \bar{s}\ _m\ w$, $s \in S$, s является D-свободным, и $u \neq v\ _n\ \bar{s}D^i$, $s \in S$. Здесь u, v, w — нормальные ассоциативные слова, запись $\bar{s}D^i$ означает, что D^i применяется к последней букве слова $\bar{s}$.

3. Базисы Грёбнера—Ширшова для групп и полугрупп

3.1. Группы Новикова—Буна. Такое название было предложено Б. А. Трахтенбротом [106] для групп Новикова, групп Буна и их вариаций.

Первый пример группы с неразрешимой проблемой равенства был построен П. С. Новиковым [25]. Несколько лет спустя более простой пример предложил В. В. Бун [51]. В данном разделе мы рассмотрим эту группу Буна, следуя [48].

По машине Тьюринга T определим «специальную» полугруппу, порожденную множеством

$$\{s_b \mid b \in B\} \cup \{q_a \mid a \in A\}$$

(здесь A, B — некоторые конечные упорядоченные множества) с определяющими соотношениями

$$\Sigma_i = \Gamma_i, \quad 1 \leqslant i \leqslant N,$$

где

$$\Sigma_i = \Sigma_{i1} q_{n_i} \Sigma_{i2}, \quad \Gamma_i = \Gamma_{i1} q_{m_i} \Gamma_{i2},$$

и $\Sigma_{i1}, \Sigma_{i2}, \Gamma_{i1}, \Gamma_{i2}$ — положительные слова в алфавите $\{s_b \mid b \in B\}$.

Пусть q — выделенная буква (заключительное состояние машины T) множества $\{q_a \mid a \in A\}$. Специальная проблема равенства $(?\Sigma = q)$ в этой полугруппе эквивалентна проблеме остановки машины T. Обозначим полученную полугруппу снова через T.

Группой Буна $G(T, q)$ пары (T, q) называется группа, порожденная множеством

$$\mathcal{X} \cup \mathcal{S} \cup \mathcal{L} \cup \mathcal{Q} \cup \{t\} \cup \{k\},$$
$$\mathcal{X} = \{x, y\}, \quad \mathcal{S} = \{s_b \mid b \in B\},$$
$$\mathcal{L} = \{l_i, r_i \mid 1 \leqslant i \leqslant N\}, \quad \mathcal{Q} = \{q_a \mid a \in A\}$$

с определяющими соотношениями

$$y^2 s_b = s_b y, \quad x s_b = s_b x^2, \tag{3.1.1}$$
$$s_b l_i = y l_i y s_b, \quad s_b x r_i x = r_i s_b, \tag{3.1.2}$$
$$\Sigma_i = l_i \Gamma_i r_i, \tag{3.1.3}$$
$$l_i t = t l_i, \quad yt = ty, \tag{3.1.4}$$

$$r_ik = kr_i, \quad xk = kx, \quad q^{-1}tqk = kq^{-1}tq, \tag{3.1.5}$$

где $b \in B$, $a \in A$, $1 \leqslant i \leqslant N$.

Определим башню HNN-расширений G_i, $0 \leqslant i \leqslant 5$, где $G_5 = G(T, q)$. На каждом шаге мы добавляем к построенной группе новые буквы, считая что все они (как положительные, так и отрицательные) больше букв старого алфавита. Кроме того, на каждом шаге мы используем башенную упорядоченность групповых слов.

Группа G_0 — это свободная группа, порожденная $\mathcal{X}$. Упорядочим порождающие

$$x > x^{-1} > y > y^{-1}.$$

Минимальный БГШ группы G_0 состоит из тривиальных соотношений, т.е.

$$xx^{-1} = 1, \quad x^{-1}x = 1, \quad \ldots$$

(тривиальные соотношения замкнуты относительно композиций!). Определим на словах G_0 deg-lex порядок.

Пусть G_1 — расширение G_0 множеством $\mathcal{S}$ и соотношениями (3.1.1). Положим $s_b > s_b^{-1} > s_{b_1}$ для $b > b_1$. Нетрудные вычисления композиций показывают, что верна следующая теорема.

Теорема 3.1.1. *Минимальный БГШ G_1 состоит из тривиальных соотношений G_1 и следующих соотношений*:

$$\begin{aligned} y^2s_b &= s_by, \qquad y^{-1}s_b = ys_by^{-1}, \qquad y^{-1}s_b^{-1} = s_b^{-1}y^{-2}, \qquad ys_b^{-1} = s_b^{-1}y^2, \\ xs_b &= s_bx^2, \qquad x^{-1}s_b = s_bx^{-2}, \qquad xs_b^{-1} = x^{-1}s_b^{-1}x, \qquad x^{-2}s_b^{-1} = s_b^{-1}x^{-1}, \end{aligned} \tag{3.1.6}$$

где $b \in B$.

Для построения G_2 добавим к G_1 множество образующих $\mathcal{L}$ с естественным порядком (как раньше) и соотношения (3.1.2).

Теорема 3.1.2. *Минимальный БГШ группы G_2 состоит из соотношений* (3.1.6)*, тривиальных соотношений и следующих соотношений*:

$$\begin{aligned} s_bV(x^2,y)l_i &= V(x,y^2)yl_iys_b, & s_b^{-1}V(x,y^2)yl_i &= V(x^2,y)l_is_b^{-1}y^{-1}, \\ s_bV(x^2,y)l_i^{-1} &= V(x^2,y)y^{-1}l_i^{-1}y^{-1}s_b, & s_b^{-1}\overline{V(x,y^2)y^{-1}}l_i^{-1} &= V(x^2,y)l_i^{-1}s_b^{-1}y, \\ s_b\overline{V(x^2,y)x}r_ix &= V(x,y^2)r_is_b, & s_b^{-1}V(x,y^2)r_i &= V(x^2,y)xr_ixs_b^{-1}, \\ s_b\overline{V(x^2,y)x^{-1}}r_i^{-1} &= V(x,y^2)r_i^{-1}s_bx, & s_b^{-1}V(x,y^2)r_i^{-1} &= \overline{V(x^2,y)x^{-1}}r_i^{-1}x^{-1}s_b^{-1}, \end{aligned} \tag{3.1.7}$$

где $b \in B$, $1 \leqslant i \leqslant N$, все слова V несократимы и $\overline{W}$ означает несократимое слово, равное W.

Определим группу G_3. Добавим к G_2 новые образующие $\mathcal{Q}$ с естественным порядком и соотношения (3.1.3).

Позднее мы используем следующие формулы:

$$V(y^{-1}s_b) = ySy^{-1}, \qquad V(ys_b) = y^{-1}Sy,$$

где S — проекция V на алфавит $\mathcal{S}$.

Теорема 3.1.3. *Минимальный БГШ группы G_3 состоит из соотношений* (3.1.6), (3.1.7)*, тривиальных соотношений и следующих соотношений*:

$$\begin{aligned} l_i\overline{y^{-1}Sy\Gamma_{i1}}q_{m_i} &= \overline{ySy^{-1}\Sigma_{i1}}q_{n_i}\Sigma_{i2}r_i^{-1}\Gamma_{i2}^{-1}, \\ l_i^{-1}\overline{ySy^{-1}\Sigma_{i1}}q_{n_i} &= \overline{y^{-1}Sy\Gamma_{i1}}q_{m_i}\Gamma_{i2}r_i\Sigma_{i2}^{-1}, \\ r_i^{-1}\overline{xSx^{-1}\Gamma_{i2}^{-1}}q_{m_i}^{-1} &= \overline{x^{-1}Sx\Sigma_{i2}^{-1}}q_{n_i}^{-1}\Sigma_{i1}^{-1}l_i\Gamma_{i1}, \\ r_i^{-1}\overline{xSx^{-1}\Sigma_{i2}^{-1}}q_{n_i}^{-1} &= \overline{x^{-1}Sx\Gamma_{i2}^{-1}}q_{m_i}^{-1}\Gamma_{i1}^{-1}l_i^{-1}\Sigma_{i1}, \end{aligned} \tag{3.1.8}$$

где $1 \leqslant i \leqslant N$, все слова S несократимы и, например, $\overline{y^{-1}Sy\Gamma_{i1}}$ означает редуцированную или PBW форму $y^{-1}Sy\Gamma_{i1}$ (после исключения старших слов соотношений БГШ группы G_1).

Определим группу G_4. Добавим к G_3 букву t и соотношения (3.1.4). Как обычно, $t > t^{-1}$.

Теорема 3.1.4. *БГШ группы G_4 состоит из соотношений* (3.1.6)–(3.1.8)*, тривиальных соотношений и равенств*

$$\begin{aligned} y^\delta t^\varepsilon &= t^\varepsilon y^\delta, \\ l_i\overline{y^{-1}SyY}t^\varepsilon &= \overline{ySy^{-1}}t^\varepsilon l_i Y, \\ l_i^{-1}\overline{ySy^{-1}Y}t^\varepsilon &= y^{-1}Syt^\varepsilon l_i^{-1}Y, \end{aligned} \tag{3.1.9}$$

где $\varepsilon, \delta = \pm 1$, $1 \leqslant i \leqslant N$, S — неприводимые слова в алфавите $\mathcal{S}$ и Y — степени y.

Наконец, определим группу $G_5 = G(T, q)$. Добавим к G_4 букву k и соотношения (3.1.5).

Теорема 3.1.5. *БГШ группы G_5 состоит из соотношений* (3.1.6)–(3.1.9)*, тривиальных соотношений и следующих соотношений*:

$$\begin{aligned} x^\delta k^\varepsilon &= k^\varepsilon x^\delta, \\ r_i\overline{x^{-1}SxX}k^\varepsilon &= \overline{xSx^{-1}}k^\varepsilon r_i X, \\ r_i^{-1}\overline{xSx^{-1}X}k^\varepsilon &= \overline{x^{-1}Sx}k^\varepsilon r_i^{-1}X, \\ t^\delta\overline{V(l_i,y)qW(r_i,x)}k^\varepsilon &= V(l_i,y)qk^\varepsilon q^{-1}t^\delta qW(r_i,x). \end{aligned} \tag{3.1.10}$$

где $\varepsilon, \delta = \pm 1$, $1 \leqslant i \leqslant N$, $S = S(s_b), V(l_i, y), W(r_i, x)$ — несократимые слова X — степени x.

Следствие 3.1.6. *Множество* $\mathrm{PBW}(S_5)$ *образует линейный базис групповой алгебры $\Bbbk G(T, q)$, т.е. множество нормальных форм элементов группы Буна $G(T, q)$.* $\mathrm{PBW}(S_5)$ *— это не что иное как стандартный базис* (*стандартная нормальная форма*) *группы $G(T, q)$, построенная в* [6, 7] (*см. также* [46]).

Следствие 3.1.7 (ср. с [103])**.** *Проблема равенства для $G(T, q)$* (*алгоритмически*) *неразрешима, если неразрешима специальная проблема равенства для T* (*т.е. проблема остановки для машины Тьюринга T*).

Следствие 3.1.6 дает новое доказательство (см. [6, 7, 46]) следующей теоремы [28, 52, 62]. Ее первоначальные доказательства были довольно сложными.

Теорема 3.1.8. *Проблема равенства для группы $G(T, q)$ эквивалентна в смысле общей* (*тьюринговой*) *сводимости специальной проблеме равенства в специальной полугруппе T.*

3.2. Расширение Адяна. В своей знаменитой работе [1] С. И. Адян доказал алгоритмическую нераспознаваемость марковских свойств конечно определенных групп. Основным инструментом доказательства была конструкция некоторого расширения группы Новикова с неразрешимой проблемой равенства. Основная трудность работы С. И. Адяна заключалась в доказательстве вложимости группы Новикова в построенную группу.

В этом пункте мы изложим подход к анализу конструкции С. И. Адяна на основе БГШ [41]. На самом деле, нам не нужно приводить оригинальную конструкцию С. И. Адяна. Достаточно только заметить, что эта конструкция удовлетворяет условиям следующего определения.

Определение 3.2.1. Пусть G — группа с 4 независимыми элементами q_0, a_0, a, a_1, т.е. подгруппа $F_4 = \langle\Sigma\rangle \subset G$, $\Sigma = \{q_0, a_0, a, a_1\}$ свободно порождена этими элементами. *Расширением Адяна* группы G с фиксированной свободной подгруппой F_4 мы называем следующую группу (которую мы представляем для удобства как полугруппу):

$$A(G, F_4) = \langle G, q, q^{-1} \mid q_0 q = q a_0,\ a_1 q a = q a_1 q^{-1},\ q^\varepsilon q^{-\varepsilon} = 1,\ \varepsilon = \pm 1\rangle. \tag{3.2.1}$$

Вполне упорядочим множество G следующим образом. Введем deg-lex порядок на F_4 с помощью

$$q_0^{-1} < q_0 < a_0^{-1} < a_0 < a^{-1} < a < a_1^{-1} < a_1.$$

Пусть

$$G = F_4 \dot\cup U, \quad U = \{u_i \mid i \in I\},$$

где I — вполне упорядоченное множество, и положим $u_i < u_j$, если $i < j$. Наконец, будем считать, что любая буква Σ меньше любой буквы u_i, $i \in I$.

Тогда G можно представить как группу с порождающими

$$\mathcal{Y} = (\Sigma \cup \Sigma^{-1}) \dot\cup U$$

и определяющими соотношениями

$$\begin{aligned} &u_i u_j = w, && w \in F_4 \cup U, && i,j \in I; \\ &u_i c = u_j, && cu_i = u_k, && i,j,k \in I; \\ &c^{-1}c = 1, && cc^{-1} = 1, && c \in \Sigma. \end{aligned} \tag{3.2.2}$$

Эти равенства определяют умножение в G единственным образом; в частности, поскольку $cu_i, u_i c \notin F_4$, эти произведения лежат в U.

В дальнейшем мы будем обозначать для краткости правые части равенств (3.2.2) через $\overline{u_i u_j}$, $\overline{u_i c}$, $\overline{cu_i}$, соответственно.

Группа $A(G, F_4)$ порождается множеством $\mathcal{X} = \mathcal{Y} \dot\cup \{q, q^{-1}\}$ и определяющими соотношениями (3.2.1), (3.2.2). Определим башенный порядок слов алфавита $\mathcal{X}$ с выделенным подмножеством $\mathcal{Z} = \{q, q^{-1}\}$, $q > q^{-1}$, (см. раздел 2).

Введем обозначения

$$\begin{aligned} &\mathcal{A}_q = q_0^n = \mathcal{B}_{q^{-1}}, && \mathcal{B}_q = a_0^n = \mathcal{A}_{q^{-1}}, \\ &a_q = q_0^\delta = b_{q^{-1}}, && b_q = a_0^\delta = a_{q^{-1}}, \quad \delta = \pm 1, \end{aligned}$$

где число n предполагается одним и тем же во всех $\mathcal{A}_{q^\varepsilon}$, $\mathcal{B}_{q^\varepsilon}$ ($\varepsilon = \pm 1$), входящих в одно и то же равенство.

Найдем сначала БГШ группы $A(G, F_4)$ для случая $G = F_4$ (т.е. $U = \emptyset$).

Теорема 3.2.2. *Пусть $A(F_4) = A(F_4, F_4)$, где $F_4 = \langle q_0, a_0, a, a_1 \rangle$. Тогда БГШ группы $A(F_4)$ состоит из тривиальных соотношений и следующих соотношений*:

$$a_{q^\varepsilon} q^\varepsilon = q^\varepsilon b_{q^\varepsilon}, \tag{3.2.3}$$

$$q^\varepsilon \mathcal{B}_{q^\varepsilon} a_1 q^{-\varepsilon} = \mathcal{A}_{q^\varepsilon} a_1 q^\varepsilon a^\varepsilon, \tag{3.2.4}$$

$$q^\varepsilon \mathcal{B}_{q^\varepsilon} a_1^{-1} q^{-\varepsilon} = \mathcal{A}_{q^\varepsilon} a^{-\varepsilon} q^{-\varepsilon} a_1^{-1}, \tag{3.2.5}$$

$$q^\varepsilon \mathcal{B}_{q^\varepsilon} a^\varepsilon q^\varepsilon = \mathcal{A}_{q^\varepsilon} a_1^{-1} q^\varepsilon a_1, \tag{3.2.6}$$

$$a_1 q^\varepsilon a^\varepsilon \mathcal{B}_{q^{-\varepsilon}} a_1^{-1} q^\varepsilon = q^\varepsilon a_1 \mathcal{A}_{q^{-\varepsilon}} a^\varepsilon q^\varepsilon a_1^{-1}, \tag{3.2.7}$$

$$a_1 q^\varepsilon a^\varepsilon \mathcal{B}_{q^{-\varepsilon}} a^{-\varepsilon} q^{-\varepsilon} = q^\varepsilon a_1 \mathcal{A}_{q^{-\varepsilon}} a_1^{-1} q^{-\varepsilon} a_1, \tag{3.2.8}$$

$$a_1 q^\varepsilon a^\varepsilon \mathcal{B}_{q^{-\varepsilon}} a_1 q^\varepsilon = q^\varepsilon a_1 \mathcal{A}_{q^{-\varepsilon}} a_1 q^{-\varepsilon} a^{-\varepsilon}, \tag{3.2.9}$$

$$a^{-\varepsilon} q^{-\varepsilon} a_1^{-1} \mathcal{B}_{q^{-\varepsilon}} a_1 q^\varepsilon = q^\varepsilon a_1^{-1} \mathcal{A}_{q^{-\varepsilon}} a_1 q^{-\varepsilon} a^{-\varepsilon}, \tag{3.2.10}$$

$$a^{-\varepsilon} q^{-\varepsilon} a_1^{-1} \mathcal{B}_{q^{-\varepsilon}} a_1^{-1} q^\varepsilon = q^\varepsilon a_1^{-1} \mathcal{A}_{q^{-\varepsilon}} a^\varepsilon q^\varepsilon a_1^{-1}, \tag{3.2.11}$$

$$a^{-\varepsilon} q^{-\varepsilon} a_1^{-1} \mathcal{B}_{q^{-\varepsilon}} a^{-\varepsilon} q^{-\varepsilon} = q^\varepsilon a_1^{-1} \mathcal{A}_{q^{-\varepsilon}} a_1^{-1} q^{-\varepsilon} a_1, \tag{3.2.12}$$

$$a_1^{-1} q^\varepsilon a_1 \mathcal{B}_{q^\varepsilon} a_1 q^{-\varepsilon} = q^\varepsilon a^\varepsilon \mathcal{A}_{q^\varepsilon} a_1 q^\varepsilon a^\varepsilon, \tag{3.2.13}$$

$$a_1^{-1} q^\varepsilon a_1 \mathcal{B}_{q^\varepsilon} a_1^{-1} q^{-\varepsilon} = q^\varepsilon a^\varepsilon \mathcal{A}_{q^\varepsilon} a^{-\varepsilon} q^{-\varepsilon} a_1^{-1}, \tag{3.2.14}$$

$$a_1^{-1} q^\varepsilon a_1 \mathcal{B}_{q^\varepsilon} a^\varepsilon q^\varepsilon = q^\varepsilon a^\varepsilon \mathcal{A}_{q^\varepsilon} a_1^{-1} q^\varepsilon a_1. \tag{3.2.15}$$

Поясним, что соотношения (3.2.3)–(3.2.6) являются композицией соотношений (3.2.1) и тривиальных соотношений. Другие соотношения суть композиции пересечения этих. Например, (3.2.7) есть композиция пересечения (3.2.4) и (3.2.5). Для доказательства теоремы нужно установить, что все композиции соотношений (3.2.3)–(3.2.15) тривиальны. Это делается прямыми вычислениями.

Рассмотрим теперь общий случай $A(G, F_4)$ для любой группы $G \supset F_4$. Для построения БГШ группы $A(G, F_4)$ мы должны дополнить соотношения (3.2.3)–(3.2.15), (3.2.2) всеми нетривиальными композициями.

Например, композиция (3.2.3)

$$\mathcal{A}_{q^\varepsilon} q^\varepsilon = q^\varepsilon \mathcal{B}_{q^\varepsilon}$$

с соотношениями группы G

$$u\mathcal{A}_{q^\varepsilon} = \overline{u\mathcal{A}_{q^\varepsilon}}, \quad u \in U, \tag{3.2.16}$$

имеет следующий вид:

$$\overline{u\mathcal{A}_{q^\varepsilon}} q^\varepsilon = u q^\varepsilon \mathcal{B}_{q^\varepsilon}, \quad \overline{u\mathcal{A}_{q^\varepsilon}} > u. \tag{3.2.17}$$

Далее, соотношения (3.2.7) имеют нетривиальные композиции с соотношениями (3.2.17). Эти композиции по модулю (3.2.16), (3.2.17) имеют вид

$$\overline{u\mathcal{A}_{q^\varepsilon} a_1 \mathcal{A}_{1q^\varepsilon}} q^\varepsilon \mathcal{B}_{1q^\varepsilon}^{-1} a^\varepsilon \mathcal{B}_{2q^{-\varepsilon}} a_1^{-1} q^\varepsilon = u q^\varepsilon \mathcal{B}_{q^\varepsilon} a_1 \mathcal{A}_{2q^{-\varepsilon}} a^\varepsilon q^\varepsilon a_1^{-1}, \tag{3.2.18}$$

где мы используем обозначения $\mathcal{A}_{iq^\varepsilon}$, $i = 1, 2$, чтобы различить слова с различными n.

Теорема 3.2.3. *БГШ группы $A(G, F_4)$ состоит из соотношений группы G, соотношений группы $A(F_4)$* (3.2.3)–(3.2.15)*, вместе с соотношениями* (3.2.17), (3.2.18) *и аналогичными им для* (3.2.8)–(3.2.15).

Очевидно, $\mathrm{PBW}(A(G, F_4)) \supset G$, так что из CD-леммы и теоремы 3.2.3 вытекает следующее утверждение.

Следствие 3.2.4. *Группа G является подгруппой группы $A(G, F_4)$.*

3.3. Группы Кокстера и полугруппы Артина. В этом разделе мы рассмотрим группы Кокстера типов A_l, B_l, D_l (см., например, [18,76]), как это сделано в [47]. Все эти группы определены с помощью порождающих элементов и определяющих соотношений. Поэтому возникает естественная задача найти БГШ этих групп.

Рассмотрим группы Кокстера. Пусть $S = \{s_1, \ldots, s_l\}$ — конечное множество. Симметрическая $(l \times l)$-матрица $M = (m_{ij})$ над натуральными числами с ∞ называется *матрицей Кокстера*, если $m_{ii} = 1$, $2 \leqslant m_{ij} \leqslant \infty$ для $i \neq j$. Тогда следующее полугрупповое представление фактически задает группу, которая называется группой Кокстера $W = W(M)$:

$$W = W(M) = \mathrm{sgr}\langle S \mid (s_i s_j)^{m_{ij}} = 1,\ 1 \leqslant i, j \leqslant l,\ m_{ij} \neq \infty \rangle.$$

Задача состоит в том, чтобы найти БГШ для любой группы Кокстера W.

Как было указано выше, в [47] эта задача решена для групп Кокстера типов A_l, B_l, D_l, для $W(M)$ с $m_{ij} = 2$ или ∞ при $i \neq j$, а также для $W(M)$ с $m_{ij} \geqslant 3$ при $i \neq j$. Мы также сформулируем общую гипотезу о БГШ любой группы Кокстера. Это будет сделано в контексте частично коммутативных алгебр (ср. с [68]). Вид найденных БГШ групп Кокстера типов A_l, B_l, D_l, а также указанных выше двух семейств групп Кокстера подтверждает эту гипотезу.

Группа Кокстера A_l порождается элементами $s_1, \ldots, s_l$ с определяющими соотношениями

$$\begin{aligned} &s_i^2 = 1, && \\ &s_i s_j = s_j s_i, && i - j > 1, \\ &s_{i+1} s_i s_{i+1} = s_i s_{i+1} s_i, && 1 \leqslant i \leqslant l - 1. \end{aligned} \tag{3.3.1}$$

Зафиксируем deg-lex порядок слов от s_i, $i = 1, \ldots, l$. Положим

$$s_{ij} = s_i s_{i-1} \cdots s_j, \quad i > j; \qquad s_{ii} = s_i, \quad s_{ii+1} = 1.$$

Легко заметить, что

$$s_{i+1j} s_{i+1} = s_i s_{i+1j}, \quad 1 \leqslant j < i. \tag{3.3.2}$$

Эти соотношения вместе с нормальной формой (3.3.3) были найдены еще А. А. Марковым [27] в 1945 г. (см. теорему 3.4.4 ниже). Мы отождествляем соотношение $u = v$ с многочленом $u - v$.

Используя исключение старших слов соотношений (3.3.1), (3.3.2), любое слово от S можно представить в виде

$$s_{1j_1} s_{2j_2} \cdots s_{lj_l}, \quad 1 \leqslant j_i \leqslant i + 1. \tag{3.3.3}$$

Теорема 3.3.1. *Минимальный БГШ R группы Кокстера A_l состоит из соотношений* (3.3.2) *вместе с исходными соотношениями* (3.3.1). *Соответствующее множество редуцированных слов* $\mathrm{PBW}(R)$ *состоит из слов вида* (3.3.3).

Эта теорема также следует из [82, предложение 4.3].

Группа Кокстера B_l порождается множеством элементов s_i, $1 \leqslant i \leqslant l$, с определяющими соотношениями

$$\begin{aligned} &s_i^2 = 1, \\ &s_i s_j = s_j s_i, && i - j > 1, \\ &s_{i+1} s_i s_{i+1} = s_i s_{i+1} s_i, && 1 \leqslant i \leqslant l-2, \\ &s_l s_{l-1} s_l s_{l-1} = s_{l-1} s_l s_{l-1} s_l. \end{aligned} \tag{3.3.4}$$

Определим элементы s_{ij}, $1 \leqslant j \leqslant i+1$, $i \leqslant l$, как это было сделано выше.

В B_l выполняются следующие соотношения:

$$\begin{aligned} &s_{i+1j} s_{i+1} = s_i s_{i+1j}, && j \leqslant i \leqslant l-2, \\ &s_{lj} s_{lj} = s_{l-1} s_{lj} s_{lj+1}, && j < l. \end{aligned} \tag{3.3.5}$$

Пусть R состоит из исходных соотношений (3.3.4) вместе с (3.3.5). Используя исключение старших слов соотношений из R, каждый элемент B_l можно представить в виде

$$s_{1i_1} \cdots s_{l-1i_{l-1}} s_{lj_1} \cdots s_{lj_k}, \tag{3.3.6}$$

где $i_1 \leqslant 2, \ldots, i_{l-1} \leqslant l$, $1 \leqslant j_1 < \cdots < j_k \leqslant l$, $k \geqslant 0$.

Теорема 3.3.2. *Соотношения* (3.3.4), (3.3.5) *образуют минимальный БГШ R группы B_l при deg-lex порядке на словах. Соответствующее множество редуцированных слов* $\mathrm{PBW}(R)$ *состоит из слов вида* (3.3.6).

Группа Кокстера D_l порождается множеством элементов s_i, $1 \leqslant i \leqslant l$, с определяющими соотношениями A_{l-1} вместе с

$$s_l^2 = 1, \quad s_l s_{l-1} = s_{l-1} s_l, \quad s_l s_{l-2} s_l = s_{l-2} s_l s_{l-2}. \tag{3.3.7}$$

Определим s_{ij}, $1 \leqslant j \leqslant i+1 \leqslant l$, как это было сделано в случае A_l. Положим

$$s_{lj} = s_l s_{l-2} \cdots s_j, \quad j \leqslant l-2, \qquad s_{ll-1} = s_l, \quad s_{ll} = 1.$$

Следующие соотношения выполнены в D_l:

$$\begin{aligned} &s_{lj} s_{l-1j} = s_{l-1} s_{lj} s_{l-1j+1}, && j \leqslant l-2, \\ &s_{lj} s_{l-1} s_l = s_{l-2} s_{lj} s_{l-1}, && j \leqslant l-2, \\ &s_{lj} s_{l-1k} s_{lk} = s_{l-2} s_{lj} s_{l-1k} s_{lk+1}, && j < k \leqslant l-2. \end{aligned} \tag{3.3.8}$$

Теорема 3.3.3. *Пусть R — множество соотношений* (3.3.8) *вместе с исходными соотношениями D_l и базисами Грёбнера—Ширшова групп A_{l-1} и $A_{l-1}(s_1, \ldots, s_{l-2}, s_l)$* (*повторяющиеся соотношения учитываются один раз*). *Тогда R является БГШ группы D_l при deg-lex порядке на словах. Соответствующее множество приведенных слов* $\mathrm{PBW}(R)$ *состоит из слов вида*

$$s_{1i_1} \cdots s_{l-1i_{l-1}} s_{lj_1} s_{l-1j_2} s_{lj_3} s_{l-1j_4} \cdots,$$

где $i_1 \leqslant 2, \ldots, i_{l-1} \leqslant l$, $1 \leqslant j_1 < j_2 < j_3 < \cdots < j_k \leqslant l-1$, $k \geqslant 0$.

Сформулируем теперь общую гипотезу о БГШ для любой группы Кокстера.

Используем следующее представление для группы Кокстера W, соответствующей матрице Кокстера M. Пусть S — линейно упорядоченное l-элементное множество, $M = (m_{ss'})$ — матрица Кокстера размера $l \times l$. Тогда

$$W = \mathrm{sgr}\langle S \mid s^2 = 1,\ (ss')^{m_{ss'}} = 1 \text{ для } s \neq s',\ s, s' \in S \text{ и конечного } m_{ss'} \rangle.$$

Для любого конечного $m_{ss'}$ определим

$$\begin{aligned} m(s, s') &= ss' \ldots && \text{(здесь } m_{ss'} \text{ чередующихся букв } s,\ s'\text{)}, \\ (m-1)(s, s') &= ss' \ldots && \text{(здесь } m_{ss'} - 1 \text{ чередующихся букв } s,\ s'\text{)}, \end{aligned}$$

и т. д. Например, если $m_{ss'} = 2$, то $m(s, s') = ss'$, $(m-1)(s, s') = s$. Если $m_{ss'} = 3$, то $m(s, s') = ss's$, $(m-1)(s, s') = ss'$.

В этих обозначениях определяющие соотношения группы W принимают вид

$$s^2 = 1, \quad m(s, s') = m(s', s), \quad s > s', \tag{3.3.9}$$

для любых $s, s' \in S$ и конечного $m_{ss'}$.

Два слова от S назовем *эквивалентными*, если они равны по модулю соотношений коммутативности из (3.3.9), т.е. соответствующих $m_{ss'} = 2$. Более точно, это означает, что эквивалентные слова равны в так называемой свободной частично коммутативной полугруппе (или алгебре), порожденной множеством S с соотношениями коммутативности из (3.3.9). Ниже мы приведем решение проблемы равенства в этой полугруппе (и алгебре). Два соотношения $a = b$ и $c = d$ группы W называются эквивалентными, если a и b эквивалентны соответственно c и d.

Гипотеза 3.3.4. *БГШ группы W при deg-lex порядке на словах состоит из исходных соотношений* (3.3.9) *и соотношений, эквивалентных следующим*:

$$\begin{aligned}(m-1)(s, s')(m-1)(s_1, s_2)\dots(m-1)(s_{2k-1}, s_{2k})m(s_{2k+1}, s_{2k+2}) = \\ = (m)(s', s)(m-1)(s_1, s_2)\dots(m-1)(s_{2k-1}, s_{2k})(m-1)(s_{2k+1}, s_{2k+2}),\end{aligned} \tag{3.3.10}$$

где $s > s'$, $s_1 < s_2$, …, $s_{2k-1} < s_{2k}$, $s_{2k+1} < s_{2k+2}$, любые соседние пары $(s', s,)$, (s_1, s_2), …, (s_{2k+1}, s_{2k+2}) различны и

$$s_2 = \begin{cases} s', & \text{если } m_{ss'} \text{ четно}, \\ s, & \text{если } m_{ss'} \text{ нечетно}, \end{cases} \quad \dots, \quad s_{2k+2} = \begin{cases} s_{2k}, & \text{если } m_{s_{2k-1}s_{2k}} \text{ четно}, \\ s_{2k-1}, & \text{если } m_{s_{2k-1}s_{2k}} \text{ нечетно}. \end{cases}$$

Нетрудно убедиться, что БГШ групп A_l, B_l, D_l имеет именно такой вид [47].

Интересно отметить, что из положительного решения гипотезы 3.3.4 следует существование групп Кокстера в общем случае (в книге [18] это доказательство занимает более 100 страниц!).

Следующая теорема [47] также подтверждает нашу гипотезу.

Теорема 3.3.5. *Пусть $W(M)$ — группа Кокстера такая, что $m_{ss'} \geqslant 3$ для любого $s > s'$. Тогда БГШ для W при deg-lex порядке на словах состоит из исходных соотношений группы W и соотношений, эквивалентных* (3.3.10).

Определение 3.3.6 (см. [45])**.** Следующую полугруппу будем называть полугруппой Артина W^+, соответствующей матрице Кокстера M:

$$W^+ = \operatorname{sgr}\langle s_1, \dots, s_n \mid m_{ss'}(s, s') = m_{ss'}(s', s),\ s > s',\ s, s' \in S,\ m_{ss'} < \infty\rangle. \tag{3.3.11}$$

Также мы будем использовать обозначение $(m, i)(s, s')$ для слова, получающегося из $m(s, s')$ удалением первых i букв, $1 \leqslant i \leqslant m$.

Назовем слова a и b в S эквивалентными, если они равны по модулю соотношений коммутативности из (3.3.11). Аналогично, два соотношения $a = b$ и $c = d$ в W^+ назовем эквивалентными, если a и b эквивалентны соответственно словам c и d.

Гипотеза 3.3.7. *БГШ R полугруппы W^+ состоит из исходных соотношений* (3.3.11) *и соотношений, эквивалентных следующим*:

$$\begin{aligned}(m-i_0)(s, s')(m-i_1)(s_1, s_2)\dots(m-i_k)(s_{2k-1}, s_{2k})m(s_{2k+1}, s_{2k+2}) = \\ = m(s', s)(m, i_0)(s_2, s_1)\dots(m, i_{k-1})(s_{2k}, s_{2k-1})(m, i_k)(s_{2k+2}, s_{2k+1}),\end{aligned} \tag{3.3.12}$$

где $s > s'$, $s_1 < s_2$, …, $s_{2k-1} < s_{2k}$, $s_{2k+1} < s_{2k+2}$, и

$$\begin{aligned}(m-i_k)(s_{2k-1}, s_{2k})m(s_{2k+2}, s_{2k+1}) &\doteq m(s_{2k-1}, s_{2k})(m, i_k)(s_{2k+2}, s_{2k+1}), \\ (m-i_{k-1})(s_{2k-3}, s_{2k-2})m(s_{2k}, s_{2k-1}) &\doteq m(s_{2k-3}, s_{2k-2})(m, i_{k-1})(s_{2k}, s_{2k-1}), \\ &\dots \\ (m-i_1)(s_1, s_2)m(s_4, s_3) &\doteq m(s_1, s_2)(m, i_1)(s_4, s_3), \\ (m-i_0)(s, s')m(s_2, s_1) &\doteq m(s, s')(m, i_0)(s_2, s_1).\end{aligned}$$

В приведенных выражениях $\doteq$ означает равенство в свободной полугруппе.

Зафиксируем обе части в (3.3.12). *Если равенство $A = B$ имеет вид* (3.3.12), *то преобразование $A \to B$ будем называть положительной цепью, а $B \to A$ — отрицательной цепью.*

Остальные соотношения из R эквивалентны

$$X = Y, \tag{3.3.13}$$

где X переходит в некоторое X' последовательностью отрицательных цепей

$$X \to X_1 \to \cdots \to X_k = X'$$

(*в свободной частично коммутативной полугруппе*), *$X' = AY_1$ и $Y = BY_1$, где $A \to B$ — положительная цепь.*

Сравним эту гипотезу с гипотезой 3.3.4 о БГШ групп Кокстера. Соотношения (3.3.10) — это соотношения (3.3.12) с $i_0 = i_1 = \cdots = i_k = 1$ и с дополнительным условием, что все соседние пары (s, s'), (s_1, s_2), …, (s_{2k+1}, s_{2k+2}) различны. В частности, предполагается, что в группах Кокстера отрицательные цепи не возникают.

3.4. Группы и полугруппы кос. Группу кос B_{n+1}, $n \geqslant 0$, обычно определяют как группу, порожденную множеством $\Sigma = \{\sigma_1, \dots, \sigma_n\}$ с определяющими соотношениями

$$\begin{aligned} &\sigma_{i+1}\sigma_i\sigma_{i+1} = \sigma_i\sigma_{i+1}\sigma_i, && i = 1, \dots, n, \\ &\sigma_i\sigma_j = \sigma_j\sigma_i, && i - j > 1, \quad 1 \leqslant i, j \leqslant n+1. \end{aligned} \tag{3.4.1}$$

Особенный интерес представляют проблемы равенства и сопряженности для групп кос B_{n+1}. Отметим основополагающую работу Э. Артина [30], а также [27, 31, 38, 73]. В этих работах, особенно в [73], показана решающая роль полугруппы положительных кос в B_{n+1}. Обозначим эту полугруппу через B^+_{n+1} и назовем ее *полугруппой положительных кос* типа $n+1$. Она имеет следующее представление в порождающих Артина a_i, $1 \leqslant i \leqslant n$:

$$\begin{aligned} &a_i a_j = a_j a_i, && i - j \geqslant 2, \\ &a_{i+1} a_i a_{i+1} = a_i a_{i+1} a_i, && 1 \leqslant i \leqslant n. \end{aligned}$$

Легко заметить, что полугруппа положительных кос B^+_{n+1} является полугруппой Артина типа A_n.

Через $w(a_j, \dots, a_i) = w(j, i)$ или $v(a_j, \dots, a_i) = v(j, i)$ мы обозначаем любое слово в алфавите $a_j, a_{j+1}, \dots, a_i$, если $j \leqslant i$, или пустое слово, если $j > i$.

Введем следующее обозначение, аналогичное использованному в [47]:

$$a_{ij} = a_i a_{i-1} \dots a_j, \ i \geqslant j, \quad a_{ii} = a_i, \quad a_{ii+1} = 1.$$

Теорема 3.4.1 (см. [45]). *БГШ полугруппы $A^+_n = B^+_{n+1}$ состоит из следующих соотношений*:

$$a_{i+1} a_i v(1, i-1) w(j, i) a_{i+1 j} = a_i a_{i+1} a_i v(1, i-1) a_{ij} w'(j+1, i+1),$$
$$a_s a_k = a_k a_s, \quad s - k \geqslant 2,$$

где $1 \leqslant i \leqslant n-1$, $1 \leqslant j \leqslant i+1$, $w' = w(a_{j+1}, \dots, a_{i+1})$, и слово w начинается с буквы a_i, если оно непустое.

Полученный результат согласуется с гипотезой 3.3.7.

Для самой группы кос B_{n+1} рассмотрим результат А. А. Маркова [27], полученный также Э. Артином [31]. Именно, найденная в этих работах нормальная форма слов в B_{n+1} возникает в связи с БГШ этой группы в некотором специальном представлении.

Введем элементы

$$s_{i,i+1} = \sigma_i^2, \quad s_{i,j+1} = \sigma_j \dots \sigma_{i+1} \sigma_i^2 \sigma_{i+1}^{-1} \dots \sigma_j^{-1},$$

где $1 \leqslant i \leqslant n$ и $1 \leqslant i < j \leqslant n$ соответственно.

Обозначим $S_j = \{s_{i,j}, s_{i,j}^{-1}\}$, $j = 2, \dots, n+1$, $\Sigma^{-1} = \{\sigma_1^{-1}, \dots, \sigma_n^{-1}\}$. Множество

$$S = S_{n+1} \cup S_{n-1} \cup \cdots \cup S_2 \cup \Sigma^{-1}$$

рассматривается как новое множество порождающих B_{n+1} как полугруппы. Это означает, что в этом представлении не нужны положительные порождающие σ_i и тривиальные групповые соотношения на Σ. Вместо σ_i А. А. Марков [27] использовал $s_{i,i+1}\sigma_i^{-1}$, а вместо соотношений $\sigma_i^{-1}\sigma_i = 1$, $\sigma_i\sigma_i^{-1} = 1$ — соотношения $\sigma_i^{-2} = s_{i,i+1}^{-1}$. Упорядочим множество S следующим образом:

$$S_{n+1} < S_n < \cdots < S_2 < \Sigma^{-1};$$

это означает, что любая буква в S_n меньше, чем все буквы в S_{n-1} и т. д.,

$$s_{1,j}^{-1} < s_{1,j} < s_{2,j}^{-1} < \cdots < s_{j-1,j}, \qquad \sigma_1^{-1} < \sigma_2^{-1} < \ldots \sigma_n^{-1}.$$

Упорядочим слова от S при помощи обратного башенного порядка.

Следуя [27], мы будем использовать следующее обозначение:

$$\sigma_{i,j+1} = \sigma_i^{-1} \ldots \sigma_j^{-1}, \quad 1 \leqslant i \leqslant j \leqslant n-1; \qquad \sigma_{ii} = 1.$$

Допуская некоторую неточность в обозначениях, положим

$$\{a, b\} = b^{-1}ab.$$

(Оригинальное обозначение в [27]: $b^{-1}ab = [a, b]$.)

В [27, 31] было показано, что в B_{n+1} выполняются следующие соотношения ($\varepsilon, \delta = \pm 1$):

$$\sigma_k^{-1}s_{i,j}^{\delta} = s_{i,j}^{\delta}\sigma_k^{-1}, \quad k \neq i-1, i, j-1, j, \tag{3.4.2}$$

$$\sigma_i^{-1}s_{i,i+1}^{\delta} = s_{i,i+1}^{\delta}\sigma_i^{-1}, \tag{3.4.3}$$

$$\sigma_{i-1}^{-1}s_{i,j}^{\delta} = s_{i-1,j}^{\delta}\sigma_{i-1}^{-1}, \tag{3.4.4}$$

$$\sigma_i^{-1}s_{i,j}^{\delta} = \{s_{i+1,j}^{\delta}, s_{i,i+1}\}\sigma_i^{-1}, \tag{3.4.5}$$

$$\sigma_{j-1}^{-1}s_{i,j}^{\delta} = s_{i,j-1}^{\delta}\sigma_{j-1}^{-1}, \tag{3.4.6}$$

$$\sigma_j^{-1}s_{i,j}^{\delta} = \{s_{i,j+1}^{\delta}, s_{j,j+1}\}\sigma_j^{-1}, \tag{3.4.7}$$

$$s_{j,k}^{-1}s_{k,l}^{\varepsilon} = \{s_{k,l}^{\varepsilon}, s_{j,l}^{-1}\}s_{j,k}^{-1}, \tag{3.4.8}$$

$$s_{j,k}s_{k,l}^{\varepsilon} = \{s_{k,l}^{\varepsilon}, s_{j,l}s_{k,l}\}s_{j,k}, \tag{3.4.9}$$

$$s_{j,k}^{-1}s_{j,l}^{\varepsilon} = \{s_{j,l}^{\varepsilon}, s_{k,l}^{-1}s_{j,l}^{-1}\}s_{j,k}^{-1}, \tag{3.4.10}$$

$$s_{j,k}s_{j,l}^{\varepsilon} = \{s_{j,l}^{\varepsilon}, s_{k,l}\}s_{j,k}, \tag{3.4.11}$$

$$s_{i,k}^{-1}s_{j,l}^{\varepsilon} = \{s_{j,l}^{\varepsilon}, s_{k,l}s_{i,l}s_{k,l}^{-1}s_{i,l}^{-1}\}s_{i,k}^{-1}, \tag{3.4.12}$$

$$s_{i,k}s_{j,l}^{\varepsilon} = \{s_{j,l}^{\varepsilon}, s_{i,l}^{-1}s_{k,l}^{-1}s_{i,l}s_{k,l}\}s_{i,k}. \tag{3.4.13}$$

Также для $j < i < k < l$ или $i < k < j < l$, $\varepsilon, \delta = \pm 1$

$$s_{i,k}^{\delta}s_{j,l}^{\varepsilon} = s_{j,l}^{\varepsilon}s_{i,k}^{\delta}. \tag{3.4.14}$$

Замечание 3.4.2. Мы также отсылаем читателя к соотношениям из [31]. Как было замечено в [37], соотношения Артина верны для $\varepsilon = 1$ (это (3.4.9), (3.4.11), (3.4.13)), но неверны для для $\varepsilon = -1$ (правильные соотношения — (3.4.8), (3.4.10), (3.4.12)). Те же соотношения приведены в [94, с. 174].

Замечание 3.4.3. Соотношения (3.4.8)–(3.4.14) эквивалентны известным соотношениям Бурау [58]

$$s_{i,j}s_{k,l} = s_{k,l}s_{i,j}, \qquad j < k \text{ или } i < k < l < j,$$

$$s_{i,j}s_{i,k}s_{j,k} = s_{i,k}s_{j,k}s_{i,j},$$

$$s_{i,k}s_{j,k}s_{i,j} = s_{j,k}s_{i,j}s_{i,k},$$

$$s_{i,k}s_{j,k}s_{j,l}s_{j,k}^{-1} = s_{j,k}s_{j,l}s_{j,k}^{-1}s_{i,k}, \qquad i < j < k < l$$

(см. [27, гл. 6]). Обе эти системы задают определяющие соотношения для нормальной подгруппы P_{n+1} (известной как группа крашеных кос) в B_{n+1}, порожденной элементами σ_i^2, $1 \leqslant i \leqslant n$.

Кроме того, в группе B_{n+1} выполняются следующие соотношения (см. [27]):

$$\sigma_j^{-1}\sigma_k^{-1} = \sigma_k^{-1}\sigma_j^{-1}, \qquad j < k-1, \tag{3.4.15}$$

$$\sigma_{j,j+1}\sigma_{k,j+1} = \sigma_{k,j+1}\sigma_{j-1,j}, \quad k < j, \tag{3.4.16}$$

$$\sigma_i^{-2} = s_{i,i+1}^{-1}. \tag{3.4.17}$$

Отметим, что стандартные соотношения Артина для B_{n+1} вытекают из предыдущих соотношений, поскольку $\sigma_i = s_{ii+1}\sigma_i^{-1}$. Так, например, из (3.4.16) для $k = j-1$ получается

$$\sigma_j^{-1}\sigma_{j-1}^{-1}\sigma_j^{-1} = \sigma_{j-1}^{-1}\sigma_j^{-1}\sigma_{j-1}^{-1}.$$

Кроме того,

$$\sigma_i^{-1}\sigma_i = \sigma_i^{-1}s_{i,i+1}\sigma_i^{-1} = s_{i,i+1}\sigma_i^{-2} = s_{i,i+1}s_{i,i+1}^{-1} = 1$$

и т. д.

Назовем соотношения (3.4.2)–(3.4.17) вместе с

$$s_{i,j}^{\pm 1}s_{i,j}^{\mp 1} = 1$$

системой соотношений Артина—Маркова для B_{n+1} в порождающих Артина—Бурау.

Теорема 3.4.4 (см. [41])**.** *Соотношения Артина—Маркова R образуют минимальный БГШ для группы кос B_{n+1} в порождающих Артина—Бурау относительно обратного башенного порядка на словах от этих порождающих. Кроме того,* $\mathrm{PBW}(R)$ *состоит из слов*

$$f_n f_{n-1}\dots f_2\sigma_{i_n n}\sigma_{i_{n-1}n-1}\dots\sigma_{i_2 2}, \tag{3.4.18}$$

где f_j — несократимые слова от $\{s_{ij} \mid i < j,\ 2 \leqslant j \leqslant n\}$.

Для доказательства этой теоремы достаточно проверить, что R замкнуто относительно композиции [41].

Теперь из CD-леммы вытекает следующее утверждение.

Следствие 3.4.5 (см. [27, 31])**.** *Любое слово в B_{n+1} имеет единственное представление в виде* (3.4.18).

Это хорошо известная нормальная форма в группе кос, найденная Марковым и Ивановским [27, теорема 6] и Артином [31, теорема 17 и замечание после теоремы 18].

Пусть P_n — группа крашеных кос. Из теоремы 3.4.4 и следствия 3.4.5 вытекает следующее утверждение.

Следствие 3.4.6 (см. [27, 31])**.** *Группа P_n порождается множеством $\{s_{ij}\}$ с определяющими соотношениями* (3.4.8)–(3.4.14). *Эти соотношения вместе с тривиальными образуют минимальный БГШ группы P_n относительно обратного башенного порядка на словах от порождающих.*

Замечание 3.4.7. В [27] следствие 3.4.5 использовалось для алгебраического доказательства точности представления Артина [30] группы кос автоморфизмами свободной группы. С использованием другого чисто алгебраического метода это было сделано в работе Боненблюста [39], на которую ссылается Артин в [31]. Еще один алгебраический подход, использующий процесс Райдемайстера—Шрайера, приведен в статье В.-Л. Чоу [61].

3.5. Относительные базисы Грёбнера—Ширшова. Как было отмечено в [47] (см. также следствие 3.1.6), стандартный базис группы, представленной в виде башни HNN-расширений, совпадает с PBW-базисом этой группы. С другой стороны, в [10] было введено понятие относительного стандартного базиса. Это понятие широко использовалось в [9,11,12] для решения проблемы Мальцева в классе полугрупповых алгебр.

В этом разделе мы приведем определение относительного БГШ для алгебр и групп. Мы заметим, что относительные канонические слова, построенные для некоторых групп в [9, 11, 12], суть то же самое, что PBW-слова для относительного БГШ этих групп. Также мы приведем другие примеры групп с относительным БГШ, показывающие, что любая группа G из системы Титса (G, B, N, S)

(см., например, [18]) имеет относительный БГШ R такой, что $\mathrm{PBW}(R)$ есть в точности множество слов Брюа для G. Для иллюстрации этого утверждения будет рассмотрен пример группы $SL_2(\Bbbk)$.

Приведем «относительный» вариант понятий, введенных в разделе 2, следуя [49]. Везде в этом разделе $\mathcal{X} = \{x_i \mid i \in I\}$ — вполне упорядоченное множество ($x_i \leqslant x_j$ при $i \leqslant j$), Γ — группа (элементы из Γ обозначаем строчными греческими буквами). Пусть для каждого $x \in \mathcal{X}$ определены две изоморфные подгруппы $\Gamma_x \simeq \Gamma'_x \subset \Gamma$ и зафиксирован изоморфизм

$$\partial_x : \Gamma_x \to \Gamma'_x. \tag{3.5.1}$$

Пусть μ обозначает групповое умножение в Γ. Через $\Bbbk\langle\mathcal{X};\Gamma\rangle$ обозначим свободную Γ-алгебру, порожденную множеством $\mathcal{X}$ над полем $\Bbbk$ (см. [40]):

$$\Bbbk\langle\mathcal{X};\Gamma\rangle = \Bbbk\langle\mathcal{X}\dot\cup\Gamma \mid \gamma\gamma_1 = \mu(\gamma,\gamma_1),\ \gamma x = x\partial_x(\gamma),\ \gamma \in \Gamma_x,\ x \in \mathcal{X}\rangle. \tag{3.5.2}$$

В случае $\Gamma = \{1\}$ это в точности свободная алгебра, порожденная $\mathcal{X}$ над $\Bbbk$.

Γ-*словом* мы называем слово вида

$$u = \gamma_0 x_{i_1}\gamma_1 \dots x_{i_k}\gamma_k, \tag{3.5.3}$$

где $k \geqslant 0$, $\gamma_i \in \Gamma$, $x_{i_j} \in \mathcal{X}$. Для Γ-слова u через $[u]$ мы обозначим проекцию u на алфавит $\mathcal{X}$:

$$[u] = x_{i_1} \dots x_{i_k}. \tag{3.5.4}$$

Функция длины для Γ-слова вида (3.5.3) определена как $|u| = |[u]| = k$.

Легко заметить, что два Γ-слова

$$u = \gamma_0 x_{i_1}\gamma_1 \dots x_{i_k}\gamma_k \quad \text{и} \quad v = \delta_0 x_{j_1}\delta_1 \dots x_{j_l}\delta_l$$

равны тогда и только тогда, когда

$$k = l, \quad x_{i_s} = x_{j_s}, \quad s = 1, \dots, k = l,$$
$$\gamma_0 = \delta_0\gamma_{x_{i_1}}, \quad \gamma'_{x_{i_1}}\gamma_1 = \delta_1\gamma_{x_{i_2}}, \quad \dots, \quad \gamma'_{x_{i_k}}\gamma_k = \delta_k.$$

Если для некоторых Γ-слов u, u_1, u_2, v выполнено равенство $u = u_1 v u_2$, то v называется Γ-подсловом слова u. Кроме того, из условия $uv = wt$ следует, что $u = wa$, $t = av$ или $w = ua$, $v = at$ для некоторого Γ-слова a.

Зафиксируем мономиальный (вполне) порядок $\leqslant$ на словах от $\mathcal{X}$, который согласуется с порядком на $\mathcal{X}$. Это приводит к квазипорядку на Γ-словах:

$$u \preceq v \overset{\text{def}}{\iff} [u] \leqslant [v]. \tag{3.5.5}$$

Тогда из $u \preceq v$ следует, что $aub \preceq avb$ для всех Γ-слов u, v, a, b.

Пусть $f \in \Bbbk\langle\mathcal{X};\Gamma\rangle$. Предположим, что f представлено в виде

$$f = \sum \alpha_i u_i,$$

где $\alpha_i \in \Bbbk$ и u_i — попарно различные Γ-слова. Через $\bar f$ (старшее слово в f) мы обозначим любое максимальное слово, встречающееся в f. Обозначим через $\ell(f)$ число старших слов в f. Если $\ell(f) = 1$, то мы называем f *строгим многочленом*. Строгий многочлен f называется *унитарным*, если его старший коэффициент равен 1. Подмножество $S \subset \Bbbk\langle\mathcal{X};\Gamma\rangle$ называется *унитарным строгим*, если оно состоит из унитарных строгих многочленов.

Всюду ниже S — унитарное строгое множество. Понятие композиции двух многочленов $f, g \in S$ определяется так же, как и в случае $\Gamma = \{1\}$ (ср. с (2.2.1), (2.2.2)):

$$(f,g)_w = \begin{cases} fv - ug, & w = \bar f v = u\bar g,\ |\bar f| > |u|, \\ f - ugv, & w = \bar f = u\bar g v, \end{cases} \tag{3.5.6}$$

где u, v, w — Γ-слова. Для второго случая из (3.5.6) преобразование

$$f \mapsto f - ugv \tag{3.5.7}$$

называется ИСС g в f (ср. с (2.2.3)). Можно также рассматривать ИСС унитарного строгого многочлена g в произвольном (может быть, не строгом) многочлене f. Именно, пусть $\bar f$ — некоторое старшее слово в f. Без ограничения общности можно предполагать, что f является $\bar f$-унитарным,

т.е. $f = \bar{f} + \sum \alpha_i u_i$, $u_i \preceq \bar{f}$. Если $\bar{f} = u\bar{g}v$ для некоторых Γ-слов u, v и $g \in S$, то для $f_1 = f - ugv$ выполнено неравенство $\ell(f_1) < \ell(f)$. Поскольку число $\ell(f)$ конечно, процесс ИСС унитарных строгих многочленов в любом слове f конечен.

В обоих случаях в (3.5.6) выполнено

$$\overline{(f,g)_w} \prec w, \tag{3.5.8}$$

хотя $(f,g)_w$ не обязательно строгий многочлен.

Композиция (3.5.6) называется *тривиальной относительно* S (более точно, относительно S и w), если

$$(f,g)_w = \sum \alpha_i u_i s_i v_i, \tag{3.5.9}$$

где $\alpha_i \in \Bbbk$, $s_i \in S$, u_i, v_i — Γ-слова, и

$$u_i \bar{s}_i v_i \prec w. \tag{3.5.10}$$

В частности, если $(f,g)_w$ обращается в нуль при ИСС соотношений из S, то $(f,g)_w$ тривиальна относительно S. Как и выше, условие тривиальности обозначим через $(f,g)_w \equiv 0 \pmod{S,w}$.

Определение 3.5.1. Унитарное строгое множество $S \subset \Bbbk\langle \mathcal{X}; \Gamma\rangle$ называется Γ-*относительным БГШ*, если каждая композиция элементов из S тривиальна относительно S.

Теорема 3.5.2 (относительная лемма о композиции)**.** *Пусть $S \subset \Bbbk\langle \mathcal{X}; \Gamma\rangle$ — Γ-относительный БГШ. Если $f \in \mathrm{I}(S)$, то для некоторого старшего слова $\bar{f}$ в f выполнено равенство $\bar{f} = a\bar{s}b$, $s \in S$. Обратное также верно.*

Следствие 3.5.3 (лемма о композиции—diamond-лемма)**.** *Пусть $S \subset \Bbbk\langle \mathcal{X}; \Gamma\rangle$ — унитарное строгое множество. Тогда S является БГШ в том и только в том случае, когда*

$$\mathrm{PBW}(S) = \{u \mid u \neq a\bar{s}b,\ s \in S\}$$

есть линейный базис Γ-алгебры, представленной множеством порождающих $\mathcal{X}$ и определяющими соотношениями S.

Если S состоит из полугрупповых соотношений (т.е. $u - v$, где u и v — Γ-слова), то $\Bbbk\langle X; \Gamma | S\rangle = \Bbbk P$, где $\Bbbk P$ — полугрупповая алгебра полугруппы

$$P = \mathrm{sgr}\langle \mathcal{X}; \Gamma | S\rangle \equiv \mathrm{sgr}\langle \mathcal{X} \dot\cup \Gamma | S \cup S_\Gamma\rangle$$

и S_Γ состоит из тех же соотношений, что и (3.5.2). В этом случае P называется Γ-*полугруппой*. Аналогично, легко понять, что подразумевается под Γ-группой: следует только добавить элементы $\{x^{-1} \mid x \in \mathcal{X}\}$ к множеству порождающих и тривиальные групповые тождества — к определяющим соотношениям.

Рассмотрим два примера групп с относительным БГШ.

Первый пример связан с понятием системы Титса. Покажем, что хорошо известное разложение Брюа для элементов группы из системы Титса (G, B, N, S) есть не что иное, как PBW-представление слов для B-относительного БГШ группы G.

Напомним определение системы Титса [18]. Пусть G — некоторая группа, B и N — подгруппы в G такие, что подгруппа $T = B \cap N$ нормальна в G, и пусть $S \subset W = N/(B \cap N)$. Представим группы B, N и T через их таблицы умножения:

$$B = \langle \{b\} \mid bb' = b''\rangle, \quad N = \langle \{n\} \mid nn' = n''\rangle, \quad T = \langle \{t\} \mid tt' = t''\rangle. \tag{3.5.11}$$

Предположим, что выполняются следующие четыре аксиомы.

(T1) Группа G порождена множеством $B \cup N$, т.е. для любого $g \in G$ существует разложение

$$g = b_0 n_1 \dots b_{k-1} n_k b_k, \tag{3.5.12}$$

где $k \geqslant 0$, $b_i \in B$, $n_i \in N$.

Выберем систему $\{w\}$ представителей смежных классов nT, $n \in N$:

$$wT = w'T \;\Rightarrow\; w = w', \quad wT = T \;\Rightarrow\; w = 1.$$

Тогда

$$\begin{gathered}(\forall n \in N)(\exists w \in \{w\}, t \in T)\ n = wt,\\ (\forall w, w' \in \{w\})(\exists w'' \in \{w\}, t \in T)\ ww' = w''t,\\ (\forall t \in T, w \in \{w\})(\exists t' \in T)\ tw = w't.\end{gathered} \tag{3.5.13}$$

В последнем равенстве для любого w соответствие $t \mapsto t'$ определяет автоморфизм группы T.

Из (3.5.12), (3.5.13) получается представление

$$g = b_0 w_1 b_1 \dots b_{k-1} w_k b_k$$

для любого $g \in G$ ($k \geqslant 0$, $b_i \in B$, $w_i \in \{w\}$).

(T2) Множество S порождает W и состоит из элементов порядка 2.

Пусть $S = \{sT\}$, где $\{s\}$ — множество представителей смежных классов из S. Тогда для любых $w \in \{w\}$, $s \in \{s\}$ выполнены соотношения

$$w = s_1 \cdots s_n t, \quad s_i \in S,\ t \in T, \tag{3.5.14}$$

$$s^2 = t(s) \in T. \tag{3.5.15}$$

(T3) Для любых $w \in \{w\}$, $s \in \{s\}$ выполняется соотношение

$$sbw = b_1 s^\delta w b_2, \tag{3.5.16}$$

где $\delta \in \{0, 1\}$, $b_1, b_2 \in B$.

Из соотношений (3.5.13), (3.5.14) и (3.5.16) следует, что для любых $w_1, w_2 \in \{w\}$, $b \in B$ имеет место равенство

$$w_1 b w_2 = b_1 w b_2 \tag{3.5.17}$$

для некоторых $w \in \{w\}$, $b_1, b_2 \in B$.

(T4) Для каждого $s \in S$ имеем $sBs \not\subset B$.

Определение 3.5.4 (см. [18]). Четверка (G, B, N, S) называется системой Титса, если она удовлетворяет аксиомам (T1)–(T4).

Из аксиом (T1)–(T3) следует, что G порождается множеством $B \cup \{w\}$ с определяющими соотношениями (3.5.11), (3.5.13), (3.5.17). Для любого $w \in \{w\}$ определим

$$\begin{aligned}\Gamma_w &= \{\gamma \in B \mid \gamma w = w\gamma' \ \text{ для некоторого } \ \gamma' \in B\},\\ \Gamma'_w &= \{\gamma' \in B \mid w\gamma' = \gamma w' \ \text{ для некоторого } \ \gamma \in B\}.\end{aligned} \tag{3.5.18}$$

Тогда Γ_w, Γ'_w — изоморфные подгруппы в B, $T \subset \Gamma_w$, $T \subset \Gamma'_w$. Изоморфизм ∂_w переводит γ в γ', он продолжает автоморфизм группы T, введенный выше: $t \mapsto t'$.

Таким образом, мы получили, что алгебра $\Bbbk G$ группы G из системы Титса (G, B, N, S) является B-алгеброй со следующими определяющими соотношениями:

$$w_1 b w_2 = b_1 w b_2, \quad w_1 w_2 = wt, \tag{3.5.19}$$

где $w, w_i \in \{w\}$, $b, b_i \in B$, $t \in T$. Из (3.5.19) следует [18], что каждый элемент $g \in G$ может быть представлен в виде

$$g = b_1 w b_2, \quad b_1, b_2 \in B, \quad w \in \{w\}, \tag{3.5.20}$$

называемом разложением Брюа. Хорошо известно, что разложение Брюа единственно (см., например, [18]). Слова из правой части (3.5.20) называются словами Брюа. Таким образом, из CD-леммы вытекает следующий результат.

Теорема 3.5.5 (см. [49]). *Пусть (G, B, N, S) — система Титса. Тогда множество R соотношений* (3.5.19) *является B-относительным БГШ алгебры $\Bbbk G$ (следовательно, и группы G) как B-алгебры (или B-группы соответственно) в порождающих w_i. Множество* $\mathrm{PBW}(R)$ *приведенных слов является множеством слов Брюа для G.*

Приведем более конкретный пример, иллюстрирующий теорему 3.5.5. Рассмотрим группу $G = SL_2(\Bbbk)$. Пусть

$$u(b) = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, \quad t(a) = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \quad w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

где $a \in \Bbbk \setminus \{0\}$, $b \in \Bbbk$. Пусть $T = \{t(a) \mid \Bbbk \setminus \{0\}\}$, $U = \{u(b) \mid b \in \Bbbk\}$,

$$B = UT = \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \;\middle|\; a \in \Bbbk \setminus \{0\},\ b \in \Bbbk \right\},$$

$$N = T \cup wT = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \begin{pmatrix} 0 & a^{-1} \\ a & 0 \end{pmatrix} \;\middle|\; a \in \Bbbk \setminus \{0\} \right\}.$$

Тогда $(G, B, N, S = \{wT\})$ является системой Титса и выполняются следующие соотношения:

$$\begin{gathered} wu(a)w = u(a)wt(-a)u(a), \quad w^2 = t(-1), \quad u(b)u(b_1) = u(b + b_1), \\ t(a)t(a_1) = t(aa_1), \quad t(a)u(b) = u(ba^2)t(a), \quad t(a)w = wt(a). \end{gathered} \tag{3.5.21}$$

В этом случае $\Gamma_w = \Gamma'_w = T$.

Система соотношений (3.5.21) является B-относительным БГШ группы G в порядке deg-lex на B-словах от $\{w\}$.

Замечание 3.5.6. В случае $G = SL_2(\Bbbk)$ из (3.5.21) можно получить «абсолютный» БГШ. Именно, рассмотрим некоторый полный порядок на U и T и упорядочим слова от $U \cup T$ в deg-lex порядке, считая, что $u(b) > t(a)$. После этого введем на словах от $(U \cup T)\dot\cup\{w\}$ башенный порядок. Теперь легко заметить, что (3.5.21) замкнуто относительно композиции не только как множество соотношений B-алгебры, но также и в абсолютном смысле (как множество полиномов в свободной ассоциативной алгебре).

Следовательно, из обычной CD-леммы вытекает следующая теорема.

Теорема 3.5.7. *Любой элемент из $SL_2(\Bbbk)$ имеет единственное представление в виде*

$$u(b)t(c) \quad \textit{или} \quad u(b)wu(c)t(a),$$

где $a, c \in \Bbbk \setminus \{0\}$, $b \in \Bbbk$.

Другой пример тесно связан с проблемой поиска (полугрупповой) алгебры, не вложимой в тело, но такой, что ее мультипликативная полугруппа вложима в группу. Эта проблема была поставлена А. И. Мальцевым (см. [24, с. 4]). При решении этой проблемы в работах [9, 11, 12] применялась техника относительных переписывающих систем для групп. Оказывается, эта техника может быть полностью заменена понятием относительного БГШ, которое делает рассуждения более прозрачными. Другие примеры, решающие проблему Мальцева, но не являющиеся полугрупповыми кольцами, были найдены А. Баутеллом [54] и А. А. Кляйном [84].

Пусть $GF(2)$ — поле из двух элементов, и пусть Q означает полугруппу, порожденную конечным множеством $\mathcal{X}$ с определяющими соотношениями вида $w_i h_i = u_i f_i$, где $w_i, h_i, u_i, f_i \in \mathcal{X}$ с некоторыми дополнительными условиями. Рассмотрим замыкание $\overline{GF(2)Q}$ полугрупповой алгебры $GF(2)Q$ до алгебры формальных степенных рядов, и пусть $\overline{GF(2)Q}^*$ — ее мультипликативная полугруппа (алгебра $\overline{GF(2)Q}$ не имеет делителей нуля). Под $G = G(\overline{GF(2)Q}^*)$ мы подразумеваем группу частных этой полугруппы. Каждая группа G такого типа имеет следующие свойства.

1) Группа G является Γ-группой, где Γ — группа обратимых рядов в $\overline{GF(2)Q}^*$. Для каждого порождающего $p \in \overline{GF(2)Q}^*$ выполнены соотношения

$$\Gamma_p = \{1 + pA \mid A \in \overline{GF(2)Q}\}, \quad \Gamma'_p = \{1 + Ap \mid A \in \overline{GF(2)Q}\};$$

2) существует множество порождающих $\Sigma \subset G$ и переписывающая система (так называемая полу-туевская система)

$$\Pi = [\Sigma; \Gamma \mid A_j \to B_j,\ j \in J]$$

такие, что множество терминальных слов (не содержащих подслов вида A_j) является Γ-базисом группы G (т.е. любое Γ-слово равно некоторому единственному с точностью до

преобразований $\gamma p \leftrightarrow p\gamma'$, $\gamma' p^{-1} \leftrightarrow p^{-1}\gamma$ терминальному Γ-слову). На самом деле $A_j > B_j$ относительно башенного порядка на Σ-словах.

Из последнего свойства и следствия 3.5.3 следует, что множество Γ-соотношений

$$S = \{A_j - B_j \mid j \in J\} \subset GF(2)\langle \Sigma; \Gamma \rangle$$

является Γ-относительным БГШ группы G. Множество $\mathrm{PBW}(S)$ есть в точности Γ-относительный стандартный базис группы G [10].

Для решения проблемы Мальцева в работах [5,9,12] использовалась следующая полугруппа Q_4:

$$Q_4 = \mathrm{sgr}\left\langle v_0,\ v_1,\ a_i,\ b_i,\ c_i,\ s_i\ (1 \leqslant i \leqslant 4) \;\middle|\; a_i s_i = c_i v_0,\ b_i s_{i+1} = c_i v_1,\ b_i t_{i+1} = a_i t_i \right\rangle, \qquad (3.5.22)$$

где $i \leqslant 1 \leqslant 4$, $s_5 = s_1$, $t_5 = t_1$.

Если $GF(2)Q_4$ вкладывается в некоторое тело D, то $(v_0^{-1}v_1)^4 = 1$. Это означает, что

$$(v_0^{-1}v_1 - 1)^4 = 0$$

в D, т.е. $v_0 = v_1$ в D, противоречие. Следовательно, алгебра $GF(2)Q_4$ не вкладывается ни в какое тело, так что основная трудность доказательства состоит в том, чтобы доказать вложимость полугруппы $\overline{GF(2)Q_4}^*$ в группу.

В [12] для группы $G = G(\overline{GF(2)Q_4}^*)$ была построена переписывающая система Π со свойством 2) (см. выше). Там были использованы обозначение $p = v_0^{-1}v_1$ и правила $p^4 \to 1$, $p^3 \to p^{-1}$. Но эти правила могут быть заменены на

$$v_0^{-1}v_1v_0^{-1}v_1 \to v_1^{-1}v_0v_1^{-1}v_0, \qquad (3.5.23)$$

$$v_0v_1^{-1}v_0v_1^{-1} \to v_1v_0^{-1}v_1v_0^{-1}, \qquad (3.5.24)$$

соответственно. Действительно, непосредственное вычисление показывает, что соотношения

$$v_0^{-1}v_1v_0^{-1}v_1 = v_1^{-1}v_0v_1^{-1}v_0, \quad v_0v_1^{-1}v_0v_1^{-1} = v_1v_0^{-1}v_1v_0^{-1}$$

образуют Γ-относительный БГШ для группы $\langle v_0, v_1; \Gamma \mid (v_0^{-1}v_1)^4 = 1\rangle$ относительно башенного порядка, определенного посредством $v_1^{\varepsilon} > v_0^{\delta}$, $v_i > v_i^{-1}$, $\varepsilon, \delta \in \{-1, 1\}$, $i \in \{0, 1\}$.

Таким образом, из [11,12] вытекает следующая теорема.

Теорема 3.5.8. *Пусть*

$$\Pi = [\Sigma; \Gamma \mid A_j \to B_j,\ j \in J]$$

— переписывающая (полу-туевская) система, построенная для $G(\overline{GF(2)Q_4}^*)$ *в* [12]*, но с* (3.5.23) *и* (3.5.24) *вместо* $p^4 \to 1$ *и* $p^3 \to p^{-1}$ *соответственно. Тогда множество соотношений*

$$S = \{A_j - B_j \mid j \in J\}$$

является Γ*-относительным БГШ группы* $G(\overline{GF(2)Q_4}^*)$.

С использованием относительной CD-леммы основной результат [11,12] получается в качестве следствия.

Теорема 3.5.9. *Полугруппа* $\overline{GF(2)Q_4}^*$ *вкладывается в группу.*

Замечание 3.5.10. Имеется следующая классификация областей (колец без делителей нуля, см. [15]):

$\mathcal{D}_0$ — класс всех областей;

$\mathcal{D}_1$ — все области с мультипликативными полугруппами, вложимыми в группу;

$\mathcal{D}_2$ — все обратимые области, т.е. такие, что их мультипликативные полугруппы вложимы в группы единиц некоторых областей;

$\mathcal{D}_3$ — все области, вложимые в тела.

Очевидно,

$$\mathcal{D}_0 \supseteq \mathcal{D}_1 \supseteq \mathcal{D}_2 \supseteq \mathcal{D}_3. \tag{3.5.25}$$

Пример Мальцева [95] показывает, что $\mathcal{D}_0 \neq \mathcal{D}_1$; пример первого автора, приведенный выше, показывает, что $\mathcal{D}_1 \neq \mathcal{D}_2$ (это примеры полугрупповых алгебр). Из результата В. Н. Герасимова [19] следует, что примеры Баутелла [54] и Кляйна [84] принадлежат $\mathcal{D}_2 \setminus \mathcal{D}_3$. Пока нет примеров полугрупповых алгебр из $\mathcal{D}_2 \setminus \mathcal{D}_3$.

Наиболее интересные вопросы возникают при рассмотрении (3.5.25) для групповых алгебр. Именно, рассмотрим следующую классификацию:

$\mathcal{K}$ — групповые алгебры групп без кручения;
$\mathcal{K}_0$ — групповые алгебры без делителей нуля;
$\mathcal{K}_1$ — все групповые алгебры без делителей нуля с мультипликативными полугруппами, вложимыми в группу;
$\mathcal{K}_2$ — все обратимые групповые алгебры;
$\mathcal{K}_3$ — все групповые алгебры, вложимые в тело.

Очевидно,

$$\mathcal{K} \supseteq \mathcal{K}_0 \supseteq \mathcal{K}_1 \supseteq \mathcal{K}_2 \supseteq \mathcal{K}_3.$$

Строгость каждого из этих вложений представляет собой открытую проблему. Многие из них хорошо известны, например:

$\mathcal{K} \neq \mathcal{K}_0$ — знаменитая проблема Капланского;
$\mathcal{K}_0 \neq \mathcal{K}_3$ — проблема вложения Ван дер Вардена в классе групповых алгебр;
$\mathcal{K}_1 \neq \mathcal{K}_3$ — проблема вложения Мальцева в классе групповых алгебр.

3.6. Базисы Грёбнера—Ширшова для модулей. Впервые понятие БГШ для модулей было введено С.-Ж. Кангом и К.-Х. Ли [81]. Другой подход к этому понятию был предложен Е. С. Чибриковым [60] при попытке построения линейных базисов свободных вертексной и лиевой конформной алгебр.

Мы приведем обе конструкции. Везде в этом разделе $\mathcal{X} = \{x_i \mid i \in I\}$ означает вполне упорядоченное множество.

Основные идеи и результаты работы [81] можно представить следующим образом. Для любой (ассоциативной) алгебры A, порожденной множеством $\mathcal{X}$, рассмотрим множество определяющих соотношений S такое, что $A = \Bbbk\langle\mathcal{X}|S\rangle$. Рассмотрим (левый) A-модуль $M = A/I$, где I — левый идеал в A. Пусть $\overline{T}$ означает множество порождающих идеала I над A, где T — некоторое множество прообразов элементов из T в свободной алгебре $\Bbbk\langle\mathcal{X}\rangle$. Без ограничения общности можно полагать, что S и T — подмножества унитарных многочленов в $\Bbbk\langle\mathcal{X}\rangle$. Таким образом, представление алгебры A, соответствующее A-модулю M, определяется парой множеств (S, T).

Для $f, g \in \Bbbk\langle\mathcal{X}\rangle$, $w \in X^*$ мы пишем $f \equiv g \pmod{S, T, w}$, если

$$f - g = \sum \alpha_i a_i s_i b_i + \sum \beta_j c_j t_j,$$

где $\alpha_i, \beta_j \in \Bbbk$, $a_i, b_i, c_i \in \mathcal{X}^*$, $s_i \in S$, $t_j \in T$, и $a_i \bar{s}_i b_i < w$, $c_j \bar{t}_j < w$ в смысле порядка deg-lex.

Определение 3.6.1 (см. [81]). *Композицией правого включения* (right-justified) называется

$$(f, g)_w = f - ag, \tag{3.6.1}$$

где $f \in S \cup T$, $g \in T$, $a \in \mathcal{X}^*$, $w = \bar{f} = a\bar{g}$.

Определение 3.6.2 (см. [81]). Пара (S, T) подмножеств унитарных многочленов в $\Bbbk\langle\mathcal{X}\rangle$ называется *парой Грёбнера—Ширшова* (ГШ-парой), если S замкнуто относительно композиции в смысле определения 2.2.1 и для любых $f \in T \cup S$, $g \in T$, $w \in \mathcal{X}^*$ таких, что композиция (3.6.1) определена, выполнено условие $(f, g)_w \equiv 0 \pmod{S, T, w}$.

Обозначим через $\mathrm{PBW}(S, T)$ множество приведенных слов:

$$\mathrm{PBW}(S, T) = \{u \in \mathcal{X}^* \mid u \neq a\bar{s}b,\ u \neq c\bar{t},\ s \in S,\ t \in T\}.$$

Следующий результат является аналогом CD-леммы.

Теорема 3.6.3 (см. [81]). *Пусть (S,T) — пара подмножеств унитарных многочленов в $\Bbbk\langle\mathcal{X}\rangle$. Обозначим через A и M соответственно алгебру и левый A-модуль, определенный парой (S,T). Тогда следующие утверждения эквивалентны*:

1) *(S,T) является ГШ-парой*;
2) *для каждого $f\in\Bbbk\langle\mathcal{X}\rangle$ такого, что f равен нулю в M, выполнено $\bar f\notin \mathrm{PBW}(S,T)$.*

Если одно из этих условий выполнено, то $\mathrm{PBW}(S,T)$ является линейным базисом модуля M. Обратное утверждение верно для конечномерных модулей или для градуированных модулей с конечномерными однородными подпространствами.

Любая пара (S,T) подмножеств унитарных многочленов может быть дополнена до ГШ-пары $(S^{\mathrm{comp}},T^{\mathrm{comp}})$ при помощи алгоритма, аналогичного тому, что используется обычно для алгебр.

В целях иллюстрации применения этого утверждения в [81] построены ГШ-пары и мономиальные PBW-базисы для конечномерных неприводимых представлений лиевой алгебры SL_3 (т.е. ее универсальной обертывающей). Другие примеры приведены в [82].

Представим также другой подход к понятию БГШ для представлений [60].

Для некоторой ассоциативной алгебры A и произвольного (левого) A-модуля M рассмотрим множества порождающих: $\mathcal{X}$ для алгебры A, и $\mathcal{Y}$ для модуля M над A. Предположим, что $\mathcal{X}$ и $\mathcal{Y}$ вполне упорядочены.

Пусть сначала $A=\Bbbk\langle\mathcal{X}\rangle$. Обозначим через $M=\mathrm{mod}_A\langle\mathcal{Y}\rangle$ свободный модуль над A, порожденный множеством $\mathcal{Y}=\{y_j\mid j\in J\}$. Пусть

$$M^*=\{x_{i_1}\dots x_{i_k}y_j\mid x_{i_p}\in\mathcal{X},\ y_j\in\mathcal{Y},\ k\geqslant 0\}.$$

Рассмотрим deg-lex порядок $\leqslant$ на M^*.

Поскольку $M=\Bbbk M^*$, любой многочлен $f\in M$ может быть единственным образом представлен в виде

$$f=\alpha_{\bar f}\bar f+\sum_j\alpha_j u_j,\quad \alpha_{\bar f},\alpha_j\in\Bbbk,\quad u_j\in M^*,\quad u_j<\bar f.$$

Как и выше, f называется унитарным, если $\alpha_{\bar f}=1$.

Определение 3.6.4 (см. [60]). Для двух унитарных многочленов $f,g\in M$ их *композицией* называется выражение $(f,g)_w=f-ag$, если существует $a\in\mathcal{X}^*$ такое, что $\bar f=a\bar g=w$.

Для данного непустого подмножества $S\subset M$ композиция $(f,g)_w$ называется *тривиальной по модулю* (S,w), если

$$(f,g)_w=\sum_j\alpha_j a_j s_j,$$

где $\alpha_j\in\Bbbk$, $a_j\in\mathcal{X}^*$, $s_j\in S$ и $a_j\bar s_j<w$. В этом случае мы пишем $(f,g)_w\equiv 0\ (\mathrm{mod}\ S,w)$.

Определение 3.6.5 (см. [60]). Пусть $S\subset M$ — множество унитарных многочленов. Множество S называется *базисом Грёбнера—Ширшова* (БГШ), если $(f,g)_w\equiv 0\ (\mathrm{mod}\ S,w)$ для любых $f,g\in S$.

Теорема 3.6.6 (лемма о композиции для модулей [60]). *Пусть $S\subset M$ — БГШ в смысле определения* 3.6.5. *Если $f\in\Bbbk\langle\mathcal{X}\rangle S$, то $\bar f=a\bar s$ для некоторых $s\in S$ и $a\in\mathcal{X}^*$. Обратное утверждение также верно.*

Следствие 3.6.7 (лемма о композиции—diamond-лемма для модулей [60]). *Пусть $S\subset M$ — множество унитарных многочленов. Множество S является БГШ тогда и только тогда*

$$\mathrm{PBW}(S)=\{u\in M^*\mid u\neq a\bar u\ \text{ ни для какого }\ s\in S,\ a\in\mathcal{X}^*\}$$

является линейным базисом $\Bbbk\langle\mathcal{X}\rangle$-модуля N, порожденного множеством $\mathcal{Y}$ с определяющими соотношениями S:

$$N=\mathrm{mod}_{\Bbbk\langle\mathcal{X}\rangle}\langle\mathcal{Y}|S\rangle=\mathrm{mod}_{\Bbbk\langle\mathcal{X}\rangle}\langle\mathcal{Y}\rangle/\Bbbk\langle\mathcal{X}\rangle S.$$

Последнее утверждение выглядит аналогичным теореме 3.6.3 (для случая $S = \emptyset$), но и для произвольной (не обязательно свободной) алгебры A определения 3.6.4 и 3.6.5 предоставляют более простую технику для вычисления БГШ для модулей.

Именно, пусть A — ассоциативная алгебра, порожденная множеством $\mathcal{X}$ с определяющими соотношениями R:

$$A = \Bbbk\langle \mathcal{X} | R\rangle.$$

Пусть N — A-модуль, порожденный (над A) множеством $\mathcal{Y}$ с определяющими соотношениями S:

$$N = \operatorname{mod}_A\langle \mathcal{Y} | S\rangle,$$

где $S \subset \operatorname{mod}_A\langle \mathcal{Y}\rangle$.

Допуская некоторую неточность в обозначениях, мы полагаем, что

$$S \subset \operatorname{mod}_{\Bbbk\langle\mathcal{X}\rangle}\langle \mathcal{Y}\rangle = M$$

есть множество «многочленов» от $\mathcal{X}$ и $\mathcal{Y}$. Тогда N есть также $\Bbbk\langle\mathcal{X}\rangle$-модуль вида

$$N = \operatorname{mod}_{\Bbbk\langle\mathcal{X}\rangle}\langle \mathcal{Y} | S \cup \{fu \mid f \in R,\, u \in M^*\}\rangle.$$

В таком виде теорема 3.6.6 и следствие 3.6.7 могут быть применены к модулю, представленному порождающими элементами и определяющими соотношениями над любой алгеброй A, также представленной порождающими элементами и определяющими соотношениями. Этот путь выглядит проще, чем вычисление БГШ для алгебры A и построение ГШ-пары для модуля, как предложено в [81]. Представленный в [60] подход дает возможность изучить строение собственно представления алгебры A, соответствующего A-модулю M вместо вычисления БГШ для самой алгебры A.

В [60] CD-лемма для модулей (следствие 3.6.7) применяется для изучения структуры свободной конформной алгебры Ли.

Следуя М. Ройтману [100], удобно рассматривать свободные конформные алгебры Ли вложенными в свободные вертексные алгебры. Понятие вертексной алгебры возникло в математической физике [35], формальное определение было дано Р. Борчердсом в [53]. Вертексные алгебры использовались в [53] для разрешения Moonshine-гипотезы в теории конечных групп (см. также [71]).

Определение 3.6.8 (см. [78])**.** Вертексная алгебра представляет собой линейное пространство $\mathfrak{B}$ над полем $\Bbbk$, $\operatorname{char}\Bbbk = 0$, с выделенным элементом $\mathbf{1} \in \mathfrak{B}$, снабженное линейным оператором $D : \mathfrak{B} \to \mathfrak{B}$, и семейством билинейных операций $(\cdot\ {}_{[n]}\ \cdot)$, $n \in \mathbb{Z}$, такое, что

(V1) $D\mathbf{1} = 0$;
(V2) $\mathbf{1}\ {}_{[n]}\ a = \delta_{-1,n}a$;
(V3) $a\ {}_{[-1]}\ \mathbf{1} = a$ и $a\ {}_{[n]}\ \mathbf{1} = 0$ для $n \geqslant 0$;
(V4) $D(a\ {}_{[n]}\ b) = a\ {}_{[n]}\ (Db) - na\ {}_{[n-1]}\ b$;
(V5) для любых $a, b \in \mathfrak{B}$ существует неотрицательное целое число $N(a,b)$ такое, что

$$Y(a,w)Y(b,z)(w-z)^{N(a,b)} = 0,$$

где операция $Y : \mathfrak{B} \to gl(\mathfrak{B})[[z, z^{-1}]]$ определена по правилу

$$Y(a,z) = \sum_{n\in\mathbb{Z}} (a\ {}_{[n]}\ \cdot)z^{-n-1}.$$

Из (V3), (V4) следует, что $a\ {}_{[-n-1]}\ \mathbf{1} = D^{(n)}a$, $n \geqslant 0$, где $D^{(n)} = D^n/n!$.

Числа $N(a,b)$, $a, b \in \mathfrak{B}$, определяют функцию локальности $N : (\mathfrak{B}\times\mathfrak{B}) \to \mathbb{Z}_+$. Любая вертексная алгебра является, в частности, конформной алгеброй Ли [78].

В [53] упоминается о существовании свободных вертексных алгебр. Такие объекты были построены М. Ройтманом [100]. Отношение между свободной алгеброй Ли и свободной вертексной алгеброй во многом схоже с отношением между алгеброй Ли и ее универсальной обертывающей ассоциативной алгеброй.

Именно, пусть $C(B,N)$ — свободная конформная алгебра Ли, порожденная множеством B с функцией локальности N. Тогда ее алгебра коэффициентов $L = \operatorname{Coeff} C(B,N)$ может быть представлена в виде

$$L = \operatorname{Lie}\langle \mathcal{X} | R_N\rangle,$$

где $\mathcal{X} = \{a(n) \mid a \in B,\ n \in \mathbb{Z}\}$, R_N состоит из соотношений

$$\sum_{s=0}^{N(a,b)} (-1)^s \binom{N(a,b)}{s} [a(n-s), b(m+s)] = 0, \quad a, b \in B, \quad n, m \in \mathbb{Z} \tag{3.6.2}$$

(см. [100]).

Пусть $\mathfrak{F}_N(B)$ — свободная вертексная алгебра, порожденная множеством B с функцией локальности $N : B \times B \to \mathbb{Z}_+$. Как показано в [100], $\mathfrak{F}_N(B)$ представляет собой модуль старшего веса над $U(L)$, порожденный элементом $\mathbf{1}$. В частности,

$$\mathfrak{F}_N(B) \simeq U(L) \otimes_{U(L_+)} \Bbbk\mathbf{1} = U(L)\mathbf{1},$$

где L_+ — подалгебра в L, порожденная множеством $\{a(n) \mid a \in B,\ n \geqslant 0\}$, и $a(n)\mathbf{1} = 0$ для $n \geqslant 0$.

Исходя из конструкции $\mathfrak{F}_N(B)$ (см. [100]), получаем

$$C(B, N) \simeq \sum_{\substack{j \geqslant 1 \\ a \in B}} U(L_+) a(-j)\mathbf{1}.$$

Используя вложение $C(B, N) \subset \mathfrak{F}_N(B)$, можно получить следующий результат, дающий определенное приближение к построению линейного базиса $C(B, N)$ в терминах конформных операций.

Теорема 3.6.9 (см. [60]). *Пусть $C(B, N)$ — свободная конформная алгебра Ли, порожденная множеством B с функцией локальности, равной константе (т.е. $N(a, b) \equiv N$ для всех $a, b \in B$). Тогда следующие элементы порождают $C(B, N)$ как линейное пространство*:

$$a_k(n_k)a_{k-1}(n_{k-1}) \dots a_0(n_0)b(-i-1)\mathbf{1} = a_k\ {}_{[n_k]}\ (a_{k-1}\ {}_{[n_{k-1}]} \dots (a_0\ {}_{[n_0]}\ D^{(i)}b) \dots),$$

где для любого $1 \leqslant j \leqslant k$ выполнено

$$n_j - n_{j-1} \leqslant \begin{cases} N, & a_j \leqslant a_{j-1}, \\ N-1, & a_j > a_{j-1}, \end{cases}$$

и либо

$$n_0 + i + 1 \leqslant \begin{cases} N, & a_0 \leqslant b, \\ N-1, & a_0 > b, \end{cases}$$

либо

$$n_0 + i + 1 > \begin{cases} N, & a_0 \leqslant b, \\ N-1, & a_0 > b. \end{cases}$$

Кроме того,

$$n_s + \dots + n_1 + 2n_0 \leqslant \begin{cases} \left(\frac{s(s+1)}{2} + 1\right) N - s - 2, & a_0 > b, \\ \left(\frac{s(s+1)}{2} + 1\right) N - s - 1, & a_0 \leqslant b \end{cases}$$

для всех $s = 0, \dots, k$.

Конформные мономы, описанные в теореме 3.6.9, не являются, вообще говоря, линейно независимыми, но в подпространстве, порожденном мономами длины 2, они образуют базис.

Предложение 3.6.10 (см. [60]). *Пусть $C(B, N)$ — свободная конформная алгебра Ли, порожденная множеством B с постоянной функцией локальности N. Тогда следующие мономы образуют линейный базис подпространства в $C(B, N)$, порожденного мономами длины* 2:

$$a_0\ {}_{[n_0]}\ D^i b, \quad a_0, b \in B,$$

где либо

$$n_0 + i + 1 \leqslant \begin{cases} N, & a_0 \leqslant b, \\ N-1, & a_0 > b, \end{cases}$$

либо

$$n_0 + i + 1 > \begin{cases} N, & a_0 \leqslant b, \\ N-1, & a_0 > b \end{cases}$$

и $0 \leqslant n_0 < \frac{N}{2}$.

4. Конформные алгебры и псевдоалгебры

Теория конформных алгебр (см. [78–80]) является сравнительно новой областью алгебры, тесно связанной с математической физикой. Общий категорный подход к этой теории связан с понятием псевдотензорной категории [34] (или мультикатегории [89]). Многие факты, общие для обычных и конформных алгебр, могут быть объяснены с более общей точки зрения.

4.1. Псевдоалгебры. Понятие псевдоалгебры [32, 34] появилось как «многомерный» аналог конформной алгебры. Обобщение состоит в том, что полиномиальная алгебра $\Bbbk[D]$ заменяется на некоторую алгебру Хопфа H.

Пусть H — кокоммутативная алгебра Хопфа с копроизведением $\Delta : H \to H \otimes H$, коединицей $\varepsilon : H \to \Bbbk$ ($\operatorname{char}\Bbbk = 0$), и антиподом $S : H \to H$ (см., например, [104]).

Чтобы упростить обозначения, мы будем использовать следующее сокращение:

$$\Delta(h) = \sum_{(h)} h_{(1)} \otimes h_{(2)} = h_{(1)} \otimes h_{(2)}.$$

Определим $\Delta^{[n]} : H \to H^{\otimes n}$ следующим образом:

$$\Delta^{[1]} = \mathrm{id},$$
$$\Delta^{[k+1]} = (\Delta^{[k]} \otimes \mathrm{id})\Delta = (\mathrm{id} \otimes \Delta^{[k]})\Delta, \quad 1 \leqslant k \leqslant n-1,$$
$$\Delta^{[n]}(h) = h_{(1)} \otimes \cdots \otimes h_{(n)}.$$

На векторном пространстве $H^{\otimes n} = H \otimes \cdots \otimes H$ имеется естественная структура правого H-модуля:

$$(f_1 \otimes \cdots \otimes f_n)h = f_1 h_{(1)} \otimes \cdots \otimes f_n h_{(n)}, \quad f_i, h \in H.$$

Поскольку алгебра Хопфа H кокоммутативна, любая перестановка тензорных множителей в $H^{\otimes n}$ является изоморфизмом H-модулей. Кроме того, H действует на двойственном пространстве $X = H^*$ посредством левых/правых сдвигов:

$$\langle xf, g\rangle = \langle x, gS(f)\rangle, \quad \langle fx, g\rangle = \langle x, S(f)g\rangle, \quad f, g \in H,\ x \in X.$$

Это действие согласовано с умножением на X (двойственным к копроизведению на H) таким образом, что X является H-дифференциальной алгеброй:

$$h(xy) = (h_{(1)}x)(h_{(2)}y), \quad (xy)h = (h_{(2)}x)(h_{(1)}y), \quad x, y \in X,\ h \in H.$$

Определение 4.1.1 (см. [32])**.** Пусть P — левый H-модуль. Билинейное по H отображение

$$* : P \otimes P \to (H \otimes H) \otimes_H P$$

называется *псевдопроизведением*.

Определение 4.1.2 (см. [32])**.** *Псевдоалгеброй* над H (или *H-псевдоалгеброй*) называется H-модуль P, снабженный псевдопроизведением $*$. Псевдоалгеброй *конечного типа* называется псевдоалгебра, представляющая собой конечно порожденный H-модуль.

В данной работе мы рассматриваем следующие классы алгебр Хопфа: $H = U(\mathfrak{h})$ и $H = U(\mathfrak{h})\#\Bbbk[\Gamma]$, где $\mathfrak{h}$ — алгебра Ли, Γ — группа, действующая автоморфизмами на $U(\mathfrak{h})$. Эти классы алгебр исчерпывают все кокоммутативные алгебры Хопфа над алгебраически замкнутым полем характеристики нуль (см., например, [104]). Для алгебр Хопфа из этих классов имеет место следующая лемма.

Лемма 4.1.3 (см. [32]). *Пусть $\{h_i\}$ — базис алгебры H. Тогда любой элемент $f \in H \times H$ может быть единственным образом представлен в виде*

$$f = \sum_i (h_i \otimes 1)\Delta(l_i), \quad l_i \in H. \tag{4.1.1}$$

Полезно рассмотреть способ нахождения формы (4.1.1) для произвольного элемента из $H \otimes H$:

$$(f \otimes g) = (fS(g_{(1)}) \otimes 1)\Delta(g_{(2)}).$$

Из леммы 4.1.3 следует, что для любых $a, b \in P$ и фиксированного базиса $\{h_i\}$ алгебры H единственным образом определено конечное семейство $\{c_i\} \subset P$ такое, что

$$a * b = \sum_i h_i \otimes 1 \otimes_H c_i.$$

Тогда можно определить операцию

$$(a \ {}_x \ b) = \sum_i \langle x, S(h_i)\rangle c_i,$$

где $x \in X \equiv H^*$. Полученные *x-произведения* обладают следующими свойствами:

$$\operatorname{codim}\{x \in X \mid (a \ {}_x \ b) = 0\} < \infty, \tag{4.1.2}$$

$$(ha \ {}_x \ b) = a \ {}_{xh} \ b, \quad (a \ {}_x \ hb) = h_{(2)}(a_{S(h_{(1)})x}b). \tag{4.1.3}$$

Соотношения (4.1.2) и (4.1.3) подобны свойствам локальности (C1) и полуторалинейности (C2) соответственно.

Как было указано выше, понятие псевдоалгебры является более общим, чем понятия обычной и конформной алгебры. Действительно, обычная алгебра A над полем $\Bbbk$ есть в точности $\Bbbk$-псевдоалгебра: для $a, b \in A$ имеем

$$a * b = (1 \otimes 1) \otimes ab.$$

Для $H = \Bbbk[D]$ понятие H-псевдоалгебры совпадает с понятием конформной алгебры [32]: соответствие между n-произведениями и псевдопроизведением задано формулой

$$a * b = \sum_{n \geqslant 0} (-D)^{(n)} \otimes 1 \otimes_H a \ {}_n \ b.$$

4.2. Тождества на псевдоалгебрах. Псевдопроизведение в смысле определения 4.1.1 есть частный случай мультиоперации в псевдотензорной категории [34] $\mathcal{M}^*(H)$ левых H-модулей (см. также [32]). Именно, мультиоперацией на H-модулях называется H-полилинейное отображение

$$\varphi : M_1 \otimes \cdots \otimes M_n \to H^{\otimes n} \otimes_H M, \tag{4.2.1}$$

где $M, M_1, \ldots, M_n$ — H-модули. Обозначим через $\mathcal{P}\big(\{M_i\}_{i=1}^n, M\big)$ множество отображений вида (4.2.1). Пусть

$$\varphi \in \mathcal{P}\big(\{N_i\}_{i=1}^m, M\big), \quad \psi_i \in \mathcal{P}\big(\{M_j\}_{j=n_i+1}^{n_{i+1}}, N_i\big),$$

где $i = 1, \ldots, m$, $0 = n_1 < n_2 < \cdots < n_{m+1} = n$. Тогда можно определить следующую мультиоперацию [34]:

$$\chi = \varphi(\psi_1, \ldots, \psi_m) \in \mathcal{P}\big(\{M_i\}_{i=1}^n, M\big),$$

$$\chi(F_1 \otimes_H a_1, \ldots, F_m \otimes_H a_m) = (F_1 \otimes \cdots \otimes F_m \otimes_H 1)(\Delta^{[k_1]} \otimes \cdots \otimes \Delta^{[k_m]} \otimes_H \mathrm{id})\varphi(a_1, \ldots, a_m), \tag{4.2.2}$$

где $k_j = n_{j+1} - n_j$, $F_j \in H^{\otimes k_j}$, $j = 1, \ldots, m$ (ср. с [32]).

Пусть P — псевдоалгебра. Суперпозиция (4.2.2) позволяет рассматривать длинные термы, построенные по бинарной операции $*$ как мультиоперации над P. Например, если обозначить $\varphi = \psi_1 = *$, $\psi_2 = \mathrm{id}$, то

$$(\varphi(\psi_1, \psi_2))(a, b, c) = (a * b) * c \in H^{\otimes 3} \otimes_H P, \quad a, b, c \in P,$$

и т. д. Перестановка аргументов мультиопераций реализуется при помощи действия симметрической группы [32]:

$$\varphi^{\sigma}(a_{1\sigma},\dots,a_{m\sigma}) = (\sigma^{-1}\otimes_H \mathrm{id}_P)\varphi(a_1,\dots,a_m), \quad \sigma\in\mathbb{S}_m,$$

которое эквивариантно относительно суперпозиции (4.4.2).

Рассмотрим псевдоалгебру A над $H=\Bbbk$ (обычную алгебру). Пусть φ обозначает псевдопроизведение (т.е. обычное умножение) на A. Тогда, например, уравнение $x(yz)=(zx)y$ может быть переписано в виде

$$(\varphi(\mathrm{id},\varphi))(x,y,z) = (\varphi(\varphi,\mathrm{id}))^{\sigma}(x,y,z),$$

где $\sigma=(1\,2\,3)\in\mathbb{S}_3$.

В общем случае любое полилинейное однородное выражение в обычной алгебре может быть записано в виде

$$\sum_{\sigma\in\mathbb{S}_n} t_\sigma(x_{1\sigma},\dots,x_{n\sigma}) = 0, \tag{4.2.3}$$

где каждое слагаемое $t_\sigma(y_1,\dots,y_n)$ представляет собой линейную комбинацию неассоциативных слов, полученных из ассоциативного слова $y_1\dots y_n$ некоторой расстановкой скобок.

Каждый терм t_σ может быть отождествлен с мультиоперацией, построенной из φ и id с использованием суперпозиций вида (4.2.2) и линейных комбинаций. Тогда выражение (4.2.3) может быть переписано в следующей форме:

$$\sum_{\sigma\in\mathbb{S}_n} t_\sigma^{\sigma^{-1}}(x_1,\dots,x_n) = 0.$$

Это соотношение может быть перенесено на случай псевдоалгебр как непосредственный аналог (4.2.3).

Определение 4.2.1. Пусть Ω — некоторое многообразие псевдоалгебр, заданное семейством однородных полилинейных тождеств вида (4.2.3). Псевдоалгебра P считается принадлежащей многообразию псевдоалгебр Ω, если на ней выполнены соответствующие «псевдо»-аналоги этих тождеств:

$$\sum_{\sigma\in\mathbb{S}_n} (\sigma\otimes_H \mathrm{id})t_\sigma^*(x_{1\sigma},\dots,x_{n\sigma}) = 0, \tag{4.2.4}$$

где t^* означает терм t относительно псевдопроизведения $*$.

Это определение согласуется с определением 2.3.2, а именно, имеет место следующая теорема.

Теорема 4.2.2 (см. [88])**.** *Пусть C — конформная алгебра, т.е. $\Bbbk[D]$-псевдоалгебра. Тогда C удовлетворяет тождеству* (4.2.4) *если и только если* $\operatorname{Coeff} C$ *удовлетворяет* (4.2.3).

Например, приведем аналоги некоторых широко известных тождеств (см. [32, 80, 100]):

$$\begin{aligned}
\text{ассоциативность:}&\quad a*(b*c) = (a*b)*c;\\
\text{(анти)коммутативность:}&\quad a*b \pm (\sigma_{12}\otimes_H \mathrm{id})(b*a) = 0;\\
\text{тождество Якоби:}&\quad (a*(b*c)) - (\sigma_{12}\otimes_H \mathrm{id})(b*(a*c)) = (a*b)*c.
\end{aligned}$$

Точно таким же способом легко получить йорданово тождество для псевдоалгебр:

$$\begin{aligned}
&(a*(b*(c*d))) + (\sigma_{14}\otimes_H \mathrm{id})(d*(b*(c*a))) + (\sigma_{13}\otimes_H \mathrm{id})(c*(b*(a*d))) =\\
&\quad = ((a*b)*(c*d)) + (\sigma_{23}\otimes_H \mathrm{id})((a*c)*(b*d)) + (\sigma_{24}\otimes_H \mathrm{id})((a*d)*(c*b)).
\end{aligned} \tag{4.2.5}$$

Предложение 4.2.3 (см. [32, 88])**.** *Пусть P — ассоциативная псевдоалгебра с псевдопроизведением $*$. Тогда новые операции, заданные на P по формулам*

$$[a*b] = (a*b) - (\sigma_{12}\otimes_H \mathrm{id})(b*a), \quad (a\circ b) = (a*b) + (\sigma_{12}\otimes_H \mathrm{id})(b*a),$$

также являются псевдопроизведениями на P. Более того, $P^{(-)} = (P,[\cdot*\cdot])$ является лиевой псевдоалгеброй, а $P^{(+)} = (P,(\cdot\circ\cdot))$ — йордановой.

Для лиевой конформной алгебры мы также будем использовать символ $(\cdot\ {}_{[n]}\ \cdot)$, $n\geqslant 0$, для обозначения конформных операций.

4.3. Комодульные конструкции псевдоалгебр. Пусть H — кокоммутативная алгебра Хопфа. Тогда H-комодульной алгеброй мы называем алгебру A (не обязательно ассоциативную), снабженную гомоморфизмом алгебр $\Delta_A : A \to H \otimes A$, удовлетворяющим условию

$$(\Delta \otimes \mathrm{id}_A)\Delta_A = (\mathrm{id}_H \otimes \Delta_A)\Delta_A.$$

Предложение 4.3.1 (см. [87]). *Пусть A — ассоциативная H-комодульная алгебра. Тогда свободный H-модуль $\mathfrak{A} = H \otimes A$ с псевдопроизведением*

$$(h \otimes a) * (g \otimes b) = (hb_{(1)} \otimes g) \otimes_H (1 \otimes ab_{(2)}) \tag{4.3.1}$$

или

$$(h \otimes a) * (g \otimes b) = (h \otimes gS(a_{(1)})) \otimes_H (1 \otimes a_{(2)}b) \tag{4.3.2}$$

является ассоциативной псевдоалгеброй.

Предложение 4.3.2. *Пусть H — коммутативная алгебра Хопфа и A — ассоциативная H-комодульная алгебра. Тогда $\mathfrak{A} = H \otimes A$ с псевдопроизведением*

$$(h \otimes a) * (g \otimes b) = (h \otimes ga_{(1)}) \otimes_H (1 \otimes a_{(2)}b) \tag{4.3.3}$$

является ассоциативной псевдоалгеброй.

Для доказательства двух последних предложений достаточно непосредственно проверить условие ассоциативности:

$$x * (y * z) = (x * y) * z, \quad x, y, z \in \mathfrak{A}.$$

Предложение 4.3.3. *Пусть H — коммутативная* (*и кокоммутативная*) *алгебра Хопфа, A — некоторая H-комодульная алгебра. Тогда $H \otimes A$ с псевдопроизведением*

$$(h \otimes a) * (g \otimes b) = (hb_{(1)} \otimes ga_{(1)}) \otimes_H (1 \otimes a_{(2)}b_{(2)}) \tag{4.3.4}$$

является H-псевдоалгеброй.

Если A удовлетворяет тождеству (4.2.3)*, то псевдоалгебра $H \otimes A$ с псевдопроизведением* (4.3.4) *удовлетворяет тождеству* (4.2.4).

Достаточно заметить, что из условия предложения 4.3.3 следует

$$t^*(a_1, \dots, a_n) = \left(\bigoplus_{k=1}^{n} a_{1(k-1)} \dots a_{k-1(k-1)} a_{k+1(k)} \dots a_{n(k)} \right) \otimes_H (1 \otimes t(a_{1(n)}, \dots, a_{n(n)})).$$

Пример 4.3.4. Пусть A — произвольная алгебра. Ее можно рассматривать как H-комодульную алгебру относительно $\Delta_A : a \mapsto 1 \otimes a$, $a \in A$. Тогда $H \otimes A$ с псевдопроизведением (4.3.4) есть не что иное, как известная *псевдоалгебра петель* (или *токов*) $\mathrm{Cur}^H A$.

Пример 4.3.5. Пусть $H = \Bbbk[D]$ и $A = \Bbbk[v]$, $\Delta_A(v) = D \otimes 1 + 1 \otimes v$. Алгебра $W = H \otimes A$, снабженная одним из псевдопроизведений (4.3.1)–(4.3.3), известна как *конформная алгебра Вейля*. Ее присоединенная конформная алгебра Ли $W^{(-)}$ содержит так называемую *конформную алгебру Вирасоро* $\mathrm{Vir} = \Bbbk[D] \otimes \Bbbk v$:

$$v\ {}_{[0]}\ v = Dv, \quad v\ {}_{[1]}\ v = 2v, \quad v\ {}_{[n]}\ v = 0, \quad n \geqslant 2.$$

Пример 4.3.6. Любая кокоммутативная алгебра Хопфа H может рассматриваться как H-комодульная алгебра с регулярной структурой: $\Delta_H = \Delta$. Если $\mathfrak{h}$ — конечномерная алгебра Ли и $H = U(\mathfrak{h})$, то $W(H) = H \otimes H$ с псевдопроизведением (4.3.1) является ассоциативной псевдоалгеброй. Ее присоединенная псевдоалгебра Ли $W(H)^{(-)}$ содержит псевдоалгебру *векторных полей* $W(\mathfrak{h})$ [32].

Замечание 4.3.7. Как было показано в [32, 34], каждая псевдоалгебра Ли конечного типа над $H = U(\mathfrak{h})$, $\dim \mathfrak{h} < \infty$, $\Bbbk = \mathbb{C}$, изоморфна либо алгебре петель над конечномерной простой алгеброй Ли, либо алгебре петель над некоторой подалгеброй в $W(\mathfrak{h})$. В случае конформных алгебр ($\dim \mathfrak{h} = 1$) $W(\mathfrak{h})$ есть в точности конформная алгебр Вирасоро.

Пример 4.3.8. Пусть A — ассоциативная алгебра и $A[v]$ — алгебра полиномов от v над A. Тогда $A[v]$ можно рассматривать как $\Bbbk[D]$-комодульную алгебру относительно Δ_F, заданного правилом

$$\begin{aligned} \Delta_F : a &\mapsto 1 \otimes a, \quad a \in A, \\ v &\mapsto D \otimes 1 + 1 \otimes v. \end{aligned} \tag{4.3.5}$$

В этом случае $\mathfrak{A}[v] = \Bbbk[D] \otimes A[v]$ с псевдопроизведением (4.3.1) является ассоциативной конформной алгеброй. Если $A = U(\mathfrak{g})$, где $\mathfrak{g}$ — алгебра Ли, то $\mathfrak{A}[v]^{(-)}$ содержит полупрямое произведение $\operatorname{Cur}\mathfrak{g} \ltimes \operatorname{Vir}$ конформных алгебр $\operatorname{Cur}\mathfrak{g}$ и Vir (ср. [16, 67]).

Комодульная конструкция, приведенная в предложении 4.3.1, оказывается достаточно универсальной. Рассмотрим произвольное множество порождающих B и пусть $F(B) = \Bbbk\langle B \cup \{v\}\rangle$ — свободная ассоциативная алгебра, порожденная множеством B с добавочным элементом v («элементом Вирасоро»). Алгебра $F(B)$ наделена структурой комодульной алгебры, аналогичной (4.3.5). Обозначим через $\mathcal{F}(B)$ псевдоалгебру $H \otimes F(B)$ с псевдопроизведением (4.3.1).

Теорема 4.3.9. *Зафиксируем неотрицательную функцию $n(a) \in \mathbb{Z}_+$, $a \in B$. Тогда псевдоалгебра $\mathcal{F}_n(B)$, порожденная в $\mathcal{F}(B)$ элементами $\{1 \otimes v^{(n(a)-1)}a \mid a \in B\}$, изоморфна свободной ассоциативной конформной алгебре, порожденной множеством B с функцией локальности $N(a,b) = n(b)$.*

Здесь мы использовали символ $v^{(m)}$ для обозначения элемента $v^m/m!$. Для доказательства этой теоремы достаточно заметить, что образы нормальных слов (2.3.2) в $C(B,N)$ линейно независимы в $\mathcal{F}(B)$.

Следствие 4.3.10. *Любая конечно порожденная ассоциативная конформная алгебра является гомоморфным образом некоторой подалгебры в $\mathcal{F}(B)$.*

4.4. Ассоциативные обертывающие псевдоалгебры. Предложение 4.2.3 позволяет ввести естественное понятие ассоциативной обертывающей псевдоалгебры для псевдоалгебры Ли.

Определение 4.4.1. *Ассоциативной обертывающей* псевдоалгеброй для данной псевдоалгебры Ли L (H считается кокоммутативной) мы называем пару (A, φ), где A — ассоциативная H-псевдоалгебра, $\varphi : L \to A^{(-)}$ — гомоморфизм H-псевдоалгебр Ли и A порождена образом $\varphi(L)$ как ассоциативная H-псевдоалгебра.

Обозначим класс всех ассоциативных обертывающих псевдоалгебр для данной псевдоалгебры Ли L через $\operatorname{Env}(L)$. Если существует такая псевдоалгебра $(A, \varphi) \in \operatorname{Env}(L)$, что гомоморфизм φ инъективен, то псевдоалгебра L называется *специальной*.

Замечание 4.4.2. Как было показано М. Ройтманом [101], свободная конформная алгебра Ли $\operatorname{Lie} C(B,N)$ не является специальной. Остается открытым вопрос, является ли любая псевдоалгебра Ли (или даже конформная алгебра) конечного типа специальной. Легко заметить (см. пример 4.3.6 и замечание 4.3.7), что любая простая (и полупростая) псевдоалгебра Ли конечного типа специальна.

В общем случае имеет место следующее свойство.

Теорема 4.4.3 (см. [87])**.** *Пусть L — лиева $U(\mathfrak{h})\#\Bbbk[\Gamma]$-псевдоалгебра, имеющая конечный тип над $U(\mathfrak{h})$, $\dim \mathfrak{h} < \infty$. Тогда любая ассоциативная обертывающая псевдоалгебра для L удовлетворяет условию обрыва возрастающих цепей левых идеалов* (*т.е. является нетеровой*).

Следствие 4.4.4 (см. [16])**.** *Конечно порожденная ассоциативная коммутативная конформная алгебра нетерова.*

Последнее утверждение было высказано в качестве гипотезы В. Кацем (2000 г., устное сообщение).

Одним из канонических приложений CD-леммы является доказательство утверждений о вложении в духе теоремы Пуанкаре—Биркгофа—Витта. Естественно использовать этот же метод для

случая конформных алгебр. Действительно, пусть L — конформная алгебра Ли, порожденная множеством $B = \{a_i \mid i \in I\}$ как $\Bbbk[D]$-модуль. Предположим, что функция локальности ограничена: $N(a_i, a_j) \leqslant N$ для всех $i, j \in I$. Запишем таблицу умножения для L:

$$a_{i\ [n]}\ a_j = \sum_k \alpha_{ij}^{kn} a_k, \quad \alpha_{ij}^{kn} \in \Bbbk[D], \quad i \geqslant j, \quad i, j \in I, \quad n < N.$$

Обозначим через $U_N(L)$ универсальную обертывающую ассоциативную конформную алгебру для L, соответствующую данным B, N (см. [101]). По определению

$$U_N(L) = C\Big(B, N \;\Big|\; s_{ij}^n = a_{i\ n}\ a_j - \{a_j\ _n\ a_i\} - a_{i\ [n]}\ a_j = 0, \quad i \geqslant j, \quad i, j \in I, \quad n < N\Big),$$

где

$$\{a\ _n\ b\} = \sum_{s \geqslant 0} (-1)^{n+s} D^{(s)} (a\ _{n+s}\ b).$$

Пусть $S = \{s_{ij}^n \mid i \geqslant j,\ i, j \in I,\ n < N\}$.

К сожалению, в общем случае множество S не замкнуто относительно композиции (см. замечание 4.4.2). Тем не менее, следующая «частичная» замкнутость имеет место (1/2-PBW теорема для конформных алгебр Ли).

Теорема 4.4.5 (см. [29, 44])**.** *Любой многочлен $s_{ij\ m}^n\ a_k - a_{i\ n}\ s_{jk}^m$, где $i > j > k$, $n < N$, $m < N$, тривиален по модулю (S, w), где $w = a_{i\ n}\ a_{j\ m}\ a_k$.*

Для любой простой конформной алгебры Ли L ее универсальная обертывающая ассоциативная конформная алгебра (соответствующая некоторой функции «ассоциативной» локальности) либо равна нулю, либо содержит L. В работе [44] были найдены БГШ «минимальных» универсальных обертывающих для конформных алгебр $L = \mathrm{Vir}$, $\mathrm{Cur}\,\mathfrak{g}$, $\mathrm{Cur}\,\mathfrak{g} \ltimes \mathrm{Vir}$ (см. также [16]). Мы приведем конструкцию и найдем БГШ минимальной универсальной обертывающей ассоциативной конформной алгебры для простой конформной супералгебры Ли серии W_N.

Конформная супералгебра представляет собой, как обычно, прямую сумму четного и нечетного подмодулей:

$$C = C_0 \oplus C_1, \quad C_{i\ n}\ C_j \subseteq C_{(i+j) \bmod 2}.$$

Антикоммутативность и тождество Якоби естественно преобразуются для этого $\mathbb{Z}_2$-градуированного случая. Четность однородного элемента a будем обозначать через $p(a)$.

Рассмотрим конструкцию алгебры W_N и ее минимальной универсальной обертывающей [22, 59, 72]. Пусть A_N — ассоциативная алгебра с единицей, порожденная множеством $\mathcal{X} = \{v, \xi_i, \partial_i \mid i = 1, \ldots, N\}$ со следующими определяющими соотношениями:

$$[v, x] = 0,\ x \in \{\xi_i, \partial_i\}, \qquad \xi_j \xi_k = -\xi_k \xi_j, \qquad \partial_i \partial_k + \partial_k \partial_i = 0, \qquad \partial_i \xi_j + \xi_j \partial_i = \delta_{ij}.$$

Превратим A_N в $H = \Bbbk[D]$-комодульную алгебру следующим образом:

$$\Delta(v) = 1 \otimes v + D \otimes 1, \quad \Delta(\xi_i) = 1 \otimes \xi_i, \quad \Delta(\partial_i) = 1 \otimes \partial_i$$

(легко проверить, что все необходимые свойства выполнены).

Обозначим через $\mathfrak{A}_N$ ассоциативную псевдоалгебру $H \otimes A_N$ с псевдопроизведением (4.3.3). Определим четность на A_N соотношениями $p(v) = 0$, $p(\xi_i) = p(\partial_i) = 1$, $i = 1, \ldots, N$. Подалгебра в $\mathfrak{A}_N^{(-)}$, порожденная элементами

$$h \otimes \xi_{i_1} \ldots \xi_{i_r} v, \quad h \otimes \xi_{i_1} \ldots \xi_{i_r} \partial_i, \quad h \in H, \tag{4.4.1}$$

и есть конформная алгебра W_N. В дальнейшем мы будем отождествлять $-\xi_1 \ldots \xi_i v$ с $\xi_1 \ldots \xi_i$.

Замечание 4.4.6. Как показано в [59, 72], любая простая конформная супералгебра Ли конечного типа ($\Bbbk = \mathbb{C}$) изоморфна либо алгебре петель, либо некоторой подалгебре в W_N для подходящего N.

Вложение $W_N \to \mathfrak{A}_N^{(-)}$ является на самом деле универсальным: ассоциативная конформная подалгебра, порожденная в $\mathfrak{A}_N$ элементами (4.4.1), изоморфна минимальной универсальной обертывающей $U_L(W_N)$, где L — минимальная функция ассоциативной локальности $L : \mathcal{X}^2 \to \mathbb{Z}_+$ такая, что $U_L(W_N) \neq 0$ [22]. Эта функция L задана следующим образом:

$$L(v,\xi_i) = L(v,\partial_j) = L(v,v) = 2, \quad L(\xi_i,\partial_j) = 2, \quad L(\partial_j,\xi_i) = 1,$$
$$L(\xi_i,\xi_j) = \begin{cases} 2, & i \neq j, \\ 0, & i = j, \end{cases} \quad L(\partial_i,\partial_j) = \begin{cases} 1, & i \neq j, \\ 0, & i = j. \end{cases} \tag{4.4.2}$$

Определяющие соотношения для $U_L(W_N)$ имеют вид

$$\begin{gathered} \partial_j \,{}_0\, \xi_i + \xi_i \,{}_0\, \partial_j - D(\xi_i \,{}_1\, \partial_j) = \delta_{ij} v, \\ 2\xi_i \,{}_0\, \xi_j + 2\xi_j \,{}_0\, \xi_i = D(\xi_i \,{}_1\, \xi_j) + D(\xi_j \,{}_1\, \xi_i), \quad v \,{}_1\, v = v, \\ \partial_i \,{}_0\, \partial_j + \partial_j \,{}_0\, \partial_i = 0, \quad v \,{}_0\, \xi_i - \xi_i \,{}_0\, v + D(\xi_i \,{}_1\, v) = D\xi_i, \\ \xi_i \,{}_0\, v - v \,{}_0\, \xi_i + D(v \,{}_1\, \xi_i) = D\xi_i, \quad \xi_i \,{}_1\, v + v \,{}_1\, \xi_i = 2\xi_i, \\ \partial_j \,{}_0\, v - v \,{}_0\, \partial_j + D(v \,{}_1\, \partial_j) = 0, \quad \partial_j \,{}_1\, v + v \,{}_1\, \partial_j = \partial_j. \end{gathered} \tag{4.4.3}$$

Теорема 4.4.7. *БГШ универсальной обертывающей конформной алгебры $U_L(W_N)$ состоит из соотношений* (4.4.2) *и* (4.4.3)*, соотношений*

$$\begin{gathered} \partial_i \,{}_0\, \partial_j = -\partial_j \,{}_0\, \partial_i, \ i > j, \\ \partial_i \,{}_0\, \xi_j + \xi_j \,{}_0\, \partial_i - D(\xi_j \,{}_1\, \partial_i) = v\delta_{ij}, \quad \partial_i \,{}_0\, v - v \,{}_0\, \partial_i + D\partial_i = 0, \\ \xi_i \,{}_1\, \xi_j = -\xi_j \,{}_1\, \xi_i, \quad \xi_i \,{}_0\, \xi_j = -\xi_j \,{}_0\, \xi_i, \quad i > j, \\ v \,{}_1\, v = v, \quad \xi_i \,{}_0\, v = v \,{}_0\, \xi_i, \quad \xi_i \,{}_1\, v = \xi_i, \quad v \,{}_1\, \xi_i = \xi_i, \quad v \,{}_1\, \partial_j = \partial_j, \end{gathered} \tag{4.4.4}$$

соотношений

$$\begin{gathered} [v \,{}_0\, \xi_{i_1} \,{}_0\, \cdots \,{}_0\, \xi_{i_k} \,{}_1\, \xi_{i_{k+1}}] = [\xi_{i_1} \,{}_0\, \cdots \,{}_0\, \xi_{i_{k-1}} \,{}_0\, \xi_{i_k} \,{}_0\, \xi_{i_{k+1}}], \quad i_1 < \cdots < i_{k+1}, \\ [v \,{}_0\, \xi_{i_1} \,{}_0\, \cdots \,{}_0\, \xi_{i_k} \,{}_1\, \partial_j] = [\xi_{i_1} \,{}_0\, \cdots \,{}_0\, \xi_{i_{k-1}} \,{}_0\, \xi_{i_k} \,{}_0\, \partial_j], \quad i_1 < \cdots < i_k, \\ [\partial_i \,{}_0\, v \,{}_0\, x] = [v \,{}_0\, \partial_i \,{}_0\, x], \quad x \in X, \\ [\partial_i \,{}_0\, \xi_j \,{}_0\, \xi_k] + [\xi_j \,{}_0\, \partial_i \,{}_0\, \xi_k] = \delta_{ij} v \,{}_0\, \xi_k, \quad j \neq k, \\ [\partial_i \,{}_0\, \xi_j \,{}_1\, \xi_k] + [\xi_j \,{}_1\, \partial_i \,{}_0\, \xi_k] = \delta_{ij}\xi_k, \quad j \neq k, \\ [\partial_i \,{}_0\, \xi_j \,{}_0\, \partial_k] + [\xi_j \,{}_0\, \partial_i \,{}_0\, \partial_k] = \delta_{ij} v \,{}_0\, \partial_k, \\ [\partial_i \,{}_0\, \xi_j \,{}_1\, \partial_k] + [\xi_j \,{}_1\, \partial_i \,{}_0\, \partial_k] = \delta_{ij}\partial_k, \\ [\xi_i \,{}_1\, \xi_j \,{}_0\, x] = 2[\xi_i \,{}_0\, \xi_j \,{}_1\, x], \quad x > \xi_j, \quad i < j, \end{gathered} \tag{4.4.5}$$

а также соотношений

$$[\xi_i \,{}_0\, \partial_J \,{}_0\, \xi_j] + [\xi_j \,{}_0\, \partial_J \,{}_0\, \xi_i] = \sum_{t=1}^{q} (-1)^{t+1} (\delta_{ij_t} [v \,{}_0\, \partial_{J_t} \,{}_0\, \xi_j] + \delta_{jj_t} [v \,{}_0\, \partial_{J_t} \,{}_0\, \xi_i]), \quad i > j, \tag{4.4.6}$$

$$[\xi_i \,{}_0\, \partial_J \,{}_0\, \xi_i] = \sum_{t=1}^{q} (-1)^{t+1} \delta_{ij_t} [v \,{}_0\, \partial_{J_t} \,{}_0\, \xi_i], \tag{4.4.7}$$

$$[\xi_i \,{}_1\, \partial_J \,{}_0\, \xi_j] + [\xi_j \,{}_1\, \partial_J \,{}_0\, \xi_i] = \sum_{t=1}^{q} (-1)^{t+1} (\delta_{ij_t} [\partial_{J_t} \,{}_0\, \xi_j] + \delta_{jj_t} [\partial_{J_t} \,{}_0\, \xi_i]), \quad i > j, \tag{4.4.8}$$

$$[\xi_i \,{}_1\, \partial_J \,{}_0\, \xi_i] = \sum_{t=1}^{q} (-1)^{t+1} \delta_{ij_t} [\partial_{J_t} \,{}_0\, \xi_i], \tag{4.4.9}$$

$$[\xi_i \,{}_0\, \partial_J \,{}_0\, v] - (-1)^q [v \,{}_0\, \partial_J \,{}_0\, \xi_i] = \sum_{t=1}^{q} (-1)^{t+1} \delta_{ij_t} [v \,{}_0\, \partial_{J_t} \,{}_0\, \xi_i], \tag{4.4.10}$$

$$[\xi_{i\ 1}\ \partial_{J\ 0}\ v] - (-1)^q[\partial_{J\ 0}\ \xi_i] = \sum_{t=1}^{q}(-1)^{t+1}\delta_{ij_t}[\partial_{J_t\ 0}\ v], \tag{4.4.11}$$

где $[\dots]$ *означает правонормированную расстановку скобок,* $J = \{j_1, \dots, j_q\}$ *— упорядоченное подмножество в* $\{1, \dots, N\}$*,* $J_t = J \setminus \{j_t\}$*,* $\partial_J = \partial_{j_1} \dots \partial_{j_q}$*.*

Пусть S — множество соотношений (4.4.2)–(4.4.5). Тогда $\mathrm{PBW}(S)$ — линейный базис $U_L(W_N)$, но S не замкнуто относительно композиции. Чтобы замкнуть S, необходимо добавить соотношения (4.4.6)–(4.4.11).

Следствие 4.4.8. *Элементы*

$$\begin{aligned} D^t u^{(0)}_{n,I,J} &:= D^t[\underbrace{v\ _0 \cdots {}_0\ v}_{n\ раз}{}_0\, \xi_{i_1\ 0} \cdots {}_0\ \xi_{i_s\ 0}\ \partial_{j_1\ 0} \cdots {}_0\ \partial_{j_q}], \quad n > 0, \\ D^t u^{(1)}_{r,I,J} &:= D^t[\xi_{i_1\ 0} \cdots {}_0\ \xi_{i_r\ 1} \cdots {}_1\ \xi_{i_s\ 1}\ \partial_{j_1\ 0} \cdots {}_0\ \partial_{j_q}], \quad r \leqslant s+1, \end{aligned} \tag{4.4.12}$$

где $I = \{i_1, \dots, i_s\}$*,* $J = \{j_1, \dots, j_q\}$*,* $i_1 < \dots < i_s$*,* $j_1 < \dots < j_q$*,* $t \geqslant 0$*, образуют линейный базис универсальной обертывающей конформной алгебры* $U_L(W_N)$*.*

Приведем также некоторые примеры конформных подалгебр в W_1, показывающие различия в структуре обычных и конформных универсальных обертывающих алгебр. Именно, мы рассмотрим две (собственных) конформных подалгебры K_1 и S_1 в W_1.

Хорошо известная в физике конформная супералгебра Невью—Шварца K_1 является представителем серии простых подалгебр K_N в W_N.

Используя комодульную конструкцию W_N, мы можем выписать элементы $\mathfrak{A}_N$, порождающие K_N над $\Bbbk[D]$ (ср. [59]):

$$g_I = 2\xi_I + (-1)^{|I|}\sum_{i=1}^{N}[D(\xi_i\xi_I\partial_i) + \partial_i(\xi_I)\xi_i + \partial_i(\xi_I)\partial_i],$$

где $I = \{i_1, \dots, i_k\} \subseteq \{1, \dots, N\}$ — упорядоченное подмножество, $\xi_I = \xi_{i_1} \dots \xi_{i_k}$, $0 \leqslant k \leqslant N$. В частности, супералгебра K_1 порождается элементами $g_0 = (1/2)g_\emptyset$, $g_1 = (1/2)g_{\{\xi_1\}}$ со следующими конформными произведениями:

$$g_{0\ [0]}\ g_0 = Dg_0, \quad g_{0\ [1]}\ g_0 = 2g_0, \quad g_{0\ [0]}\ g_1 = Dg_1, \quad g_{0\ [1]}\ g_1 = (3/2)g_1, \quad g_{1\ [0]}\ g_1 = -(1/2)g_0.$$

Индуцированная функция локальности L принимает значения

$$L(g_0, g_0) = 3, \quad L(g_1, g_0) = L(g_0, g_1) = L(g_1, g_1) = 2.$$

Другая конформная подалгебра $S_1 \subset W_1$ порождается над $\Bbbk[D]$ элементами $a = v - D(\xi_1\partial_1)$ и $b = \partial_1$. Таблица умножения этой конформной алгебры имеет вид

$$a_{\ [0]}\ x = Dx, \quad a_{\ [1]}\ x = 2x, \quad a_{\ [n]}\ x = 0,\ n \geqslant 2, \quad x \in \{a, b\}$$

(все невыписанные произведения могут быть вычислены по конформной антикоммутативности). Индуцированная функция локальности принимает значения

$$L(a, a) = 3, \quad L(a, b) = L(b, a) = 2, \quad L(b, b) = 0.$$

Теорема 4.4.9 (см. [22])**.** 1) $U_L(K_1) \simeq U_L(W_1)$;

2) *естественный гомоморфизм* $U_L(S_1) \to U_L(W_1)$ *не является инъективным.*

4.5. Йордановы псевдоалгебры конечного типа. Общая схема, известная как конструкция Титса—Кантора—Кёхера (ТКК), описанная в [21, 86, 105], осуществляет вложение йордановой алгебры в алгебру Ли. В [108] построен аналог этой конструкции для конформных алгебр с использованием алгебр коэффициентов. Мы покажем, что аналог ТКК-конструкции может быть построен для йордановых псевдоалгебр конечного типа.

Напомним ТКК-конструкцию для обычных алгебр (ср. [77]). Для любой йордановой алгебры J множество $\mathrm{Der}(J)$ ее дифференцирований образует алгебру Ли относительно коммутатора. Рассмотрим (формальную) прямую сумму $\mathrm{Der}(J)$ и $L(J)$, где $L(J)$ — линейное пространство операторов левого умножения $L_a : b \mapsto ab$. Определим новую операцию на $\mathrm{S}(J) = \mathrm{Der}(J) \oplus L(J)$:

$$[(L_a + D), (L_b + T)] = L_{Db} - L_{Ta} + [L_a, L_b] + [D, T]. \tag{4.5.1}$$

Тогда $\mathrm{S}(J)$ относительно коммутатора (4.5.1) называется структурной алгеброй Ли для J. Наконец, рассмотрим

$$\mathrm{T}(J) = J^- \oplus \mathrm{S}_0(J) \oplus J^+,$$

где $J^\pm \simeq J$, $\mathrm{S}_0(J)$ — подалгебра в $\mathrm{S}(J)$, порожденная элементами $U_{a,b} = L_{ab} + [L_a, L_b] \in \mathrm{S}(J)$, $a, b \in J$. Введем на $\mathrm{T}(J)$ следующую операцию:

$$\begin{gathered} [S, a^-] = (Sa)^-, \quad [a^-, b^+] = U_{a,b}, \quad [a^+, b^+] = [a^-, b^-] = 0, \\ [a^-, S] = -(Sa)^-, \quad [a^+, S] = -(S^*a)^+, \quad [S, a^+] = (S^*a)^+, \quad [a^+, b^-] = U^*_{a,b}. \end{gathered} \tag{4.5.2}$$

Коммутатор на элементах из $\mathrm{S}_0(J)$ тот же, что в (4.5.1). Здесь мы использовали обозначение $S^* = -L_a + D$ для $S = L_a + D \in \mathrm{S}(J)$. Операция (4.5.2) превращает $\mathrm{T}(J)$ в алгебру Ли, называемую ТКК-конструкцией для йордановой алгебры J.

Для случая псевдоалгебр следует заменить алгебру линейных преобразований на псевдоалгебру конформных линейных отображений (см. [32]). Именно, пусть J — йорданова H-псевдоалгебра. Обозначим через $\mathrm{Cend}^l(J)$ множество отображений $\varphi : J \to H \otimes H \otimes_H J$ со свойством

$$\varphi(ha) = (1 \otimes h \otimes_H 1)(\varphi(a)).$$

Это частный случай мультиоперации [34] (см. п. 4.2). Чтобы унифицировать обозначения, будем писать $\varphi * a$ вместо $\varphi(a)$. Легко заметить, что если J конечно порождена над H, то $\mathrm{Cend}^l(J)$ является ассоциативной H-псевдоалгеброй, где

$$(\varphi * \psi) * a = \varphi * (\psi * a), \quad \varphi, \psi \in \mathrm{Cend}^l(J), \quad a \in J.$$

Поэтому мы будем предполагать, что J — йорданова псевдоалгебра конечного типа.

Замечание 4.5.1. Указанное условие конечной порожденности не является необходимым требованием на J. Условие операторной локальности, введенное в [108] для случая конформных алгебр, по сути означает, что $\mathrm{Cend}^l(J)$ является ассоциативной псевдоалгеброй.

Отображение $T \in \mathrm{Cend}^l(J)$ называется (левым) *псевдодифференцированием*, если

$$T * (a * b) = (T * a) * b + (\sigma_{12} \otimes_H \mathrm{id}_J)(a * (T * b))$$

для любых $a, b \in J$. Множество всех псевдодифференцирований на J обозначим через $\mathrm{Der}^l(J)$.

Понятие «расширенного» псевдопроизведения (4.2.2) позволяет применять к йордановой псевдоалгебре конечного типа все рассуждения, которые используются для обычных алгебр. В частности, $\mathrm{Der}^l(J)$ является псевдоалгеброй Ли, лежащей в $\mathrm{Cend}^l(J)^{(-)}$ [88], и

$$[L(J) * L(J)] \subset H \otimes H \otimes_H \mathrm{Der}^l(J).$$

В этом случае структурной псевдоалгеброй Ли для J назовем формальную прямую сумму H-модулей

$$\mathrm{S}(J) = L(J) \oplus \mathrm{Der}^l(J),$$

снабженную псевдопроизведением $[\cdot * \cdot]$:

$$[(L_a + D) * (L_b + T)] = L_{D*b} - (\sigma_{12} \otimes_H \mathrm{id}) L_{T*a} + [L_a * L_b] + [D * T]. \tag{4.5.3}$$

Рассмотрим элементы

$$U_{a,b} = L_{a*b} + [L_a * L_b] \in H \otimes H \otimes_H \mathrm{S}(J), \quad U^x_{a,b} = L_{(a\,{}_x\,b)} + [L_{a\ x}\ L_b], \quad a, b \in J, \quad x \in X.$$

Векторное пространство $\mathrm{S}_0(J)$, порожденное множеством $\{U^x_{a,b} \mid a, b \in J,\ x \in X\}$, является H-подмодулем в $\mathrm{S}(J)$, замкнутым относительно всех x-произведений.

Рассмотрим формальную прямую сумму H-модулей

$$\mathrm{T}(J) = J^- \oplus \mathrm{S}_0(J) \oplus J^+,$$

где J^+, J^- — изоморфные копии H-модуля J. Для $a \in J$ (или $A \in H^{\otimes n} \otimes_H J$) обозначим через $a^\pm$ (или $A^\pm$) образ этого элемента в $J^\pm$ (или $H^{\otimes n} \otimes_H J^\pm$). Определим псевдопроизведение на $\mathrm{T}(J)$ по следующему правилу: для $a^\pm, b^\pm \in J^\pm$, $S \in \mathrm{S}_0(J)$ положим

$$\begin{gathered}[S * a^-] = (S * a)^-, \quad [a^- * b^+] = U_{a,b}, \quad [a^+ * b^+] = [a^- * b^-] = 0, \\ [a^- * S] = -(\sigma_{12} \otimes_H \mathrm{id})(S * a)^-, \quad [a^+ * S] = -(\sigma_{12} \otimes_H \mathrm{id})(S^* * a)^+, \\ [S * a^+] = (S^* * a)^+, \quad [a^+ * b^-] = U^*_{a,b}.\end{gathered} \tag{4.5.4}$$

Псевдопроизведение на $\mathrm{S}_0(J)$ то же, что и (4.5.2). Здесь мы обозначили $S^* = -L_a + D$ для $S = L_a + D \in \mathrm{S}(J)$.

Теорема 4.5.2. *Пусть J — йорданова псевдоалгебра конечного типа, $\mathcal{L} = \mathrm{T}(J)$. Тогда $\mathcal{L}$ является псевдоалгеброй Ли конечного типа. Если J простая (т.е. $J * J \neq 0$ и J не имеет нетривиальных идеалов), то $\mathcal{L}$ также простая.*

Этот результат позволяет описать простые йордановы псевдоалгебры конечного типа, используя классификацию [32] простых псевдоалгебр Ли.

Пусть J — простая йорданова $H = U(\mathfrak{h})$-псевдоалгебра конечного типа; тогда либо $\mathrm{T}(J) = \mathrm{Cur}\,\mathfrak{g}$, где $\mathfrak{g}$ — простая конечномерная алгебра Ли, либо $\mathrm{T}(J)$ изоморфна подалгебре $\mathrm{Cur}^H_{H'} W(\mathfrak{h}')$, где $H' = U(\mathfrak{h}')$, $\mathfrak{h}'$ — подалгебра в $\mathfrak{h}$ (см. замечание 4.3.7). Легко заметить, что второй случай не может иметь места, поскольку псевдоалгебры вида $\mathrm{Cur}^H_{H'} W(\mathfrak{h}')$ не содержат абелевых подалгебр. Это основной момент рассуждений, приводящих к следующему утверждению.

Теорема 4.5.3 (см. [88])**.** *Пусть J — простая йорданова псевдоалгебра над $H = U(\mathfrak{h})\#\mathbb{C}[\Gamma]$, $\dim \mathfrak{h} < \infty$, такая, что J конечно порождена над $U(\mathfrak{h})$. Тогда*

$$J \simeq \bigoplus_{i=1}^{m} \mathrm{Cur}^{U(\mathfrak{h})}\, \mathfrak{j}_i,$$

где $\mathfrak{j}_i$ — простые конечномерные йордановы алгебры, причем группа Γ действует на $\mathrm{Cur}^{U(\mathfrak{h})}\, \mathfrak{j}_i$, $i = 1, \ldots, m$, транзитивно.

В частности, если Γ — тривиальная группа и $\dim \mathfrak{h} = 1$, то мы получаем следующее утверждение.

Следствие 4.5.4 (см. [108])**.** *Простая йорданова конформная алгебра конечного типа изоморфна конформной алгебре петель над простой конечномерной йордановой алгеброй.*

СПИСОК ЛИТЕРАТУРЫ

1. *Адян С. И.* Неразрешимость некоторых алгоритмических проблем в теории групп// Тр. Моск. мат. о-ва. — 1957. — *6*. — С. 231–298.
2. *Адян С. И.* Определяющие соотношения и алгоритмические проблемы для полугрупп и групп// Тр. мат. ин-та им. В. А. Стеклова. — 1966. — *85*.
3. *Бокуть Л. А.* Некоторые теоремы вложения для колец и полугрупп. I// Сиб. мат. ж. — 1963. — *4*, № 3. — С. 500–518.
4. *Бокуть Л. А.* Некоторые теоремы вложения для колец и полугрупп. II// Сиб. мат. ж. — 1963. — *4*, № 4. — С. 729–743.
5. *Бокуть Л. А.* Некоторые примеры колец без делителей нуля// Алгебра и логика. — 1964. — *3*, № 5–6. — С. 5–28.
6. *Бокуть Л. А.* Об одном свойстве групп Буна// Алгебра и логика. — 1966. — *5*, № 5. — С. 5–23.
7. *Бокуть Л. А.* Об одном свойстве групп Буна, II// Алгебра и логика. — 1967. — *6*, № 1. — С. 15–24.
8. *Бокуть Л. А.* О группах Новикова// Алгебра и логика. — 1967. — *6*, № 1. — С. 25–38.
9. *Бокуть Л. А.* О вложении колец в тела// Докл. АН СССР. — 1967. — *175*, № 4. — С. 755–758.
10. *Бокуть Л. А.* Группы с относительным стандартным базисом// Сиб. мат. ж. — 1968. — *9*, № 4. — С. 755–758.

11. *Бокуть Л. А.* Группы частных мультипликативных полугрупп некоторых колец, I, II, III// Сиб. мат. ж. — 1969. — *10*, № 2. — С. 246–286; Сиб. мат. ж. — 1969. — *10*, № 4. — С. 744–799; Сиб. мат. ж. — 1969. — *10*, № 4. — С. 800–819.
12. *Бокуть Л. А.* О проблеме Мальцева// Сиб. мат. ж. — 1969. — *10*, № 5. — С. 965–1005.
13. *Бокуть Л. А.* Неразрешимость проблемы равенства и подалгебры конечно определенных алгебр Ли// Изв. АН СССР. Сер. мат. — 1972. — *36*, № 6. — С. 1173–1219.
14. *Бокуть Л. А.* Вложения в простые ассоциативные алгебры// Алгебра и логика. — 1976. — *15*, № 2. — С. 117–142.
15. *Бокуть Л. А.* Вложение колец// Усп. мат. наук. — 1987. — *42*, № 4 (256). — С. 87–111.
16. *Бокуть Л. А., Фонг Ю., Ке В.-Ф., Колесников П. С.* Базисы Грёбнера—Ширшова в алгебре и конформные алгебры// Фундам. прикл. мат. — 2000. — *6*, №. 3. — С. 669–706.
17. *Бокуть Л. А., Колесников П. С.* Базисы Грёбнера–Ширшова: от зарождения до наших дней// Зап. научн. семин. ПОМИ. — 2000. — *272*. — С. 26–67.
18. *Бурбаки Н.* Группы и алгебры Ли. Гл. IV–VI. Группы Кокстера и системы Титса. Группы порожденные отражениями. Системы корней. — М.: Мир, 1972.
19. *Герасимов В. Н.* Дистрибутивные решетки подпространств и проблема равенства для алгебр с одним соотношением// Алгебра и логика. — 1976. — *15*, № 4. — С. 384–435.
20. *Горин Е. А., Лин В. Я.* Алгебраические уравнения с непрерывными коэффициентами и некоторые вопросы алгебраической теории кос// Мат. сб. — 1969. — *78*, №. 4. — С. 579–610.
21. *Кантор И. Л.* Классификация неприводимых транзитивно-дифференциальных групп// Докл. АН СССР. — 1964. — *158*, № 6. — С. 1271–1274.
22. *Колесников П. С.* Универсальные представления некоторых конформных супералгебр Ли// Вестн. НГУ. Сер. мат., мех., информ. — 2002. — *2*, №. 3. — С. 30–45.
23. *Латышев В. Н.* Комбинаторная теория колец. Стандартные базисы. — М.: МГУ, 1988.
24. *Мальцев А. И.* Избранные труды. Т. 1. Классическая алгебра. — М.: Наука, 1970.
25. *Новиков П. С.* Об алгоритмической неразрешимости проблемы тождества слов в группах// Тр. Мат. ин-та им. В. А. Стеклова. — 1955. — *44*.
26. *Ширшов А. И.* Некоторые алгоритмические проблемы для алгебр Ли// Сиб. мат. ж. — 1962. — *3*. — С. 292–296.
27. *Марков А. А.* Основы алгебраической теории кос// Тр. Мат. ин-та им. В. А. Стеклова. — 1945. — *16*.
28. *Фридман А. А.* Степени неразрешимости проблемы тождества для конечно-определенных групп. — М.: Наука, 1967.
29. *Чубаров Д. Л.* Применение леммы о композиции для построения универсальных обертывающих конформных алгебр Ли/ Магистер. дисс. — Новосибирский государственный университет, 2000.
30. *Artin E.* Theory der Zöpfe// Abh. Math. Semin., — Hamburg Univ., 1925. — *4*. — С. 47–72.
31. *Artin E.* Theory of braids// Ann. Math. — 1947. — *48*, С. 101–126.
32. *Bakalov B., D'Andrea A., Kac V. G.* Theory of finite pseudoalgebras// Adv. Math. — 2001. — *162*, № 1.
33. *Beidar K. I., Martindale W. S., Mikhalev A. V.* Rings with generalized identities/ Pure Appl. Math. — New York: Marcel Dekker, 1996. — *196*.
34. *Beilinson A. A., Drinfeld V. G.* Chiral algebras/ Preprint.
35. *Belavin A. A., Polyakov A. M., Zamolodchikov A. B.* Infinite conformal symmetry in two-dimensional quantum field theory// Nucl. Phys. — 1984. — *B241*. — С. 333–380.
36. *Bergman G. M.* The diamond lemma for ring theory// Adv. Math. — 1978. — *29*. — С. 178–218.
37. *Birman J. S.* Braids, links, and mapping class groups/ Ann. Math. Stud. — Princeton Univ. Press, 1975. — *82*.
38. *Birman J., Ko K. H., Lee S. J.* A new approach to the word and conjugacy problems in the braid groups// Adv. Math. — 1998. — *139*. — С. 322–353.
39. *Bohnenblust F.* The algebraical braid group// Ann. Math. — 1947. — *48*. — С. 127–136.
40. *Bokut L. A.* Abstract semigroups and groups of formal series of dependent variables// Sib. Adv. Math. — 1996. — *6*, № 3. — С. 1–26.
41. *Bokut L. A., Chainikov V. V.* Gröbner–Shirshov basis of Adjan extension of the Novikov group// J. Algebra Appl. (в печати).
42. *Bokut L. A., Fong Y., Ke W.-F.* Free associative conformal algebras// Proc. 2nd Tainan–Moscow Algebra and Combinatorics Workshop, Tainan 1997, 13–25. — Hong Kong: Springer-Verlag, 2000.
43. *Bokut L. A., Fong Y., Ke W.-F.* Gröbner–Shirshov bases and composition lemma for associative conformal algebras: an example// Contemp. Math. — 2000. — *264*. — С. 63–90.

44. *Bokut L. A., Fong Y., Ke W.-F.* Composition–diamond lemma for associative conformal algebras// J. Algebra (в печати).
45. *Bokut L. A., Fong Y., Ke W.-F., Shiao L.-S.* Gröbner-Shirshov bases for the braid semigroup/ (в печати).
46. *Bokut L. A., Kukin G. P.* Algorithmic and combinatorial algebra/ Math. Appl. — Dordrecht: Kluwer Academic Publishers Group, 1994. — *255*.
47. *Bokut L. A., Shiao L.-S.* Gröbner–Shirshov bases for Coxeter groups// Commun. Algebra. — 2001. — *29*, № 9. — С. 4305–4319.
48. *Bokut L. A., Shiao L.-S.* Gröbner–Shirshov bases for Novikov and Boone groups// Algebra Colloq. (в печати).
49. *Bokut L. A., Shum K. P.* Relative Gröbner–Shirshov bases for algebras and groups/ Preprint.
50. *Bokut L. A., Vesnin A. Yu.* New rewriting system for the braid group B_4// Proc. Buchberger Conf. — Linz, Austria, 2002. — С. 48–60.
51. *Boone W. W.* The word problem// Ann. Math. — 1959. — *70*. — С. 207–265.
52. *Boone W. W.* Finitely presented group whose word problem has the same degree as that of an arbitrary given Thue system (an application of methods of Britton)// Proc. Nat. Acad. Sci. U.S.A. — 1965. — *53*, № 2. — С. 265–269.
53. *Borcherds R. E.* Vertex algebras, Kac–Moody algebras, and the Monster// Proc. Nat. Acad. Sci. U.S.A. — 1986. — *83*. — С. 3068–3071.
54. *Bowtel A.* On a question of Mal'cev// J. Algebra. — 1967. — *7*. — С. 126–139.
55. *Britton J. L.* The word problem// Ann. Math. — 1963. — *77*, № 1. — С. 16–32.
56. *Buchberger B.* An algorithm for finding a basis for the residue class ring of a zero-dimensional polynomial ideal/ Ph.D. thesis. — University of Insbruck, 1965.
57. *Buchberger B.* An algorithmical criteria for the solvability of algebraic systems of equations// Aequat. Math. — 1970. — *4*. — С. 374–383.
58. *Burau W.* Über Zopfinvarianten// Abh. Math. Semin. — Hamburg Univ., 1932. — *9*, № 2. — С. 117–124.
59. *Cheng S.-J., Kac V. G.* A new $N = 6$ superconformal algebra// Commun. Math. Phys. — 1997. — *186*. — С. 219–231.
60. *Chibrikov E. S.* On free vertex and Lie conformal algebras/ Preprint.
61. *Chow W.-L.* On the algebraical braid group// Ann. Math. — 1948. — *49*, № 3. — С. 654–658.
62. *Clapham C. R. L.* Finitely presented groups with word problems an arbitrary degrees of unsolvability// Proc. Lond. Math. Soc. — 1964. — *14*. — С. 633–676.
63. *Cohn P. M.* Embedding in semigroup with one-sided division// J. London Math. Soc. — 1956. — *31*. — С. 169–180.
64. *Cohn P. M.* Embedding in sesquilaterial division semigroups// J. London Math. Soc. — 1956. — *31*. — С. 181–198.
65. *Cohn P. M.* Some remarks on the invariant basis property// Topology. — 1966. — *5*. — С. 215–228.
66. *Cohn P. M.* Universal algebra/ Math. Appl. — Dordrecht–Boston: Reidel, 1981. — *6*.
67. *D'Andrea A., Kac V. G.* Structure theory of finite conformal algebras// Sel. Math., New Ser. — 1998. — *4*. — С. 377–418.
68. *Dobrynin N. A.* The free partially commutative Lie algebras: elimination of variables// Lie Algebras, Rings and Related Topics (Fong Y. et al, eds.). — Hong Kong: Springer-Verlag, 2000. — С. 32–48.
69. *Dong C., Lepowsky J.* Generalized vertex algebras and relative vertex operators. — Boston: Birkhäuser, 1993.
70. *Epstein D. B. A., Cannon J. W., Holt D. F., Levy S. V. F., Paterson M. S., Thurston W. P.* Word processing in groups. — Boston–London: Jones and Barlett, 1992.
71. *Frenkel I. B., Lepowsky J., Meurman A.* Vertex operator algebras and the Monster/ Pure Appl. Math. — Academic Press, 1998. — *134*.
72. *Fattori D., Kac V. G.* Classification of finite Lie conformal superalgebras/ Preprint.
73. *Garside A. F.* The braid group and other groups// Oxford Q. J. Math. — 1969. — *20*. — С. 235–254.
74. *Gerdt V. P., Kornyak V. V.* Construction of finitely presented Lie algebras and superalgebras// J. Symbol. Comput. — 1996. — *21*. — С. 337–349.
75. *Hironaka H.* Resolution of singularities of an algebraic variety over a field of characteristic zero, I, II// Ann. Math. — 1964. — *79*. — С. 109–203; Ann. Math. — 1964. — *79*. — С. 205–326.
76. *Humphreys J. E.* Reflection groups and Coxeter groups/ Cambridge Stud. Adv. Math. — Cambridge: Cambridge University Press, 1990. — *29*.
77. *Jacobson N.* Structure theory of Jordan algebras. — Univ. Arkansas, 1981.
78. *Kac V. G.* Vertex algebras for beginners/ Univ. Lect. Ser. — Amer. Math. Soc., 1996. — *10*.

79. *Kac V. G.* The idea of locality// In: Physical applications and mathematical aspects of geometry, groups and algebras/ (H.-D. Doebner et al., eds.). — Singapore: World Scientific, 1997. — C. 16–32.
80. *Kac V. G.* Formal distribution algebras and conformal algebras// XII Int. Congr. Math. Phys., Brisbane. — Cambridge: Internat. Press, 1999. — C. 80–97.
81. *Kang S.-J., Lee K.-H.* Gröbner–Shirshov bases for representation theory// J. Korean Math. Soc. — 2000. — *37*, № 1. — C. 55–72.
82. *Kang S.-J., Lee I.-S., Lee K.-H., Oh H.* Hecke algebras, Specht modules and Gröbner–Shirshov bases// J. Algebra. — 2002. — *252*, № 2. — C. 258–292.
83. *Kharchenko V. K.* A combinatorial approach to the quantification of Lie algebras// Pac. J. Math. — 2002. — *203*, № 1. — C. 191–233.
84. *Klein A. A.* Rings nonembeddable in fields with multiplicative semigroups embeddable in groups// J. Algebra. — 1967. — *7*. — C. 100–127.
85. *Knuth D. E., Bendix P. B.* Simple word problems in universal algebras// Computational problems in abstract algebra/ Proc. Conf., Oxford, 1967. — Oxford: Pergamon, 1970. — C. 263–297.
86. *Koecher M.* Embedding of Jordan algebras into Lie algebras, I, II// Amer. J. Math. — 1967. — *89*. — C. 787–816; Amer. J. Math. — 1968. — *90*. — C. 476–510.
87. *Kolesnikov P. S.* Associative enveloping pseudoalgebras of finite Lie pseudoalgebras// Commun. Algebra. — 2003. — *31*, № 6. — C. 2909–2925.
88. *Kolesnikov P. S.* Simple Jordan pseudoalgebras/ ArXive `math.QA/0210264`.
89. *Lambek J.* Deductive systems and categories, II// Standard constructions and closed categories/ Lect. Notes Math. — Berlin: Springer-Verlag, 1969. — *86*. — C. 76–122.
90. *Latyshev V. N.* Lie nilpotency: recognition and word problem// First Int. Tainan–Moscow Algebra Workshop, Tainan, 1994. — Berlin: de Gruyter, 1996. — C. 237–239.
91. *Latyshev V. N.* Canonization and standard bases of filtered structures// Lie Algebras, Rings, and Related Topics (Fong Y., Mikhalev A. A., Zelmanov E., eds.). — Hong Kong: Springer-Verlag, 2000. — C. 61–79.
92. *Latyshev V. N.* An improved version of standard bases// Formal power series and algebraic combinatorics/ Proc. 12 Int. Conf. Moscow, June 2000 (Krob D., Mikhalev A. A., Mikhalev A. V., eds.). — Berlin: Springer-Verlag, 2000. — C. 496–505.
93. *Latyshev V. N.* General version of standard bases in linear structures// Proc. Int. Algebraic Conf. on the occasion of the 90th birthday of A. G. Kurosh. Moscow, Russia, May 25–30, 1998 (Bakhturin Yu. A., ed.). — Berlin–New York: Walter de Gruyter, 2000. — C. 215–226.
94. *Magnus W., Karras A., Solitar D.* Combinatorial group theory. — New York–London–Sydney: Interscience, John Wiley and Sons, 1966.
95. *Malcev A. I.* On immersion of an algebraic ring into a field// Math. Ann. — 1937. — *113*. — C. 686–691.
96. *Mikhalev A. A., Vasilieva E.* Standard bases of ideals of free supercommutative polynomial algebras (ε-Gröbner bases)// Lie Algebras, Rings, and Related Topics (Fong Y., Mikhalev A.A., Zelmanov E., eds.). — Hong Kong: Springer-Verlag, 2000. — C. 61–79
97. *Mikhalev A. A., Zolotykh A. A.* Standard Gröbner–Shirshov bases of free algebras over rings. I. Free associative algebras// Int. J. Algebra Comput. — 1998. — *8*, № 6. — C. 689–726.
98. *Mora T.* An introduction to commutative and noncommutative Gröbner bases// 2 Int. Colloq. on Words, Languages, and Combinatorics, Kyoto, 1992/ Theor. Comput. Sci. — 1994. — *134*. — C. 131–173.
99. *Newman M. H. A.* On theories with a combinatorial definition of “equivalence”// Ann. Math. — 1942. — *43*. — C. 223–243.
100. *Roitman M.* On free conformal and vertex algebras// J. Algebra. — 1999. — *217*. — C. 496–527.
101. *Roitman M.* Universal enveloping conformal algebras// Sel. Math. New Ser. — 2000. — *6*, № 3. — C. 319–345.
102. *Rolfsen D.* New developments in the theory of Artin’s braid groups// Topology Appl. — 2003. — *127*. — C. 77–90.
103. *Rotman J. J.* An introduction to the theory of groups/ Grad. Texts Math. — New York: Springer-Verlag, 1995. — *148*.
104. *Sweedler M.* Hopf algebras. — New York, Benjamin, 1969.
105. *Tits J.* Une classe d’algebres de Lie en relation avec algebres de Jordan// Indag. Math. — 1962. — *24*. — C. 530–535.
106. *Trakhtenbrot B. A.* On the complexity of reduction algorithms in Novikov–Boone constructions// Algebra Logic. — 1969. — *8*. № 1. — C. 93–128.

107. *Ufnarovski V.* Introduction to noncommutative Gröbner bases theory// Gröbner Bases and Applications (Buchberger B., Winkler F., eds.)/ London Math. Soc. Lect. Note Ser. — Cambridge Univ. Press, 1998. — *251*. — С. 259–280.
108. *Zelmanov E. I.* On the structure of conformal algebras// Int. Conf. on Combinatorial and Computational Algebra, May 24–29, 1999, Hong Kong/ Contemp. Math. — 2000. — *264*. — С. 139–153.

Л. А. Бокуть
Институт математики им. С. Л. Соболева СО РАН
E-mail: bokut@math.nsc.ru

П. С. Колесников
Институт математики им. С. Л. Соболева СО РАН
E-mail: pavelsk@math.nsc.ru

Современная математика и ее приложения. Том 13 (2004). С. 131–139

УДК 512.58

ЭЛЕМЕНТАРНАЯ ЭКВИВАЛЕНТНОСТЬ КАТЕГОРИЙ МОДУЛЕЙ И ДРУГИХ АЛГЕБРАИЧЕСКИХ СТРУКТУР

© 2004 г. **Е. И. БУНИНА, А. В. МИХАЛЕВ**

Аннотация. Данная работа представляет собой обзор недавних результатов по элементарной эквивалентности линейных и алгебраических групп, а также содержит новые, принадлежащие авторам результаты по элементарной эквивалентности категорий модулей, колец эндоморфизмов модулей и групп автоморфизмов модулей.

1. Основополагающие результаты А. И. Мальцева. *Языком первого порядка* некоторой алгебраической теории (например, теории групп или теории колец) называется такой язык, в котором в формулах используются кванторы $\forall$ и $\exists$, логические символы $\neg$, $\wedge$, $\vee$, $\Rightarrow$, скобки и переменные, а также предикатные, функциональные и константные символы этой теории. Например, в теории групп можно использовать подформулы $x \cdot y$, x^{-1}, 1, в теории колец — подформулы $x \cdot y$, x^{-1}, 1, $x + y$, $-x$, 0 и т. д.

Две модели $\mathcal{U}$ и $\mathcal{B}$ языка $\mathcal{L}$ (например, две группы или два кольца) называются *элементарно эквивалентными*, если любое предложение φ языка $\mathcal{L}$ истинно в модели $\mathcal{U}$ тогда и только тогда, когда оно истинно в модели $\mathcal{B}$. Это отношение между моделями обозначается через $\mathcal{U} \equiv \mathcal{B}$.

Первый результат по элементарной эквивалентности линейных групп был получен А. И. Мальцевым в 1961 г. (см. [6]). Им была доказана следующая теорема.

Теорема 1.1. *Группа $G_m(K_1)$ элементарно эквивалентна группе $G_n(K_2)$ ($G = GL$, PGL, SL, PSL, $m \geqslant n \geqslant 3$, K_1, K_2 — поля характеристики 0) тогда и только тогда, когда $m = n$ и $K_1 \equiv K_2$.*

В доказательстве А. И. Мальцев использовал приведение матриц к нормальной жордановой форме, и для каждой матрицы M он явно находил формулу $\varphi(A)$, истинную в данной группе тогда и только тогда, когда матрица A имела жорданову форму, совпадающую с жордановой формой матрицы M.

2. Ультрапроизведения и ультрастепени. Теорема Кейслера—Шелаха. Если мы рассматриваем линейные группы над телами или кольцами, у нас отсутствует какой-либо адекватный аналог теории жордановых нормальных форм. Однако прогресс в теории моделей, достигнутый в последние годы (см. [8]), позволил продолжить исследования в этой области.

Пусть I — некоторое непустое множество. Через $\mathcal{P}(I)$ обозначим множество всех подмножеств множества I. *Фильтр* D над множеством I — это множество $D \subset \mathcal{P}(I)$, удовлетворяющее следующим условиям:

1) $I \in D$;
2) если $X, Y \in D$, то $X \cap Y \in D$;
3) если $X \in D$ и $X \subset Z \subset I$, то $Z \in D$.

Так как $I \in D$, то любой фильтр D непуст. В качестве примеров можно привести *тривиальный фильтр* $D = \{I\}$, *несобственный фильтр* $D = \mathcal{P}(I)$ и фильтр $D = \{X \subset I : Y \subset X\}$ для каждого множества $Y \subset I$ (этот фильтр называется *главным фильтром*, порожденным множеством Y).

Фильтр D над множеством I называется *ультрафильтром* над I, если для всякого $X \in \mathcal{P}(I)$

$$X \in D \quad \text{если и только если} \quad (I \setminus X) \notin D.$$

ISSN 1512–1712

Пусть I — некоторое непустое множество, D — собственный фильтр над I и A_i — непустое множество для каждого $i \in I$. Рассмотрим декартово произведение

$$C = \prod_{i \in I} A_i$$

этих множеств. Иначе говоря, C — это множество всех отображений f, определенных на I и таких, что $f(i) \in A_i$ для каждого $i \in I$. Отображения $f, g \in C$ называются *D-эквивалентными* (обозначение $f =_D g$), если

$$\{i \in I : f(i) = g(i)\} \in D.$$

Отношение $=_D$ является отношением эквивалентности на множестве C.

Пусть f_D — класс эквивалентности, содержащий функцию f:

$$f_D = \{d \in C : f =_D g\}.$$

Определим *фильтрованное произведение множеств A_i по фильтру D* как множество всех классов эквивалентности отношения $=_D$. Обозначим это множество через $\prod\limits_D A_i$. Таким образом,

$$\prod_D A_i = \left\{ f_D : f \in \prod_{i \in I} A_i \right\}.$$

Множество I называется *множеством индексов* произведения $\prod\limits_D A_i$. Если D является ультрафильтром над I, то фильтрованное произведение $\prod\limits_D A_i$ называется *ультрапроизведением*.

Если все A_i совпадают (т.е. $A_i = A$), то фильтрованное произведение обозначается через $\prod\limits_D A$ и называется *фильтрованной степенью множества A по фильтру D*. В частности, если D является ультрафильтром, то $\prod\limits_D A$ называется *ультрастепенью множества A по фильтру D*.

Дадим теперь определение фильтрованного произведения моделей. Пусть I — некоторое непустое множество, D — собственный фильтр над множеством I, $\mathcal{U}_i$ — модель языка $\mathcal{L}$ для каждого $i \in I$. Мы предполагаем, что предикатные символы P интерпретируются в модели $\mathcal{U}_i$ как P_i, функциональные символы F — как F_i, а константные символы c — как c_i.

По определению, *фильтрованное произведение* $\prod\limits_D \mathcal{U}_i$ — это модель языка $\mathcal{L}$, описываемая следующим образом.

(i) Универсумом модели является множество $\prod\limits_D A_i$.

(ii) Пусть P — некоторый n-местный предикатный символ языка $\mathcal{L}$. Этот символ P интерпретируется в модели $\prod\limits_D \mathcal{U}_i$ как отношение $\overline{P}$, удовлетворяющее следующему условию:

$$\overline{P}(f_D^1, \ldots, f_D^n) \quad \text{тогда и только тогда, когда} \quad \{i \in I : P_i(f^1(i), \ldots, f^n(i))\} \in D.$$

(iii) Пусть F — некоторый n-местный функциональный символ языка $\mathcal{L}$. Символ F интерпретируется в $\prod\limits_D \mathcal{U}_i$ посредством функции $\overline{F}$, определяемой следующим образом:

$$\overline{F}(f_D^1, \ldots, f_D^n) = \big(F_i(f^1(i), \ldots, f^n(i)) : i \in I\big)_D.$$

(iv) Пусть c — константный символ языка $\mathcal{L}$. Этот символ интерпретируется как элемент

$$\overline{c} = (c_i : i \in I)_D$$

множества $\prod\limits_D A_i$.

Предложение 2.1. *Пусть $\prod\limits_D \mathcal{U}$ — ультрастепень модели $\mathcal{U}$. Тогда $\prod\limits_D \mathcal{U} \equiv \mathcal{U}$.*

Следующая важная теорема была доказана Кейслером и Шелахом (доказательство можно найти в книге [8]).

Теорема 2.1 (теорема об изоморфизме)**.** *Пусть $\mathcal{U}$ и $\mathcal{B}$ — модели языка $\mathcal{L}$. Тогда $\mathcal{U}$ и $\mathcal{B}$ элементарно эквивалентны в том и только том случае, когда они имеют изоморфные ультрастепени.*

3. Обобщение теоремы Мальцева. Результаты К. И. Бейдара и А. В. Михалева. Используя теорему об изоморфизме, в 1992 г. К. И. Бейдар и А. В. Михалев нашли общий подход к проблемам элементарной эквивалентности различных алгебраических структур (см. [7]). Взяв на вооружение некоторые результаты теории линейных групп над кольцами (см., например, [5]), они получили довольно легкие доказательства теорем, подобных теореме Мальцева, в довольно общих ситуациях (для линейных групп над первичными кольцами, мультипликативных полугрупп, решеток подмодулей и т. д.).

Приведем некоторые результаты К. И. Бейдара и А. В. Михалева, полученные в [7].

Пусть R и S — некоторые ассоциативные кольца с 1. Как обычно, $M_n(R)$ и $M_n(S)$ обозначают кольца матриц размера $(n \times n)$ над R и S соответственно. С каждым левым R-модулем M ассоциируем решетку всех его подмодулей $\mathcal{L}(M)$ и частично упорядоченное множество всех его конечно порожденных подмодулей $FGL(M)$. Мультипликативная полугруппа кольца R обозначается через R^*. *Противоположное кольцо кольца* R — это кольцо R^{op}, состоящее из того же множества элементов, что и R, с тем же законом сложения, но с законом умножения, определенном формулой $r * s = sr$. В дальнейшем $\mathcal{U}$, $\mathcal{V}$ и $\mathcal{W}$ будут обозначать классы алгебраических систем с языками Ω_u, Ω_v и Ω_w соответственно.

Определение 3.1. Отображение $\mathcal{F}$ из класса $\mathcal{U}$ в класс $\mathcal{V}$ называется *соответствием* из $\mathcal{U}$ в $\mathcal{V}$. Предположим, что классы $\mathcal{U}$ и $\mathcal{V}$ замкнуты относительно ультрастепеней. Соответствие $\mathcal{F}$ называется *регулярным*, если $\mathcal{F}$ перестановочно с ультрастепенями; это означает, что для любой алгебраической системы $R \in \mathcal{U}$ и любого ультрафильтра α

$$\mathcal{F}\left(\prod_\alpha R\right) \cong \prod_\alpha \mathcal{F}(R).$$

Теорема 3.1. *Пусть $\mathcal{U}$, $\mathcal{V}$ и $\mathcal{W}$ — классы алгебраических систем языков Ω_u, Ω_v и Ω_w соответственно, замкнутые относительно взятия ультрастепеней,*

$$\mathcal{F} = \{F_i \mid i = 1, 2, \dots\}, \quad \mathcal{G} = \{G_{ij} \mid i, j = 1, 2, \dots\}$$

— регулярные семейства соответствий из $\mathcal{U}$ в $\mathcal{V}$ и из $\mathcal{U}$ в $\mathcal{W}$ соответственно. Предположим, что имеется натуральное число m такое, что для любых алгебраических систем $R, S \in \mathcal{U}$ и любых целых $p, q \geqslant m$ соотношение $F_p(R) \cong F_q(S)$ равносильно существованию таких номеров $r, s \geqslant 1$, что $G_{rp}(R) \cong G_{sq}(S)$. Теперь пусть $R, S \in \mathcal{U}$ и $p, q \geqslant m$. Тогда $F_p(R) \equiv F_q(S)$ если и только если существуют такие номера $r, s \geqslant 1$, что $G_{rp}(R) \equiv G_{sq}(S)$.

Из этой теоремы можно вывести несколько полезных следствий.

Следствие 3.1. *Пусть R и S — первичные ассоциативные кольца с 1 (или $1/2$), $m, n \geqslant 3$ (или $m, n \geqslant 2$). Тогда $GL_m(R) \equiv GL_n(S)$ если и только если либо $M_m(R) \equiv M_n(S)$, либо $M_m(R) \equiv M_n(S)^{\mathrm{op}}$.*

Следствие 3.2. *Пусть R и S — тела, $m, n \geqslant 3$. Тогда $GL_m(R) \equiv GL_n(S)$ если и только если либо $m = n$ и $R \equiv S$, либо $m = n$ и $R \equiv S^{\mathrm{op}}$.*

Следствие 3.3. *Пусть $\mathcal{U}$ — класс всех ассоциативных колец с 1 таких, что каждый левый 2-порожденный идеал является главным проективным левым идеалом. Пусть, кроме того, $R, S \in \mathcal{U}$ и $m, n \geqslant 3$. Тогда соотношение $FGL(R^m) \equiv FGL(S^n)$ равносильно соотношению $M_m(R) \equiv M_n(S)$.*

Следствие 3.4. *Пусть R и S — ассоциативные кольца с 1, $m, n \geqslant 3$. Тогда из $\mathcal{L}(R^m) \equiv \mathcal{L}(S^n)$ следует $M_n(R) \equiv M_n(S)$.*

4. Элементарная эквивалентность унитарных линейных групп над полями. В 1998–2001 гг. Е. И. Бунина продолжила изучение элементарных свойств линейных групп (см. [1–4]). В 1998 г. (см. [1, 4]) результаты А. И. Мальцева были распространены на унитарные линейные группы над полями с инволюцией. Доказательства, как и в [6], базировались на жордановой нормальной форме матриц.

Пусть K — бесконечное поле характеристики, не равной 2, с инволюцией j (инволюция — это антиавтоморфизм второго порядка), $M_n(K)$ — кольцо матриц размера $(n\times n)$ над полем K, $GL_n(K)$ — общая линейная группа над K. Пусть Q_{2n} обозначает следующую матрицу из $GL_{2n}(K)$:

$$\left.\begin{pmatrix} 0 & 1 & \dots & 0 & 0 \\ -1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & \dots & -1 & 0 \end{pmatrix}\right\} 2n.$$

Пусть $U_{2n}(K, j, Q)$ — *унитарная группа* всех матриц $A \in GL_{2n}(K)$ таких, что

$$AQ_{2n}A^* = Q_{2n},$$

где

$$A^* = (A^j)^T = \begin{pmatrix} a^j_{11} & \dots & a^j_{1n} \\ \vdots & \ddots & \vdots \\ a^j_{n1} & \dots & a^j_{nn} \end{pmatrix}^T = \begin{pmatrix} a^j_{11} & \dots & a^j_{n1} \\ \vdots & \ddots & \vdots \\ a^j_{1n} & \dots & a^j_{nn} \end{pmatrix}.$$

Следующая теорема была доказана Е. И. Буниной (см. [1, 4]).

Теорема 4.1. *Группы $U_{2n}(K_1, j_1, Q_{2n})$ и $U_{2m}(K_2, j_2, Q_{2m})$, где K_1 и K_2 — бесконечные поля характеристик, не равных 2, с инволюциями j_1 и j_2 соответственно, $n, m \geqslant 2$, элементарно эквивалентны тогда и только тогда, когда $m = n$ и поля K_1 и K_2 элементарно эквивалентны как поля с инволюциями.*

Элементарная эквивалентность полей с инволюцией означает, что в предложениях помимо операций кольца можно использовать операцию взятия инволюции.

5. Элементарная эквивалентность унитарных линейных групп над кольцами и телами. Так же, как это было сделано для линейных групп над кольцами, используя теорему Кейслера—Шелаха об изоморфизме, в 1998 г. Е. И. Бунина (см. [2, 4]) рассмотрела элементарную эквивалентность унитарных линейных групп над кольцами и телами с инволюцией.

Если K — кольцо с инволюцией j, то через τ обозначается инволюция кольца $M_{2n}(K)$ матриц над K, имеющая вид

$$\tau : A = \begin{pmatrix} a_{11} & \dots & a_{1\,2n} \\ \vdots & \ddots & \vdots \\ a_{2n\,1} & \dots & a_{2n\,2n} \end{pmatrix} \longmapsto Q_{2n} \circ \begin{pmatrix} a^j_{1\,1} & \dots & a^j_{2n\,1} \\ \vdots & \ddots & \vdots \\ a^j_{1\,2n} & \dots & a^j_{2n\,2n} \end{pmatrix} \circ Q^{-1}_{2n},$$

где Q_{2n} — матрица из предыдущего раздела.

Унитарная линейная группа $U_{2n}(K, j, Q_{2n})$ над кольцом K с инволюцией j — это группа, состоящая из всех матриц $A \in M_{2n}(K)$ таких, что

$$AA^\tau = E.$$

Сформулируем теперь две теоремы, доказанные Е. И. Буниной.

Теорема 5.1. *Если K_1 и K_2 — ассоциативные (коммутативные) кольца с $1/2$ и $1/3$, j_1 и j_2 — инволюции в кольцах K_1 и K_2 соответственно, $n, m > 2$ ($n, m > 1$), то унитарные линейные группы $U_{2n}(K_1, j_1, Q_{2n})$ и $U_{2m}(K_2, j_2, Q_{2m})$ элементарно эквивалентны тогда и только тогда, когда кольца $M_{2n}(K_1)$ и $M_{2m}(K_2)$ элементарно эквивалентны как кольца с инволюциями τ_1 и τ_2 соответственно.*

Теорема 5.2. *Если тела (поля) F_1 и F_2 имеют характеристику, отличную от 2, j_1 и j_2 — инволюции в телах (полях) F_1 и F_2 соответственно, $n, m > 2$ $(n, m > 1)$, то унитарные линейные группы $U_{2n}(F_1, j_1, Q_{2n})$ и $U_{2m}(F_2, j_2, Q_{2m})$ элементарно эквивалентны тогда и только тогда, когда тела (поля) F_1 и F_2 элементарно эквивалентны как тела (поля) с инволюциями j_1 и j_2 соответственно.*

6. Элементарная эквивалентность групп Шевалле. В 2001 г. Е. И. Бунина (см. [3, 4]) изучила элементарные свойства групп Шевалле над алгебраически замкнутыми полями. Класс всех групп Шевалле содержит множество классических групп, таких как $SL_n(K)$, $PSL_n(K)$, $SO_n(K)$, $Spin_n(K)$, $PSO_n(K)$, $Sp_{2n}(K)$, $PSp_{2n}(K)$. Таким образом, изучаемые группы пересекаются с группами, рассмотренными А. И. Мальцевым, но существует также много не рассмотренных им алгебраических групп в этом классе.

Дадим сначала определение группы Шевалле над полем.

Пусть $\mathcal{L}$ — полупростая алгебра Ли над $\mathbb{C}$ с фиксированной картановской подалгеброй $\mathcal{H}$ и V — конечномерное пространство представления алгебры $\mathcal{L}$. Вектор $v \in V$ назовем *весовым вектором* (веса λ), если существует линейная функция λ на $\mathcal{H}$ такая, что $Hv = \lambda(H)v$ для всех $H \in \mathcal{H}$. Если такой ненулевой вектор v существует, соответствующая функция называется *весом* представления. Пространство всех весовых векторов v, соответствующих весу λ, обозначается через V_λ.

Если V — векторное пространство над $\mathbb{C}$, а M — конечно порожденная (свободная абелева) подгруппа в V с $\mathcal{L}$-базисом, который является также $\mathbb{C}$-базисом пространства V, мы назовем M *решеткой* над V.

Аддитивная группа, порожденная всеми весами точного представления алгебры $\mathcal{L}$ в пространстве V, порождает решетку L_V. Аддитивная группа, порожденная всеми корнями, является подрешеткой L_0 решетки L_V. Решетка L_0 имеет конечный индекс в L_V.

Пусть K — поле, Σ — система корней алгебры Ли $\mathcal{L}$. Рассмотрим автоморфизмы пространства V^K, имеющие форму $\exp tX_\alpha$ $(t \in K,\ \alpha \in \Sigma)$, где

$$\exp tX_\alpha = \sum_{n=0}^{\infty} \frac{t^n}{n!} X_\alpha^n.$$

Правая часть этого отношения понимается следующим образом. Так как $X_\alpha^n/n! \in \mathcal{U}_\mathbb{Z}$, имеем действие $X_\alpha^n/n!$ на M. Значит, $\lambda^n X_\alpha^n/n!$ действует на $M \otimes_\mathbb{Z} \mathbb{Z}(\lambda)$. Оператор X_α^n равен нулю, если n велико; следовательно, $\sum\limits_{n=0}^{\infty} \lambda^n X_\alpha^n/n!$ действует на $M \otimes_\mathbb{Z} \mathbb{Z}[\lambda]$ и на $M \otimes_\mathbb{Z} \mathbb{Z}[\lambda] \otimes_\mathbb{Z} K$. Полагая $\lambda = t$, получим оператор $\sum\limits_{n=0}^{\infty} t^n X_\alpha^n/n!$ на пространстве $V^n = M \otimes_\mathbb{Z} K$. Обозначим оператор $\exp tX_\alpha$ через $x_\alpha(t)$, а группу $\{x_\alpha(t) \mid t \in K\}$ — через X_α. Группа, порожденная всеми группами X_α $(\alpha \in \Sigma)$, называется *группой Шевалле*.

Основным результатом является следующая теорема.

Теорема 6.1. *Предположим, что группы Шевалле $\mathcal{G}_1$ и $\mathcal{G}_2$ построены, соотетственно, по алгебраически замкнутым полям K_1 и K_2 характеристик, не равных 2, простым алгебрам Ли $\mathcal{L}_1$ и $\mathcal{L}_2$ и решеткам $M := L_{V_1}$ и $N := L_{V_2}$. Пусть $M/M_0 \cong \varphi_1$ и $N/N_0 \cong \varphi_2$, где φ_1 и φ_2 — конечные группы. Тогда $\mathcal{G}_1 \equiv \mathcal{G}_2$ если и только если $K_1 \equiv K_2$, $\mathcal{L}_1 \cong \mathcal{L}_2$ и $\varphi_1 \cong \varphi_2$, исключая случай, когда алгебры $\mathcal{L}_1$ и $\mathcal{L}_2$ имеют один и тот же тип D_{2l}, $l \geqslant 3$, и $\varphi_1 \cong \varphi_2 \cong \mathbb{Z}_2$. В этом случае существуют две неэквивалентные группы при элементарно эквивалентных полях.*

7. Элементарная эквивалентность категорий модулей над кольцом. В 2003 г. авторами были изучены или элементарные свойства категорий модулей над кольцами, колец эндоморфизмов модулей и групп автоморфизмов модулей над кольцами. Наш интерес к этим вопросам возник благодаря работе [11] В. Толстых.

В этом параграфе рассмотрим такую алгебраическую систему, как категория.

Категория — это алгебраическая система C, состоящая из двух классов Obj и Mor, а также трех операций: *коллекции*, *композиции* (которая обозначается через $\circ$) и *отождествления*, удовлетворяющих следующим условиям (записанным в неформальном виде):

1) Каждому элементу класса Mor коллекция ставит в соответствие упорядоченную пару элементов класса Obj (если f — элемент класса Mor, $A, B \in \mathrm{Obj}$ — соответствующие ему элементы, то пишется $f \in \mathrm{Mor}(A, B)$).
2) Каждой паре элементов из класса Mor композиция ставит в соответствие элемент из класса Mor (если f, g — элементы из Mor, h — соответствующий элемент из Mor, пишется $h = f \circ g$); кроме того, для любых $A, B, C \in \mathrm{Obj}$, $f \in \mathrm{Mor}(A, B)$, $g \in \mathrm{Mor}(B, C)$ существует элемент $h \in \mathrm{Mor}(A, C)$ такой, что $h = g \circ f$.
3) Каждому элементу A класса Obj отождествление ставит в соответствие некоторый элемент $f \in \mathrm{Mor}(A, A)$ (пишется $f = 1_A$).
4) Для любых $A, B, C, D \in \mathrm{Obj}$, $w \in \mathrm{Mor}(A, B)$, $v \in \mathrm{Mor}(B, C)$, $u \in \mathrm{Mor}(C, D)$ имеем
$$(u \circ v) \circ w = u \circ (v \circ w).$$
5) Для любых $A, B \in \mathrm{Obj}$, $u \in \mathrm{Mor}(B, A)$, $v \in \mathrm{Mor}(A, B)$ имеем
$$1_A \circ u = u, \quad v \circ 1_A = v.$$

Элементы $u \in \mathrm{Mor}(A, B)$ называются *морфизмами* из объекта A в объект B.

Категория mod-R левых модулей над фиксированным кольцом R состоит из всех левых модулей над кольцом R и всех гомоморфизмов между ними.

Нам бы хотелось сформулировать необходимые и достаточные условия, при которых две категории mod-R и mod-S элементарно эквивалентны.

Модуль $P \in \text{mod-}R$ называется *прообразующим*, если он является конечно порожденным проективным образующим модулем категории mod-R.

Два кольца R и S называются *подобными* (обозначение через $R \sim S$), если существует прообразующий модуль $P \in \text{mod-}R$ и изоморфизм колец $S \cong \mathrm{End}_R P$.

Теорема 7.1 (теорема Мориты)**.** *Следующие условия равносильны*:
1) *категории* mod-R *и* mod-S *Морита-эквивалентны*;
2) $R \sim S$.

Выясним сначала, что происходит, если одно из этих колец конечно.

Теорема 7.2. *Если категории* mod-R *и* mod-S *элементарно эквивалентны и кольцо* R *конечно, то* $R \cong \mathrm{End}_S P$ *для некоторого прообразующего модуля* P *категории* mod-S.

Следствие 7.1. *Категории* mod-R *и* mod-S*, где кольцо* R *конечно, элементарно эквивалентны тогда и только тогда, когда они морита-эквивалентны.*

Предположим теперь, что кольца R и S оба бесконечны.

При доказательстве результатов этого параграфа использованы результаты С. Шелаха [10] об интерпретации теории множеств в категории.

Рассмотрим структуру $\langle Cn, ring\rangle$, состоящую из класса Cn всех кардинальных чисел, который состоит из множеств мощности $\varkappa$ для каждого $\varkappa \in Cn$, и кольца $ring$ с обычными кольцевыми операциями $+$ и $\circ$. *Логика второго порядка* структуры $(L_2(\langle Cn, ring\rangle))$ позволяет в формулах использовать произвольные предикатные символы вида
$$P_{\lambda_1,\ldots,\lambda_k}(c_1, \ldots, c_k; v_1, \ldots, v_n),$$
где $\lambda_1, \ldots, \lambda_k$ — фиксированные кардинальные числа, $c_1, \ldots, c_k$ — переменные для элементов из $\lambda_1, \ldots, \lambda_k$, соответственно, $v_1, \ldots, v_n$ — переменные для элементов кольца.

Таким образом, в формулах этого языка мы можем использовать следующие подформулы:
1) $\forall r \in ring$ $(\exists r \in ring)$;
2) $\forall \varkappa \in Cn$ $(\exists \varkappa \in Cn)$;
3) $\forall \alpha \in \varkappa$ $(\exists \alpha \in \varkappa)$;
4) $r_1 = r_2 + r_3$;
5) $r_1 = r_2 \cdot r_3$;
6) $r_1 = r_2$;
7) $\varkappa_1 = \varkappa_2$;

8) $\alpha_1 = \alpha_2$.
9) $\forall P_{\varkappa_1,\ldots,\varkappa_k}(c_1,\ldots,c_k;v_1,\ldots,v_n)$ $(\exists P_{\varkappa_1,\ldots,\varkappa_k}(c_1,\ldots,c_k;v_1,\ldots,v_n))$;
10) $P_{\varkappa_1,\ldots,\varkappa_k}(\alpha_1,\ldots,\alpha_k;r_1,\ldots,r_n)$.

Теорема 7.3. *Пусть R и S — кольца. Предположим, что существует предложение ψ языка $L_2(\langle Cn, ring\rangle)$, истинное в кольце R и ложное в любом кольце, подобном кольцу R и не эквивалентном ему в языке $L_2(\langle Cn, ring\rangle)$. Если категории* mod-$R$ *и* mod-S *элементарно эквивалентны, то существует кольцо S', подобное кольцу S и такое, что структуры $\langle Cn, R\rangle$ и $\langle Cn, S'\rangle$ эквивалентны в логике L_2.*

Следующая теорема (обратная к предыдущей) выполняется для произвольных ассоциативных колец с единицей.

Теорема 7.4. *Если структуры $\langle Cn, R\rangle$ и $\langle Cn, S\rangle$ эквивалентны в логике второго порядка L_2, то категории* mod-R *и* mod-S *элементарно эквивалентны.*

Следующая теорема непосредственно вытекает из теорем 7.3 и 7.4.

Теорема 7.5. *Пусть R и S — кольца. Предположим, что существует предложение ψ языка $L_2(\langle Cn, ring\rangle)$, истинное в кольце R и ложное в любом кольце, подобном кольцу R и не эквивалентном ему в языке $L_2(\langle Cn, ring\rangle)$. Категории* mod-$R$ *и* mod-S *элементарно эквивалентны тогда и только тогда, когда существует кольцо S', подобное кольцу S и такое, что структуры $\langle Cn, R\rangle$ и $\langle Cn, S'\rangle$ эквивалентны в логике L_2.*

Следствие 7.2. *Для любых тел (локальных колец, областей целостности) F_1 и F_2 категории* mod-F_1 *и* mod-F_2 *элементарно эквивалентны тогда и только тогда, когда структуры $\langle Cn, F_1\rangle$ и $\langle Cn, F_2\rangle$ эквивалентны в логике второго порядка L_2.*

Следствие 7.3. *Для любых коммутативных колец R_1 и R_2 категории* mod-R_1 *и* mod-R_2 *элементарно эквивалентны тогда и только тогда, когда структуры $\langle Cn, R_1\rangle$ и $\langle Cn, R_2\rangle$ эквивалентны в логике второго порядка L_2.*

Следствие 7.4. *Для артиновых колец R_1 и R_2 категории* mod-R_1 *и* mod-R_2 *элементарно эквивалентны тогда и только тогда, когда существуют кольца S_1 и S_2 такие, что кольцо S_1 подобно кольцу R_1, кольцо S_2 подобно кольцу R_2 и структуры $\langle Cn, S_1\rangle$ и $\langle Cn, S_2\rangle$ эквивалентны в логике второго порядка L_2.*

8. Элементарная эквивалентность колец эндоморфизмов модулей. Рассмотрим теперь кольца эндоморфизмов модулей.

Предположим, что мы имеем некоторое ассоциативное кольцо R с единицей, бесконечное кардинальное число $\varkappa$ и свободный модуль $V = V_{\varkappa}^{R}$, имеющий ранг $\varkappa$ над R.

В кольце $\mathrm{End}_R(V)$ можно интерпретировать категорию C_V с выделенным объектом $V \in \mathrm{Obj}(C_V)$, состоящую из всех фактормодулей модуля V и всех гомоморфизмов между ними.

Лемма 8.1. *Соотношение $\mathrm{End}_{R_1}(V_1) \equiv \mathrm{End}_{R_2}(V_2)$ равносильно соотношению $C_{V_1} \equiv C_{V_2}$.*

Таким образом, вопрос об элементарной эквивалентности колец эндоморфизмов $\mathrm{End}_{R_1}(V_1)$ и $\mathrm{End}_{R_2}(V_2)$ сводится к вопросу об элементарной эквивалентности категорий C_{V_1} и C_{V_2} с выделенными объектами V_1 и V_2 соответственно.

Заметим, что рассматриваемая ситуация очень напоминает ситуацию категории модулей над кольцом (см. раздел 7). Имеем категорию C_V, являющуюся подкатегорией в категории mod-R, замкнутую относительно взятия фактормодулей и прямых произведений мощности $\leqslant \varkappa$. Такая категория похожа на категорию mod-R, но ограничена данным кардинальным числом $\varkappa$. Кроме того, в этой категории модуль V является выделенным.

Действительно, для этих объектов мы можем получить аналогичные результаты. Для этого рассмотрим, помимо полного языка $L_2(\langle Cn, ring\rangle)$, его часть, которая может быть описана следующим образом.

Теорией данной модели $\mathcal{U}$ языка $\mathcal{L}$ называется множество всех предложений этого языка, истинных в модели $\mathcal{U}$. Ясно, что две модели $\mathcal{U}$ и $\mathcal{B}$ одного языка $\mathcal{L}$ эквивалентны в языке $\mathcal{L}$ тогда и только тогда, когда их теории в этом языке совпадают.

Теорию структуры $\langle Cn, R\rangle$ в языке L_2 мы будем обозначать через $\mathrm{Th}_2(\langle Cn, R\rangle)$.

Мы можем также рассмотреть структуру $\langle \varkappa, R\rangle$, состоящую из множества мощности $\varkappa$ и кольца R с кольцевыми операциями $+$ и $\circ$.

Через $\mathrm{Th}_2^{\varkappa}(\langle \varkappa, R\rangle)$ будем обозначать часть теории $\mathrm{Th}_2(\langle \varkappa, R\rangle)$, ограниченную кардинальным числом $\varkappa$, т.е. такие предложения $\varphi \in \mathrm{Th}_2(\langle \varkappa, R\rangle)$, что кванторы $\forall$ и $\exists$ стоят только у предикатных символов

$$P(c_1, \ldots, c_k; v_1, \ldots, v_n),$$

для которых множество

$$\{\langle \alpha_1, \ldots, \alpha_k, r_1, \ldots, r_n\rangle | \alpha_1, \ldots, \alpha_k \in \varkappa \wedge r_1, \ldots, r_n \in R \wedge P(\alpha_1, \ldots, \alpha_k; r_1, \ldots, r_n)\}$$

имеет мощность, не большую, чем $\varkappa$.

Тогда имеет место следующий аналог теоремы 7.5.

Теорема 8.1. *Пусть V_1 и V_2 — свободные модули бесконечных рангов $\varkappa_1$ и $\varkappa_2$ над кольцами R_1 и R_2 соответственно. Предположим, что существует предложение $\psi \in \mathrm{Th}_2^{\varkappa_1}(\langle \varkappa_1, R_1\rangle)$ такое, что $\varphi \notin \mathrm{Th}_2^{\varkappa_1}(\langle \varkappa_1, R'\rangle)$ для каждого кольца R', подобного R_1 и такого, что $\mathrm{Th}_2^{\varkappa_1}(\langle \varkappa_1, R_1\rangle) \neq \mathrm{Th}_2^{\varkappa_1}(\langle \varkappa_1, R'\rangle)$. Категории C_{V_1} и C_{V_1} элементарно эквивалентны тогда и только тогда, когда существует кольцо S, подобное кольцу R_2 и такое, что теории $\mathrm{Th}_2^{\varkappa_1}(\langle \varkappa_1, R_1\rangle)$ и $\mathrm{Th}_2^{\varkappa_2}(\langle \varkappa_2, S\rangle)$ совпадают.*

Из предыдущих результатов вытекает следующая теорема.

Теорема 8.2. *Пусть V_1 и V_2 — свободные модули бесконечных рангов $\varkappa_1$ и $\varkappa_2$ над кольцами R_1 и R_2 соответственно. Предположим, что существует предложение $\psi \in \mathrm{Th}_2^{\varkappa_1}(\langle \varkappa_1, R_1\rangle)$ такое, что $\varphi \notin \mathrm{Th}_2^{\varkappa_1}(\langle \varkappa_1, R'\rangle)$ для любого кольца R', подобного R_1 и такого, что $\mathrm{Th}_2^{\varkappa_1}(\langle \varkappa_1, R_1\rangle) \neq \mathrm{Th}_2^{\varkappa_1}(\varkappa_1, R'\rangle)$. Кольца $\mathrm{End}_{R_1}(V_1)$ и $\mathrm{End}_{R_2}(V_1)$ элементарно эквивалентны если и только если существует кольцо S, подобное кольцу R_2 и такое, что теории $\mathrm{Th}_2^{\varkappa_1}(\langle \varkappa_1, R_1\rangle)$ и $\mathrm{Th}_2^{\varkappa_2}(\langle \varkappa_2, S\rangle)$ совпадают.*

Следствие 8.1. *Для свободных модулей V_1 и V_2 бесконечных рангов $\varkappa_1$ и $\varkappa_2$ над телами (коммутативными кольцами, локальными кольцами, областями целостности) F_1 и F_2 соответственно кольца $\mathrm{End}_{F_1}(V_1)$ и $\mathrm{End}_{F_2}(V_2)$ элементарно эквивалентны если и только если теории $\mathrm{Th}_2^{\varkappa_1}(\langle \varkappa_1, F_1\rangle)$ и $\mathrm{Th}_2^{\varkappa_2}(\langle \varkappa_2, F_2\rangle)$ совпадают.*

Следствие 8.2. *Для свободных модулей V_1 и V_2 бесконечных рангов $\varkappa_1$ и $\varkappa_2$ над артиновыми кольцами F_1 и F_2 соответственно кольца $\mathrm{End}_{F_1}(V_1)$ и $\mathrm{End}_{F_2}(V_2)$ элементарно эквивалентны если и только если существуют кольца R_1 и R_2 такие, что кольцо R_1 подобно кольцу F_1, кольцо R_2 подобно кольцу F_2 и теории $\mathrm{Th}_2^{\varkappa_1}(\langle \varkappa_1, R_1\rangle)$ и $\mathrm{Th}_2^{\varkappa_2}(\langle \varkappa_2, R_2\rangle)$ совпадают.*

9. Элементарная эквивалентность групп автоморфизмов модулей. В 1983 г. И. З. Голубчик и А. В. Михалев доказали [5], что если кольца R и S с $1/2$ не содержат центральных идемпотентов, не равных 0 и 1, то группы $\mathrm{Aut}_R(R^{(n)})$ и $\mathrm{Aut}_S(S^{(m)})$ изоморфны тогда и только тогда, когда либо $\mathrm{End}_R(R^{(n)}) \cong \mathrm{End}_S(S^{(m)})$, либо $\mathrm{End}_R(R^{(n)}) \cong \mathrm{End}_S(S^{(m)})^{\mathrm{op}}$. Используя эту теорему, можно доказать следующее утверждение.

Теорема 9.1. *Предположим, что кольца R, S содержат $1/2$ и не содержат центральных идемпотентов, отличных от 1 и 0; V, V' — свободные модули бесконечных рангов над кольцами R и S соответственно. Группы $\mathrm{Aut}_R(V)$ и $\mathrm{Aut}_S(V')$ элементарно эквивалентны если и только если кольца $\mathrm{End}_R(V)$ и $\mathrm{End}_S(V')$ элементарно эквивалентны.*

Таким образом, в случае, когда мы имеем ассоциативные кольца с $1/2$, не содержащие центральных идемпотентов, отличных от 0 и 1, то вопрос элементарной эквивалентности групп автоморфизмов сводится к вопросу элементарной эквивалентности колец эндоморфизмов, решенному в предыдущем разделе. Отсюда вытекает следующая теорема.

Теорема 9.2. *Предположим, что кольца R_1 и R_2 содержат $1/2$ и не содержат центральных идемпотентов, отличных от 1 и 0. Пусть V_1 и V_2 — свободные модули бесконечных рангов $\varkappa_1$ и $\varkappa_2$ над кольцами R_1 и R_2 соответственно и пусть существует предложение $\psi \in \mathrm{Th}_2^{\varkappa_1}(\langle \varkappa_1, R_1\rangle)$ такое, что $\psi \notin \mathrm{Th}_2^{\varkappa_1}(\langle \varkappa_1, R'\rangle)$ для любого кольца R', подобного кольцу R_1 и такого, что $\mathrm{Th}_2^{\varkappa_1}(\langle \varkappa_1, R_1\rangle) \neq \mathrm{Th}_2^{\varkappa_1}(\varkappa_1, R'\rangle)$. Группы $\mathrm{Aut}_{R_1}(V_1)$ и $\mathrm{Aut}_{R_2}(V_2)$ элементарно эквивалентны если и только если существует кольцо S, подобное кольцу R_2 и такое, что теории $\mathrm{Th}_2^{\varkappa_1}(\langle \varkappa_1, R_1\rangle)$ и $\mathrm{Th}_2^{\varkappa_2}(\langle \varkappa_2, S\rangle)$ совпадают.*

Следствие 9.1 (ср. с [11])**.** *Для свободных модулей V_1 и V_2 бесконечных рангов $\varkappa_1$ и $\varkappa_2$ над телами (областями целостности, коммутативными или локальными кольцами без центральных идемпотентов, отличных от 1 и 0) F_1 и F_2 с $1/2$ соответственно, группы $\mathrm{Aut}_{F_1}(V_1)$ и $\mathrm{Aut}_{F_2}(V_2)$ элементарно эквивалентны если и только если теории $\mathrm{Th}_2^{\varkappa_1}(\langle \varkappa_1, F_1\rangle)$ и $\mathrm{Th}_2^{\varkappa_2}(\langle \varkappa_2, F_2\rangle)$ совпадают.*

Следствие 9.2. *Для свободных модулей V_1 и V_2 бесконечных рангов $\varkappa_1$ и $\varkappa_2$ над артиновыми кольцами без центральных идемпотентов, отличных от 1 и 0, F_1 и F_2, с $1/2$, соответственно, группы $\mathrm{Aut}_{F_1}(V_1)$ и $\mathrm{Aut}_{F_2}(V_2)$ элементарно эквивалентны если и только если существуют кольца R_1 и R_2 такие, что кольцо F_1 подобно кольцу R_1, кольцо F_2 подобно кольцу R_2 и теории $\mathrm{Th}_2^{\varkappa_1}(\langle \varkappa_1, R_1\rangle)$ и $\mathrm{Th}_2^{\varkappa_2}(\langle \varkappa_2, R_2\rangle)$ совпадают.*

СПИСОК ЛИТЕРАТУРЫ

1. *Бунина Е. И.* Элементарная эквивалентность унитарных линейных групп над полями// Фундам. прикл. мат. — 1998. — *4*. — С. 1–14.
2. *Бунина Е. И.* Элементарная эквивалентность унитарных линейных групп над кольцами и телами// Усп. мат. наук. — 1998. — *53*, № 2. — С. 137–138.
3. *Бунина Е. И.* Элементарная эквивалентность групп Шевалле// Усп. мат. наук. — 2001. — *156*, № 1. — С. 157–158.
4. *Бунина Е. И.* Элементарная эквивалентность линейных и алгебраических групп/ Дисс. ... канд. физ.-мат. наук. — М., 2001.
5. *Голубчик И. З., Михалев А. В.* Изоморфизмы общих линейных групп над ассоциативными кольцами// Вестн. МГУ. Сер. мат., мех. — 1983. — *3*. — С. 61–72.
6. *Мальцев А. И.* Об элементарных свойствах линейных групп// Проблемы математики и механики. — Новосибирск, 1961. — С. 110–132.
7. *Beidar K. I. Mikhalev A. V.* On Malcev's theorem on elementary equivalence of linear groups// Contemp. Math. — 1992. — *131*. — С. 29–35.
8. *Chang C. C., Keisler H. J.* Model theory. — Amsterdam–London: North-Holland, 1973.
9. *Faith C.* Algebra: Rings, Modules, and Categories. Part I. — Springer-Verlag, 1973.
10. *Shelah S.* Interpreting set theory in the endomorphism semi-group of a free algebra or in the category// Ann. Sci. L'univ. Clermont. — 1976. — *13*. — С. 1–29.
11. *Tolstykh V.* Elementary equivalence of infinite-dimensional classical groups// Ann. Pure Appl. Logic. — 2000. — *105*. — С. 103–156.

Е. И. Бунина
Московский государственный университет
А. В. Михалев
Московский государственный университет