Летняя школа «Современная математика»
Дубна, июль 2007

И. В. Аржанцев

Градуированные алгебры и 14-я проблема Гильберта

Учебное пособие

Москва
Издательство МЦНМО
2009

УДК 512.815.4
ББК 22.14
А80

Проведение летних школ «Современная математика» и издание её материалов поддержано Московской городской Думой и Департаментом образования г. Москвы, а также фондом «Династия», фирмой «НИКС» и корпорацией Boeing.

Рецензенты: д. ф.-м. н., профессор Э. Б. Винберг
к. ф.-м. н., доцент Т. Е. Панов

Аржанцев И. В.

А80 Градуированные алгебры и 14-я проблема Гильберта: Учебное пособие. — М.: МЦНМО, 2009. — 64 с.

ISBN 978-5-94057-491-0

Учебное пособие посвящено классическим задачам коммутативной алгебры и теории инвариатов. Помимо начальных сведений о градуированных алгебрах, их рядах Пуанкаре и многочленах Гильберта, приводятся доказательства теоремы Маколея о размерностях компонент стандартных градуированных алгебр, формулы Молина для ряда Пуанкаре алгебры инвариантов конечной линейной группы и теоремы Нагаты—Стейнберга о том, что алгебра инвариантов некоторой явно заданной линейной алгебраической группы не является конечно порожденной. Последний результат является контрпримером к 14-й проблеме Гильберта. Пособие содержит более 40 задач, к каждой из которых даны подробные указания. Излагаемый материал доступен студентам младших курсов физико-математических специальностей университетов.

Для студентов, аспирантов, преподавателей и научных работников, интересующихся алгеброй, геометрией и комбинаторикой.

ББК 22.14

Оглавление

Введение

Что такое современная математика? Это стройные теории, состоящие из цепочки определений, несложных утверждений и эффектных примеров? Или это глубокие и технически сложные теоремы, на разбор только схем доказательств которых может понадобиться несколько часов или дней? Пожалуй, это и то и другое, и трудно отыскать золотую середину, лежащую между двумя описанными крайностями. В этом пособии мы продолжаем поиск недостижимой середины. Здесь излагаются как фрагменты классических теорий, так и доказательства двух трудных результатов: теоремы Маколея о последовательностях размерностей компонент стандартных градуированных алгебр и теоремы Нагаты—Стейнберга о том, что алгебра инвариантов некоторой линейной группы не является конечно порожденной. Последний результат обеспечивает контрпример к 14-й проблеме Гильберта. В настоящее время стало возможным провести доказательства этих теорем, опираясь только на факты из курса линейной алгебры. Этот подход и будет реализован ниже.

Остановимся подробнее на содержании пособия. В первых параграфах излагаются стандартные факты о коммутативных градуированных алгебрах, определяются ряды Пуанкаре и многочлены Гильберта, доказывается теорема о представимости ряда Пуанкаре конечно порожденной градуированной алгебры рациональной функцией. Затем мы переходим к изучению последовательностей размерностей компонент $\dim A_i$ градуированной алгебры $A = \bigoplus_{s \geqslant 0} A_i$. Какие числовые последовательности так реализуются? Этот вопрос наиболее интересен для конечно порожденных алгебр, которые порождаются элементами первой степени. Такие алгебры являются факторалгебрами $\mathbb{K}[x_1, \ldots, x_n]/I$ алгебры многочленов со стандартной градуировкой. Несложно показать, что идеал I можно заменить на идеал, порожденный одночленами, так, что последовательность размерностей компонент не изменится. Трудная часть теоремы Маколея — это обоснование перехода от произвольного мономиального идеала к лекссегментному идеалу, т. е. идеалу, являющемуся линейной оболочкой конечных отрезков последовательностей одночленов фиксированных степеней в лексикографическом порядке. В § 5 мы доказываем этот результат, следуя работе [10]. Теперь проверка реа-

лизуемости данной числовой последовательности сводится к проверке того, что линейная оболочка некоторого набора одночленов есть идеал. Такой критерий является эффективно проверяемым, однако его можно улучшить.

В работе П. Макмюллена [14] в связи с проблемой характеризации g-векторов симплициальных многогранников возникли числовые неравенства, связанные с разложениями натуральных чисел в суммы биномиальных коэффициентов. Это позволило Р. Стенли включить в теорему еще одно эквивалентное условие — числовое неравенство на следующий член последовательности, определяемое предыдущим членом. В терминах этого условия М. Грин получил индуктивное доказательство трудной части теоремы Маколея, в котором используется переход от алгебры A к факторалгебре $A/(a)$, где a — элемент общего положения компоненты A_1. Результаты Грина приведены в § 6. О приложениях теоремы Маколея в теории выпуклых многогранников и топологии можно прочитать в гл. 1 книги [2].

В последних параграфах обсуждаются подалгебры инвариантов линейных групп в алгебре многочленов. Хорошо известно, что алгебра инвариантов конечной группы конечно порождена. Мы приводим три доказательства этой теоремы. Одно из них, принадлежащее Э. Нётер, показывает, что если основное поле имеет нулевую характеристику, то алгебра инвариантов порождается многочленами, степени которых не превосходят порядка группы. Это позволяет для групп небольших порядков явно находить образующие алгебры инвариантов. Параграф 8 посвящен формуле для ряда Пуанкаре алгебры инвариантов конечной группы, которая была найдена Ф. Э. Молиным в 1897 г. Дальнейшие сведения о рядах Пуанкаре алгебр инвариантов линейных групп можно найти в работах [4, § 3] и [7].

Пусть G — бесконечная подгруппа группы $\mathrm{GL}_n(\mathbb{K})$. Верно ли, что алгебра инвариантов $\mathbb{K}[x_1, \ldots, x_n]^G$ конечно порождена? Этот вопрос известен как 14-я проблема Гильберта. История этой проблемы весьма драматична[1]. На втором Международном конгрессе математиков, проходившем в августе 1900 года в Париже, Д. Гильберт поставил несколько проблем, решение которых, по его мнению, должно было определить основные направления развития математики XX века. В самом докладе Гильберт предложил 10 проблем, и интересующая нас проблема там не фигурировала. Однако в опубликованном тексте доклада проблем было уже 23, и проблема о конечной порожденности

[1] Приведенные здесь сведения заимствованы из комментариев В. Л. Попова в книге [5]. Там же дан обзор известных в настоящее время результатов, связанных с 14-й проблемой.

алгебры инвариантов имела номер 14. На самом деле при постановке этой проблемы Гильберт ссылается на работу Л. Маурера 1899 г., в которой конечная порожденность алгебры инвариантов была доказана для любой подгруппы $G \subseteq \mathrm{GL}_n(\mathbb{K})$, и ставит более общий вопрос.

• Пусть $K \subset \mathbb{K}(x_1, \ldots, x_n)$ — некоторое подполе поля рациональных функций, содержащее поле $\mathbb{K}$. Верно ли, что алгебра $\mathbb{K}[x_1, \ldots, x_n] \cap K$ является конечно порожденной?[1]

Однако, как вскоре выяснилось, работа Маурера содержала ошибку, и с тех пор 14-я проблема Гильберта рассматривается именно как проблема о конечной порожденности алгебры инвариантов. В первой половине XX в. было получено несколько положительных результатов в этом направлении. Однако в 1958 г. на конгрессе в Эдинбурге М. Нагата — весьма неожиданно — привел пример группы, для которой алгебра инвариантов не допускает конечного числа порождающих, см. [16] и [17]. Недавно Р. Стейнбергу удалось модифицировать контрпример Нагаты и заменить в доказательстве тонкие соображения из алгебраической геометрии плоских кривых вполне элементарными аргументами; см. [20]. Эти аргументы мы приводим в § 9. В настоящее время 14-ю проблему естественно формулировать так: охарактеризовать те подгруппы $G \subseteq \mathrm{GL}_n(\mathbb{K})$, для которых алгебра инвариантов $\mathbb{K}[x_1, \ldots, x_n]^G$ конечно порождена. В такой формулировке проблема еще очень далека от окончательного решения.

Наш текст включает много заданий для самостоятельного решения. Они разделены на упражнения и задачи. Упражнения — это или совсем простые утверждения, или рутинные проверки. Читатель легко справится с ними самостоятельно. В свою очередь, все задачи снабжены решениями или подробными указаниями.

Для дальнейшего изучения предмета хочется рекомендовать работы Р. Стенли [18] и [19]. Помню свое впечатление от прочтения этих работ: вот каким должен быть математический текст! Часть изложенного ниже материала заимствована оттуда. В будущем я надеюсь развить намеченный Р. Стенли элегантный подход к изучению коэн-маколеевых и горенштейновых алгебр, полных пересечений и сизигий, где абстрактные понятия коммутативной алгебры вводятся для градуированных алгебр и иллюстрируются на примерах алгебр инвариантов конечных групп, и расширить пособие за счет включения этих тем.

[1] Вопрос о конечной порожденности алгебры инвариантов является частным случаем этого вопроса: достаточно рассмотреть в качестве подполя K подполе рациональных функций, инвариантных относительно действия группы.

Основой для пособия послужили материалы курсов, прочитанных на IV и VII летних школах «Современная математика». Эти школы проводятся ежегодно в июле в доме отдыха «Ратмино» недалеко от города Дубна. Также излагаемые темы обсуждались на совместном с Д. А. Тимашёвым спецсеминаре «Алгебраические группы и теория инвариантов» на механико-математическом факультете МГУ им. М. В. Ломоносова и на спецкурсе в Независимом московском университете. Я благодарен слушателям этих курсов и семинаров за ценные замечания и оригинальные решения ряда задач.

Хочу поблагодарить рецензентов пособия профессора Э. Б. Винберга и доцента Т. Е. Панова, а также П. В. Бибикова, А. Ю. Перепечко и Н. А. Печёнкина, прочитавших предварительную версию текста и сделавших ряд ценных замечаний и исправлений.

Дальнейшие замечания прошу высылать на электронный адрес автора `arjantse@mccme.ru`.

§ 1. Основные понятия и примеры

Напомним, что *алгеброй* над полем $\mathbb{K}$ называется $\mathbb{K}$-векторное пространство A с заданной на нем бинарной операцией (умножением) $A \times A \to A$, $(a, b) \to ab$, удовлетворяющей следующим требованиям:

1) $a(b+c) = ab + ac$, $(b+c)a = ba + ca$ для любых $a, b, c \in A$;

2) $(\lambda a)b = a(\lambda b) = \lambda(ab)$ для любых $\lambda \in \mathbb{K}$, $a, b \in A$.

Всюду далее мы будем дополнительно предполагать, что

3) в A имеется *единица*, т. е. такой элемент 1, что $1a = a1 = a$ для любого $a \in A$;

4) алгебра A *ассоциативна*, т. е. $(ab)c = a(bc)$ для любых $a, b, c \in A$.

Заметим, что наличие единицы позволяет считать поле $\mathbb{K}$ канонически вложенным в алгебру A по формуле $\lambda \to \lambda 1$ (проверьте, что это вложение).

Укажем несколько примеров алгебр:

1) алгебра многочленов $\mathbb{K}[x_1, \ldots, x_n]$;

2) алгебра квадратных матриц $\mathrm{Mat}_{n\times n}(\mathbb{K})$;

3) алгебра $C[0, 1]$ непрерывных вещественнозначных функций на отрезке $[0, 1]$ с поточечным умножением на скаляр, сложением и умножением функций. В этом примере $\mathbb{K} = \mathbb{R}$.

Для двух подпространств $U, V \subseteq A$ определим их произведение UV как линейную оболочку элементов вида ab, где $a \in U$ и $b \in V$. Аналогично определяется произведение любого конечного набора подпространств.

Определение 1. *Градуировкой* на алгебре A называется такое разложение A в прямую сумму подпространств

$$A = \bigoplus_{s\in\mathbb{Z}_+} A_s,$$

что

$$A_{s_1}A_{s_2} \subseteq A_{s_1+s_2} \quad \text{для любых } s_1, s_2 \geqslant 0.$$

Градуированная алгебра — это алгебра с фиксированной градуировкой. Градуировку будем называть *тривиальной*, если $A_0 = A$ и, значит, $A_s = 0$ при $s > 0$. Тривиальная градуировка имеется на любой алгебре.

Подпространства A_s называются (однородными) *компонентами* градуированной алгебры A. Элемент a называют *однородным*, если $a \in A_s$ для некоторого $s \geqslant 0$. В этом случае говорят, что элемент a имеет

степень s, и записывают $\deg a = s$. Степень элемента 0 не определена, и можно считать, что она принимает все возможные значения.

Произвольный элемент $a \in A$ единственным образом записывается в виде суммы $a = a_{j_1} + \ldots + a_{j_k}$ однородных элементов, которые мы будем называть (однородными) *компонентами* этого элемента.

Задача 1. Докажите, что единица — это однородный элемент степени нуль.

Приведем примеры градуировок на алгебре многочленов:

1) $A = \mathbb{K}[x]$, $\deg x = 1$, $\mathbb{K}[x] = \mathbb{K} \oplus \langle x \rangle \oplus \langle x^2 \rangle \oplus \langle x^3 \rangle \oplus \ldots$;

2) более общим образом, $A = \mathbb{K}[x_1, \ldots, x_n]$ и $\deg x_1^{i_1} \ldots x_n^{i_n} = i_1 + \ldots + i_n$;

3) $A = \mathbb{K}[x_1, \ldots, x_n]$ и $\deg x_1^{i_1} \ldots x_n^{i_n} = 2i_1$.

Эти примеры можно обобщить, рассмотрев градуировку алгебры $A = \mathbb{K}[x_1, \ldots, x_n]$, определенную условиями $\deg x_i = d_i$. Целые неотрицательные числа d_i называют *весами* переменных. Назовем такие градуировки на алгебре многочленов *весовыми*. Для весовой градуировки $\deg x_1^{i_1} \ldots x_n^{i_n} = i_1 d_1 + \ldots + i_n d_n$. В частности, во втором примере $d_1 = \ldots = d_n = 1$, а в третьем $d_1 = 2$ и $d_2 = \ldots = d_n = 0$.

Упражнение 1. Приведите пример градуировки на $\mathbb{K}[x]$, для которой x не является однородным элементом.

Задача 2. Докажите, что алгебры а) $\mathrm{Mat}_{n \times n}(\mathbb{K})$; б) $C[0, 1]$ допускают только тривиальную градуировку.

Всюду далее мы считаем алгебру A *коммутативной*, т. е. предполагаем, что $ab = ba$ для любых $a, b \in A$.

Определение 2. 1. Элемент $a \in A$ называется *обратимым*, если найдется такой элемент $b \in A$, что $ab = 1$.

2. Элемент $a \in A$ называется *делителем нуля*, если $a \neq 0$ и найдется такой элемент $b \in A$, $b \neq 0$, что $ab = 0$.

3. Элемент $a \in A$ называется *нильпотентным*, если $a \neq 0$ и найдется такое $n \in \mathbb{N}$, что $a^n = 0$.

Упражнение 2. Докажите, что в конечномерной градуированной алгебре однородный элемент положительной степени является нильпотентным.

Определение 3. Подпространство U градуированной алгебры A называется *однородным*, если

$$U = \bigoplus_{s \geqslant 0} (U \cap A_s).$$

Упражнение 3. Проверьте, что подпространство U однородно тогда и только тогда, когда для каждого $u \in U$ все его компоненты лежат в U.

Напомним, что *подалгеброй* алгебры A называется подпространство B, которое само является алгеброй относительно той же операции умножения. Мы предполагаем, что подалгебра содержит единицу.

Подалгебра B градуированной алгебры A называется *однородной*, если она является однородным подпространством в A. Заметим, что однородная подалгебра B является градуированной алгеброй с однородными компонентами $B_s = B \cap A_s$.

Для изучения градуированных алгебр важно уметь эффективно задавать такие алгебры, а также конструировать новые градуированные алгебры из уже имеющихся. Помимо перехода к однородной подалгебре нам будет полезна конструкция градуировки на факторалгебре.

Напомним, что *идеал* алгебры A — это такое подпространство $I \subseteq A$, что $aI \subseteq I$ для любого $a \in A$. Отметим, что идеал $I \neq A$ не является подалгеброй в A, так как не содержит единицу. На множестве A/I смежных классов по подпространству I формулы

$$(a+I)+(b+I) = a+b+I, \quad \lambda(a+I) = \lambda a+I, \quad (a+I)(b+I) = ab+I$$

корректно определяют операции сложения, умножения на скаляр и умножения. Полученная таким образом алгебра называется *факторалгеброй* алгебры A по идеалу I. Предположим, что идеал I является однородным подпространством градуированной алгебры A. Тогда A/I есть прямая сумма подпространств $A_s + I$, причем $(A_{s_1} + I)(A_{s_2} + I) \subseteq \subseteq A_{s_1+s_2} + I$. Тем самым, для однородного идеала I факторалгебра A/I имеет каноническую градуировку.

С каждым подмножеством $F \subseteq A$ можно связать идеал

$$I = \{r_1 f_1 + \ldots + r_k f_k : k \in \mathbb{N},\ r_i \in A,\ f_i \in F\}.$$

Этот идеал называется идеалом, *порожденным* подмножеством F, и обозначается (F). Легко проверить, что (F) является наименьшим идеалом в A, содержащим F. Если алгебра A градуирована и все элементы подмножества F однородны, то идеал (F) также однороден. Обратно, в однородном идеале можно выбрать однородные порождающие.

Пример 1. Пусть

$$A = \mathbb{K}[x_1, x_2]/(x_1^2, x_1x_2), \quad \deg x_1 = \deg x_2 = 1.$$

Тогда

$$A = \mathbb{K} \oplus \langle x_1, x_2\rangle \oplus \langle x_2^2\rangle \oplus \langle x_2^3\rangle \ldots,$$

$\dim A_1 = 2$, а прочие компоненты одномерны.

Упражнение 4. Можно ли эту градуированную алгебру реализовать в качестве однородной подалгебры некоторой градуированной алгебры многочленов?

Задача 3. Приведите пример градуированной алгебры, в которой есть неоднородный обратимый элемент.

Напомним, что *гомоморфизм* из алгебры A в алгебру A' — это такое линейное отображение $\varphi: A \to A'$, что $\varphi(ab) = \varphi(a)\varphi(b)$ для любых $a, b \in A$ и $\varphi(1) = 1'$, где 1 (соответственно $1'$) — это единичный элемент алгебры A (соответственно A'). Легко проверить, что ядро гомоморфизма $\operatorname{Ker}\varphi$ является идеалом алгебры A.

Подмножество $S \subseteq A$ называется системой *порождающих* (или *образующих*) алгебры A, если каждый элемент алгебры A выражается как многочлен от конечного числа элементов множества S. Последнее условие равносильно тому что A совпадает с наименьшей подалгеброй $\mathbb{K}[S]$ в A, содержащей S. Алгебра A называется *конечно порожденной*, если систему порождающих можно выбрать конечной.

Упражнение 5. Докажите, что факторалгебра конечно порожденной алгебры конечно порождена.

Алгебра многочленов $\mathbb{K}[x_1, \ldots, x_n]$ обладает следующим универсальным свойством: для каждой алгебры A и каждого набора ее элементов $a_1, \ldots, a_n$ существует единственный гомоморфизм $\varphi: \mathbb{K}[x_1, \ldots, x_n] \to A$, для которого $\varphi(x_i) = a_i$. Образом многочлена $f(x_1, \ldots, x_n)$ при этом гомоморфизме является элемент $f(a_1, \ldots, a_n)$. В частности, алгебра A может быть порождена n элементами тогда и только тогда, когда имеется сюръективный гомоморфизм $\varphi: \mathbb{K}[x_1, \ldots, x_n] \to A$. Согласно теореме Гильберта о базисе (см. [3, гл. 9, § 4, теорема 2]), каждый идеал в алгебре $\mathbb{K}[x_1, \ldots, x_n]$ может быть порожден конечным множеством. Следовательно, каждая n-порожденная алгебра A может быть представлена в виде

$$\mathbb{K}[x_1, \ldots, x_n]/(f_1, \ldots, f_m),$$

где $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$.

Если алгебра градуирована, то образующие можно считать однородными. В самом деле, произвольную систему образующих можно заменить на набор их однородных компонент.

Определение 4. Конечно порожденная градуированная алгебра $A = \bigoplus_{s \geqslant 0} A_s$ называется *стандартной*, если $A_0 = \mathbb{K}$ и алгебра A порождается компонентой A_1.

Упражнение 6. 1. Докажите, что если $A = \bigoplus_{s \geqslant 0} A_s$ — конечно порожденная градуированная алгебра и $A_0 = \mathbb{K}$, то $\dim A_s < \infty$ для любого s.

2. Приведите пример градуированной алгебры A, которая не конечно порождена и для которой $\dim A_s < \infty$ для любого s.

3. Докажите, что если $A_0 = \mathbb{K}$, то условие $\dim A_s < \infty$ для любого s равносильно тому, что в алгебре A можно выбрать систему порождающих, содержащую конечное число элементов каждой степени.

Выбор системы порождающих неоднозначен. Однако градуировка накладывает некоторые ограничения на такой выбор.

Упражнение 7. Проверьте, что элементы $-x_3$, $-x_1 + x_3^3 + 2x_2x_3$, $x_2 - 2x_3^3$ порождают алгебру $\mathbb{K}[x_1, x_2, x_3]$.

Задача 4. а) Пусть $A = \bigoplus_{s \geqslant 0} A_s$ — конечно порожденная градуированная алгебра и $A_0 = \mathbb{K}$. Назовем однородную систему образующих *минимальной*, если никакое собственное подмножество этой системы не является системой образующих. Докажите, что число элементов в минимальной системе не зависит от выбора минимальной системы.

б) Покажите, что без ограничения $A_0 = \mathbb{K}$ утверждение предыдущего пункта неверно.

Задача 5. Докажите, что каждая подалгебра в алгебре $\mathbb{K}[x]$ конечно порождена.

Приведем два примера не конечно порожденных подалгебр в алгебре $\mathbb{K}[x, y]$. В обоих примерах подалгебра A порождается одночленами, поэтому является однородной для любой весовой градуировки алгебры $\mathbb{K}[x, y]$.

$A = \mathbb{K}[x, xy, xy^2, xy^3, \ldots]$

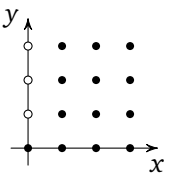

Рис. 1

$A = \mathbb{K}[x^i y^j : i \geqslant \sqrt{2}j]$

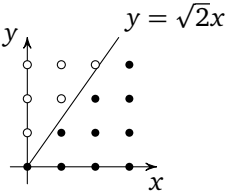

Рис. 2

Задача 6. Докажите, что эти две подалгебры не являются конечно порожденными.

Подалгебра алгебры многочленов называется *мономиальной*, если она может быть порождена одночленами.

Упражнение 8. Докажите, что мономиальная подалгебра является линейной оболочкой некоторого множества одночленов.

Упражнение 9. Докажите, что подалгебра алгебры многочленов мономиальна тогда и только тогда, когда она однородна относительно любой весовой градуировки.

Было бы интересно найти геометрическое описание не конечно порожденных мономиальных подалгебр в $\mathbb{K}[x, y]$.

Мы завершим этот параграф несколькими полезными определениями и задачами.

Задача 7. Пусть $A = \bigoplus_{s\geqslant 0} A_s$ — конечно порожденная градуированная алгебра и $A_0 = \mathbb{K}$. Определим *m-разрежение* алгебры A как однородную подалгебру

$$A^{(m)} = \bigoplus_{k\geqslant 0} A_{km}.$$

Введем на алгебре $A^{(m)}$ новую градуировку, считая, что $A^{(m)}_k = A_{km}$. Докажите, что число m можно подобрать так, что $A^{(m)}$ будет стандартной алгеброй.

Пример 2. Пусть $A = \mathbb{K}[x, y]$, $\deg x = 2$, $\deg y = 3$. Тогда $A^{(2)}_1 = \langle x\rangle$, но $y^2 \in A^{(2)}$. Поэтому алгебра $A^{(2)}$ не стандартна. С другой стороны, $A^{(6)}_1 = \langle x^3, y^2\rangle$, и если $x^i y^j \in A^{(6)}$, то либо $i \geqslant 3$, либо $j \geqslant 2$. Отсюда с помощью индукции заключаем, что $x^i y^j = (x^3)^{i_1}(y^2)^{j_1}$, и, значит, алгебра $A^{(6)}$ стандартна.

Определение 5. Элементы $a_1, \ldots, a_n$ алгебры A называются *алгебраически независимыми*, если $F(a_1, \ldots, a_n) \neq 0$ для любого ненулевого многочлена F от n переменных. Алгебра A называется *свободной*, если она порождается алгебраически независимыми элементами.

Свободные алгебры — это в точности алгебры, изоморфные алгебрам многочленов.

Задача 8. Пусть $A = \bigoplus_{s\geqslant 0} A_s$ — свободная градуированная алгебра, для которой $A_0 = \mathbb{K}$. Докажите, что алгебраически независимые образующие можно выбрать однородными.

Пусть A — произвольная алгебра без делителей нуля. Нам понадобится конструкция *поля частных* QA. Рассмотрим множество пар элементов из A, второй элемент которых отличен от нуля. Нам будет

удобно записывать пары как дроби $\frac{a}{b}$. Элементами множества QA будут классы эквивалентности пар, где $\frac{a}{b} \sim \frac{c}{d}$ тогда и только тогда, когда $ad = bc$. По аналогии с рациональными числами на классах вводятся операции сложения, вычитания, умножения и деления на ненулевой класс, и множество QA становится полем. Алгебру A можно рассматривать как подалгебру в QA, отобразив элемент a в $\frac{a}{1}$.

Определение 6. Алгебра A без делителей нуля называется *целозамкнутой*, если для любых $a_1, \ldots, a_n \in A$, $p \in QA$ из соотношения $p^n + a_1 p^{n-1} + \ldots + a_n = 0$ следует, что $p \in A$.

Задача 9. Докажите, что алгебра многочленов $\mathbb{K}[x_1, \ldots, x_n]$ целозамкнута.

Пример 3. Пусть A — подалгебра в $\mathbb{K}[x]$, порожденная элементами $a = x^2$ и $b = x^3$. Тогда $x = \frac{b}{a} \in QA \setminus A$ и $x^2 = a$. Значит, алгебра A не является целозамкнутой.

Наша ближайшая цель — найти критерий целозамкнутости мономиальной подалгебры $A \subseteq \mathbb{K}[x_1, \ldots, x_n]$. С каждым одночленом $m = x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$ свяжем точку $p(m) = (i_1, \ldots, i_n)$ с целыми неотрицательными координатами. Определим $P(A) = \{p(m) : m \in A\}$. Тогда $P(A)$ — подмножество в решетке $\mathbb{Z}^n$, которое содержит нуль и вместе с любыми двумя элементами содержит их сумму. Такие подмножества называют *моноидами*. Пусть $H(A)$ — множество элементов из $P(A)$, которые нельзя представить в виде суммы двух ненулевых элементов из $P(A)$. Множество $H(A)$ называется *базисом Гильберта* моноида $P(A)$. Пусть $G(A) = \{m : p(m) \in H(A)\}$.

Упражнение 10. Докажите, что $G(A)$ порождает A и каждая система порождающих алгебры A, состоящая из одночленов, содержит $G(A)$. В частности, подалгебра A конечно порождена тогда и только тогда, когда базис Гильберта конечен.

С каждым подмножеством H решетки $\mathbb{Z}^n$ свяжем порожденные им подрешетку

$$L(H) = \{z_1 h_1 + \ldots + z_k h_k : k \in \mathbb{N},\ z_i \in \mathbb{Z},\ h_i \in H\},$$

моноид

$$M(H) = \{n_1 h_1 + \ldots + n_k h_k : k \in \mathbb{N},\ n_i \in \mathbb{Z}_{\geqslant 0},\ h_i \in H\}$$

и конус

$$K(H) = \{q_1 h_1 + \ldots + q_k h_k : k \in \mathbb{N},\ q_i \in \mathbb{Q}_{\geqslant 0},\ h_i \in H\}.$$

Ясно, что $M(H) \subseteq L(H) \cap K(H)$.

Определение 7. Подмножество $H \subseteq \mathbb{Z}^n$ называется *насыщенным*, если $M(H) = L(H) \cap K(H)$.

Пример 4. Рассмотрим подмножество

$$H = \{(1,3),\ (2,2),\ (3,1),\ (2,4), (4,2)\} \subset \mathbb{Z}^2.$$

Для него $L(H)$ — это решетка целых точек с четной суммой координат, а конус $K(H)$ изображен на рис. 3.

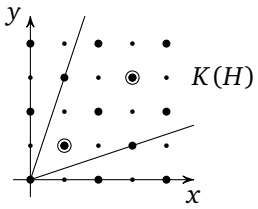

Рис. 3

Точка $(1,1)$ лежит в $L(H) \cap K(H)$, но в $M(H)$ не попадает, поэтому подмножество H не насыщенно.

Упражнение 11. Проверьте, что подмножество $H \subseteq \mathbb{Z}^n$ насыщенно тогда и только тогда, когда из условия $ka \in M(H)$ для некоторых $k \in \mathbb{N}$ и $a \in L(H)$ следует, что $a \in M(H)$.

Упражнение 12. Докажите, что для мономиальной подалгебры A следующие условия эквивалентны:

1) базис Гильберта $H(A)$ является насыщенным подмножеством;

2) существует такое насыщенное подмножество H, что $H(A) \subseteq H \subseteq P(A)$;

3) любое такое подмножество H, что $H(A) \subseteq H \subseteq P(A)$, насыщенно.

Задача 10. Докажите, что мономиальная подалгебра A целозамкнута тогда и только тогда, когда $P(A)$ является насыщенным подмножеством в $\mathbb{Z}^n$.

Задача 11. Перенесите предыдущие результаты на мономиальные подалгебры в алгебре многочленов Лорана $\mathbb{K}[x_1, x_1^{-1}, \ldots, x_n, x_n^{-1}]$.

Задача 12. Пусть $A \subseteq \mathbb{K}[x,y]$ — целозамкнутая однородная относительно стандартной градуировки подалгебра, содержащая элемент x. Предположим, что поле частных QA совпадает с полем рациональных дробей $\mathbb{K}(x,y)$. Докажите, что подалгебра A мономиальна.

§ 2. Ряды Пуанкаре и многочлены Гильберта

Пусть $A = \bigoplus_{s \geqslant 0} A_s$ и все компоненты A_s конечномерны. Определим *ряд Пуанкаре* градуированной алгебры A как формальный ряд от переменной t:

$$P(A, t) = \sum_{s \geqslant 0} \dim A_s \, t^s.$$

Пример 5. Пусть $A = \mathbb{K}[x]$ и $\deg x = d > 0$. Тогда

$$P(A, t) = 1 + t^d + t^{2d} + t^{3d} + \ldots = \frac{1}{1 - t^d}.$$

Пусть $A = \mathbb{K}[x_1, \ldots, x_n]$ — алгебра многочленов с весовой градуировкой $\deg x_i = d_i > 0$. Тогда размерность $\dim A_s$ равна числу способов разбить s в сумму слагаемых $d_1, \ldots, d_n$ (с повторениями). Отсюда следует, что

$$P(A, t) = (1 + t^{d_1} + t^{2d_1} + \ldots)(1 + t^{d_2} + t^{2d_2} + \ldots)\ldots(1 + t^{d_n} + t^{2d_n} + \ldots) = \\ = \frac{1}{(1 - t^{d_1})(1 - t^{d_2})\ldots(1 - t^{d_n})}.$$

Пусть $A = \mathbb{K}[x_1, x_2]/(x_1 x_2)$, $\deg x_1 = \deg x_2 = 1$. Тогда при $s \geqslant 1$ компонента A_s есть линейная оболочка элементов x_1^s и x_2^s. Поэтому $\dim A_0 = 1$ и $\dim A_s = 2$ при $s \geqslant 1$. Значит,

$$P(A, t) = (1 + t + t^2 + t^3 + \ldots) + (t + t^2 + t^3 + \ldots) = \frac{1}{1 - t} + \frac{t}{1 - t} = \frac{1 + t}{1 - t}.$$

Задача 13. Приведите пример конечно порожденной градуированной алгебры A, для которой $P(A, t) = \frac{2}{1 - t}$.

Задача 14. Пусть для конечно порожденной градуированной алгебры A без делителей нуля ряд Пуанкаре имеет вид

$$\frac{1}{(1 - t^{d_1})(1 - t^{d_2})\ldots(1 - t^{d_n})}.$$

Верно ли, что A изоморфна алгебре многочленов $\mathbb{K}[x_1, \ldots, x_n]$ с весовой градуировкой $\deg x_i = d_i$?

Задача 15. Пусть градуированная алгебра A порождена однородными элементами $a_1, a_2, \ldots, a_n$ степеней $d_1, d_2, \ldots, d_n$ соответственно. Докажите, что $a_1, a_2, \ldots, a_n$ алгебраически независимы тогда и только тогда, когда

$$P(A, t) = \frac{1}{(1 - t^{d_1})(1 - t^{d_2})\ldots(1 - t^{d_n})}.$$

В рассмотренных примерах нам удавалось записать ряд Пуанкаре в виде рациональной функции от переменной t. Оказывается, для конечно порожденной алгебры A такая запись всегда возможна. Соответствующую теорему естественно формулировать и доказывать в более широком контексте градуированных модулей.

Напомним, что *модуль* над $\mathbb{K}$-алгеброй A — это $\mathbb{K}$-векторное пространство M с заданным билинейным отображением $A \times M \to M$, $(a, m) \to am$, удовлетворяющим набору аксиом, аналогичным аксиомам векторного пространства над полем; см. [3, гл. 9, § 3]. Модуль M называется *конечно порожденным*, если найдутся такие элементы $m_1, \ldots, m_n \in M$, что любой элемент $m \in M$ можно представить в виде $m = a_1 m_1 + \ldots + a_n m_m$ для некоторых $a_1, \ldots, a_n \in A$. *Подмодуль* A-модуля M — это такое подпространство $L \subseteq M$, что $al \in L$ для любых $a \in A$ и $l \in L$. Например, каждая алгебра A является A-модулем относительно естественного умножения. Это модуль порождается одним элементом — единицей. Подмодули такого модуля — это идеалы алгебры A. Заметим также, что 1-порожденные A-модули — это в точности факторалгебры алгебры A.

Хорошо известное обобщение теоремы Гильберта о базисе утверждает, что если алгебра A конечно порождена, то каждый подмодуль конечно порожденного A-модуля конечно порожден; см. [3, гл. 9, § 4].

Предположим, что алгебра A градуирована. Тогда *градуированный* A-модуль — это A-модуль M с таким разложением в прямую сумму подпространств $M = \bigoplus_{k \geqslant 0} M_k$, что $am \in M_{s+k}$ для любых $a \in A_s$ и $m \in M_k$. Если все подпространства M_k конечномерны, можно определить ряд Пуанкаре градуированного модуля

$$P(M, t) = \sum_{k \geqslant 0} \dim M_k \, t^k.$$

Теорема 1 (Д. Гильберт, Ж.-П. Серр)**.** *Пусть A — градуированная алгебра, порожденная элементами $a_1, \ldots, a_n$ положительных степеней $d_1, \ldots, d_n$, и M — конечно порожденный A-модуль. Тогда найдется такой многочлен $f(t) \in \mathbb{Z}[t]$, что*

$$P(M, t) = \frac{f(t)}{(1 - t^{d_1})(1 - t^{d_2}) \ldots (1 - t^{d_n})}.$$

Доказательство. Будем вести индукцию по n. Если $n = 0$, то $A = \mathbb{K}$, M — конечномерное векторное $\mathbb{K}$-пространство и $P(M, t)$ является многочленом с целыми неотрицательными коэффициентами. Пусть $n > 0$. Рассмотрим алгебру $B = A/(a_1)$, которая порождена образами элементов $a_2, \ldots, a_n$, и фактормодуль $N = M/a_1 M$. Определим однородный подмодуль S модуля M как $S = \{m \in M \colon a_1 m = 0\}$. Тогда S

является также B-модулем и его конечный набор образующих как A-модуля является и набором образующих над B. Рассмотрим точную последовательность линейных отображений векторных пространств:

$$0 \to S_k \to M_k \to M_{k+d_1} \to N_{k+d_1} \to 0,$$

где вторая стрелка — это естественное вложение, третья — умножение на a_1 и четвертая — естественная проекция на фактормодуль. Отсюда для любого $k \geqslant 0$ получаем

$$\dim S_k - \dim M_k + \dim M_{k+d_1} - \dim N_{k+d_1} = 0.$$

Заметим, что при $r < d_1$ выполняется равенство $M_r = N_r$, поэтому

$$t^{d_1}P(S,t) - t^{d_1}P(M,t) + P(M,t) - P(N,t) = 0.$$

Значит,

$$P(M,t) = \frac{P(N,t) - t^{d_1}P(S,t)}{1-t^{d_1}}.$$

Поскольку к B-модулям N и S применимо предположение индукции, мы получаем требуемый вид для $P(M,t)$. □

Задача 16. Существует ли градуированная алгебра $A = \bigoplus_{s\geqslant 0} A_s$ без делителей нуля, для которой все компоненты A_s конечномерны, но ряд Пуанкаре не представим в виде рациональной функции от переменной t?

Задача 17. Верно ли, что если ряд Пуанкаре градуированной алгебры без делителей нуля представим в виде рациональной функции, то эта алгебра конечно порождена?

Предположим, что алгебра A стандартна. Ряд Пуанкаре такой алгебры можно задать более явно.

Упражнение 13. Докажите, что число одночленов степени s в стандартной алгебре многочленов $\mathbb{K}[x_1, \ldots, x_n]$ равно $\dfrac{(s+n-1)!}{s!(n-1)!}$.

Тем самым, ряд Пуанкаре стандартной алгебры многочленов имеет вид $\displaystyle\sum_{s\geqslant 0} \frac{(s+n-1)!}{s!(n-1)!}t^s$.

Определение 8. Многочлен $F(x)$ с рациональными коэффициентами называется *целозначным*, если для некоторого натурального m значение $F(s)$ цело для любого натурального $s \geqslant m$.

Задача 18. Докажите, что для целозначного многочлена $F(x)$ значение $F(s)$ является целым для любого целого s.

Задача 19. Докажите, что для целозначного многочлена $F(x)$ степени d найдутся целые $c_0, c_1, \ldots, c_d$ такие, что

$$F(x) = c_d C_x^d + \ldots + c_1 C_x^1 + c_0, \quad \text{где } C_x^s = \frac{1}{s!}x(x-1)\ldots(x-s+1).$$

Обратно, каждый многочлен такого вида целозначен.

Теорема 2. *Для стандартной алгебры A найдутся такое натуральное m и такой целозначный многочлен $H(x)$, что $\dim A_s = H(s)$ для любого $s \geqslant m$.*

Доказательство. Из теоремы 1 следует, что $P(A,t) = \frac{f(t)}{(1-t)^n}$ для некоторого $f(t) \in \mathbb{Z}[t]$. Тогда

$$P(A,t) = f(t)\left(\sum_{s\geqslant 0} \frac{(s+n-1)!}{s!(n-1)!}t^s\right).$$

Пусть $f(t) = b_0 + b_1 t + \ldots + b_m t^m$. Тогда для любого $s \geqslant m$ получаем

$$\dim A_s = \sum_{i=0}^{m} b_i \frac{(s-i+n-1)!}{(s-i)!(n-1)!}.$$

Остается положить

$$H(x) = \sum_{i=0}^{m} \frac{b_i}{(n-1)!}(x-i+n-1)(x-i+n-2)\ldots(x-i+1).$$

Этот многочлен целозначен, поскольку при $s \geqslant m$ значение $H(s) = \dim A_s$ — целое число. □

Определение 9. Многочлен $H(x)$ называется *многочленом Гильберта* стандартной алгебры A.

Задача 20. Пусть $P(A,t) = \frac{f(t)}{(1-t)^n}$ и $f(t) = (1-t)^r g(t)$, где $g(1) \neq 0$. Докажите, что старший член многочлена Гильберта равен

$$\frac{g(1)}{(n-r-1)!}x^{n-r-1}.$$

Задача 21. Найдите многочлен Гильберта алгебры

$$\mathbb{K}[x_1, x_2, x_3, x_4]/(h),$$

где $h \in \mathbb{K}[x_1, x_2, x_3, x_4]$ — однородный многочлен степени d.

§ 3. Последовательности размерностей компонент

Пусть $A = \bigoplus_{s \geqslant 0} A_s$ — градуированная алгебра, для которой $A_0 = \mathbb{K}$ и $\dim A_s < \infty$ для любого s.

Рассмотрим последовательность размерностей компонент

$$p_0 = \dim A_0 = 1,\ p_1 = \dim A_1,\ p_2 = \dim A_2,\ p_3 = \dim A_3,\ \ldots$$

Какие числовые последовательности могут так возникать? Если не накладывать на алгебру дополнительных ограничений, этот вопрос малоинтересен.

Задача 22. Докажите, что для любой последовательности $1, p_1, p_2, p_3, \ldots$ целых неотрицательных чисел найдется такая градуированная алгебра A, что $\dim A_s = p_s$ для каждого s.

Если ограничиться конечно порожденными алгебрами, вопрос становится более содержательным, но, как показывает следующая задача, на конструктивное решение рассчитывать все равно не приходится.

Задача 23. а) Докажите, что любая конечная последовательность $1, p_1, p_2, \ldots, p_m$ целых неотрицательных чисел может выступать в качестве начального отрезка последовательности размерностей компонент конечно порожденной градуированной алгебры.

б) Приведите пример последовательности $1, p_1, p_2, p_3, \ldots$ целых неотрицательных чисел, которая не совпадает с последовательностью размерностей компонент ни для какой конечно порожденной градуированной алгебры.

Ниже мы будем изучать числовые последовательности, которые реализуются в качестве последовательностей размерностей компонент стандартных алгебр.

Упражнение 14. Докажите, что минимальное число образующих стандартной алгебры равно $p_1 = \dim A_1$.

Отсюда для стандартной алгебры A вытекает неравенство

$$p_s \leqslant \frac{(s+n-1)!}{s!(n-1)!},$$

где $n = p_1$. Однако это необходимое условие на последовательность размерностей компонент не является достаточным.

Задача 24. Докажите, что последовательность $\{1, 2, 2, 4, 0, 0, 0, \ldots\}$ не является последовательностью размерностей компонент стандартной алгебры.

Перейдем к изложению результатов Ф. С. Маколея; см. [13] (1927). Будем рассматривать стандартную алгебру A как факторалгебру алгебры многочленов $\mathbb{K}[x_1, \ldots, x_n]$, где $n = p_1$. При изучении последовательности размерностей компонент естественно начать с нахождения удобного базиса алгебры A как векторного пространства.

Обозначим через $\mathscr{M}$ множество одночленов от переменных $x_1, \ldots, x_n$ с коэффициентом 1.

Определение 10. Назовем подмножество $\mathscr{N} \subseteq \mathscr{M}$ *нормальным*, если $\mathscr{N} \neq \varnothing$ и из условий $m_1 \in \mathscr{N}$, m_2 делит m_1 следует, что $m_2 \in \mathscr{N}$.

Упражнение 15. Докажите, что подмножество $\mathscr{N} \subset \mathscr{M}$ нормально тогда и только тогда, когда линейная оболочка одночленов из $\mathscr{M} \setminus \mathscr{N}$ является идеалом в $\mathbb{K}[x_1, \ldots, x_n]$.

Предложение 1. *Пусть $A = \mathbb{K}[x_1, \ldots, x_n]/I$ — стандартная алгебра. Тогда найдется нормальное множество одночленов $\mathscr{N}$, образ которого в A является базисом A как векторного пространства.*

Доказательство. Введем на множестве $\mathscr{M}$ лексикографический порядок. Напомним, что в этом порядке $x_1^{i_1} \ldots x_n^{i_n} \prec x_1^{j_1} \ldots x_n^{j_n}$, если найдется такое k, что $i_1 = j_1, \ldots, i_{k-1} = j_{k-1}, i_k < j_k$. Лексикографический порядок позволяет линейно упорядочить члены произвольного многочлена f, в частности однозначно определить старший член $\tilde{f}$ многочлена f. Рассмотрим векторное пространство $\tilde{I}$, порожденное одночленами $\{\tilde{f} : f \in I\}$, и множество $\mathscr{N} = \mathscr{M} \setminus \tilde{I}$.

Упражнение 16. Проверьте, что $\tilde{I}$ — идеал в алгебре $\mathbb{K}[x_1, \ldots, x_n]$ и множество $\mathscr{N}$ нормально.

Покажем, что множество $\mathscr{N}$ является искомым.

1. *Элементы из $\mathscr{N}$ линейно независимы в A.* В самом деле, линейная комбинация таких элементов равна нулю в A тогда и только тогда, когда эта комбинация лежит в I. Тогда ее старший член лежит в $\tilde{I}$.

2. *Любой элемент из A есть линейная комбинация элементов из $\mathscr{N}$.* Для данного $a \in A$ рассмотрим его прообраз f в $\mathbb{K}[x_1, \ldots, x_n]$. Выберем среди членов многочлена f старший одночлен m, который лежит в $\tilde{I}$. Найдется $F \in I$, для которого $\tilde{F} = m$. Заменим в f член m на $m - F$. При этом новый элемент будет соответствовать тому же элементу a в факторалгебре и старший член многочлена f, лежащий в $\tilde{I}$, уменьшится. Остается заметить, что в лексикографическом порядке нет бесконечных строго убывающих цепочек одночленов. □

Разложение элемента $a \in A$ по базису $\mathcal{N}$ принято называть *нормальной формой* элемента a.

Предложение 2. *Последовательность целых неотрицательных чисел* $1, p_1, p_2, p_3, \ldots$ *является последовательностью размерностей компонент некоторой стандартной алгебры A тогда и только тогда, когда найдется такое нормальное подмножество* $\mathcal{N} \subseteq \mathcal{M}$, *что* p_s — *число элементов этого подмножества степени s.*

Доказательство. Импликация $\Rightarrow$ доказана в предложении 1. Для доказательства обратной импликации рассмотрим линейную оболочку I элементов из $\mathcal{M} \setminus \mathcal{N}$. Тогда I является идеалом и последовательность размерностей компонент факторалгебры $\mathbb{K}[x_1, \ldots, x_n]/I$ является искомой. □

Будем обозначать через $\mathcal{M}_k^s$ первые (наименьшие) k одночленов степени s от $x_1, \ldots, x_n$ в лексикографическом порядке.

Определение 11. Последовательность $1, p_1, p_2, p_3, \ldots$ называется *O-последовательностью*, если множество одночленов

$$\bigcup_{s=0}^{\infty} \mathcal{M}_{p_s}^s$$

от $n = p_1$ переменных нормально.

Пример 6. Последовательность $1, 3, 2, 2$ является O-последовательностью, а последовательность $1, 3, 2, 3$ — нет:

$$1$$
$$x_3 \quad x_2 \quad x_1$$
$$x_3^2 \quad x_2x_3 \quad x_2^2 \quad x_1x_3 \quad x_1x_2 \quad x_1^2$$
$$x_3^3 \quad x_2x_3^2 \quad x_2^2x_3 \quad x_2^3 \quad x_1x_3^2 \quad x_1x_2x_3 \quad x_1x_2^2 \quad x_1^2x_3 \quad x_1^2x_2 \quad x_1^3.$$

В самом деле, во втором случае одночлен $x_2^2x_3$ делится на одночлен x_2^2, который в подмножество не попадает.

Задача 25. Если в определении O-последовательности отсчитывать не наименьшие, а наибольшие одночлены, будет ли такое определение эквивалентно исходному?

Из предложения 2 следует, что любая O-последовательность реализуется как последовательность размерностей компонент стандартной алгебры.

§ 4. Теорема Маколея

Напомним, что *биномиальный коэффициент* C_m^s определяется для целых чисел m и s как $\frac{m!}{s!(m-s)!}$ при $m \geqslant s \geqslant 0$ и как 0, если $m < s$ или если хотя бы одно из чисел отрицательно. При этом мы полагаем $0! = 1$.

Предложение 3. *Пусть m и d — фиксированные натуральные числа. Тогда найдется ровно одна такая последовательность целых неотрицательных чисел*

$$k(d) > k(d-1) > \ldots > k(1) \geqslant 0,$$

что

$$m = C_{k(d)}^d + C_{k(d-1)}^{d-1} + \ldots + C_{k(1)}^1.$$

Определение 12. Данное выражение называется *d-разложением Маколея* числа m, а числа $k(d), k(d-1), \ldots, k(1)$ — *d-коэффициентами Маколея* числа m.

Пример 7. Пусть $m = 5$ и $d = 7$. Тогда

$$5 = C_7^7 + C_6^6 + C_5^5 + C_4^4 + C_3^3 + C_1^2 + C_0^1.$$

Пусть теперь $m = 8$ и $d = 2$. Здесь $8 = C_4^2 + C_2^1$.

Доказательство предложения 3. Воспользуемся индукцией по d. При $d = 1$ имеем $k(1) = m$. Пусть теперь $d > 1$.

Лемма 1. *Если $k(d) > k(d-1) > \ldots > k(1) \geqslant 0$, то*

$$C_{k(d)}^d + \ldots + C_{k(1)}^1 < C_{k(d)+1}^d.$$

Доказательство. Вновь используем индукцию по d. При $d = 1$ имеем $C_{k(1)}^1 < C_{k(1)+1}^1$ — верно. Теперь утверждение леммы следует из равенства $C_{k(d)+1}^d - C_{k(d)}^d = C_{k(d)}^{d-1}$ и неравенств

$$C_{k(d-1)}^{d-1} + C_{k(d-2)}^{d-2} + \ldots + C_{k(1)}^1 < C_{k(d-1)+1}^{d-1} \leqslant C_{k(d)}^{d-1},$$

первое из которых верно по предположению индукции. □

Итак, из существования разложения следует, что $C_{k(d)}^d \leqslant m < C_{k(d)+1}^d$. Заметим, что для данных m и d найдется ровно одно число $k(d)$, для которого $C_{k(d)}^d \leqslant m < C_{k(d)+1}^d$. По предположению индукции

$$m - C_{k(d)}^d = C_{k(d-1)}^{d-1} + \ldots + C_{k(1)}^1,$$

и последовательность $k(d-1) > \ldots > k(1) \geqslant 0$ определена однозначно. Остается показать, что $k(d) > k(d-1)$, или что $m - C^d_{k(d)} < C^{d-1}_{k(d)}$. Последнее неравенство равносильно неравенству $m < C^d_{k(d)+1}$, которое верно в силу выбора числа $k(d)$. □

Как показывает доказательство, коэффициенты $k(i)$ удобно находить последовательно: $k(i)$ — это наибольшее число, для которого

$$C^i_{k(i)} \leqslant m - C^d_{k(d)} - \ldots - C^{i+1}_{k(i+1)}.$$

Лемма 2. *Если $k(d), \ldots, k(1)$ — d-коэффициенты Маколея числа n, а $k'(d), \ldots, k'(1)$ — d-коэффициенты Маколея числа n', то $n > n'$ тогда и только тогда, когда лексикографически $(k(d), \ldots, k(1)) > (k'(d), \ldots, k'(1))$.*

Доказательство. Если $k(d) = k'(d)$, то вычтем из n и n' число $C^d_{k(d)}$ и воспользуемся индукцией по d. Если $k(d) > k'(d)$, то достаточно доказать, что

$$C^d_{k(d)} > C^d_{k'(d)} + C^{d-1}_{k'(d-1)} + \ldots + C^1_{k'(1)}.$$

Это следует из того, что $C^d_{k(d)} \geqslant C^d_{k'(d)+1}$, и из леммы 1. □

Объясним, как разложение Маколея связано с лексикографическим порядком на множестве одночленов. Ниже мы рассматриваем одночлены с коэффициентом единица. Пусть u — одночлен степени d от переменных $x_1, \ldots, x_n$. Обозначим через $\mathscr{L}(u)$ множество одночленов степени d, меньших u. Нам удобно будет записать u в виде $x_{j(1)}x_{j(2)}\ldots x_{j(d)}$, где $1 \leqslant j(1) \leqslant j(2) \leqslant \ldots \leqslant j(d) \leqslant n$. Обозначим через $[x_k, \ldots, x_n]_s$ множество одночленов от $x_k, \ldots, x_n$ степени s при $k \leqslant n$. При $k > n$ полагаем $[x_k, \ldots, x_n]_s$ пустым множеством.

Если одночлен v имеет степень d и $v < u$, то некоторые начальные отрезки одночленов u и v совпадают, а затем в v следует переменная с бóльшим номером. Отсюда получаем разложение

$$\mathscr{L}(u) = [x_{j(1)+1}, \ldots, x_n]_d \sqcup x_{j(1)}[x_{j(2)+1}, \ldots, x_n]_{d-1} \sqcup \ldots$$
$$\ldots \sqcup (x_{j(1)}\ldots x_{j(d-1)})[x_{j(d)+1}, \ldots, x_n]_1,$$

которое определяет d-разложение Маколея числа $|\mathscr{L}(u)|$:

$$|\mathscr{L}(u)| = C^d_{n-j(1)+d-1} + C^{d-1}_{n-j(2)+d-2} + \ldots + C^1_{n-j(d)}.$$

Определение 13. Пусть

$$m = C^d_{k(d)} + C^{d-1}_{k(d-1)} + \ldots + C^1_{k(1)}.$$

Тогда определим число

$$m^{\langle d \rangle} = C^{d+1}_{k(d)+1} + C^d_{k(d-1)+1} + \ldots + C^2_{k(1)+1}.$$

Лемма 3. *Для произвольного одночлена и степени d выполняется равенство*

$$|\mathscr{L}(ux_n)| = |\mathscr{L}(u)|^{\langle d\rangle}.$$

Доказательство. Поскольку $ux_n = x_{j(1)}x_{j(2)}\ldots x_{j(d)}x_n$, получаем

$$|\mathscr{L}(ux_n)| = C^{d+1}_{n-j(1)+d} + C^{d}_{n-j(2)+d-1} + \ldots + C^{2}_{n-j(d)+1} + C^{1}_{n-n+1-1},$$

и последнее слагаемое равно нулю. □

Теперь мы готовы сформулировать основной результат.

Теорема 3 (Ф. С. Маколей, П. Макмюллен, Р. Стенли)**.** *Пусть $P = \{1, p_1, p_2, p_3, \ldots\}$ — последовательность целых неотрицательных чисел. Тогда следующие условия эквивалентны*:

(1) *P — это последовательность размерностей компонент некоторой стандартной алгебры*;

(2) *P является O-последовательностью*;

(3) *$p_{d+1} \leqslant p_d^{\langle d\rangle}$ для любого $d \geqslant 1$.*

Импликация (2) $\Rightarrow$ (1) доказана в предыдущем параграфе.

Доказательство эквивалентности условий (2) и (3). Условие (2) означает, что в множестве $\mathscr{M}$ одночленов от $n = p_1$ переменных подмножество $\mathscr{N} = \bigcup_{s=0}^{\infty} \mathscr{M}^{s}_{p_s}$ нормально. Это равносильно тому, что для любого одночлена, не попавшего в $\mathscr{N}$, все кратные ему одночлены также не попали в $\mathscr{N}$. Для каждой степени d одночлены, не попавшие в $\mathscr{N}$, — это одночлены w, имеющие в лексикографическом порядке (по возрастанию) номера $p_d + 1$ и выше. Значит, условие нормальности множества $\mathscr{N}$ равносильно тому, что номер одночлена wx_i не меньше $p_{d+1} + 1$ для любых d, w и i. Но номер одночлена wx_i не меньше номера одночлена w_0x_n, где w_0 — одночлен степени d с номером $p_d + 1$. Согласно лемме 3, номер многочлена w_0x_n равен $p_d^{\langle d\rangle} + 1$, поэтому условие (2) равносильно условию $p_{d+1} \leqslant p_d^{\langle d\rangle}$ для любого $d \geqslant 1$.

Трудной частью доказательства теоремы 3 является вывод последних условий из первого. В следующих параграфах приводятся независимые друг от друга доказательства импликаций (1) $\Rightarrow$ (2) и (1) $\Rightarrow$ (3) соответственно.

Задача 26. Является ли O-последовательностью последовательность 1, 40, 100, 134, 148, 152, 248, 290, 0, 0, 0, 0, …?

Задача 27. Докажите, что для произвольной O-последовательности $1, p_1, p_2, p_3, \ldots$ найдется такое $m \in \mathbb{N}$, что $p_{s+1} = p_s^{\langle s\rangle}$ для любого $s \geqslant m$.

Задача 28. Докажите, что для произвольной O-последовательности найдутся такое натуральное m и такие целые $a_1 \geqslant a_2 \geqslant \ldots \geqslant a_m \geqslant -1$, что

$$p_s = C_{s+a_1}^{a_1} + C_{s+a_2-1}^{a_2} + \ldots + C_{s+a_m-m+1}^{a_m}$$

для любого $s \geqslant m$.

Задача 29. Пусть для O-последовательности $1, p_1, p_2, p_3, \ldots$ найдется такое $m \in \mathbb{N}$, что $p_m \leqslant m$. Докажите, что $p_{s+1} \leqslant p_s$ для любого $s \geqslant m$.

§ 5. Комбинаторный вариант теоремы Маколея

В этом параграфе мы следуем работе [10]. Обозначим через F множество всех наборов из n целых неотрицательных чисел. Упорядочим F лексикографически. Для каждого $v \in \mathbb{N}$ определим

$$F_v = \{(a_1, \ldots, a_n) \colon a_1 + \ldots + a_n = v\}.$$

Пусть $H \subseteq F$ — подмножество и $H_v = H \cap F_v$. Обозначим через CH_v первые (т. е. наименьшие) $|H_v|$ элементов множества F_v, где $|H_v|$ — число элементов в H_v, и положим $CH = \bigcup_v CH_v$. С каждым $a \in F$ свяжем подмножество

$$\Gamma(a) = \{(a_1 - 1, a_2, \ldots, a_n), (a_1, a_2 - 1, \ldots, a_n), \ldots, (a_1, a_2, \ldots, a_n - 1)\} \cap F.$$

Определим $\Gamma H = \bigcup_{a \in H} \Gamma(a)$.

Теорема 4. *Справедливо включение* $\Gamma(CH_v) \subseteq C(\Gamma H_v)$.

Доказательство. Будем называть подмножество $M \subseteq F_v$ *сжатым*, если $CM = M$.

Лемма 4. *Если множество* $M \subseteq F_v$ *сжато, то и* $\Gamma M \subseteq F_{v-1}$ *сжато.*

Доказательство. Пусть $a = (a_1, \ldots, a_n)$, $b = (b_1, \ldots, b_n)$, $a, b \in F_{v-1}$ и $a < b$. Надо доказать, что из условия $(b_1, \ldots, b_j + 1, \ldots, b_n) \in M$ следует, что $a \in \Gamma M$. Но $(a_1, \ldots, a_j + 1, \ldots, a_n) < (b_1, \ldots, b_j + 1, \ldots, b_n)$, и в силу сжатости множества M имеем $(a_1, \ldots, a_j + 1, \ldots, a_n) \in M$, откуда следует, что $a \in \Gamma M$. □

Теперь для доказательства теоремы 4 достаточно доказать, что $|\Gamma(CH_v)| \leqslant |\Gamma H_v|$. В самом деле, $C(\Gamma H_v)$ — это первые $|\Gamma H_v|$ элементов множества F_{v-1}, а как следует из леммы 4, $\Gamma(CH_v)$ — это первые $|\Gamma(CH_v)|$ элементов множества F_{v-1}.

Лемма 5. *Теорема* 4 *верна при* $n = 2$.

Доказательство. Надо показать, что $|\Gamma(CH_v)| \leqslant |\Gamma H_v|$. При $H_v = F_v$ утверждение очевидно. При $|H_v| = k < v + 1$ имеем $|\Gamma(CH_v)| = k$,

$$(0,5) \quad (1,4) \quad (2,3) \quad (3,2) \quad (4,1) \quad (5,0)$$
$$(0,4) \quad (1,3) \quad (2,2) \quad (3,1) \quad (4,0),$$

а проверка неравенства $|\Gamma H_v| \geqslant k$ предоставляется читателю. □

Далее будем использовать индукцию по n. Определим

$$H_{i:d} = \{(a_1, \ldots, a_n) \colon a_i = d\} \cap H,$$

и через $(VH_\nu)_{i:d}$ обозначим множество первых $|(H_\nu)_{i:d}|$ элементов множества $(F_\nu)_{i:d}$. Будем говорить, что подмножество H_ν является *i-сжатым*, если $(VH_\nu)_{i:d} = (H_\nu)_{i:d}$ для всех значений d.

Упражнение 17. Покажите, что при $n = 2$ каждое подмножество в F_ν является 1- и 2-сжатым. При $n \geqslant 3$ приведите пример подмножества в F_ν, которое i-сжато для всех $i = 1, 2, \ldots, n$, но сжатым не является.

Лемма 6. *Пусть $n \geqslant 3$ и $g = (g_1, \ldots, g_{n-1}, g_n) < h = (h_1, \ldots, h_{n-1}, 0)$, причем $g, h \in F_\nu$. Если подмножество $S \subseteq F_\nu$ i-сжато при $i = 1, 2, n$ и $h \in S$, то $g \in S$.*

Доказательство. Достаточно построить возрастающую цепочку элементов из F_ν, начинающуюся в g и заканчивающуюся в h, в которой у любых двух соседних элементов хотя бы одна из координат с номерами 1, 2 или n совпадает.

1. Пусть $g_1 = h_1$. Подходит цепочка $g < h$.

2. Пусть $h_1 = g_1 + 1$ и хотя бы одно из чисел $g_2, \ldots, g_{n-1}$ отлично от нуля. Положим $\tilde{g} = (g_1 + 1, 0, \ldots, 0, g_2 + \ldots + g_{n-1} - 1, g_n)$. Тогда $g < \tilde{g} \leqslant h$ — искомая цепочка, так как если у многочлена h только h_1 и h_{n-1} отличны от нуля, то $h_{n-1} = (g_1 + \ldots + g_n) - h_1 = g_2 + \ldots + g_n - 1 \geqslant \geqslant g_2 + \ldots + g_{n-1} - 1$, причем равенство достигается только при $g_n = 0$.

3. Пусть $h_1 = g_1 + 1$ и $g_2 = \ldots = g_{n-1} = 0$. Тогда $g < (g_1, g_n, 0, \ldots, 0) < h$.

4. Пусть $h_1 = g_1 + k$, $k \geqslant 2$. Тогда заменим g на $(g_1 + 1, g_2, \ldots, g_i - 1, \ldots, g_n)$, $g_i > 0$ и воспользуемся индукцией по k. □

Определим множества H_ν^j индуктивно: $H_\nu^1 = H_\nu$ и $H_\nu^{j+1} = \bigcup_d (VH_\nu^j)_{i:d}$, где $i \equiv j \pmod n$.

Лемма 7. *Найдется такое $p > 0$, для которого H_ν^p является i-сжатым для всех $i = 1, 2, \ldots, n$.*

Доказательство. Занумеруем элементы множества F_ν в лексикографическом порядке. Переход от H_ν^j к H_ν^{j+1} не изменяет количество элементов, и у каждого изменяемого элемента уменьшается номер. Следовательно, через конечное число шагов процессы i-сжатия прекратятся. □

Лемма 8. *Предположим, что теорема 4 верна для наборов длины $n - 1$ и $\Gamma H_\nu \subseteq H_{\nu-1}$. Тогда $\Gamma H_\nu^j \subseteq H_{\nu-1}^j$ для любого j.*

Доказательство. Воспользуемся индукцией по j. При $j = 1$ включение $\Gamma H_\nu \subseteq H_{\nu-1}$ выполнено по условию. Докажем включение $\Gamma H_\nu^{j+1} \subseteq \subseteq H_{\nu-1}^{j+1}$. По предположению индукции $\Gamma((H_\nu^j)_{i:d}) \cap (F_{\nu-1})_{i:d} \subseteq (H_{\nu-1}^j)_{i:d}$.

Применяя теорему 4 ко всем координатам кроме i-й получим

$$\Gamma((VH_\nu^j)_{i:d}) \cap (F_{\nu-1})_{i:d} \subseteq (VH_{\nu-1}^j)_{i:d}. \tag{1}$$

Из включения $\Gamma H_\nu^j \subseteq H_{\nu-1}^j$ при $d \geqslant 1$ следует, что $|(H_\nu^j)_{i:d}| \leqslant |(H_{\nu-1}^j)_{i:d-1}|$, откуда при $d \geqslant 1$ получаем

$$\Gamma((VH_\nu^j)_{i:d}) \cap (F_{\nu-1})_{i:d-1} \subseteq (VH_{\nu-1}^j)_{i:d-1}. \tag{2}$$

В самом деле, левая часть — это первые $|(H_\nu^j)_{i:d}|$ элементов множества $(F_{\nu-1})_{i:d-1}$, а правая часть — это первые $|(H_{\nu-1}^j)_{i:d-1}|$ элементов того же множества.

Из соотношения (1) следует, что $\Gamma((VH_\nu^j)_{i:0}) \subseteq (VH_{\nu-1}^j)_{i:0}$, а при $d \geqslant 1$ из соотношений (1) и (2) следует, что

$$\Gamma((VH_\nu^j)_{i:d}) \subseteq (VH_{\nu-1}^j)_{i:d} \cup (VH_{\nu-1}^j)_{i:d-1}.$$

Учитывая, что $H_\nu^{j+1} = \bigcup_d (VH_\nu^j)_{i:d}$, получаем $\Gamma H_\nu^{j+1} \subseteq H_{\nu-1}^{j+1}$. □

Завершим доказательство теоремы 4. Пусть множество $S = H_\nu^p$ является i-сжатым для $i = 1, 2, \ldots, n$. Положим $(\Gamma H_\nu)^p = T$. Применяя лемму 8 к $H_{\nu-1} = \Gamma H_\nu$, получим $\Gamma(H_\nu^p) \subseteq (\Gamma H_\nu)^p$, или $\Gamma S \subseteq T$. Будем постепенно изменять S и T так, чтобы в конце получить $S = CH_\nu$ и $T \subseteq C(\Gamma H_\nu)$.

Если $S = F_\nu$, то и $H_\nu = F_\nu$, а значит, $\Gamma(CH_\nu) = F_{\nu-1} = C(\Gamma H_\nu)$. Пусть $g = (g_1, \ldots, g_n)$ — первый элемент из $F_\nu \setminus S$ и $h = (h_1, \ldots, h_n)$ — последний элемент из S. Если $h < g$, то $S = CH_\nu$ и $|\Gamma(CH_\nu)| = |\Gamma S| \leqslant |T| = |\Gamma H_\nu|$. Пусть теперь $h > g$. Если $h_n = 0$, то по лемме 6 мы получаем $g \in S$, что приводит к противоречию. Положим $h^* = (h_1, \ldots, h_{n-1}, h_n - 1)$ и $g^* = (g_1, \ldots, g_{n-1}, g_n - 1)$ при $g_n > 0$. Из включения $\Gamma S \subseteq T$ следует, что $h^* \in T$. Если $x \in S \setminus \{h\}$, то для любого $y \in \Gamma(x)$ имеем $y < x < h$. Отсюда $h^* \notin \Gamma(x)$ для любого $x \in S \setminus \{h\}$. Положим $S' = (S \setminus \{h\}) \cup \{g\}$ и

$$T' = \begin{cases} (T \setminus \{h^*\}) \cup \{g^*\}, & \text{если } g_n > 0; \\ T, & \text{если } g_n = 0. \end{cases}$$

Проверим, что $\Gamma S' \subseteq T'$. Для этого достаточно показать, что $\Gamma(g) \subseteq T'$. Если $g_n > 0$, то g^* лежит в T' по построению. Элемент $(g_1, \ldots, g_i - 1, \ldots, g_n)$ лежит в $\Gamma((g_1, \ldots, g_i - 1, \ldots, g_n + 1))$ и $(g_1, \ldots, g_i - 1, \ldots, g_n + 1) < g$, поэтому $(g_1, \ldots, g_i - 1, \ldots, g_n + 1) \in S$. Отсюда следует, что

$$\Gamma((g_1, \ldots, g_i - 1, \ldots, g_n + 1)) \subseteq T.$$

Надо понять, что $(g_1, \ldots, g_i - 1, \ldots, g_n) \neq h^* = (h_1, \ldots, h_{n-1}, h_n - 1)$. Но в силу 1-сжатости имеем $h_1 > g_1$. Заметим также, что множество S' является i-сжатым для всех i.

После конечного числа переходов от (S, T) к (S', T') мы получим $S = CH_v$, $\Gamma(CH_v) \subseteq T$ и $|\Gamma(CH_v)| \leqslant |T| = |\Gamma H_v|$. □

Доказательство импликации (1) ⇒ (2) в теореме 3. Согласно предложению 2 найдется нормальное подмножество $\mathscr{N} \subseteq \mathscr{M}$, число элементов степени s которого равно p_s. Пусть H — множество наборов степеней элементов подмножества $\mathscr{N}$. Из теоремы 4 следует, что множество одночленов $\mathscr{K}$, наборы степеней которых принадлежат CH, является нормальным. С другой стороны, $\mathscr{K} = \bigcup_{s=0}^{\infty} \mathscr{M}_{p_s}^{s}$.

§ 6. Теорема Грина

В этом параграфе доказан результат из работы [11]. В изложении мы следуем книге [9, § 4.2]. Пусть

$$m = C^d_{k(d)} + C^{d-1}_{k(d-1)} + \ldots + C^1_{k(1)}.$$

Определим число

$$m_{\langle d\rangle} = C^d_{k(d)-1} + C^{d-1}_{k(d-1)-1} + \ldots + C^1_{k(1)-1}.$$

Из леммы 2 вытекает, что $m'_{\langle d\rangle} \leqslant m_{\langle d\rangle}$ при $m' \leqslant m$.

Лемма 9. *Если последнее ненулевое слагаемое в d-разложении Маколея числа m не равно 1, то $(m-1)_{\langle d\rangle} < m_{\langle d\rangle}$.*

Доказательство. Пусть $k'(d), \ldots, k'(1)$ — коэффициенты Маколея числа $m-1$. Согласно лемме 2 имеем $k'(d) \leqslant k(d)$. Если $k'(d) < k(d)$, то первый d-коэффициент Маколея числа $m_{\langle d\rangle}$ равен $k(d)-1$, а первый d-коэффициент числа $(m-1)_{\langle d\rangle}$ равен $k'(d)-1$ и требуемое неравенство следует из леммы 2.

Пусть $k'(d) = k(d)$. Заменим m на $m' = m - C^d_{k(d)}$ и воспользуемся индукцией по d. Нужно лишь проверить, что $m' - 1 > 0$. Это следует из того, что в этой ситуации у числа m более одного слагаемого в d-разложении Маколея отлично от нуля и последнее из ненулевых слагаемых больше 1. □

Определение 14. Пусть поле $\mathbb{K}$ бесконечно и P — некоторое условие, зависящее от точки конечномерного векторного $\mathbb{K}$-пространства V. Будем говорить, что условие P выполнено для *точки общего положения* пространства V, если имеется такой ненулевой многочлен F на пространстве V, что условие P выполнено во всех точках пространства V, где F не обращается в нуль.

Если условия $P_1, \ldots, P_m$ выполнены для точек общего положения пространства V, то для точек общего положения эти условия выполнены одновременно. В самом деле, в качестве многочлена F надо рассмотреть произведение многочленов $F_1, \ldots, F_m$.

Теорема 5 (М. Грин, 1989)**.** *Пусть $\mathbb{K}$ — бесконечное поле, $s \in \mathbb{N}$ и A — стандартная $\mathbb{K}$-алгебра. Для каждого элемента $a \in A_1$ рассмотрим стандартную алгебру $B = A/(a)$. Тогда для элемента $a \in A_1$ общего положения имеет место неравенство* $\dim B_s \leqslant (\dim A_s)_{\langle s\rangle}$.

Доказательство. Пусть $M=\max_{a\in A_1}\dim(aA_{s-1})$. Тогда $\dim(aA_{s-1})=M$ для элемента $a\in A_1$ общего положения. В самом деле, ранг оператора $L_a\colon A_{s-1}\to A_s$ умножения на a равен максимальному порядку отличного от нуля минора матрицы этого оператора.

Воспользуемся индукцией по параметру $\min(s,\dim A_1)$. Если $s=1$, то $\dim B_1=\dim A_1-1\leqslant(\dim A_1)_{\langle 1\rangle}=\dim A_1-1$. Если $\dim A_1=1$, то $\dim B_s=0$ для всех $s\geqslant 1$. Далее предполагаем, что $s>1$ и $\dim A_1>1$.

Зафиксируем такой элемент $a\in A_1$, что $\dim(aA_{s-1})=M$, и рассмотрим элемент $c\in A_1$, который не пропорционален a и для которого $\dim(cA_{s-1})$ и $\dim(cB_{s-1})$ одновременно принимают максимально возможные значения. Ясно, что $\dim B_s=\dim(B_s/cB_{s-1})+\dim cB_{s-1}$. По предположению индукции $\dim(B_s/cB_{s-1})\leqslant(\dim B_s)_{\langle s\rangle}$. Оценим второе слагаемое:

$$\dim(cB_{s-1})=\dim(cA_{s-1}/(cA_{s-2}\cap aA_{s-2}))\leqslant$$
$$\leqslant\dim(cA_{s-1}/acA_{s-2})=\dim(aA_{s-1}/acA_{s-2}).$$

Последнее равенство справедливо, так как $\dim(cA_{s-1})$ и $\dim(aA_{s-1})$ являются максимально возможными.

Можно также считать, что для элемента c значение $\dim(acA_{s-2})$ максимально. Рассмотрим идеал $I=\{x\in A\colon ax=0\}$ алгебры A. Этот идеал однороден, и факторалгебра $P=A/I$ стандартна. Размерность $\dim(aA_{s-1})$ совпадает с $\dim P_{s-1}$. Применяя к алгебре P предположение индукции, получаем

$$\dim(aA_{s-1}/acA_{s-2})=\dim(P_{s-1}/cP_{s-1})\leqslant$$
$$\leqslant(\dim P_{s-1})_{\langle s-1\rangle}=(\dim(aA_{s-1}))_{\langle s-1\rangle}=(\dim A_s-\dim B_s)_{\langle s-1\rangle}.$$

Окончательно получаем

$$\dim B_s\leqslant(\dim B_s)_{\langle s\rangle}+(\dim A_s-\dim B_s)_{\langle s-1\rangle}.$$

Остается доказать следующий факт.

Лемма 10. *Пусть для натуральных чисел s и $h<m$ выполнено неравенство $h\leqslant h_{\langle s\rangle}+(m-h)_{\langle s-1\rangle}$. Тогда $h\leqslant m_{\langle s\rangle}$.*

Доказательство. Рассмотрим разложение Маколея

$$h=C^s_{k(s)}+\ldots+C^1_{k(1)}.$$

Будем рассуждать от противного. Пусть $m_{\langle s\rangle}<h$. Тогда по лемме 2 получаем $m<C^s_{k(s)+1}+\ldots+C^1_{k(1)+1}$ и $m-h<C^{s-1}_{k(s)}+\ldots+C^0_{k(1)}$. Значит,

$$(m-h)_{\langle s-1\rangle}<C^{s-1}_{k(s)-1}+\ldots+C^1_{k(2)-1}$$

и

$$h_{\langle s\rangle} = C^s_{k(s)-1} + \ldots + C^1_{k(1)-1}.$$

По условию

$$h \leqslant h_{\langle s\rangle} + (m-h)_{\langle s-1\rangle} < C^s_{k(s)} + \ldots + C^2_{k(2)} + C^1_{k(1)-1} \leqslant h,$$

и мы получаем противоречие. □

Теорема 5 доказана. □

Доказательство импликации (1) ⇒ (3) *в теореме* 3. Начнем со вспомогательного утверждения.

Лемма 11. *Пусть* $k(s), \ldots, k(1)$ — *s-коэффициенты Маколея числа* m *и* $j = \min\{i : k(i) \geqslant i\}$. *Тогда*

$$(m+1)^{\langle s\rangle} = \begin{cases} m^{\langle s\rangle} + k(1) + 1, & \text{если } j = 1, \\ m^{\langle s\rangle} + 1, & \text{если } j > 1. \end{cases}$$

Доказательство. При $j > 1$ имеем

$$m + 1 = C^s_{k(s)} + \ldots + C^j_{k(j)} + C^{j-1}_{j-1},$$

откуда следует требуемое утверждение. Пусть $j = 1$ и i — максимальный индекс, для которого $k(i) = k(1) + i - 1$. Тогда

$$m = C^s_{k(s)} + \ldots + C^{i+1}_{k(i+1)} + \sum_{r=1}^{i} C^r_{k(1)+r-1} = C^s_{k(s)} + \ldots + C^{i+1}_{k(i+1)} + C^i_{k(1)+i} - 1.$$

Значит,

$$m + 1 = C^s_{k(s)} + \ldots + C^{i+1}_{k(i+1)} + C^i_{k(1)+i}$$

является s-разложением Маколея для $m+1$, поскольку $k(i+1) > > k(1) + i$. Тогда

$$\begin{aligned} m^{\langle s\rangle} &= C^{s+1}_{k(s)+1} + \ldots + C^{i+2}_{k(i+1)+1} + \sum_{r=1}^{i} C^{r+1}_{k(1)+r} = \\ &= C^{s+1}_{k(s)+1} + \ldots + C^{i+2}_{k(i+1)+1} + \sum_{r=2}^{i+1} C^r_{k(1)+r-1} = \\ &= C^{s+1}_{k(s)+1} + \ldots + C^{i+2}_{k(i+1)+1} + C^{i+1}_{k(1)+i+1} - k(1) - 1. \end{aligned}$$

Наконец,

$$(m+1)^{\langle s\rangle} = C^{s+1}_{k(s)+1} + \ldots + C^{i+2}_{k(i+1)+1} + C^{i+1}_{k(1)+i+1} = m^{\langle s\rangle} + k(1) + 1. \quad \square$$

Тензорно умножая алгебру A на бесконечное расширение поля $\mathbb{K}$, мы можем считать, что основное поле бесконечно. Напомним, что B — это факторалгебра $A/(a)$, снабженная стандартной градуировкой, где $a \in A_1$ — элемент, для которого выполнено заключение теоремы 5. Умножение на a определяет линейное отображение из A_{s-1} в A_s. Поскольку размерность образа этого отображения не превосходит $\dim A_{s-1}$, имеет место неравенство $\dim A_s \leqslant \dim A_{s-1} + \dim B_s$. Тогда из теоремы 5 следует, что $\dim A_s \leqslant \dim A_{s-1} + (\dim A_s)_{\langle s \rangle}$. Пусть $m = \dim A_s$ и $p = \dim A_{s-1}$. Надо показать, что из неравенства $m \leqslant p + m_{\langle s \rangle}$ следует неравенство $m \leqslant p^{\langle s-1 \rangle}$. Поскольку

$$m_{\langle s \rangle} = C^s_{k(s)-1} + \ldots + C^1_{k(1)-1},$$

получаем

$$p \geqslant C^{s-1}_{k(s)-1} + \ldots + C^1_{k(2)-1} + C^0_{k(1)-1}.$$

Положим $j = \min\{i : k(i) \geqslant i\}$. Если $j > 1$, то $k(1) = 0$ и

$$p^{\langle s-1 \rangle} \geqslant C^s_{k(s)} + \ldots + C^2_{k(2)} = m.$$

Если $j = 1$, то, учитывая, что $C^0_{k(1)-1} = 1$, и применяя лемму 11, получаем

$$p^{\langle s-1 \rangle} \geqslant (C^{s-1}_{k(s)-1} + \ldots + C^1_{k(2)-1} + 1)^{\langle s-1 \rangle} = C^s_{k(s)} + \ldots + C^2_{k(2)} + (k(2) - 1) + 1.$$

Но $k(2) > k(1)$, поэтому $p^{\langle s-1 \rangle} > m$.

§ 7. Алгебра инвариантов линейных преобразований

Рассмотрим линейный оператор S на алгебре многочленов $\mathbb{K}[x_1, \ldots, x_n]$, определенный на образующих линейным преобразованием:

$$S(x_1) = a_{11}x_1 + \ldots + a_{n1}x_n, \quad \ldots, \quad S(x_n) = a_{1n}x_1 + \ldots + a_{nn}x_n$$

и продолжающийся на произвольный многочлен по правилу

$$(S(f))(x_1, \ldots, x_n) = f(S(x_1), \ldots, S(x_n)).$$

Оператор S удовлетворяет условию $S(fh) = S(f)S(h)$ для любых $f, h \in \mathbb{K}[x_1, \ldots, x_n]$. Будем считать, что преобразование S *обратимо*, т. е. существует такое линейное преобразование S^{-1}, что композиции $S \circ S^{-1}$ и $S^{-1} \circ S$ определяют тождественное преобразование. Ясно, что множество обратимых линейных преобразований переменных $x_1, \ldots, x_n$ образует группу относительно операции композиции. Более того, сопоставление преобразованию S матрицы (a_{ij}) позволяет отождествить группу обратимых линейных преобразований с группой обратимых матриц $\mathrm{GL}_n(\mathbb{K})$.

Определение 15. Будем говорить, что многочлен $F(x_1, \ldots, x_n)$ *инвариантен* относительно преобразования S, если $F(S(x_1), \ldots, S(x_n)) = F(x_1, \ldots, x_n)$.

Пример 8. Рассмотрим преобразование $S(x_1) = x_2$, $S(x_2) = x_3$, $\ldots$, $S(x_{n-1}) = x_n$, $S(x_n) = x_1$. Тогда многочлен $x_1 + x_2 + \ldots + x_n$ инвариантен относительно S, а $x_1 + x_2^2 + \ldots + x_n^n$ — нет.

Можно также рассматривать множество обратимых линейных преобразований $C = \{S_\omega : \omega \in \Omega\}$, где Ω — некоторое множество индексов, и множество всех многочленов $\mathbb{K}[x_1, \ldots, x_n]^C$, инвариантных относительно преобразований из C. Ясно, что $\mathbb{K}[x_1, \ldots, x_n]^C$ содержит константы и замкнуто относительно сложения и умножения многочленов, т. е. $\mathbb{K}[x_1, \ldots, x_n]^C$ — подалгебра в $\mathbb{K}[x_1, \ldots, x_n]$. Более того, если G — подгруппа в $\mathrm{GL}_n(\mathbb{K})$, порожденная элементами множества C, то $\mathbb{K}[x_1, \ldots, x_n]^G = \mathbb{K}[x_1, \ldots, x_n]^C$.

Основная задача теории инвариантов. Пусть G — подгруппа в $\mathrm{GL}_n(\mathbb{K})$. Опишите алгебру инвариантов $\mathbb{K}[x_1, \ldots, x_n]^G$.

Задача 30. Докажите, что в группе $\mathrm{GL}_2(\mathbb{K})$ нет подгруппы, алгебра инвариантов которой совпадает с $\mathbb{K}[x_1, x_1x_2]$.

Пример 9. Пусть $G = S_n$ — группа перестановок, действующая линейными преобразованиями переменных $x_1, \ldots, x_n$ по формуле $\tau(x_i) = x_{\tau(i)}$ для каждой перестановки $\tau \in S_n$. Напомним, что многочлен $F(x_1, \ldots, x_n)$ называется *симметрическим*, если $F(x_{\tau(1)}, \ldots, x_{\tau(n)}) = F(x_1, \ldots, x_n)$ для каждой перестановки $\tau \in S_n$, или, другими словами, $F(x_1, \ldots, x_n)$ является S_n-инвариантным. Рассмотрим набор многочленов

$$\begin{aligned}
\sigma_1 &= x_1 + x_2 + \ldots + x_n,\\
\sigma_2 &= x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
\sigma_n &= x_1x_2\ldots x_n.
\end{aligned}$$

Ясно, что эти многочлены являются симметрическими. Их называют *элементарными* симметрическими многочленами. Основная теорема о симметрических многочленах утверждает, что для каждого симметрического многочлена $F(x_1, \ldots, x_n)$ существует единственный такой многочлен $H(y_1, \ldots, y_n)$, что $F(x_1, \ldots, x_n) = H(\sigma_1, \ldots, \sigma_n)$; см. [3, гл. 3, § 8]. Тем самым, алгебра $\mathbb{K}[x_1, \ldots, x_n]^{S_n}$ свободно порождается элементарными симметрическими многочленами.

Пример 10. Пусть G — группа порядка 2, состоящая из тождественного преобразования и преобразования $x_1 \to -x_1, \ldots, x_n \to -x_n$. Под действием такого преобразования одночлен $x_1^{i_1}x_2^{i_2}\ldots x_n^{i_n}$ умножается на $(-1)^{i_1+i_2+\ldots+i_n}$. Поэтому многочлен $F(x_1, \ldots, x_n)$ инвариантен тогда и только тогда, когда сумма показателей степеней каждого входящего в него одночлена четна. Это доказывает, что алгебра инвариантов порождается элементами $x_1^2, x_2^2, \ldots, x_n^2, x_1x_2, x_1x_3, \ldots, x_{n-1}x_n$.

Замечание 1. В предыдущем примере мы неявно предполагали, что $-1 \neq 1$ в поле $\mathbb{K}$. Это условие выполнено не всегда. Заметим, что согласно определению поле $\mathbb{K}$ содержит элемент 1, а значит и элементы $1 + \ldots + 1$. Говорят, что поле $\mathbb{K}$ имеет *нулевую характеристику*, если $1 + \ldots + 1$ (n раз) не равно нулю для любого натурального n. Это условие равносильно тому, что подполе в $\mathbb{K}$, порожденное 1, можно отождествить с полем рациональных чисел. Например, поля $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$ имеют нулевую характеристику. В случае, когда сумма p единиц поля $\mathbb{K}$ равна нулю и p — наименьшее натуральное число с этим свойством, говорят, что поле $\mathbb{K}$ имеет *характеристику* p. Читатель легко проверит, что число p является простым. Условие $-1 = 1$ равносильно тому, что характеристика поля равна двум.

Упражнение 18. Приведите пример бесконечного поля характеристики p для любого простого числа p.

Всюду далее мы предполагаем, что $\mathbb{K}$ — поле нулевой характеристики.

Теорема 6. *Пусть $G \subset \mathrm{GL}_n(\mathbb{K})$ — конечная подгруппа. Тогда алгебра инвариантов $\mathbb{K}[x_1, \ldots, x_n]^G$ конечно порождена.*

Мы приведем два различных доказательства теоремы 6 (третье содержится в указании к задаче 37). В первом доказательстве, восходящем к Д. Гильберту, конечная порожденность алгебры инвариантов выводится из конечной порожденности полиномиального идеала. Второе доказательство принадлежит Э. Нётер. Оно основано на основной теореме о симметрических многочленах и доставляет оценку сверху на степени порождающих.

Доказательство 1. Рассмотрим отображение $P\colon \mathbb{K}[x_1, \ldots, x_n] \to \mathbb{K}[x_1, \ldots, x_n]$:

$$P(F(x_1, \ldots, x_n)) = \frac{1}{|G|} \sum_{S \in G} F(S(x_1), \ldots, S(x_n)).$$

Несложно проверить, что для любых $F, H \in \mathbb{K}[x_1, \ldots, x_n]$ и $f \in \mathbb{K}[x_1, \ldots, x_n]^G$ выполнены следующие свойства:

$$P(F+H) = P(F) + P(H), \quad P(F) \in \mathbb{K}[x_1, \ldots, x_n]^G,$$
$$P(f) = f, \quad P(fF) = fP(F).$$

В частности, P проектирует $\mathbb{K}[x_1, \ldots, x_n]$ на $\mathbb{K}[x_1, \ldots, x_n]^G$. В силу линейности преобразований из группы G если многочлен $f(x_1, \ldots, x_n)$ инвариантен, то инвариантна и каждая его однородная компонента. Пусть I — идеал в $\mathbb{K}[x_1, \ldots, x_n]$, порожденный всеми однородными инвариантами положительной степени. Как и каждый идеал в $\mathbb{K}[x_1, \ldots, x_n]$, идеал I порожден конечным числом многочленов $f_1, \ldots, f_s$. Эти многочлены можно считать однородными инвариантами.

Утверждается, что многочлены $f_1, \ldots, f_s$ порождают алгебру инвариантов. Чтобы в этом убедиться, достаточно доказать, что каждый однородный инвариант f выражается через $f_1, \ldots, f_s$. Проведем индукцию по степени m инварианта f. В случае $m = 0$ многочлен f является константой и наше утверждение справедливо. При $m > 0$ многочлен f принадлежит I и имеет место представление $f = h_1 f_1 + \ldots + h_s f_s$, $h_1 \ldots, h_s \in \mathbb{K}[x_1, \ldots, x_n]$. Применив проектор P к обеим частям представления, получим $f = P(f) = P(h_1) f_1 + \ldots + P(h_s) f_s$. Поскольку степени f_i положительны, степени однородных инвариантов $P(h_i)$ меньше m и по предположению индукции $P(h_i)$ выражаются через $f_1, \ldots, f_s$. Значит, и f выражается через $f_1, \ldots, f_s$. □

Доказательство 2. Здесь для упрощения изложения мы будем предполагать, что $\mathbb{K} = \mathbb{C}$. Нам потребуется вспомогательное предложение.

Предложение 4. *Пусть $f(x_1, \ldots, x_n)$ — однородный многочлен степени m с комплексными коэффициентами. Тогда для некоторого натурального k найдутся такие линейные многочлены $L_j = \sum_{i=1}^{n} a_{ij} x_i$, $j = 1, \ldots, k$, $a_{ij} \in \mathbb{C}$, что*

$$f(x_1, \ldots, x_n) = L_1^m + \ldots + L_k^m.$$

Доказательство. Рассмотрим случай $n = 2$. Вычисляя коэффициенты при помощи бинома Ньютона и используя определитель Вандермонда, легко показать, что многочлены x_1^m, $(x_1 + x_2)^m$, …, $(x_1 + mx_2)^m$ линейно независимы и, следовательно, образуют базис пространства однородных многочленов степени m от переменных x_1 и x_2. Это означает, что для произвольного однородного многочлена $f(x_1, x_2)$ степени m найдутся такие комплексные числа $\alpha_0, \ldots, \alpha_m$, что

$$f(x_1, x_2) = \alpha_0 x_1^m + \ldots + \alpha_m (x_1 + mx_2)^m = (\beta_0 x_1)^m + \ldots + (\beta_k (x_1 + mx_2))^m,$$

где $\beta_i^m = \alpha_i$.

При $n > 2$ будем вести индукцию по n. Достаточно доказать, что любой одночлен $x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$ степени m представим в нужном нам виде. Можно считать, что $i_1 \geqslant 1$. По предположению индукции одночлен $x_2^{i_2} \ldots x_n^{i_n}$ представим в виде $M_1^{m-i_1} + \ldots + M_k^{m-i_1}$, где M_j — линейные многочлены от $x_2, \ldots, x_n$. Остается заметить, что, вновь по предположению индукции, многочлен $x_1^{i_1} M_j^{m-i_1}$ представим в виде суммы m-х степеней линейных многочленов от x_1 и M_j. □

Пусть теперь $f(x_1, \ldots, x_n) = L_1^m + \ldots + L_k^m$ — указанное представление однородного инварианта f. Применяя к этому представлению отображение P, мы получаем, что f есть сумма выражений вида

$$L_j^{(m)}(x_1, \ldots, x_n) := \frac{1}{|G|} \sum_{S \in G} L_j(S(x_1), \ldots, S(x_n))^m.$$

Поскольку многочлен $Y_1^m + \ldots + Y_s^m$ $(s = |G|)$ является симметрическим многочленом от $Y_1, \ldots, Y_s$, его можно выразить через элементарные симметрические многочлены от $Y_1, \ldots, Y_s$. Это показывает, что $L_j^{(m)}(x_1, \ldots, x_n)$ выражается через элементарные симметрические многочлены от $L_j(S(x_1), \ldots, S(x_n))$, которые являются однородными инвариантами степени не выше $|G|$. Пространство многочленов от $x_1, \ldots, x_n$ степени не выше $|G|$ конечномерно, и любой базис подпространства инвариантов в этом пространстве является конечной системой порождающих для $\mathbb{C}[x_1, \ldots, x_n]^G$. □

Следствие 1. *Пусть $G \subset GL_n(\mathbb{C})$ — конечная подгруппа. Тогда алгебра $\mathbb{C}[x_1, \ldots, x_n]^G$ порождается инвариантами степени не выше $|G|$.*

Это следствие позволяет получить простой (но часто очень трудоемкий) алгоритм для построения конечной системы порождающих алгебры инвариантов конечной группы G: нужно взять все одночлены от $x_1, \ldots, x_n$ степени не выше $|G|$ и применить к ним проектор P.

Задача 31. Пусть G — конечная подгруппа в $\mathrm{GL}_n(\mathbb{C})$. Докажите, что элементы

$$P(x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}), \quad i_1 + i_2 + \ldots + i_n \leqslant |G|,$$

порождают алгебру $\mathbb{C}[x_1, \ldots, x_n]^G$.

Задача 32. Докажите, что следствие 1 справедливо над любым полем нулевой характеристики.

Задача 33. Пусть $A_n \subset S_n$ — подгруппа четных перестановок. Найдите образующие алгебры инвариантов $\mathbb{K}[x_1, \ldots, x_n]^{A_n}$.

Задача 34. Пусть $\mathbb{K} = \mathbb{C}$ и $\varepsilon \in \mathbb{C}$ — первообразный корень степени n из единицы. Рассмотрим группу G, порожденную преобразованием $x_1 \to \varepsilon^k x_1$, $x_2 \to \varepsilon^k x_2$, $1 \leqslant k \leqslant n-1$. Найдите образующие алгебры инвариантов $\mathbb{C}[x_1, x_2]^G$.

Задача 35. Пусть $\mathbb{K} = \mathbb{C}$ и $\varepsilon \in \mathbb{C}$ — первообразный корень степени n из единицы. Рассмотрим группу G, порожденную преобразованием $x_1 \to \varepsilon^k x_1$, $x_2 \to \varepsilon^{-k} x_2$, $1 \leqslant k \leqslant n-1$. Найдите образующие алгебры инвариантов $\mathbb{C}[x_1, x_2]^G$.

Задача 36. Пусть $\mathbb{K} = \mathbb{R}$ и G — группа третьего порядка, порожденная преобразованием

$$x_1 \to -\frac{1}{2} x_1 + \frac{\sqrt{3}}{2} x_2, \quad x_2 \to -\frac{\sqrt{3}}{2} x_1 - \frac{1}{2} x_2.$$

Найдите образующие алгебры инвариантов $\mathbb{R}[x_1, x_2]^G$.

Задача 37. Пусть $\mathbb{K}$ — поле положительной характеристики и $G \subset \mathrm{GL}_n(\mathbb{K})$ — конечная подгруппа. Докажите, что алгебра инвариантов $\mathbb{K}[x_1, \ldots, x_n]^G$ конечно порождена. Верно ли, что она порождается инвариантами степени не выше $|G|$?

Задача 38. Предположим, что конечная группа G совпадает со своим коммутантом. Докажите, что $\mathbb{K}[x_1, \ldots, x_n]^G$ есть алгебра с однозначным разложением на простые множители. Верно ли обратное утверждение?

§ 8. Формула Молина

Поскольку группа $G \subseteq \mathrm{GL}_n(\mathbb{K})$ действует на $\mathbb{K}[x_1, \ldots, x_n]$ линейными заменами переменных, она сохраняет инвариантной каждую компоненту алгебры $\mathbb{K}[x_1, \ldots, x_n]$ относительно стандартной градуировки. Следовательно, $\mathbb{K}[x_1, \ldots, x_n]^G$ является однородной подалгеброй в $\mathbb{K}[x_1, \ldots, x_n]$. В этом параграфе мы получим явную формулу для ряда Пуанкаре этой подалгебры. Будем предполагать, что основное поле $\mathbb{K}$ является полем $\mathbb{C}$ комплексных чисел.

Теорема 7 (Ф. Э. Молин, 1897)**.** *Пусть $G \subset \mathrm{GL}_n(\mathbb{K})$ — конечная подгруппа. Тогда*

$$P(\mathbb{K}[x_1, \ldots, x_n]^G, t) = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(E - tg)}.$$

Доказательство. Пусть g_m — линейный оператор, индуцированный элементом $g \in \mathrm{GL}_n(\mathbb{K})$ на компоненте $\mathbb{K}[x_1, \ldots, x_n]_m$. Поскольку $\frac{1}{|G|} \sum\limits_{g \in G} g_m$ — это проектор из $\mathbb{K}[x_1, \ldots, x_n]_m$ на $\mathbb{K}[x_1, \ldots, x_n]_m^G$, имеем

$$\mathrm{tr}\left(\frac{1}{|G|} \sum_{g \in G} g_m\right) = \frac{1}{|G|} \sum_{g \in G} \mathrm{tr}(g_m) = \dim \mathbb{K}[x_1, \ldots, x_n]_m^G.$$

Как элемент конечной группы, оператор g имеет конечный порядок, поэтому он аннулируется некоторым многочленом вида $x^N - 1$. Значит, минимальный многочлен оператора g делит $x^N - 1$. Такие многочлены не имеют кратных корней, следовательно, оператор g диагонализируем. Можно считать, что $x_1, \ldots, x_n$ — собственные векторы для g, отвечающие собственным значениям $\lambda_1, \ldots, \lambda_n$. Тогда каждый одночлен $x_1^{i_1} \ldots x_n^{i_n}$ также является собственным вектором, отвечающим собственному значению $\lambda_1^{i_1} \ldots \lambda_n^{i_n}$. Поэтому след оператора g_m равен сумме всех $\lambda_1^{i_1} \ldots \lambda_n^{i_n}$, для которых $i_1 + \ldots + i_n = m$. Окончательно получаем

$$\sum_{m \geqslant 0} \mathrm{tr}(g_m) t^m = (1 + \lambda_1 t + \lambda_1^2 t^2 + \ldots) \ldots (1 + \lambda_n t + \lambda_n^2 t^2 + \ldots) =$$

$$= \frac{1}{(1 - t\lambda_1) \ldots (1 - t\lambda_n)} = \frac{1}{\det(E - tg)},$$

и

$$P(\mathbb{K}[x_1, \ldots, x_n]^G, t) = \sum_{m \geqslant 0} \dim \mathbb{K}[x_1, \ldots, x_n]_m^G t^m = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(E - tg)}. \quad \square$$

Замечание 2. Более общий вариант формулы Молина позволяет вычислять кратность вхождения данного неприводимого представления группы G в компоненты алгебры $\mathbb{K}[x_1, \ldots, x_n]$; см. [19, теорема 2.1]. Читатель может сам доказать это обобщение, используя соотношения ортогональности для характеров конечных групп [3, гл. 11, § 4, теорема 3].

Задача 39. Докажите, что формула Молина верна над любым полем $\mathbb{K}$ нулевой характеристики.

В некоторых ситуациях теорема 7 позволяет доказывать, что данный набор инвариантов порождает алгебру $\mathbb{K}[x_1, \ldots, x_n]^G$. Для этого достаточно проверить, что ряд Пуанкаре подалгебры, порожденной этими инвариантами, совпадает с $P(\mathbb{K}[x_1, \ldots, x_n]^G, t)$.

Пример 11. Пусть подгруппа $G \subset \mathrm{GL}_2(\mathbb{K})$ состоит из четырех матриц:

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad M = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad M^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad M^3 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Тогда

$$P(\mathbb{K}[x_1, x_2]^G, t) =$$
$$= \frac{1}{4}\left(\frac{1}{\det(E-tE)} + \frac{1}{\det(E-tM)} + \frac{1}{\det(E-tM^2)} + \frac{1}{\det(E-tM^3)}\right) =$$
$$= \frac{1}{4}\left(\frac{1}{(1-t)^2} + \frac{2}{1+t^2} + \frac{1}{(1+t)^2}\right) = \frac{1+t^4}{(1-t^2)(1-t^4)}.$$

Нетрудно заметить, что многочлены $f_1 = x_1^2 + x_2^2$, $f_2 = x_1^2 x_2^2$ и $h = x_1^3 x_2 - x_1 x_2^3$ инвариантны, причем f_1 и f_2 алгебраически независимы. Пусть

$$F_1(f_1, f_2) + hF_2(f_1, f_2) = 0.$$

Сделаем замену $x_1 \to -x_1$, $x_2 \to x_2$. Тогда $F_1(f_1, f_2) - hF_2(f_1, f_2) = 0$ и $F_1(f_1, f_2) = F_2(f_1, f_2) = 0$. Значит, подпространства $\mathbb{K}[f_1, f_2]$ и $h\mathbb{K}[f_1, f_2]$ образуют прямую сумму. Но ряд Пуанкаре такой прямой суммы совпадает с $P(\mathbb{K}[x_1, x_2]^G, t)$, поэтому f_1, f_2 и h порождают алгебру инвариантов.

Пример 12. Укажем одно приложение формулы Молина к задачам комплексного анализа. Этот пример, как и предыдущий, заимствован из работы [19]. Пусть требуется вычислить сумму

$$S(k) = \sum_{w^k=1, w\neq 1} \frac{1}{|1-w|^2}.$$

Рассмотрим циклическую группу G порядка k, порожденную преобразованием $x_1 \to \varepsilon x_1$, $x_2 \to \varepsilon^{-1} x_2$, где ε — первообразный корень степени k из единицы. Тогда

$$P(\mathbb{C}[x_1, x_2]^G, t) = \frac{1}{k} \sum_{w \in \mathbb{C},\, w^k = 1} \frac{1}{(1-wt)(1-\bar{w}t)}$$

и $S(k) = \lim\limits_{t \to 1} \Big(kP(\mathbb{C}[x_1, x_2]^G, t) - \dfrac{1}{(1-t)^2} \Big)$. С другой стороны,

$$\mathbb{C}[x_1, x_2]^G = \bigoplus_{i=0}^{k-1} x_1^i x_2^i \mathbb{C}[x_1^k, x_2^k]$$

и

$$P(\mathbb{C}[x_1, x_2]^G, t) = \frac{1 + t^2 + t^4 + \ldots + t^{2k-2}}{(1-t^k)^2}.$$

Используя правило Лопиталя, получаем

$$S(k) = \left[\frac{k(1 + t^2 + \ldots + t^{2k-2}) - (1 + t + \ldots + t^{k-1})^2}{(1-t)^2 (1 + t + \ldots + t^{k-1})^2} \right]_{t=1} = \frac{\varphi(t)}{\psi(t)}\bigg|_{t=1} =$$

$$= \frac{\varphi''(t)}{\psi''(t)}\bigg|_{t=1} = \frac{k \frac{(k-1)k(4k-5)}{3} - 2\Big(k \frac{(k-2)(k-1)k}{3} + \frac{k^2(k-1)^2}{4} \Big)}{2k^2} = \frac{k^2 - 1}{12}.$$

Задача 40. Вычислите сумму

$$S_2(k) = \sum_{w^k = 1,\, w \neq 1} \frac{1}{|1-w|^4}.$$

§ 9. Контрпример Нагаты—Стейнберга

Пусть $\mathbb{K}$ — поле нулевой характеристики. Рассмотрим векторное пространство

$$V := V_2 \oplus V_2 \oplus \ldots \oplus V_2 \quad (9 \text{ слагаемых}),$$

где каждое V_2 — это двумерное арифметическое пространство $\mathbb{K}^2$ с координатами (x_i, y_i), $1 \leqslant i \leqslant 9$. Тем самым алгебра многочленов $\mathbb{K}[V]$ на пространстве V есть алгебра $\mathbb{K}[x_1, y_1, \ldots, x_9, y_9]$. Пусть $G_a = (\mathbb{K}, +)$ и группа $G_a^9 = G_a \times G_a \times \ldots \times G_a$ (9 множителей) действует на пространстве V как $x_i \to x_i + c_i y_i$, $y_i \to y_i$ для всех $(c_1, \ldots, c_9) \in G_a^9$.

Задача 41. Докажите, что алгебра инвариантов

$$\mathbb{K}[x_1, y_1, \ldots, x_9, y_9]^{G_a^9}$$

совпадает с подалгеброй $\mathbb{K}[y_1, \ldots, y_9]$.

Зафиксируем набор $(a_1, \ldots, a_9)$, где $a_i \in \mathbb{K}$, $a_i \neq a_j$ при $i \neq j$ и $\sum_{i=1}^{9} a_i \neq$ $\neq 0$. Рассмотрим в G_a^9 подгруппу $G \cong G_a^6$, заданную условиями

$$\sum_{i=1}^{9} c_i = 0, \quad \sum_{i=1}^{9} a_i c_i = 0, \quad \sum_{i=1}^{9} a_i^3 c_i = 0.$$

Пусть $H = GT$ — расширение группы G при помощи группы T преобразований вида $x_i \to t_i x_i$, $y_i \to t_i y_i$, где $t_1, t_2, \ldots, t_9$ — произвольные элементы поля $\mathbb{K}$, для которых $t_1 t_2 \ldots t_9 = 1$. Группы G и H реализуются матрицами 18×18:

$$G = \left\{ \begin{pmatrix} \begin{pmatrix} 1 & 0 \\ c_1 & 1 \end{pmatrix} & & 0 \\ & \ddots & \\ 0 & & \begin{pmatrix} 1 & 0 \\ c_9 & 1 \end{pmatrix} \end{pmatrix} \right\},$$

$$H = \left\{ \begin{pmatrix} \begin{pmatrix} t_1 & 0 \\ t_1 c_1 & t_1 \end{pmatrix} & & 0 \\ & \ddots & \\ 0 & & \begin{pmatrix} t_9 & 0 \\ t_9 c_9 & t_9 \end{pmatrix} \end{pmatrix} \right\}.$$

Теорема 8 (М. Нагата, Р. Стейнберг). *Алгебра инвариантов $\mathbb{K}[V]^H$ не является конечно порожденной.*

Разобьем доказательство теоремы 8 на несколько лемм. Положим $Y := y_1 y_2 \dots y_9$ и

$$Z_1 := \sum_{i=1}^{9} x_i y_1 \dots \hat{y_i} \dots y_9 = \sum_{i=1}^{9} \frac{x_i Y}{y_i}, \quad Z_2 := \sum_{i=1}^{9} \frac{a_i x_i Y}{y_i}, \quad Z_3 := \sum_{i=1}^{9} \frac{a_i^3 x_i Y}{y_i}.$$

Ясно, что $Y, Z_1, Z_2, Z_3 \in \mathbb{K}[V]$.

Лемма 12. *Справедливы включения $Y, Z_1, Z_2, Z_3 \in \mathbb{K}[V]^H$.*

Доказательство. Достаточно заметить, что

$$Y \to (t_1 y_1)(t_2 y_2) \dots (t_9 y_9) = (t_1 t_2 \dots t_9)(y_1 y_2 \dots y_9) = Y;$$

$$Z_1 \to \sum_{i=1}^{9} \frac{(t_i x_i + c_i t_i y_i) Y}{t_i y_i} = \sum_{i=1}^{9} \frac{x_i Y}{y_i} + \left(\sum_{i=1}^{9} c_i \right) Y = Z_1;$$

$$Z_2 \to \sum_{i=1}^{9} \frac{a_i (t_i x_i + c_i t_i y_i) Y}{t_i y_i} = \sum_{i=1}^{9} \frac{a_i x_i Y}{y_i} + \left(\sum_{i=1}^{9} a_i c_i \right) Y = Z_2;$$

$$Z_3 \to \sum_{i=1}^{9} \frac{a_i^3 (t_i x_i + c_i t_i y_i) Y}{t_i y_i} = \sum_{i=1}^{9} \frac{a_i^3 x_i Y}{y_i} + \left(\sum_{i=1}^{9} a_i^3 c_i \right) Y = Z_3. \qquad \square$$

Лемма 13. *Имеет место равенство*

$$\mathbb{K}[V]^H = \mathbb{K}[V] \cap \mathbb{K}[Z_1, Z_2, Z_3, Y, Y^{-1}].$$

Доказательство. Группы G и H естественно действуют на алгебре $A := \mathbb{K}[x_1, \dots, x_9, y_1, \dots, y_9, Y^{-1}]$. Положим $W_i := \dfrac{x_i Y}{y_i}$. Тогда $x_i = y_i W_i Y^{-1}$, поэтому

$$A = \mathbb{K}[W_1, W_2, W_3, x_4, \dots, x_9, y_1, \dots, y_9, Y^{-1}].$$

Далее, $Z_1 = \sum\limits_{i=1}^{9} W_i$, $Z_2 = \sum\limits_{i=1}^{9} a_i W_i$, $Z_3 = \sum\limits_{i=1}^{9} a_i^3 W_i$. Перенумеровав элементы $a_1, \dots, a_9$, можно считать, что определитель

$$\begin{vmatrix} 1 & 1 & 1 \\ a_1 & a_2 & a_3 \\ a_1^3 & a_2^3 & a_3^3 \end{vmatrix} = (a_2 - a_1)(a_3 - a_1)(a_3 - a_2)(a_1 + a_2 + a_3)$$

отличен от нуля. Тогда W_1, W_2 и W_3 можно выразить как линейные функции от $Z_1, Z_2, Z_3, W_4, \dots, W_9$. Это показывает, что

$$A = \mathbb{K}[Z_1, Z_2, Z_3, x_4, \dots, x_9, y_1, \dots, y_9, Y^{-1}]. \tag{3}$$

Рассмотрим подгруппу $G_4 \subset G$, заданную условиями $c_5 = \ldots = c_9 = 0$. Вновь в силу условия на определитель для любого $c_4 \in \mathbb{K}$ найдется ровно один такой набор (c_1, c_2, c_3), что $(c_1, c_2, c_3, c_4, 0, \ldots, 0) \in G$. Все образующие алгебры A из соотношения (3), за исключением x_4, не изменяются под действием G_4, тогда как $x_4 \to x_4 + c_4 y_4$. Это показывает, что элемент $F(Z_1, Z_2, Z_3, x_4, \ldots, x_9, y_1, \ldots, y_9, Y^{-1}) \in A$ является G_4-инвариантным тогда и только тогда, когда он не зависит от x_4. Рассматривая $G_5, \ldots, G_9$, мы покажем, что G-инварианты не зависят также от $x_5, \ldots, x_9$. С другой стороны, элементы $Z_1, Z_2, Z_3, y_1, \ldots, y_9, Y^{-1}$ являются G-инвариантными, поэтому $A^G = \mathbb{K}[Z_1, Z_2, Z_3, y_1, \ldots, y_9, Y^{-1}]$. Элемент $(t_1, \ldots, t_9) \in T$ умножает одночлен $Z_1^{d_1} Z_2^{d_2} Z_3^{d_3} y_1^{b_1} \ldots y_9^{b_9} (Y^{-1})^c$ на $t_1^{b_1 - c} \ldots t_9^{b_9 - c}$. Такой одночлен T-инвариантен в точности тогда, когда $b_1 = \ldots = b_9$, поэтому $A^H = \mathbb{K}[Z_1, Z_2, Z_3, Y, Y^{-1}]$. Наконец, из включения $\mathbb{K}[V] \subset A$ следует, что $\mathbb{K}[V]^H = \mathbb{K}[V] \cap A^H$. □

Лемма 14. *Элементы $Z_1, Z_2, Z_3, Y \in \mathbb{K}[V]$ алгебраически независимы.*

Доказательство. Пусть $B := K[x_1, \ldots, x_9]$ — алгебра многочленов над полем рациональных дробей $K := \mathbb{K}(y_1, \ldots, y_9)$. По построению элементы $x_1, \ldots, x_9$ этой алгебры алгебраически независимы. Заметим, что $W_i = \dfrac{x_i Y}{y_i}$ отличается от x_i на константу $\dfrac{Y}{y_i} \in K$, поэтому элементы $W_1, W_2, W_3, x_4, \ldots, x_9$ алгебраически независимы над K. Далее, поскольку наборы $\{W_1, W_2, W_3, x_4, \ldots, x_9\}$ и $\{Z_1, Z_2, Z_3, x_4, \ldots, x_9\}$ получаются друг из друга обратимой K-линейной заменой, элементы $Z_1, Z_2, Z_3, x_4, \ldots, x_9$ (а значит, и Z_1, Z_2, Z_3) алгебраически независимы над K.

Пусть теперь

$$F(Z_1, Z_2, Z_3, Y) = \sum_{I=(i_1,i_2,i_3)} f_I(Y) Z_1^{i_1} Z_2^{i_2} Z_3^{i_3} = 0.$$

Тогда $f_I(Y)$ являются нулевыми элементами поля K, и поэтому многочлен F нулевой. □

Лемма 15. *Имеет место равенство*

$$\mathbb{K}[V]^H = \left\{ \sum_j \frac{f_j(Z_1, Z_2, Z_3)}{Y^{m_j}} \right\},$$

где f_j — однородный многочлен от Z_1, Z_2, Z_3, который делится на Y^{m_j} в алгебре $\mathbb{K}[V]$.

Доказательство. По лемме 13 любой многочлен $F \in \mathbb{K}[V]^H$ имеет вид $\sum \frac{f_j(Z_1, Z_2, Z_3)}{Y^{m_j}}$, где многочлен f_j можно считать однородными степени d_j по Z_1, Z_2, Z_3. Нам нужно показать, что $f_j(Z_1, Z_2, Z_3)$ делится на Y^{m_j} в $\mathbb{K}[V]$. Можно считать, что многочлен F является однородным степени d по совокупности переменных $x_1, \ldots, x_9, y_1, \ldots, y_9$. Степень выражения $\frac{f_j(Z_1, Z_2, Z_3)}{Y^{m_j}}$ по переменным $x_1, \ldots, x_9$ равна d_j, а по переменным $y_1, \ldots, y_9$ равна $8d_j - 9m_j$. Поэтому $d = 9(d_j - m_j)$, и, значит, d_j однозначно определяется по m_j и d. Следовательно, выражение $\frac{f_j(Z_1, Z_2, Z_3)}{Y^{m_j}}$ совпадает с однородной компонентной многочлена F по переменным $x_1, \ldots, x_9$ и поэтому принадлежит $\mathbb{K}[V]$. □

Определение 16. Ненулевой многочлен $F(x, y)$ имеет *нуль порядка не ниже* m в точке (α, β), если он допускает запись

$$F(x, y) = F_m(x - \alpha, y - \beta) + F_{m+1}(x - \alpha, y - \beta) + \ldots,$$

где F_k — некоторый однородный многочлен степени k от двух переменных.

Лемма 16. *Ненулевой однородный многочлен $f(Z_1, Z_2, Z_3)$ степени d от переменных Z_1, Z_2, Z_3 делится на Y^m тогда и только тогда, когда многочлен $\hat{f}\left(\frac{Z_2}{Z_1}, \frac{Z_3}{Z_1}\right) := \frac{f(Z_1, Z_2, Z_3)}{Z_1^d}$ имеет в точках $(a_1, a_1^3), \ldots, (a_9, a_9^3)$ нули порядка не меньше m.*

Доказательство. Сделаем замену переменных

$$Z_1' = Z_1, \quad Z_2' = Z_2 - a_1 Z_1, \quad Z_3' = Z_3 - a_1^3 Z_1.$$

После этого точка (a_1, a_1^3) переместится в начало координат. Далее,

$$Z_1' = x_1 \frac{Y}{y_1} + y_1 U_1, \quad Z_2' = y_1 U_2, \quad Z_3' = y_1 U_3,$$

где

$$U_1 = \frac{x_2 Y}{y_1 y_2} + \ldots + \frac{x_9 Y}{y_1 y_9}, \quad U_2 = (a_2 - a_1)\frac{x_2 Y}{y_1 y_2} + \ldots + (a_9 - a_1)\frac{x_9 Y}{y_1 y_9},$$

$$U_3 = (a_2^3 - a_1^3)\frac{x_2 Y}{y_1 y_2} + \ldots + (a_9^3 - a_1^3)\frac{x_9 Y}{y_1 y_9}.$$

Ясно, что многочлены U_1, U_2, U_3 не зависят от y_1. В записи

$$f(Z_1', Z_2', Z_3') = f_m(Z_2', Z_3') Z_1'^{d-m} + f_{m+1}(Z_2', Z_3') Z_1'^{d-m-1} + \ldots$$

все члены начиная со второго делятся на y_1^{m+1}, а первый член имеет вид $y_1^m f_m(U_2, U_3)\left(x_1 \frac{Y}{y_1} + y_1 U_1\right)^{d-m}$. Из условия на определитель (см.

доказательство леммы 13) следует, что

$$K(x_2, \ldots, x_9) = K(U_2, U_3, x_4, \ldots, x_9),$$

где $K = \mathbb{K}(y_1, \ldots, y_9)$. Значит, U_2 и U_3 алгебраически независимы над K (и над $\mathbb{K}$). Поэтому из условия $f_m(Z_2', Z_3') \neq 0$ следует, что $f_m(U_2, U_3) \neq 0$ как многочлен от x_i и y_i. Итак, максимальная степень элемента y_1, на которую делится $f(Z_1, Z_2, Z_3)$, равна порядку нуля многочлена $\hat{f}\left(\frac{Z_2}{Z_1}, \frac{Z_3}{Z_1}\right)$ в точке (a_1, a_1^3). Рассматривая аналогично точки (a_2, a_2^3), …, (a_9, a_9^3), получаем утверждение леммы. □

Лемма 17. *Пусть ненулевой многочлен $F(x, y)$ степени не выше $3m$ имеет нули порядка не меньше $\geqslant m$ в точках (a_1, a_1^3), …, (a_9, a_9^3). Тогда $F(x, y) = \lambda(y - x^3)^m$, $\lambda \in \mathbb{K} \setminus \{0\}$.*

Доказательство. Будем рассуждать индукцией по m. В случае $m = 0$ многочлен $F(x, y)$ является ненулевой константой и утверждение очевидно. При $m > 0$ рассмотрим запись

$$F(x, y) = c_0(x)y^{3m} + c_1(x)y^{3m-1} + \ldots + c_{3m}(x).$$

По условию степень многочлена $c_j(x)$ не превосходит j. Замена $y \to x^3$ приводит к многочлену $F(x, x^3) = c_0x^{9m} + c_1(x)x^{9m-3} + \ldots + c_{3m}(x)$, совпадающему с остатком от деления $F(x, y)$ на $y - x^3$. Многочлен $F(x, x^3)$ делится на $(x - a_i)^m$, поскольку выражение $(x - a_i)^k(y - a_i^3)^p$ после замены $y \to x^3$ делится на $(x - a_i)^{k+p}$. Итак, многочлен $F(x, x^3)$ делится на $(x - a_1)^m \ldots (x - a_9)^m$. Сравнивая степени, получаем

$$c_0x^{9m} + c_1(x)x^{9m-3} + \ldots + c_{3m}(x) = c_0(x - a_1)^m \ldots (x - a_9)^m.$$

Коэффициент при x^{9m-1} в левой части равен нулю, тогда как в правой части он равен $-c_0m\sum_{i=1}^{9} a_i$. Отсюда следует, что $c_0 = 0$, и, значит, $F(x, y)$ делится на $y - x^3$. Поскольку $y - x^3$ имеет в точках (a_i, a_i^3) нуль порядка 1, мы можем применить к частному $\frac{F(x, y)}{y - x^3}$ предположение индукции и получить требуемое утверждение. □

Лемма 18. 1. *Векторное пространство многочленов степени не выше d от переменных x и y имеет размерность*

$$C_{d+2}^2 = \frac{(d+2)(d+1)}{2}.$$

2. *Пусть $d \geqslant m$. Тогда пространство многочленов степени не выше d, имеющих в данной точке P нуль порядка не выше m, имеет размерность*

$$C_{d+2}^2 - C_{m+1}^2.$$

Доказательство. 1. Надо сосчитать число пар (i, j) с целыми $i, j \geqslant 0$, $i + j \leqslant d$. Для этого введем фиктивное слагаемое $k = d - i - j$. Тогда $d = i + j + k$, $i, j, k \geqslant 0$. Рассмотрим $d + 2$ кружочка, расположенных в ряд. Закрашивание двух из них определяет разбиение d на 3 неотрицательных слагаемых.

2. После сдвига точки P в начало координат условие на порядок нуля задается обращением в нуль C^2_{m+1} коэффициентов многочлена. □

Лемма 19. *Пусть $d \geqslant 3m$. Тогда пространство многочленов $F(x, y)$ степени не выше d, имеющих нули порядка не выше m в точках $(a_1, a_1^3), \ldots, (a_9, a_9^3)$, имеет размерность*

$$C^2_{d+2} - 9C^2_{m+1}.$$

Доказательство. По предыдущей лемме размерность пространства многочленов степени не выше $3m$ равна $C^2_{3m+2} = \dfrac{9m^2 + 9m + 2}{2}$, тогда как $9C^2_{m+1} = \dfrac{9m^2 + 9m}{2}$. По лемме 17 пространство многочленов, удовлетворяющих нашим условиям на порядки нулей, одномерно. Следовательно, $9C^2_{m+1}$ линейных условий на $F(x, y)$ оказываются линейно независимыми. При $d > 3m$ указанные условия также линейно независимы, поскольку они линейно независимы при ограничении на подпространство многочленов степени не выше $3m$. □

Лемма 20. *Существует многочлен $F(x, y)$ степени $3m + 1$, имеющий в точках $(a_1, a_1^3), \ldots, (a_9, a_9^3)$ нули порядка не меньше m и не делящийся на $y - x^3$.*

Доказательство. Пространство многочленов степени не выше $3m + 1$, имеющих нули порядка не меньше m в точках (a_i, a_i^3), имеет размерность

$$C^2_{3m+3} - 9C^2_{m+1} = \frac{(3m+3)(3m+2)}{2} - 9\frac{(m+1)m}{2} = 3m + 3.$$

Подпространство U многочленов, удовлетворяющих этим условиям и делящихся на $y - x^3$, имеет размерность

$$C^2_{3m} - 9C^2_m = \frac{3m(3m-1)}{2} - 9\frac{m(m-1)}{2} = 3m$$

(это размерность пространства многочленов степени не выше $(3m + + 1) - 3$, имеющих в точках (a_i, a_i^3) нули порядка не меньше $m - 1$). Тем самым подпространство U является собственным. □

Доказательство теоремы 8. Пусть алгебра $\mathbb{K}[V]^H$ конечно порождена. Лемма 15 позволяет выбрать систему образующих вида

$$S = \left\{ \frac{Z_1^2 Z_3 - Z_2^3}{Y},\ \frac{f_1(Z_1, Z_2, Z_3)}{Y^{m_1}},\ \ldots,\ \frac{f_r(Z_1, Z_2, Z_3)}{Y^{m_r}} \right\},$$

где $f_j(Z_1, Z_2, Z_3)$ делятся Y^{m_j} в $\mathbb{K}[V]$. Можно считать, что $f_j(Z_1, Z_2, Z_3)$ не делятся на $Z_1^2 Z_3 - Z_2^3$, иначе заменим образующую $\frac{f_j(Z_1, Z_2, Z_3)}{Y^{m_j}}$ на $\frac{f_j(Z_1, Z_2, Z_3)}{(Z_1^2 Z_3 - Z_2^3) Y^{m_j - 1}}$. Пусть d_j — это степень многочлена f_j относительно Z_1, Z_2, Z_3. Согласно лемме 17 для всех $m_j > 0$ выполнено неравенство $d_j > 3m_j$. Легко видеть, что это неравенство выполнено и при $m_j \leqslant 0$, поскольку мы можем считать, что S не содержит констант.

Зафиксируем число $m > \max(m_1, \ldots, m_r)$. Лемма 20 обеспечивает существование многочлена $F(x, y)$ степени $3m + 1$, имеющего нули порядка не меньше m в точках (a_i, a_i^3) и не делящегося на $y - x^3$. Пусть $f(Z_1, Z_2, Z_3) := F\left(\frac{Z_2}{Z_1}, \frac{Z_3}{Z_1}\right) Z_1^{3m+1}$. По лемме 16 выражение $\frac{f(Z_1, Z_2, Z_3)}{Y^m}$ определяет элемент алгебры $\mathbb{K}[V]^H$. Покажем, что он не выражается через элементы множества S. В самом деле, если такое выражение существует, его можно считать однородным по переменным Z_1, Z_2, Z_3 и по переменной Y (здесь используется лемма 14). Поскольку f не делится на $Z_1^2 Z_3 - Z_2^3$, в данном выражении имеется член, не включающий $\frac{Z_1^2 Z_3 - Z_2^3}{Y}$. Пусть это $\lambda \prod \left(\frac{f_j(Z_1, Z_2, Z_3)}{Y^{m_j}} \right)^{e_j}$, $\lambda \in \mathbb{K} \setminus \{0\}$. Приравнивая степени по Z_1, Z_2, Z_3 и по Y, получаем

$$\sum d_j e_j = 3m + 1; \tag{4}$$

$$\sum m_j e_j = m. \tag{5}$$

Тогда рассмотрим выражение (4) $-$ 3(5) и получим $\sum (d_j - 3m_j) e_j = 1$. Поскольку $d_j - 3m_j > 0$, мы заключаем, что ровно одно e_j, скажем e_{j_0}, равно 1, а прочие e_j равны нулю. Из соотношения (5) следует, что $m = m_{j_0}$, что противоречит выбору m. Это противоречие завершает доказательство теоремы 8. □

Упражнение 19. Найдите в доказательстве как можно больше мест, где существенно используется тот факт, что число точек (a_i, a_i^3) равно 9.

Будем говорить, что алгебра A градуирована некоторой группой M, если задано такое разложение $A = \bigoplus_{m \in M} A_m$ в прямую сумму векторных подпространств, что $A_{m_1} A_{m_2}$ содержится в $A_{m_1 m_2}$ для любых $m_1, m_2 \in M$. В этом случае алгебра A называется *M-градуированной*.

Упражнение 20. Покажите, что градуировки из определения 1 являются частным случаем M-градуировок. Какую группу M здесь нужно рассмотреть?

В заключительной части доказательства теоремы 8 неявно использована $\mathbb{Z}^2$-градуировка на алгебре инвариантов $\mathbb{K}[V]^H$. В следующей задаче мы формулируем соответствующее утверждение явно.

Задача 42. Пусть $A = \bigoplus_{(a,b)\in\mathbb{Z}^2} A_{(a,b)}$ — $\mathbb{Z}^2$-градуированная алгебра, удовлетворяющая следующим условиям:

— $A_{(a,b)} \neq 0 \Rightarrow a \geqslant 0$, $a \geqslant 3b$;

— $\dim A_{(3b,b)} = 1$ при всех $b \geqslant 0$;

— $A_{(3b+1,b)} \neq A_{(3b-2,b-1)} A_{(3,1)}$ при всех $b \geqslant 1$.

Докажите, что алгебра A не является конечно порожденной.

Задача 43. Докажите, что алгебра инвариантов $\mathbb{K}[V]^G$ не является конечно порожденной.

§ 10. Указания и комментарии к задачам

1. Пусть $1 = a_{j_1} + \ldots + a_{j_k}$, $j_1 < \ldots < j_k$. Тогда из $1a_{j_1} = a_{j_1}$ следует, что $j_1 = 0$ и $a_{j_1}a_{j_p} = 0$ при $p > 1$. Остается воспользоваться тем, что $1a_{j_p} = a_{j_p}$.

2. а) Если $b \in A_s$, $b \neq 0$ и $s > 0$, то линейная оболочка $\langle cbd : c, d \in A\rangle$ содержится в сумме компонент степени не ниже s. С другой стороны, для ненулевой матрицы B линейная оболочка $\langle CBD : C, D \in \mathrm{Mat}_{n\times n}(\mathbb{K})\rangle$ совпадает с $\mathrm{Mat}_{n\times n}(\mathbb{K})$.

б) Непрерывная функция обратима тогда и только тогда, когда она нигде не обращается в нуль. Непрерывная функция на отрезке $[0, 1]$ ограничена, поэтому, прибавляя к любому элементу нашей алгебры подходящую константу, можно получить обратимый элемент. Пусть имеется нетривиальная градуировка $C[0, 1] = A = \bigoplus_{s\geqslant 0} A_s$ и $a \in A_k$, $k > 0$. Тогда для подходящей константы λ найдется такой элемент $b = b_0 + b_1 + \ldots + b_N$, что $(a + \lambda)b = 1$. Отсюда следует, что $b_0 = \lambda^{-1}$ — ненулевая константа, b_k пропорционален a, b_{2k} пропорционален a^2 и т.д., а прочие компоненты элемента b равны нулю. Рассмотрите старшую компоненту произведения ab.

3. Рассмотрите $A = \mathbb{K}[x]/(x^2)$ и элемент $1 + x$. Покажите, что в алгебрах без делителей нуля такой пример невозможен.

4. а) Из конечной порожденности алгебры A следует, что A порождается подпространством $\bigoplus_{s=1}^{m} A_s$ для некоторого натурального m. Ясно, что в любую однородную систему образующих должен входить некоторый базис пространства A_1. Далее будем строить минимальную систему образующих индуктивно. Для произвольного $k > 1$ рассмотрим в A_k подпространство U_k, порожденное произведениями $A_{j_1}\ldots A_{j_p}$, где $j_1 + \ldots + j_p = k$ и $j_1 \geqslant \ldots \geqslant j_p > 0$. Заметим, что U_k не зависит от выбора образующих. Достроим некоторый базис пространства U_k до базиса пространства A_k и добавим базисные векторы к системе образующих. После того как мы дойдем до $k = m$, мы получим минимальную систему образующих алгебры A. Докажите, что произвольная однородная система образующих содержит не менее $\dim A_k - \dim U_k$ элементов степени k.

б) Рассмотрите $A = A_0 = \mathbb{K}[x, y]/(xy - 1)$ и $a_1 = x^2$, $a_2 = x^3$, $a_3 = y^6$.

5. Пусть $S \subset \mathbb{Z}_+$ — подмножество, причем $s + s' \in S$ для любых $s, s' \in S$. Используя понятие наибольшего общего делителя, докажите, что найдется конечный набор $s_1, \ldots, s_n$ элементов из S, складывая

(многократно) которые мы получим все элементы S. Пусть теперь $P \subset \mathbb{K}[x]$ — подалгебра, S — множество степеней всевозможных многочленов из P, $s_1, \ldots, s_n$ — построенный выше набор и $g_1, \ldots, g_n$ — произвольные многочлены из P, удовлетворяющие условию $\deg g_i = s_i$. Проверьте индукцией по степени, что каждый элемент из P выражается как многочлен от $g_1, \ldots, g_n$.

Можно описать все алгебры, в которых каждая подалгебра конечно порождена, а также получить G-эквивариантный аналог этого результата, где G — некоторая линейная группа автоморфизмов алгебры, см. [8].

6. Пусть алгебра конечно порождена. Можно считать, что конечная система порождающих состоит из одночленов. Пусть m — это максимальное значение отношения $\frac{j}{i}$ по всем образующим $x^i y^j$. Докажите, что для любого $x^k y^s \in A$ имеем $\frac{s}{k} \leqslant m$. Это приводит к противоречию.

7. Это решение предложила Каринэ Куюмжиян. Пусть в некоторой однородной системе образующих $a_1, \ldots, a_n$ алгебры A элементы имеют степени $d_1, \ldots, d_n$. Положим $m = nK$, где K — наименьшее общее кратное чисел $d_1, \ldots, d_n$. Пусть одночлен $a_1^{i_1} \ldots a_n^{i_n}$ имеет степень $i_1 d_1 + \ldots + i_n d_n = pnK$, $p \geqslant 2$. Достаточно доказать, что найдутся такие целые неотрицательные числа $j_1 \leqslant i_1, \ldots, j_n \leqslant i_n$, что $j_1 d_1 + \ldots + j_n d_n = nK$. Рассмотрим остатки t_r от деления $i_r d_r$ на K. Тогда $t_1 + \ldots + t_n = cK$, $c < n$. Прибавляя последовательно к числам t_r число K так, чтобы результат не превосходил $i_r d_r$, мы увеличиваем значение суммы на K, пока не получим nK.

Следующий пример, найденный И. И. Богдановым, показывает, что $m = K$ положить нельзя. Пусть $d_1 = 1$, $d_2 = 6$, $d_3 = 10$ и $d_4 = 15$. Тогда $K = 30$ и сумму

$$1 + 6 + 6 + 6 + 6 + 10 + 10 + 15 = 60$$

нельзя разбить на две подсуммы, равные 30.

В книге [1, гл. III, § 1, предложение 3] доказано, что число m можно подобрать так, что ml-разрежение алгебры A будет стандартным для любого $l \geqslant 1$.

Для знатоков отметим, что утверждение задачи полезно в алгебраической геометрии: оно позволяет доказать, что взвешенное проективное пространство является проективным многообразием.

8. Хорошо известно (см. [3, гл. 9, § 6]), что если n элементов порождают алгебру $A = \mathbb{K}[x_1, \ldots, x_n]$, то эти элементы алгебраически независимы. Для каждого набора свободных порождающих алгебры A обо-

значим через N общее число однородных компонент элементов набора. Пусть $y_1, \ldots, y_n$ — свободные порождающие, для которых значение N минимально. Тогда $y_1, \ldots, y_n$ не содержат компонент нулевой степени. Предположим, что элемент y_1 неоднороден. Никакая компонента элемента y_1 не выражается через $y_2, \ldots, y_n$, иначе можно заменить y_1 на разность y_1 и многочлена от $y_2, \ldots, y_n$. Пусть z — компонента элемента y_1 наименьшей степени. Покажем, что $z, y_2, \ldots, y_n$ порождают A. Для этого достаточно доказать, что все компоненты элемента y_1 выражаются через $z, y_2, \ldots, y_n$. Для компоненты z это ясно. Для прочих компонент z' используем индукцию по степени. В выражение $z' = F(y_1, \ldots, y_n)$ не входит член вида λy_1, $\lambda \in \mathbb{K} \setminus \{0\}$, так как иначе член λz не может сократиться. Это показывает, что z' выражается через $y_2, \ldots, y_n$ и компоненты элемента y_1 меньших степеней.

Наши рассуждения показывают, что каждая градуированная n-порожденная алгебра A, для которой $A_0 = \mathbb{K}$, может быть порождена не более чем n однородными элементами.

Заметим, что условие $A_0 = \mathbb{K}$ для данного решения существенно и, отбросив его, мы получим задачу другого уровня сложности. Одной из ярких открытых проблем современной алгебры является так называемая *проблема сокращения*. Пусть A — конечно порожденная $\mathbb{K}$-алгебра, и для некоторого натурального k алгебра многочленов $A[y_1, \ldots, y_k]$ над A изоморфна алгебре многочленов $\mathbb{K}[x_1, \ldots, x_m]$ над полем $\mathbb{K}$. Верно ли, что алгебра A изоморфна алгебре многочленов $\mathbb{K}[z_1, \ldots, z_{m-k}]$? Нетрудно показать, что решение задачи 8 без ограничения $A_0 = \mathbb{K}$ влечет положительное решение проблемы сокращения.

Если рассмотреть свободную алгебру, градуированную не целыми неотрицательными числами, а всей группой целых чисел, задача 8 станет эквивалентна *проблеме линеаризации* для действия одномерного алгебраического тора на аффинном пространстве $\mathbb{K}^n$. Положительное решение этой проблемы при $n = 1$ и 2 известно достаточно давно. Полученное около 10 лет назад положительное решение проблемы линеаризации при $n = 3$ потребовало колоссальных усилий, см. обзор [12]. При $n \geqslant 4$ проблема линеаризации остается открытой.

9. Воспользуемся тем, что в алгебре $A = \mathbb{K}[x_1, \ldots, x_n]$ разложение на простые множители однозначно; см. [3, гл. 9, § 7]. Пусть $p = \frac{p_1}{p_2} \in QA$. Элементы $p_1, p_2 \in A$ можно считать взаимно простыми. Если $p^m + a_1 p^{m-1} + \ldots + a_m = 0$ для некоторых $a_1, \ldots, a_m \in A$, то каждый простой делитель элемента p_2 делит p_1. Значит, $p \in A$.

10. Заметим, что $P(A) = M(P(A))$. Пусть

$$r \in (L(P(A)) \cap K(P(A))) \setminus P(A).$$

Тогда соответствующий r одночлен a не лежит в A. Условие $r \in L(P(A))$ позволяет рассматривать a как элемент поля QA, а условие $r \in K(P(A))$ показывает, что $a^s \in A$ для подходящего $s \in \mathbb{N}$. Следовательно, A не целозамкнута.

Обратно, пусть $p = \frac{a}{b} \in QA \setminus A$ и $p^k + a_1 p^{k-1} + \ldots + a_k = 0$. Из целозамкнутости алгебры $\mathbb{K}[x_1, \ldots, x_n]$ следует, что $p \in \mathbb{K}[x_1, \ldots, x_n]$. У многочлена p есть член, набор степеней r которого не лежит в $P(A)$. В силу равенства $a = bp$ точка r лежит в $L(P(A))$. Покажем, что r лежит в конусе $K \subseteq K(P(A))$, порожденном наборами степеней одночленов, входящих в разложения элементов $a_1, \ldots, a_k$. Пусть $r \notin K$. Поскольку конус K является замкнутым выпуклым подмножеством в $\mathbb{Q}^n$, теорема отделимости (см. [3, гл. 7, § 2, теорема 2]) гарантирует наличие линейной функции l, которая неположительна на конусе K и $l(r) > 0$. Будем называть максимальной компонентой многочлена сумму тех его членов, для которых значение функции l на наборе показателей максимально. Несложно проверить, что в выражении $p^k + a_1 p^{k-1} + \ldots + a_k$ старшая компонента многочлена p^k не может сократиться, и, значит, это выражение не равно нулю.

11. В этой ситуации множество $P(A)$ определяется аналогично, однако базис Гильберта определить не удается. Теорема о том, что мономиальная подалгебра A целозамкнута тогда и только тогда, когда $P(A)$ насыщенно в $\mathbb{Z}^n$, доказывается точно так же.

12. Эта задача взята из книги [6, гл. III, § 4.3]. Покажем сначала, что в A содержатся одночлены $x^r y^s$ с любым заданным s. Пусть

$$P = x^a y^b + \sum_{i>0} a_i x^{a+i} y^{b-i},$$

$a_i \in \mathbb{K}$, — однородный элемент из A, для которого $b > 0$. Если $k \in \mathbb{N}$ и $kb \geqslant a$, то

$$x^{kb-a} P = (x^k y)^b + \sum_{i>0} a_i x^{(k+1)i} (x^k y)^{b-i} \in A,$$

откуда ввиду целозамкнутости алгебры A следует, что $x^k y \in A$.

Покажем, что $x^a y^b \in A$; отсюда по индукции следует требуемое утверждение. Предположим, что $x^a y^b \notin A$, и пусть n — максимальное такое число, что $x^{n+a} y^b \notin A$. Тогда для всех $0 \leqslant i \leqslant b$ имеем

$$(x^{n+a+i} y^{b-i})^b = x^d (x^{n+a+1} y^b)^{b-i},$$

где

$$d = b(n+a+i) - (b-i)(n+a+1) = b(i-1) + i(n+a+1),$$

и, следовательно, $x^{n+a+i}y^{b-i} \in A$ для $i > 0$. Соотношение

$$x^n P = x^{n+a}y^b + \sum_{i>0} a_i x^{n+a+i}y^{b-i} \in A$$

приводит к противоречию.

13. Подойдет $A = \mathbb{K}[x_1, x_2]/(x_1^2)$, $\deg x_1 = 0$, $\deg x_2 = 1$.

14. Рассмотрим подалгебру A в $\mathbb{K}[x_1, x_2, x_3]$,

$$\deg x_1 = \deg x_2 = \deg x_3 = 1,$$

порожденную элементами $x_1^2, x_2^2, x_3^4, x_1x_2$. Тогда

$$A = \mathbb{K}[x_1^2, x_2^2, x_3^4] \oplus x_1x_2\mathbb{K}[x_1^2, x_2^2, x_3^4]$$

и

$$P(A,t) = \frac{1}{(1-t^2)^2(1-t^4)} + \frac{t^2}{(1-t^2)^2(1-t^4)} = \frac{1+t^2}{(1-t^2)^2(1-t^4)} = \frac{1}{(1-t^2)^3}.$$

Компонента A_2 порождена элементами x_1^2, x_2^2, x_1x_2, они алгебраически зависимы, поэтому алгебра A не может быть порождена тремя алгебраически независимыми элементами степени 2.

15. Если между $a_1, \ldots, a_n$ имеется полиномиальное соотношение, то каждая однородная компонента этого соотношения также является соотношением. С другой стороны, если между $a_1, \ldots, a_n$ имеется соотношение степени d, то размерность компоненты A_d меньше размерности компоненты $\mathbb{K}[x_1, \ldots, x_n]_d$, где $\deg x_i = d_i$.

16. Пусть $a_0 + a_1t + a_2t^2 + \ldots = \dfrac{b_0 + b_1t + \ldots + b_mt^m}{c_0 + c_1t + \ldots + c_nt^n}$.

Тогда при $N > \max(n, m)$ имеем $a_Nc_0 + a_{N-1}c_1 + \ldots + a_{N-n}c_n = 0$ и

$$|a_N| \leqslant \left| \frac{a_{N-1}c_1 + \ldots + a_{N-n}c_n}{c_0} \right| \leqslant qn \max(|a_{N-1}|, \ldots, |a_{N-n}|),$$

где q — константа. Таким образом, последовательность $\{a_i\}$ растет не быстрее геометрической прогрессии. Рассмотрите алгебру $A = \mathbb{K}[x_1, x_2, \ldots]$ многочленов от счетного числа переменных, в которой число образующих степени n равно $n!$ для каждого натурального n.

17. Для алгебры $A = \mathbb{K}[x, xy, xy^2, xy^3, \ldots]$, $\deg x = \deg y = 1$, ряд Пуанкаре имеет вид

$$P(A,t) = \frac{1}{(1-t)^2} - \frac{t}{1-t} = \frac{1-t+t^2}{(1-t)^2}.$$

18. Воспользуйтесь индукцией по степени многочлена. Для целозначного многочлена $F(x)$ многочлен $(\nabla F)(x) = F(x) - F(x-1)$

является целозначным и имеет меньшую степень. С другой стороны, $F(x-1)=F(x)-(\nabla F)(x)$.

19. Проведем индукцию по степени d. При $d=0$ многочлен является целой константой. При $d\geqslant 1$ рассмотрим многочлен $(\nabla F)(x)=$ $=F(x)-F(x-1)$. Этот многочлен также целозначный, и его степень ниже степени многочлена $F(x)$. Многочлен однозначно определяется своими значениями в целых точках, поэтому $F(x)$ восстанавливается по целому числу $F(0)$ и многочлену $(\nabla F)(x)$. По предположению индукции $(\nabla F)(x)$ имеет требуемый вид. Остается заметить, что $\nabla C_x^s=C_{x-1}^{s-1}$.

20. Повторите доказательство теоремы 2 для представления

$$P(A,t)=\frac{g(t)}{(1-t)^{n-r}}.$$

21. Имеем

$$P(A,t)=\frac{1}{(1-t)^4}-\frac{t^d}{(1-t)^4}=$$
$$=\frac{1-t^d}{(1-t)^4}=(1+t+\ldots+t^{d-1})\left(\sum_{s\geqslant 0}\frac{(s+2)(s+1)}{2}t^s\right),$$

следовательно,

$$H(x)=\frac{1}{2}((x+1)(x+2)+x(x+1)+\ldots+(x-d+2)(x-d+3)).$$

22. Достаточно рассмотреть алгебру, у которой p_s образующих степени s и произведение любых образующих равно нулю.

23. а) См. решение предыдущей задачи.

б) Найдите последовательность, которая растет быстрее последовательности размерностей компонент любой конечно порожденной алгебры. Например, подходит последовательность

$$p_0=p_1=1,\quad p_s=\sum_{k=1}^{[\frac{s}{2}]}p_kp_{s-k}+1.$$

24. Поскольку $p_1=2$, наша алгебра является факторалгеброй алгебры многочленов от двух переменных. Условие $p_2=2$ показывает, что есть соотношение степени 2. Следовательно, есть два соотношения степени 3 (они получаются умножением соотношения степени 2 на образующие), и поэтому $p_3\leqslant 2$.

25. Нет, рассмотрите последовательность 1, 3, 3, 4.

26. Нет,

$$p_5=152=C_9^5+C_6^4+C_5^3+C_2^2+C_0^1,$$

и

$$p_5^{\langle 5\rangle} = C_{10}^6 + C_7^5 + C_6^4 + C_3^3 + C_1^2 = 247 < p_6 = 248.$$

27. Линейная оболочка одночленов из $\mathscr{P} = \mathscr{M} \setminus (\bigcup_{s=0}^{\infty} \mathscr{M}_{p_s}^s)$ является идеалом. Поскольку любой полиномиальный идеал конечно порожден, найдется такое $m \in \mathbb{N}$, что $\mathscr{P}_{s+1} = x_1\mathscr{P}_s \cup \ldots \cup x_n\mathscr{P}_s$ для всех $s \geqslant m$. Элементы $\mathscr{P}_{s+1}$ образуют конечный отрезок множества одночленов степени $s+1$ в лексикографическом порядке, и первый элемент этого отрезка равен $x_n w$, где w — первый элемент из $\mathscr{P}_s$. Остается воспользоваться леммой 3.

28. Рассмотрим число m из предыдущей задачи. Пусть

$$p_m = C_{k(m)}^m + \ldots + C_{k(1)}^1.$$

Тогда при $s \geqslant m$ имеем

$$p_s = C_{k(m)+s-m}^s + C_{k(m-1)+s-m}^{s-1} + \ldots + C_{k(1)+s-m}^{s-m+1} = \\ = C_{k(m)+s-m}^{k(m)-m} + C_{k(m-1)+s-m}^{k(m-1)-m+1} + \ldots + C_{k(1)+s-m}^{k(1)-1}.$$

Остается положить $a_i = k(m+n-i) - (m+1-i)$.

Заметим, что мы получили новое доказательство теоремы 2.

29. Для числа p_m m-разложение Маколея имеет вид

$$p_m = C_m^m + C_{m-1}^{m-1} + \ldots + C_j^j + C_{j-2}^{j-1} + \ldots + C_0^1,$$

где $j = m - p_m + 1$. Тогда $p_m^{\langle m\rangle} = p_m \geqslant p_{m+1}$. В частности, $p_{m+1} \leqslant m+1$, и это рассуждение можно повторять.

30. Многочлен $x_2 = \dfrac{x_1 x_2}{x_1}$ также инвариантен.

31. Согласно следствию 1 достаточно проверить, что линейная оболочка указанных элементов совпадает с пространством инвариантов степени не выше $|G|$. Это следует из линейности проектора P.

32. Приведенное в тексте доказательство проходит над любым алгебраически замкнутым полем характеристики нуль. Значит, следствие 1 справедливо над алгебраическим замыканием $\bar{\mathbb{K}}$ поля $\mathbb{K}$. Пусть $f_1, \ldots, f_s$ — многочлены степени не выше $|G|$, которые порождают алгебру $\bar{\mathbb{K}}[x_1, \ldots, x_n]^G$. Поскольку у $f_1, \ldots, f_s$ число коэффициентов конечно, эти многочлены определены над конечно порожденным (и потому конечным; см. [3, гл. 9, § 5]) расширением $\mathbb{K}_1$ поля $\mathbb{K}$. Зафиксируем (конечный) базис поля $\mathbb{K}_1$ как векторного пространства над $\mathbb{K}$ и разложим коэффициенты элементов $f_1, \ldots, f_s$ по этому базису. Многочлен, члены которого совпадают с членами многочлена f_i, а коэффициенты являются коэффициентами нашего разложения при

данном базисном векторе, назовем компонентой многочлена f_i. Каждая компонента является элементом алгебры $\mathbb{K}[x_1, \ldots, x_n]$. Поскольку G — это подгруппа в $\mathrm{GL}_n(\mathbb{K})$, компоненты инвариантного многочлена также инвариантны. Проверьте, что компоненты многочленов $f_1, \ldots, f_s$ порождают алгебру $\mathbb{K}[x_1, \ldots, x_n]^G$.

33. Пусть многочлен $f(x_1, \ldots, x_n)$ является A_n-инвариантным и σ — нечетная подстановка. Тогда

$$f = \frac{f + (\sigma \cdot f)}{2} + \frac{f - (\sigma \cdot f)}{2}.$$

Проверьте, что первое слагаемое S_n-инвариантно, а второе обладает свойством $\sigma \cdot h = (\operatorname{sgn}\sigma)h$. Каждый многочлен с этим свойством меняет знак под действием транспозиции (ij), поэтому равен нулю на гиперплоскости $x_i = x_j$, и, значит, делится на $x_i - x_j$. Поэтому $\mathbb{K}[x_1, \ldots, x_n]^{A_n}$ порождается многочленом $\prod_{i>j}(x_i - x_j)$ и элементарными симметрическими многочленами. Отметим, что это решение подходит для любого поля, характеристика которого отлична от двух.

34. Предположим, что группа G действует на $\mathbb{K}[x_1, \ldots, x_n]$, умножая переменные $x_1, \ldots, x_n$ на некоторые константы. Докажите, что подалгебра инвариантов мономиальна. В данном случае условие инвариантности одночлена $x_1^{i_1}x_2^{i_2}$ — это условие делимости $k(i_1 + i_2)$ на n. Пусть наибольший общий делитель чисел k и n равен d. Тогда алгебра инвариантов порождается одночленами $x_1^{i_1}x_2^{i_2}$, где $i_1 + i_2 = \dfrac{n}{d}$.

35. Условие инвариантности одночлена: $k(i_1 - i_2)$ делится на n. Поэтому алгебра инвариантов порождается одночленами x_1x_2, x_1^s и x_2^s, где $s = \dfrac{n}{d}$ и d — наибольший общий делитель чисел k и n.

36. Рассмотрим алгебру многочленов с комплексными коэффициентами $\mathbb{C}[x_1, x_2] = \mathbb{R}[x_1, x_2] \oplus \imath\mathbb{R}[x_1, x_2]$, на которую G-действие продолжается по линейности. Положим $z = x_1 + \imath x_2$ и $\bar{z} = x_1 - \imath x_2$. Ясно, что $\mathbb{C}[x_1, x_2] = \mathbb{C}[z, \bar{z}]$ и G действует как $z \to \varepsilon z$, $\bar{z} \to \bar{\varepsilon}\bar{z}$, где ε — первообразный корень третьей степени из единицы. Отсюда следует, что алгебра инвариантов $\mathbb{C}[z, \bar{z}]^G$ порождается многочленами $z\bar{z}$, z^3 и $\bar{z}^3$. Значит, $\mathbb{R}[x_1, x_2]^G$ порождается действительными и мнимыми частями этих многочленов, т. е. $x_1^2 + x_2^2$, $x_1^3 - 3x_1x_2^2$ и $x_2^3 - 3x_1^2x_2$.

37. Напомним, что алгебра A является *целой* над своей подалгеброй B, если для любого $a \in A$ найдутся такое натуральное n и такие элементы $b_1, \ldots, b_n \in B$, что $a^n + b_1a^{n-1} + \ldots + b_n = 0$. Каждый элемент $f \in \mathbb{K}[x_1, \ldots, x_n]$ является корнем уравнения $\prod_{g\in G}(X - (g \cdot f)) = 0$, поэтому для конечной группы G алгебра $A = \mathbb{K}[x_1, \ldots, x_n]$ является целой над $B = \mathbb{K}[x_1, \ldots, x_n]^G$. Пусть B' — подалгебра в B, порожденная

коэффициентами b_i уравнений, которым удовлетворяют элементы $x_1, \ldots, x_n$. Тогда образующие алгебры A являются целыми над B', а значит, и вся алгебра A является целой над B'; см. [3, гл. 9, § 5]. Следовательно, A — конечно порожденный B'-модуль, и подмодуль B, как подмодуль конечно порожденного модуля, конечно порожден над B'. В частности, B — конечно порожденная алгебра.

Эти рассуждения составляют третье доказательство теоремы 6, которое не зависит от характеристики поля $\mathbb{K}$.

Ответ на последний вопрос отрицателен. Предположим, что характеристика поля $\mathbb{K}$ равно двум. Рассмотрим действие группы G из двух элементов на алгебре $\mathbb{K}[x_1, y_1, x_2, y_2, x_3, y_3]$, где неединичный элемент действует как

$$\begin{aligned} x_1 &\to x_1 + y_1, \quad & y_1 &\to y_1, \\ x_2 &\to x_2 + y_2, \quad & y_2 &\to y_2, \\ x_3 &\to x_3 + y_3, \quad & y_3 &\to y_3. \end{aligned}$$

Инварианты первой степени — это линейная оболочка элементов y_1, y_2 и y_3. Проверьте, что никакой инвариант второй степени не содержит член x_1x_2. Значит, инвариант

$$x_1x_2y_3 + x_1y_2x_3 + y_1x_2x_3 + x_1y_2y_3 + y_1x_2y_3 + y_1y_2x_3$$

нельзя выразить через инварианты первой и второй степени.

38. Пусть $f \in \mathbb{K}[x_1, \ldots, x_n]^G$ и $f = p_1^{k_1} \ldots p_m^{k_m}$ — разложение на неприводимые множители в алгебре $\mathbb{K}[x_1, \ldots, x_n]$. Рассмотрим представители $p_{11} = p_1, p_{12}, \ldots, p_{1r}$ классов пропорциональности множества многочленов $\{g \cdot p_1 : g \in G\}$. Многочлены p_{1i} неприводимы, f делится на каждый из них и поэтому делится на $P_1 = p_{11}p_{12}\ldots p_{1r}$. Аналогично определяются $P_2, \ldots, P_m$. Поскольку эти многочлены либо пропорциональны, либо взаимно просты, многочлен f есть произведение многочленов такого вида. Проверьте, что $g \cdot P_i = \alpha_i(g)P_i$, где $\alpha_i(g) \in \mathbb{K} \setminus \{0\}$. Тогда $\alpha_i : G \to \mathbb{K} \setminus \{0\}$ — гомоморфизм групп. В силу совпадения G со своим коммутантом такой гомоморфизм тривиален, и, значит, все многочлены P_i являются инвариантами. Проверьте, что P_i — простые элементы в $\mathbb{K}[x_1, \ldots, x_n]^G$. Наконец, для любого разложения f на простые множители в $\mathbb{K}[x_1, \ldots, x_n]^G$ один из множителей делится на p_1, а поэтому и на P_1.

Обратное утверждение неверно: рассмотрите действие группы из двух элементов на $\mathbb{K}[x]$, $x \to -x$.

39. Приведенное доказательство проходит над алгебраическим замыканием $\bar{\mathbb{K}}$ поля $\mathbb{K}$. Покажите, что

$$\dim_{\mathbb{K}} \mathbb{K}[x_1, \ldots, x_n]_m^G = \dim_{\bar{\mathbb{K}}} \bar{\mathbb{K}}[x_1, \ldots, x_n]_m^G$$

для любой подгруппы $G \subseteq \mathrm{GL}_n(\mathbb{K}) \subseteq \mathrm{GL}_n(\overline{\mathbb{K}})$.

40. Ответ: $\dfrac{(k^2-1)(k^2+11)}{720}$.

41. Пусть инвариантный многочлен F зависит от x_i. Тогда

$$F = a_k x_i^k + \ldots + a_1 x_i + a_0,$$

где $a_k, \ldots, a_1, a_0$ — многочлены, не зависящие от x_i. В силу инвариантности F относительно преобразования $x_i \to x_i + c_i y_i$ получаем

$$c_i^k y_i^k a_k + \ldots + c_i y_i a_1 + a_0 = a_0.$$

Значит, многочлены $y_i^{k-1} a_k, \ldots, a_1$ линейно зависимы с коэффициентами $c_i^{k-1}, \ldots, 1$. Выбирая k различных ненулевых значений c_i и используя формулу для определителя Вандермонда, получаем $a_k = \ldots = \ldots = a_1 = 0$, что противоречит нашему предположению.

42. Пусть $s_0, s_1, \ldots, s_k$ — конечная система порождающих. Можно считать, что все они однородны и $A_{(3b,b)} = \langle s_0^b \rangle$. Для однородного элемента $s \in A_{(a,b)}$ определим функцию $l(s) := a - 3b$. Тогда $l(s_1) > 0, \ldots, l(s_k) > 0$. Если $s_j \in A_{(a_j,b_j)}$, то зафиксируем $b > \max(b_1, \ldots, b_k)$ и рассмотрим элемент $x \in A_{(3b+1,b)} \setminus A_{(3b-2,b-1)} A_{(3,1)}$. В выражение x через $s_0, s_1, \ldots, s_k$ входит член $x' = \lambda s_1^{p_1} \ldots s_k^{p_k}$, не зависящий от s_0. Тогда

$$l(x) = 1 = l(x') = p_1 l(s_1) + \ldots + p_k l(s_k),$$

откуда ровно одно p_i равно 1, а прочие равны нулю. Это приводит к противоречию с выбором b.

43. Предположим, что алгебра $\mathbb{K}[V]^G$ конечно порождена. Действия групп G и T на алгебре многочленов перестановочны. Значит, $t \cdot f \in \mathbb{K}[V]^G$ для любых $t \in T$ и $f \in \mathbb{K}[V]^G$, и $(\mathbb{K}[V]^G)^T = \mathbb{K}[V]^H$. Если мы докажем, что для любой конечно порожденной T-инвариантной подалгебры A в алгебре многочленов алгебра инвариантов A^T конечно порождена, то получим противоречие с теоремой 8.

На первом этапе доказательства надо показать, что в A можно выбрать систему образующих, каждый из которых является T-собственным вектором. После этого алгебру A можно заменить на алгебру многочленов B, в которой переменные биективно соответствуют образующим алгебры A и T-действие на переменные совпадает с T-действием на образующие алгебры A. Алгебра B^T есть линейная оболочка одночленов, являющихся T-собственными векторами с собственным значением 1. Конечную порожденность такой алгебры можно вывести из леммы Гордана, которая утверждает, что моноид целых точек, лежащих в выпуклом рациональном полиэдральном конусе, конечно порожден.

Предметный указатель

Литература

1. *Бурбаки Н.* Коммутативная алгебра. М.: Мир, 1971.
2. *Бухштабер В. М., Панов Т. Е.* Торические действия в топологии и комбинаторике. М.: МЦНМО, 2004.
3. *Винберг Э. Б.* Курс алгебры. М.: Факториал Пресс, 2002.
4. *Винберг Э. Б., Попов В. Л.* Теория инвариантов. Итоги науки и техники // Совр. проб. математики, фунд. направления. Т. 55. М.: ВИНИТИ, 1989. С. 137—309.
5. *Гильберт Д.* Избранные труды. Т. 1—2. М.: Факториал, 1998.
6. *Крафт Х.* Геометрические методы в теории инвариантов. М.: Мир, 1987.
7. *Спрингер Т.* Теория инвариантов. М.: Мир, 1981.
8. *Arzhantsev I. V.* Algebras with finitely generated invariant subalgebras // Ann. Inst. Fourier (Grenoble). 2003. Vol. 53, № 2. P. 379—398.
9. *Bruns W., Herzog J.* Cohen-Macaulay Rings. Cambridge: Cambridge Univ. Press, 1993. (Cambridge Studies in Adv. Math.; Vol. 39).
10. *Clements G. F., Lindström B.* A generalization of a combinatorial theorem of Macaulay // J. Combin. Theory. 1969. Vol. 7. P. 230—238.
11. *Green M.* Restrictions of linear series to hyperplanes, and some results of Macaulay and Gotzmann / Eds. E. Ballico, C. Ciliberto // Algebraic curves and projective geometry. Berlin: Springer, 1989. (Lecture Notes in Math.; Vol. 1389). P. 76—86.
12. *Koras M., Russell P.* Linearization problems // Algebraic group actions and quotients / Ed. J. Wiśniewski. Hindawi Publ. Corp., 2004. P. 91—107.
13. *Macaulay F. S.* Some properties of enumeration in the theory of modular systems // Proc. London Math. Vol. 26. Soc. 1927. P. 531—555.
14. *McMullen P.* The number of faces of simplicial polytopes // Israel J. Math. 1971. Vol. 9. P. 559—570.
15. *Molien T.* Über die Invarianten der linearen Substitutionsgruppen. Sitzugsber. König. Preuss. Akad. Wiss., 1897. P. 1152-1156. (Русский перевод: *Молин Ф. Э.* Числовые системы. Новосибирск: Наука, 1985. С. 105—109.)
16. *Nagata M.* On the fourteenth problem of Hilbert // Proc. Internat. Congress Math. 1958. New York: Cambridge University Press, 1960. P. 459—462.
17. *Nagata M.* On the fourteenth problem of Hilbert // Amer. J. Math. 1959. Vol. 81. P. 766—772.
18. *Stanley R.* Hilbert functions of graded algebras // Adv. Math. 1978. Vol. 28. P. 57—83.
19. *Stanley R.* Invariants of finite groups and their applications to combinatorics // Bull. Amer. Math. Soc. 1979. Vol. 1. P. 475—511.
20. *Steinberg R.* Nagata's example // Algebraic Groups Lie Groups. Cambridge University Press, 1997. (Austral. Math. Soc. Lecture Series; Vol. 9). P. 375—384.

Аржанцев Иван Владимирович

ГРАДУИРОВАННЫЕ АЛГЕБРЫ И 14-Я ПРОБЛЕМА ГИЛЬБЕРТА

Подписано в печать 17.03.2009 г. Формат $60 \times 90\ 1/16$. Бумага офсетная.
Печать офсетная. Печ. л. 4. Тираж 1000 экз. Заказ № .

Издательство Московского центра
непрерывного математического образования.
119002, Москва, Большой Власьевский пер., д. 11. Тел. (499) 241–74–83

Отпечатано по CtP-технологии в ОАО «Печатный двор» им. А. М. Горького.
197110, Санкт-Петербург, Чкаловский проспект, 15.