ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

На правах рукописи

Волков Владислав Владимирович

ИНТЕГРАЛЬНАЯ ТЕОРЕМА КОШИ В АРИФМЕТИКЕ И АДДИТИВНОЙ КОМБИНАТОРИКЕ

Специальность 01.01.06 —
«Математическая логика, алгебра и теория чисел»

Диссертация на соискание учёной степени
кандидата физико-математических наук

Научный руководитель:
доктор физико-математических наук, профессор
Востоков Сергей Владимирович

Санкт-Петербург — 2016

Оглавление

Введение

Аналогия в математике играет двоякую роль: во-первых, способствует бурному развитию одних направлений за счёт методов и понятий уже активно разработанных в других направлениях, во-вторых, позволяет увидеть общую картину и объединить различные области в рамках некоторого более абстрактного подхода. Одним из классических примеров этого феномена является связь между теорией чисел и теорией функций, впервые отмеченная Леопольдом Кронекером: простые идеалы в кольцах алгебраических чисел играют роль аналогичную точкам римановой поверхности в теории алгебраических функций, дробные идеалы соответствуют дивизорам, сами числа соответствуют алгебраическим функциям и т. д.

Эта аналогия была также отмечена Давидом Гильбертом. Он замечал, что его закон взаимности произведения символов норменного вычета:

$$\prod_{\mathfrak{P}} (a,b)_{r,\mathfrak{P}} = 1\,,$$

напоминает интегральную теорему Коши об обнулении интеграла функции охватывающего все её особые точки. Напомним, что самим Гильбертом данный закон был исследован в квадратичном случае (в котором он равнозначен обычному квадратичному закону взаимности для символов Лежандра) и позже был обобщён в работах Н. Г. Чеботарёва, Э. Артина и Г. Хассе.

И. Р. Шафаревич в своей работе [1] даёт уточнение: закон взаимности Гильберта аналогичен следствию интегральной теоремы Коши, которое гласит, что сумма вычетов мероморфной 1-формы на компактной римановой поверхности равна нулю. Аналитически этот результат может быть описан следующим образом: пусть ω — мероморфная (т. е. голоморфная вне некоторого конечного множества своих полюсов S, где она имеет вычеты конечного порядка) 1-форма на римановой поверхности C, и $S = \{p_1, p_2 \dots, p_n\}$ — её полюса. Тогда

$$\sum_{i=1}^{n} \operatorname{res}_{p_i} \omega = 0.$$

Этот результат легко выводится из теоремы Коши, гласящей, что

$$\operatorname{res}_p \omega = 2\pi i \oint_{\gamma_p} \omega,$$

где γ_p — контур вокруг точки p, не содержащий полюсов ω, кроме p. И. Р. Шафаревич также отмечает, что с этой точки зрения символ Гильберта $(a,b)_{r,\mathfrak{P}}$ играет роль вычета некоторого дифференциала в точке $\mathfrak{P}$. Как и в случае вычета дифференциала значение символа $(a,b)_{r,\mathfrak{P}}$ зависит лишь от поведения a и b в точке $\mathfrak{P}$, то есть от разложения a и b в $\mathfrak{P}$-адические ряды. Тем не менее его классические определения, включая приведённое выше, имеют мало общего с данной аналогией и зависят от свойств всего поля Γ (или его $\mathfrak{P}$-пополнения K). Отсюда возникает задача построения символа $(a,b)_{r,\mathfrak{P}}$, а впоследствии и всей локальной теории полей классов, более явным и естественным образом. Эта задача решается с помощью получения явных формул для символа $(a,b)_{r,\mathfrak{P}}$ и его переопределения через данные формулы в виде вычета некоторого ряда.

Забегая вперёд отметим, что данная аналогия была развита в работе С. В. Востокова и М. А. Иванова [2]. В ней явная формула символа была построена с помощью интеграла Шнирельмана, являющегося прямым аналогом контурного интеграла, и с её помощью прояснена вышеописанная аналогия для кругового поля. В данной работе для некоторых специальных функций $\Phi(\alpha,\beta)$ и s показано, что

$$\int_{0,p} \Phi(\alpha,\beta)/s = \operatorname{res}_X(\Phi(\alpha,\beta)/s),$$
$$(\alpha,\beta)_{n,K} = \zeta^{\int_{0,p}\Phi(\alpha,\beta)},$$

где $\int_{0,p}$ — интеграл Шнирельмана, $(\cdot,\cdot)_{n,K}$ — локальный символ Гильберта порядка n, ζ — первообразный корень степени p^n из единицы содержащийся в поле K. Отсюда для кругового поля $\mathbb{Q}(\zeta)$ выводится следующий результат:

$$\begin{array}{ccc}
\left(\dfrac{\alpha}{\beta}\right)_{p^n}\left(\dfrac{\beta}{\alpha}\right)_{p^n}^{-1} & = & \zeta^{\int \Phi(\alpha,\beta)/s} \\
\| & & \| \\
\left(\dfrac{\alpha,\,\beta}{\zeta-1}\right)_{p^n} & = & \zeta^{\operatorname{res}\Phi(\alpha,\beta)/s},
\end{array}$$

где в левом столбце оказывается закон взаимности, а в правой аналог теоремы Коши.

Задача построения явных формул, описанных выше, для символа Гильберта имеет долгую историю. Её началом можно считать ещё работу Э. Куммера [3], результат которой на современном языке выглядел бы именно как явная формула для символа Гильберта между определёнными элементами кругового расширения поля p-адических чисел. Несколько другой тип явных формул имеет свои корни в работе Артина и Хассе 1928 года [4]. Дальнейшее развитие построения явных формул для символа Гильберта шло по этим двум направлениям — формул типа Артина-Хассе и типа Куммера. Формулы типа Куммера представляют символ Гильберта в виде вычета определённого ряда. В формулах типа Артина-Хассе символ Гильберта выражается через след некоторого элемента, при этом на нормирование второго аргумента накладывается некоторое ограничение, делающее формулы неполными.

Направление формул Артина-Хассе было развито в круговом поле $\mathbb{Q}_p(\zeta)$ К. Ивасавой [5], а в дальнейшем в произвольном локальном поле — Ш. Сеном [6]. Дальнейшие успехи были достигнуты в случае символа Гильберта, определённого относительно формальной группы. А. Уайлс получил формулу типа Артина-Хассе для формальных групп Любина-Тейта [7] для поля деления изогении $[\pi^m]$ и А. В. Колывагин [8] для полей, содержащих поле деления изогении $[\pi^m]$. В мультипликативном случае и в случае формальных групп Любина-Тейта продвижения были также получены Р. Коулманом [9]. Выдвинутая им гипотеза о виде формулы в общем случае формальных групп Любина-Тейта была доказана А. Де Шалитом [10]. Ф. Детрам [11] обобщил формулы Сена на случай формальных групп Любина-Тейта, а Д. Бенуа [12] — на случай p-делимых групп.

Формулы Куммеровского типа получили своё продолжение в работе И. Р. Шафаревича [1]. С помощью теоремы Гензеля [13] Шафаревич построил специальный базис группы главных единиц, и, пользуясь разложением по этому базису, дал явное определение символа Гильберта в виде вычета некоторого ряда. Более элементарные формулы в общем случае были получены в конце семидесятых годов независимо С. В. Востоковым [14] и Г. Брюкнером [15]. В работе Востокова был преобразован и развит подход, использованный Шафаревичем. Метод, предложенный в этой работе, был впоследствии успешно применён в значительном количестве других важных случаев. Изложим подробнее основные шаги этого метода.

1. В соответствующем модуле (модуль формальной группы либо мультипликативная группа поля) строится система образующих, называемая обычно системой образующих Гензеля или базисом Шафаревича (построение проводится по аналогии с методом, использованным Шафаревичем для построения базиса в работе [1]).
2. На кольце рядов строится формальное спаривание $\langle\cdot,\cdot\rangle$, заданное явной формулой как вычет некоторого ряда. Это спаривание определяется между формальными аналогами объектов, на которых задан символ Гильберта. Проверяется линейность и символьное свойство для формального спаривания. Затем с помощью разложения элементов поля K в ряды по простому элементу формальное спаривание проектируется на K до спаривания $\{\cdot,\cdot\}$. Проверяется корректность этой проекции, независимость результата от конкретного разложения в ряд и выбора простого элемента.
3. Полученное спаривание $\{\cdot,\cdot\}$ вычисляется на элементах системы образующих Гензеля, и на них проверяется её совпадение с символом Гильберта.
4. Совпадение спаривания $\{\cdot,\cdot\}$ и символа Гильберта проверяется на всех элементах с помощью независимости явного спаривания. Это, в свою очередь, даёт явную формулу символа Гильберта.

Подобная схема была использована при построении формул типа Куммера в работах [16—20] для формальных групп Любина-Тейта, в работе [21] для относительных формальных групп Любина-Тейта, в работах [22; 23] для формальных групп Хонды, в работе [24] для обобщенных формальных групп Любина-Тейта и в ряде работ посвященных многомерному локальному полю, речь о котором пойдёт ниже.

Для полноты изложения необходимо отметить, что альтернативный подход к явным формулам типа Куммера был получен В. А. Абрашкиным в работе [25] и развит Ф. Таваресом Рибейру [26].

Теория полей классов для многомерного локального поля была построена в конце семидесятых годов независимо в случае нулевой характеристики К. Като в серии работ [27—30] и более явным образом, с учётом топологии в случае ненулевой характеристики А. Н. Паршиным [31—34]. В этих работах было построено отображение Паршина-Като, выполняющее роль отображения взаимности многомерной локальной теории полей классов. А именно, для n-мерного локального поля K существует изоморфизм

$$\Xi\colon K_n(K^*) \to \mathrm{Gal}(K^{ab}/K)\,,$$

где $K_n(K^*)$ — K-группа Милнора, K^{ab} — максимальное абелево расширение поля K. Так же как и в одномерном случае с помощью отображения Ξ можно задать символ Гильберта (как мультипликативный, так и относительно некоторой формальной группы).

Явные формулы для мультипликативного случая в многомерном разнохарактеристическом поле построил Востоков в работе [35], адаптировав описанный выше метод. Эти формулы, в частности, сыграли важную роль в явном построении локальной теории полей классов многомерного разнохарактеристического поля, проведённом И. Б. Фесенко [36]. В дальнейшем для многомерного поля явные формулы были также построены в работе [37] для поля смешанной характеристики, в работах [38; 39] для полей конечной характеристики с квазиконечным и совершенным полем вычетов, в работах [40; 41] для формальных групп Хонды, в работе [42] для формальных групп Любина-Тейта.

В первой главе данной работы метод, описанный выше, применяется для получения явной формулы подобного рода для многочленной формальной группы $F_c(X,Y) = X+Y+cXY$, где c — единица в поле K, но при этом c не обязан лежать в подполе инерции T поля K (что отличает данную группу от раннее рассматриваемых). Тем самым символ Гильберта относительно формальной группы F_c представляется в виде вычета определённого ряда, и для данных групп также прослеживается аналогия со следствием теоремы Коши.

Другой интересной специализацией теоремы Коши о вычетах является комбинаторная теорема о нулях (Combinatotial Nullstellensatz).

Теорема (Алон). *Пусть $\mathbb{F}$ — произвольное поле и пусть $F = F(x_1, \dots, x_n)$ многочлен из $\mathbb{F}[x_1, x_2, \dots, x_n]$. Предположим также, что степень* $\deg(F)$ *многочлена F равна $\sum_{i=1}^{n} d_i$, где d_i — целые неотрицательные числа. Пусть кроме того, коэффициент при мономе $\prod x_i^{d_i}$ в F не равен нулю. Тогда если множества $C_1, C_2, \dots, C_n \subset \mathbb{F}$ таковы, что $|C_i| > d_i$, то найдутся такие $c_1 \in C_1$,*

$\ldots$, $c_n \in C_n$, *что*

$$F(c_1, \ldots, c_n) \neq 0.$$

Несмотря на свою достаточно короткую историю, этот результат успел зарекомендовать себя в качестве мощного инструмента в комбинаторике. Впервые метод, утилизирующий идеи, лежащие в основе комбинаторной теоремы о нулях, был представлен в работе [43] в 1996 году и использован для получения новых вариантов теоремы Коши-Девенпорта. В 1999 Н. Алон [44] кристаллизовал эти идеи в виде комбинаторной теоремы о нулях и продемонстрировал широкий спектр её возможностей в ряде областей комбинаторики. Например, им было получено короткое и элементарное доказательство результата о том, что любой планарный двудольный граф является 3-списочным, а также теоремы Эрдёша-Гинзбурга-Зива. Версия теоремы использованная Н. Алоном несколько отличается от интересующей нас в данной работе и содержит лишь утверждение об обнулении коэффициента в случае обнуления всех соответствующих значений функции, а не явную формулу описывающую коэффициент. Последняя была независимо получена М. Ласоном [45] и Р. Н. Карасёвым и Ф. В. Петровым [46]. Этот вариант формулы гласит, что для произвольного многочлена $F \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ степени не выше $\deg(F) \leq d_1 + d_2 + \cdots + d_n$, где $\mathbb{F}$ — некоторое поле, и множеств $C_1, C_2, \ldots, C_n$ в $\mathbb{F}$ таких, что $|C_i| = d_i + 1$, коэффициент при мономе $\prod x_i^{d_i}$ может быть выражен следующим образом

$$[\prod x_i^{d_i}]F = \sum_{c_1 \in C_1} \sum_{c_2 \in C_2} \cdots \sum_{c_n \in C_n} \frac{F(c_1, c_2, \ldots, c_n)}{\phi_1'(c_1)\phi_2'(c_2)\ldots\phi_n'(c_n)}, \tag{1}$$

где $[\prod x_i^{d_i}]F$ обозначает коэффициент при мономе $\prod x_i^{d_i}$ многочлена F и $\phi_i(z) = \prod_{c \in C_i}(z - c)$.

Среди значительных результатов, полученных с помощью этого метода, необходимо отметить решение гипотезы Эрдёша-Гейльбронна [47], решение одной из гипотез Сневиля [48] и гипотезу Какеи над конечными полями [49].

Интересным вопросом является понимание алгебраической природы комбинаторной теоремы о нулях. В частности удачное обобщение результата могло бы найти применение в получении нового подхода к таким результатам как соотношения Макдональда над системами корней. Н. Алон в своей работе [44] проводил аналогию между комбинаторной теоремой о нулях и теоремой Гильберта о нулях (отсюда и название), так как основная лемма в представленном им доказательстве теоремы являлась усилением теоремы Гильберта в некотором частном случае. В работе [46] была предложена аналогия с интерполяционной формулой Лагранжа, которая и привела к формуле (1). Р. Н. Карасёвым [50] было отмечено, что по своей сути формула (1) есть вариант теоремы Коши о вычетах. Более того, в случае комплексного поля им был представлен прямой вывод комбинаторной теоремы о нулях 1, из следующей формы теоремы о вычетах.

Теорема. *Пусть $D_1, \ldots, D_n$ дивизоры на компактном аналитическом многообразии M размерности n, пересечение которых имеет нулевую размерность. Тогда для любой голоморфной формы $\omega \in \Omega^n(M \setminus \cup_{i=1}^n D_i)$ имеет место соотношение:*

$$\sum_{x \in D_1 \cap \ldots \cap D_n} \operatorname{res}_x \omega = 0.$$

Аналогичный результат верен для любого алгебраически замкнутого поля, и соответствующая интерпретация комбинаторной теоремы о нулях продолжается, соответственно, естественным образом.

Также можно отметить, что формула (1) следует из основного результата работы [51], который был получен в качестве обобщения формулы Эйлера-Якоби.

Во второй главе подробно приводятся различные варианты комбинаторной теоремы о нулях и одно новое её обобщение. Также в подробностях рассматриваются её применение к различным областям комбинаторики и даются некоторые новые варианты теоремы Коши-Девенпорта.

Последняя глава работы посвящена применению новой версии комбинаторной теоремы о нулях, описанной во второй главе, к гипотезе Форрестера, сформулированной в виде соотношения на свободной член определённой рациональной функции, и ряду смежных результатов. Тем самым положительным образом решается гипотеза высказанная Форрестером [52] и в едином стиле устанавливается подход ко многим аналогичным соотношениям. Ниже приводится краткая история вопроса этих соотношений.

Пожалуй, наиболее известным из соотношений, о семействе которых пойдет речь ниже, является соотношение Дайсона. В 1962 году Ф. Дайсон [53] предложил заменить классические модели случайных матриц Вигнера (основанные на распределении Гаусса) тем, что сейчас носит название круговых ансамблей.

Изучение плотности совместного распределения их собственных чисел привело Дайсона к следующей гипотезе. Рассмотрим семейство многочленов Лорана:

$$\mathcal{D}(\boldsymbol{x};\boldsymbol{a}) := \prod_{1\le i\ne j\le n}\left(1-\frac{x_i}{x_j}\right)^{a_i}$$

параметризованное набором неотрицательных целых чисел $\boldsymbol{a}=(a_1,\ldots,a_n)$, где $\boldsymbol{x}=(x_1,\ldots,x_n)$ — независимые переменные. Обозначая через $\mathrm{CT}[\mathcal{L}(\boldsymbol{x})]$ свободный член многочлена Лорана $\mathcal{L}=\mathcal{L}(\boldsymbol{x})$, гипотезу Дайсона можно переписать в виде соотношения:

$$\mathrm{CT}[\mathcal{D}(\boldsymbol{x};\boldsymbol{a})] = \frac{(a_1+a_2+\cdots+a_n)!}{a_1!a_2!\ldots a_n!} =: \binom{|\boldsymbol{a}|}{\boldsymbol{a}},$$

где $|\boldsymbol{a}|=a_1+a_2+\cdots+a_n$.

Гипотеза Дайсона была доказана Д. Гансоном [не опубликовано] и К. Вилсоном [54] в том же году. Среди других доказательств можно отметить метод И. Гуда, основанный на интерполяции Лагранжа.

В 1975 году Г. Эндрюс [55] выдвинул в качестве гипотезы q-аналог соотношения Дайсона. Эта версия соотношения оказалось куда сложнее и, несморя на ряд предпринятых попыток [56—58], задача была решена лишь в 1985 году в работе Д. Зейлбергера и Д. Брессоуда [59]. Более короткие доказательства были получены Гесселем и Ксином [60], а также Каем [61]. В 2012 году вариант комбинаторный теоремы о нулях предложенный Р. Н. Карасёвым и Ф. В. Петровым [46], привел к очень короткому доказательству q-версии соотношения Дайсона в работе Г. Каройи и З. Нади [62].

Соотношения на свободный член полинома подобные соотношению Дайсона тесно связаны с интегральной формулой Селберга [63]:

$$S_n(\alpha,\beta,\gamma) := \int_0^1\ldots\int_0^1\prod_{i=1}^{n} t_i^{\alpha-1}(1-t_i)^{\beta-1}\prod_{1\le i<j\le n}|t_i-t_j|^{2\gamma}dt_1\ldots dt_n$$
$$=\prod_{j=0}^{n-1}\frac{\Gamma(\alpha+j\gamma)\Gamma(\beta+j\gamma)\Gamma(1+(j+1)\gamma)}{\Gamma(\alpha+\beta+(n+j-1)\gamma)\Gamma(1+\gamma)},$$

где комплексные параметры α, β, γ удовлетворяют условиям:

$$\Re(\alpha) > 0,\, \Re(\beta) > 0,\, \Re(\gamma) > -\min\{1/n, \Re(\alpha)/(n-1), \Re(\beta)/(n-1)\}.$$

Интерес к этой формуле (проявляемый например в недавней работе [64]) вызван её глубокой связью с теорией случайных матриц, статистической механикой, специальной теорией функции и другими областями. Исчерпывающий обзор можно найти в [65]. Для нас же интересна равносильная переформулировка интегральной формулы Селберга в виде соотношения Морриса:

$$\mathrm{CT}\left[\prod_{j=1}^{n}(1-x_j)^a(1-1/x_j)^b\mathcal{D}(\boldsymbol{x};k)\right] = \prod_{j=0}^{n-1}\frac{(a+b+kj)!(kj+k)!}{(a+kj)!(b+kj)!k!},$$

где параметры a, b, k являются целыми неотрицательными числами (подробности приведены в работе [66]).

В 1987 году Аомото [67] доказал расширенную версию интегральной формулы Селберга. Используя формулу Ньютона-Лейбница, Аомото получил одно из простейших известных доказательств формулы Селберга (среди других элементарных доказательств можно отметить подход Андерсона [68]). Равносильная переформулировка формулы Аомото в виде соотношения на свободный член полинома имеет следующий вид:

$$\mathrm{CT}\left[\prod_{j=1}^{n}(1-x_j)^{a+\chi(j\le m)}(1-1/x_j)^b\mathcal{D}(\boldsymbol{x};k)\right] = \\ = \prod_{j=0}^{n-1}\frac{(a+b+kj+\chi(j\ge n-m))!(kj+k)!}{(a+kj+\chi(j\ge n-m))!(b+kj)!k!}, \quad (2)$$

где $\chi(S)$ — логическая функция истинности утверждения S.

Квантовая система многих тел Каложеро-Сатерленда бесспиновых квантовых частиц на единичном круге, взаимодействующих через $1/r^2$ потенциал, для двух тел тесно связана с теорией случайных матриц, в частности с моделью Дайсона Броуновского движения [69]. Детали описаны, например, в [70, Глава 11]. Обобщения включающие внутренние степени свободы частиц были сформулированы в начале 1990-х годов. В своей работе 1995 года [52] Форрестер начал изучение аналога интегральной формулы Селберга для соответствующей точной волновой функции основного состояния. Представленный в виде свободного члена полинома Лорана

$$\mathcal{F}(\boldsymbol{x}; n_0; a,b,k) = \mathcal{M}(\boldsymbol{x}; a,b,k) \prod_{n_0<i\neq j\leq n} \left(1 - \frac{x_i}{x_j}\right),$$

где $\mathcal{M}(\boldsymbol{x}; a,b,k)$ — полином из соотношения Морриса, нормирующий множитель для наиболее интересного случая может быть переписан в виде следующего гипотетического тождества:

$$\begin{aligned}
&\mathrm{CT}\left[\mathcal{F}(\boldsymbol{x}; n_0; a,b,k)\right] = \\
&= M(n_0; a,b,k) \times \prod_{j=0}^{n-n_0-1} \frac{(j+1)(a+b+kn_0+(k+1)j)!(kn_0+(k+1)j+k)!}{(a+kn_0+(k+1)j)!(b+kn_0+(k+1)j)!k!}.
\end{aligned}$$

В работе [71] был сформулирован и изучался q-аналог описанной выше гипотезы Форрестера. Несмотря на ряд предпринятых попыток [72—78], эти гипотезы были доказаны лишь в некоторых конкретных случаях. В третьей главе данной работы получено полное доказательство гипотезы Форрестера и её q-версии, основанное на комбинаторной теореме о нулях.

Целью работы является: построение явной формулы символа Гильберта $(\cdot,\cdot)_c$ относительно многочленной формальной группы $F_c(X,Y) = X+Y+cXY$, где c — единица в поле K, для одномерного локального поля и многомерного разнохарактеристического локального поля, которая известным образом приводит к явному закону взаимности относительно данной формальной группы; изучение приложений комбинаторной теоремы о нулях в алгебраической комбинаторике; изучение обобщений комбинаторной теоремы о нулях и её применение к вопросам соотношений на свободные члены полиномов Лорана.

Актуальность исследования вопросов, рассмотренных в первой главе, подтверждается большим количеством работ многих известных математиков, посвященных явным формулам символа Гильберта, конструктивным подходам к локальной теории полей классов, и связанными с этими вопросами приложениями в криптографии. Актуальность второй и третьей главы подтверждается текущим бурным развитием рассматриваемой области, множеством работ, посвященных различным приложениям комбинаторной теоремы о нулях в алгебраической комбинаторике, а также связью полученных результатов с теоретической квантовой физикой, в которой и была поставлена гипотеза Форрестера.

Научная новизна: впервые явные формулы символа Гильберта получены для формальной группы, коэффициенты которой не обязаны лежать в подполе инерции поля K. Получены новые обобщения комбинаторной теоремы о нулях. Дан положительный ответ на гипотезу Форрестера, являвшуюся до этого момента открытой с конца 90х годов. Все основные результаты, представленные в работе, являются оригинальными.

Теоретическая и практическая значимость. Работа носит теоретический характер. Результаты первой главы работы могут быть использованы в дальнейших исследованиях явных форм символа Гильберта в более общих случаях и для построения конструктивного подхода к локальным теориям полей классов по аналогии с мультипликативным случаем. Результаты второй и третьей главы могут быть использованы для приложений в комбинаторике и соотношениях по типу Дайсона, играющих важную роль в моделях случайных матриц, подтверждение гипотезы Форрестера важно также для теоретической квантовой физики.

Методология и методы исследования. В работе используются методы общей теории локальных полей, локальной теории полей классов и теории формальных групп, а также полиномиальный метод в комбинаторике. Работа утилизирует подход к явным формулам Гильберта Куммеровского типа, представленный С. В. Востоковым, а также комбинаторную теорему о нулях в форме, представленной Р. Н. Карасёвым и Ф. В. Петровым.

Основные положения, выносимые на защиту:

1. Явная формула символа Гильберта $(\cdot,\cdot)_c$ многочленной формальной группы F_c в разнохарактеристическом многомерном локальном поле.
2. Обобщение комбинаторной теоремы о нулях для аффинных гиперповерхностей.
3. Обобщение комбинаторной теоремы о нулях на Эрмитову интерполяцию.
4. Неравенство Коши-Дэвенпорта для алгебраической сложности.
5. Положительный ответ на гипотезу Форрестера.

Достоверность результатов и апробация работы. Достоверность полученных результатов обеспечивается их строгим математическим доказательством. Основные результаты работы докладывались на Санкт-Петербургском алгебраическом семинаре имени Д. К. Фаддеева, на Санкт-Петербургском семинаре по формальным группам и теории ветвления (рук. проф. С. В. Востоков) и в виде выносного доклада на международной конференции «Arithmetic Days» (2013). Результаты находятся в соответствии с результатами, полученными другими авторами.

Публикации. Основные результаты по теме диссертации изложены в рецензируемых научных изданиях [79—83], рекомендованных ВАК. Работы [79—83] написаны в соавторстве. В работе [79] диссертанту принадлежат построение формального спаривания, док-во основной леммы и проекция формального спаривания на числа (разделы 3, 5, 7, 8), остальные результаты получены совместно. В работах [80; 81] диссертантом получены независимость спаривания от разложения в аргументы, лемма о замене переменной и основная теорема (разделы 4, 5, 6 работы [81]), остальные результаты получены совместно. В работе [82] диссертанту принадлежат результаты изложенные в §1, результаты §2 получены Ф. В. Петровым. В работе [83] общий план и основной результат в виде доказательства гипотезы Форрестера были получены независимо диссертантом совместно с Ф. В. Петровым, и Г. Каройи совместно с З. Нади. В частности диссертантом получена версия комбинаторной теоремы о нулях с Эрмитовой интерполяцией (теорема 2.4), Ф. В. Петрову принадлежит идея тензорного подхода к подобным теоремам (лемма 2.1), остальные части доказательства получены ими совместно. Г. Каройи и З. Надю принадлежит альтернативный подход к последнему шагу доказательства основного тождества, изложенный в пункте 7.4. Совместно всеми авторами получены остальные части работы, в частности обобщение гипотезы Форрестера в виде тождества Аомото-Форрестера (теорема 6.2). С. В. Востокову принадлежит общее руководство диссертационной работой.

Объем и структура работы. Диссертация состоит из введения и трёх глав. Полный объём диссертации составляет 86 страниц. Список литературы содержит 111 наименований.

Первая глава посвящена основным определениям, вспомогательным сведениям и ранее известным результатам, которые будут необходимы в последующих главах.

Во второй главе рассматривается многочленная формальная группа F_c над разнохарактеристическим многомерным локальным полем K. Основным результатом главы является получение явной формулы символа Гильберта относительно этой формальной группы.

Третья глава посвящена обобщениям комбинаторной теоремы о нулях и её приложениям в комбинаторике. Основными результатами данной главы являются комбинаторная теорема о нулях для мультимножеств (с помощью Эрмитовой интерполяции), версия комбинаторной теоремы о нулях для аффинных гиперповерхностей, а также следующее из неё неравенство Коши-Дэвенпорта для алгебраической сложности.

Последняя четвертая глава посвящена применению комбинаторной теоремы о нулях к задачам соотношений на свободный член. Здесь основным результатом является соотношение Аомото-Форрестера, из которого, в частности, следует положительный ответ на гипотезу Форрестера.

Глава 1. Определения и предварительные результаты

1.1 Многочленный формальный модуль

В данном разделе будут перечислены обозначения и известные классические результаты, используемые в главе 2.

Сама глава посвящена построению явной формулы символа Гильберта относительно многочленной формальной группы $F_c = X + Y + cXY$.

В этой части работы p — нечётное простое число; n, m, e — натуральные числа; i, j, r — целые числа. Через K^{ab} будем обозначать максимальное абелево расширение поля K. Под словом кольцо будем всегда понимать коммутативное кольцо. Через $\mathbb{Q}_p$ будем обозначать поле p-адических чисел, через $\mathbb{Z}_p$ — кольцо p-адических чисел.

Пусть

- K — n-мерное разнохарактеристическое локальное поле, с кольцом целых относительно n-мерного нормирования $\mathcal{O}_K$. K является конечным расширением поля вида $k\{\{t_1\}\}\ldots\{\{t_{n-1}\}\}$, где k — одномерное локальное поле;
- $K^{(0)}, K^{(1)}, \ldots, K^{(n)} = K$ — поля вычетов многомерного поля K;
- ζ — корень p^m-ой степени из единицы, содержащийся в K;
- $t_1, \ldots, t_{n-1}, \pi$ — система локальных параметров поля K;
- $(e_1, \ldots, e_n)$ — индекс ветвления поля K, то есть n-мерное нормирование числа p в поле K;
- $e'_i = e_i/(p-1)$;
- c — единица локального поля K;
- $\mathcal{O}_T = W(K^{(0)})$ — кольцо векторов Витта над полем $K^{(0)}$;
- T — подполе инерции в K (то есть $\mathrm{Quot}(W(K^{(0)})$, где), с кольцом целых $\mathcal{O}_T$;
- $\triangle$ — автоморфизм Фробениуса в $T/\mathbb{Q}_p$;
- tr — оператор следа в $T/\mathbb{Q}_p$;
- $\mathfrak{M}$ — максимальный идеал $\mathcal{O}_K$;

- $\mathfrak{R}$ — мультипликативная система представителей Тейхмюллера поля вычетов $K^{(0)}$ в кольце $\mathcal{O}_T$;

Формальная группа $F_c = X + Y + cXY$ задаёт формальный $\mathbb{Z}_p$-модуль $F_c(\mathfrak{M})$ на идеале $\mathfrak{M}$ и элемент $\xi = c^{-1}(\zeta - 1)$ является образующим ядра изогении $[p^m]_c(X)$ относительно действия группы F_c.

Рассмотрим кольцо рядов $\mathcal{O}_T\{\{t_1\}\}\{\{t_2\}\}\ldots\{\{t_{n-1}\}\}((t_n))$, где t_n — переменная, независимая от $t_1, \ldots, t_{n-1}$. Подстановкой $t_n = \pi$ это кольцо отображается в поле K:

$$\begin{aligned}\nu_t\colon \mathcal{O}_T\{\{t_1\}\}\{\{t_2\}\}\ldots\{\{t_{n-1}\}\}((t_n)) &\to K\\ \sum_{r\in I} a_r t_1^{r_1}\ldots t_n^{r_n} &\mapsto \sum_{r\in I} a_r t_1^{r_1}\ldots \pi^{r_n}\,,\end{aligned}$$

где $a_r \in \mathcal{O}_T$. Отображение ν_t сюръективно, поэтому для любого элемента из K можно найти прообраз в кольце рядов (неканоническим образом).

Через $\mathcal{O}_T\{\{t_1\}\}\ldots\{\{t_{n-1}\}\}[[t_n]]_1$ мы будем обозначать множество рядов лексикографической степени не ниже $(1, 0, 0, \ldots, 0)$ по $t_1, \ldots, t_n$.

Нам понадобится группа рядов $\mathcal{H}_{\mathfrak{m}} = \langle t_1\rangle \times \ldots \times \langle t_n\rangle \times \mathfrak{R} \times (1 + \mathcal{O}_T\{\{t_1\}\}\ldots\{\{t_{n-1}\}\}[[t_n]]_1)$ и кольцо $\mathcal{H}_{\mathrm{c}} = \mathcal{O}_T\{\{t_1\}\}\ldots\{\{t_{n-1}\}\}[[t_n]]_1$.

Оператор $\triangle$ можно продолжить на всё кольцо рядов $\mathcal{O}_T\{\{t_1\}\}\{\{t_2\}\}\ldots\{\{t_{n-1}\}\}((t_n))$ следующим образом:

$$\triangle\,(\sum_{r\in I} a_r t_1^{r_1}\ldots t_n^{r_n}) = \sum_{r\in I} a_r^{\triangle} t_1^{pr_1}\ldots t_n^{pr_n}\,.$$

Фиксируем некоторые ряды $\underline{c}, \underline{\zeta} \in \mathcal{H}_{\mathfrak{m}}$, $\underline{\xi} = \underline{c}^{-1}(\underline{\zeta} - 1)$ такие, что $\underline{c}(\pi) = c$, $\underline{\zeta}(\pi) = \zeta$, $\underline{\xi}(\pi) = \xi$.

На кольце рядов $\mathcal{O}_T\{\{t_1\}\}\{\{t_2\}\}\ldots\{\{t_{n-1}\}\}((t_n))$ можно задать действие группой $F_{\underline{c}} = X + Y + \underline{c}XY$, которую впоследствии будем обозначать просто F_c, так как из контекста будет ясно, идёт ли речь о рядах или о числах.

Оператор дифференцирования по t_i будем обозначать через ∂_i.

Нам также понадобятся мультипликативные функции Артина-Хассе E, ℓ для многомерного поля K, которые были введены в работе [35], §1.

1.1.1 Вспомогательные ряды

В работе [14], §3 были определены следующие ряды:

- $s_i = \underline{\zeta}^{p^i} - 1$;
- $s = s_m$;
- $u = s/s_{m-1}$.

Нам также понадобятся аналогичные ряды для формальной группы F_c:

- $s_{c,i} = [p^i]_c(\underline{\xi}) = \underline{c}^{-1}s_i$;
- $s_c = s_{c,m}$;
- $u_c = s_{c,m}/s_{c,m-1} = s/s_{m-1} = u$.

Ряд u служит в качестве “минимального” ряда обнуляющего элемент π. А именно, из построения очевидно, что $u(\pi) = 0$, но, более того, в [14], §3, лемма 6 показано, что любой другой ряд, обнуляющий π, делится на u. Как отмечено в работе [35] этот результат без труда переносится на многомерный случай.

Лемма 1. *Пусть $\nu \in \mathcal{O}_T\{\{t_1\}\}\dots\{\{t_{n-1}\}\}[[t_n]]$ такой ряд, что $\nu(\pi) = 0$, тогда найдется ряд $\mu \in \mathcal{O}_T\{\{t_1\}\}\dots\{\{t_{n-1}\}\}[[t_n]]$ такой, что*

$$\nu(t) = u(t)\mu(t)\,.$$

Кроме того, для всех $1 \leqslant i \leqslant n$ выполнены следующие легко проверяемые соотношения

$$\partial_i\gamma^{\Delta} = pt_i^{-1}(t_i\partial_i\gamma)^{\Delta} \tag{1.1}$$

$$\partial_i\ell(\gamma) = \gamma^{-1}\partial_i\gamma - t_i^{-1}(t_i\gamma^{-1}\partial_i\gamma)^{\Delta}\,. \tag{1.2}$$

Таким образом, корректно определены функции δ_i, η_i:

$$\delta_i(\gamma) = \gamma^{-1}\partial_i\gamma\,, \tag{1.3}$$

$$\eta_i(\gamma) = t_i^{-1}(t_i\delta_i(\gamma))^{\Delta} = \delta_i(\gamma) - \partial_i\ell(\gamma)\,. \tag{1.4}$$

Нам также понадобится удобная порождающая система в $K_n(\mathcal{H}_\mathfrak{m})/K_n(\mathcal{H}_\mathfrak{m})^{p^m}$. Аналогично [34], раздел 2, предложению 1 (пользуясь структурой $\mathcal{H}_\mathfrak{m}\,/\,{\mathcal{H}_\mathfrak{m}}^{p^m}$, по аналогии с [35], §1, 2°) можно получить следующее утверждение.

Предложение 1. *Элементы вида*

1. $\{t_1, \ldots, t_n\}$,

2. $\{t_1, \ldots, t_{i-1}, \varepsilon, t_{i+1} \ldots, t_n\}$, *где* $\varepsilon \in 1 + \mathcal{O}_T\{\{t_1\}\} \ldots \{\{t_{i-1}\}\}[[t_i]]_1$.

образуют порождающую систему в $K_n(\mathcal{H}_\mathfrak{m})/K_n(\mathcal{H}_\mathfrak{m})^{p^m}$.

1.1.2 Символ Гильберта

В многомерном случае спаривание Гильберта $(\cdot,\cdot)_c$ опирается на отображение Паршина-Като Ξ (отображение взаимности многомерной локальной теории полей классов):

$$\Xi\colon K_n(K^*) \to \mathrm{Gal}(K^{ab}/K)\,,$$

где K_n — K-группа Милнора. Символ Гильберта $(\cdot,\cdot)_c$ задаётся аналогичным образом:

$$(\alpha, \beta)_c = [p^m]_c^{-1}(\beta)^{\Xi(\alpha)} -_{F_c} [p^m]_c^{-1}(\beta)\,,$$

где $\alpha \in K_n(K^*)$, $\beta \in F_c(\mathfrak{M})$.

Как и в одномерном случае, спаривание $(\cdot,\cdot)_c$ обладает мультипликативностью по первому аргументу и F_c-линейностью по второму.

Для произвольного абелева расширения L/K задано норменное отображение K-групп Милнора $\mathrm{Norm}_{K_n(L)/K_n(K)}\colon K_n(L) \to K_n(K)$. Построение и свойства этого отображения описаны, например, в [84], Глава 9, §3.

Норменное свойство спаривания $(\cdot,\cdot)_c$,

$$(\alpha, \beta)_c = 0 \Longleftrightarrow \alpha \in \mathrm{Norm}_{K_n(L)/K_n(K)}(K_n(L^*)),\ \text{где}\ L = K([p^m]_c^{-1}(\beta))$$

следует из свойства, связывающего отображение Паршина-Като Ξ и норменные отображения, а именно: для $\alpha \in K$ и любого конечного абелева расширения L/K автоморфизм $\Xi(\alpha)$ действует тривиально на L тогда и только тогда, когда $\alpha \in \mathrm{Norm}_{K_n(L)/K_n(K)}(K_n(L^*))$. Этот результат изложен, например, в [28], Теорема 2, (5).

1.1.3 Примарные элементы и система образующих Гензеля

В работе [35], §1, 2° описано построение p^m-примарного элемента $\omega(a) = E(as(t_n))|_{t_n=\pi}$, $a \in \mathcal{O}_T$, $\operatorname{tr} a \not\equiv 0 \mod p$ в полной аналогии с одномерным случаем. Далее в [35], §1, 3° описано построение системы образующих Гензеля, опирающейся на $\omega(a)$. Подробное построение в более общем случае многомерного поля с совершенным последним полем вычетов проделано в [85].

Предложение 2. *Элементы* $\varepsilon'_{\theta,i} = 1 - \theta t_1^{i_1} t_2^{i_2} \ldots t_{n-1}^{i_{n-1}} \pi^{i_n}$, *где* $\theta \in \mathfrak{R}$, $\operatorname{LCM}(i_1, \ldots, i_n, p) = 1$, $0 \leqslant i_n \leqslant pe'_n$ *и последний отличный от нуля индекс* i_r *перед* i_n *должен быть положителен, если* $i_n = 0$ *и меньше* pe'_r, *если* $i_n = pe'_n$, *вместе с элементом* $\omega(a)$, *где* $a \in \mathcal{O}_T$, $\operatorname{tr} a \not\equiv 0 \mod p$ *дают систему образующих группы главных единиц поля* K^*.

1.2 Комбинаторная теорема о нулях

В данном разделе обсуждаются известные подходы и некоторые классические применения комбинаторной теоремы о нулях.

В этом разделе и главах 3 и 4 через $\mathbb{F}$ обозначается основное поле коэффициентов. Через n, m, k целые неотрицательные числа.

Комбинаторная теорема о нулях имеет довольную короткую историю и берёт своё начало в работах Н. Алона середины 1990-х годов. Наиболее полное изложение своего метода Н. Алон представил в работе [44].

Теорема 1 (Комбинаторная теорема о нулях Алона)**.** *Пусть* $\mathbb{F}$ *произвольное поле, и* $f = f(x_1, \ldots, x_n)$ *некоторый многочлен в* $\mathbb{F}[x_1, \ldots, x_n]$. *Предположим, что степень* $\deg(f)$ *многочлена* f *равна* $\sum_{i=1}^n t_i$, *где* t_i *целые неотрицательные числа. Предположим также, что коэффициент при мономе* $\prod_{i=1}^n$ *в многочлене* f *не равен нулю. Тогда, если* $S_1, \ldots, S_n$ *некоторые подмножества* F *такие, что* $|S_i| > t_i$, *то найдется набор* $s_1 \in S_1, \ldots, s_n \in S_n$ *такой, что*

$$f(s_1, \ldots, s_n) \neq 0.$$

Подход Алона к этому результату основывался на некотором усилении теоремы Гильберта о нулях для идеала порожденного многочленами $g_i(x_i) = \prod_{s\in S_i}(x_i - s)$ (Теорема 1.1. в [44]) Отсюда, скорее всего, родилось и название теоремы 1.с

Несмотря на свою, казалось бы, чисто алгебраическую природу, эта теорема проявила свою значимость, в первую очередь, в целом ряде различных задач дискретной математики. В той же работе [44] Алон продемонстрировал её применения в задачах аддитивной теории чисел, теории графов и комбинаторики. Среди продемонстрированных им приложений можно отметить простое доказательство теоремы Шевалле-Варнинга, теоремы Коши-Девенпорта, теорему Эрдёша-Хэйлброна, 3-списочность любого двудольного планарного графа и ряд результатов на суммы с ограничениями.

Идея Алона получила своё развитие в работах М. Ласона [45] и Р. Н. Карасёва и Ф. В. Петрова [46]. Независимо ими было получено следующее обобщение, описанное ниже, более удобное для целей нашей работы.

Теорема 2. *Пусть* $\mathbb{F}$ *— произвольное поле и* $F \in \mathbb{F}[x_1, x_2, \dots, x_n]$ *— многочлен степени не выше* $\deg(F) \leq d_1 + d_2 + \dots + d_n$*. Тогда для любых множеств* $C_1, C_2, \dots, C_n$ *в* $\mathbb{F}$ *таких, что* $|C_i| = d_i + 1$*, коэффициент при мономе* $\prod x_i^{d_i}$ *в* F *равен*

$$\sum_{c_1\in C_1}\sum_{c_2\in C_2}\cdots\sum_{c_n\in C_n}\frac{F(c_1, c_2, \dots, c_n)}{\phi_1'(c_1)\phi_2'(c_2)\dots\phi_n'(c_n)},$$

где $\phi_i(z) = \prod_{c\in C_i}(z - c)$.

Ключевой идеей в доказательстве этой теоремы является подход к комбинаторной теореме о нулях не как к следствию теоремы о нулях Гильберта, а как к своего рода обобщению интерполяционной формулы Лагранжа. Действительно при $n = 1$ Теорема 2 вырождается в формулу для старшего коэффициента многочлена от одной переменной, следующую из формулы Лагранжа.

Важно также отметить, что существуют и другой взгляд на комбинаторную теорему о нулях, а именно Р. Н. Карасёвым в работе [50] было замечено, что по сути теорема 2 является следствием теоремы Коши о вычетах. Это наблюдение особенно интересно в свете того, что результат о символе Гильберта, рассматриваемый в главе 2 данной работы, тесно связан с явной формой закона взаимности, которая сама по себе также является, в определенном смысле, следствием теоремы Коши о вычетах. Автору представляется особенно интересной возможность найти единый подход к этим задачам, что, однако, выходит за рамки текущей работы.

Упомянем, тем не менее, работу [51], представленную в довольно абстрактном ключе алгебраической геометрии, которая могла бы помочь прояснить наблюдаемую связь и глубже изучить природу комбинаторной теоремы о нулях. А именно, работа [51], изучает следы в полных пересечениях и в качестве одного из главных своих результатов получает формулу, обобщающую формулу Эйлера-Якоби. При достаточно пристальном рассмотрении, однако, внимательный читатель может заметить, что представленная там формула влечет за собой теорему 2, если рассмотреть решетку $C_1 \times \ldots \times C_n$ как полное пересечение образованное многочленами $g_i(x_i) = \prod_{c \in C_i}(x_i - c)$.

Другой причиной интересоваться подобными обобщениями является следующая. Изучаемые в главе 4 соотношения лежат в одном ряду с так называемыми соотношениями Макдональда, доказанными И. В. Чередником. Однако, несмотря на то, что представленный метод оказывается достаточно универсальным, чтобы в едином стиле получить доказательства многих известных соотношений на свободный член, включая до этого неразрешенную гипотезу Форрестера, соотношения Макдональда, для систем корней отличных от A, B, C, D, казалось бы, не поддаются подобному подходу. Более общая версия комбинаторной теоремы о нулях, возможно, смогла бы преодолеть этот барьер.

Напомним, что Теорема Коши – Дэвенпорта [86] утверждает, что для непустых множеств A, B остатков по простому модулю p имеет место неравенство $|A + B| \geq \min(p, |A| + |B| - 1)$. Начиная с середины 1990-х, когда появился полиномиальный метод, основанный на комбинаторной теореме о нулях [43], в этом круге вопросов было сделано многое, в том числе получены результаты для множеств точек в аффинных пространствах [87] и для общих групп [88; 89].

Глава 2. Явное спаривание в многочленном формальном модуле

В данной главе мы изучаем явный вид аналога спаривания Гильберта в многочленном формальном модуле. Мы пользуемся обозначениями раздела **??**.

2.1 Функции Артина-Хассе

Рассмотрим аналоги функций Артина-Хассе для формальной группы F_c:

Определение 1. Функцией Артина-Хассе для формальной группы F_c называется функция:

$$\begin{gathered} E_c \colon \mathcal{O}_T\{\{t_1\}\} \ldots \{\{t_{n-1}\}\}[[t_n]]_1 \to \mathcal{H}_\mathrm{c} \\ E_c(f) = \underline{c}^{-1}(E(\underline{c}f) - 1) = \lambda_c^{-1}\left(1 - \frac{\Delta}{p}\right)^{-1}(cf)\,, \end{gathered} \tag{2.1}$$

обратной к ней называется функция:

$$\begin{gathered} \ell_c \colon \mathcal{H}_\mathrm{c} \to \mathcal{O}_T\{\{t_1\}\} \ldots \{\{t_{n-1}\}\}[[t_n]]_1 \\ \ell_c(f) = \underline{c}^{-1}\ell(1 + \underline{c}f) = \underline{c}^{-1}\left(1 - \frac{\Delta}{p}\right)\lambda_c(f)\,. \end{gathered} \tag{2.2}$$

Из свойств функций E, ℓ следует:

Предложение 3. *Функции E_c, ℓ_c корректно определены, взаимно обратны и задают изоморфизм между модулем по сложению $\mathcal{O}_T\{\{t_1\}\} \ldots \{\{t_{n-1}\}\}[[t_n]]_1$ и формальным модулем $\mathcal{H}_\mathrm{c}$. В частности:*

$$E_c(f + g) = E_c(f) +_{F_c} E_c(g)\,, E_c(a \cdot f) \;= [a]_c E_c(f)\,, \tag{2.3}$$

где f, $g \in \mathcal{O}_T\{\{t_1\}\} \ldots \{\{t_{n-1}\}\}[[t_n]]_1$, $a \in \mathbb{Z}_p$;

$$\ell_c(f +_{F_c} g) = f + g)\,, \ell_c([a]_c f) \;= a \cdot f\,, \tag{2.4}$$

где f, $g \in \mathcal{H}_\mathrm{c}$, $a \in \mathbb{Z}_p$;

2.2 Примарные элементы

Аналогично Предложению 2, описанному во введении, а также работе [35] построение p^m-примарных элементов относительно группы F_c проводится также как в одномерном случае, например, описанном в работе [14]. Отметим одно важное различие, которое состоит в необходимости использовать многомерный аналог утверждения о соответствии униформизующей автоморфизму Фробениуса, а именно: элемент $\{t_1,t_2,\ldots,t_{n-1},\pi\}$ соответствует при отображении Паршина-Като некоторому продолжению Фробениуса Ξ в $\mathrm{Gal}(K^{ab}/K)$ (см. [28] Теорема 2, (4)).

Предложение 4. *Пусть $a \in \mathcal{O}_T^*$, тогда элемент $\omega_c(a) = E_c(as_c(t_n))|_{t_n=\pi}$ является p^m-примарным относительно группы F_c. Более того, $(\{t_1,t_2,\ldots,t_{n-1},\pi\},\omega_c(a))_c = [\mathrm{tr}\, a]_c(\xi)$.*

2.3 Формальное спаривание

В этом параграфе мы построим спаривание на рядах между формальной группой Милнора $K_n(\mathcal{H}_{\mathfrak{m}})$ и формальным модулем $\mathcal{H}_{\mathfrak{c}}$, дадим для него две эквивалентные формы и проверим простейшие свойства.

Определение 2. Следующим образом зададим формальное спаривание $[\cdot,\cdot]_c$ между ${\mathcal{H}_{\mathfrak{m}}}^n$ и $\mathcal{H}_{\mathrm{c}}$

$$
\begin{aligned}
[\cdot,\cdot]_c\colon (\mathcal{H}_{\mathfrak{m}})^n \times \mathcal{H}_{\mathrm{c}} &\to \mathcal{O}_T/p^m \\
\alpha, \beta &\mapsto \operatorname{res}\Phi(\alpha,\beta)\,/s_c \mod p^m,
\end{aligned}
$$

$$
\text{где } \Phi(\alpha,\beta) = \ell_c(\beta)D'_{n+1} - \sum_{i=1}^{n}\frac{1}{p^{n-i}}\ell(\alpha_i)D'_i
$$

$$
D'_{n+1} = \operatorname{Det}(\delta_i(\alpha_j))_{ij}
$$

$$
D'_i = \operatorname{Det}\begin{vmatrix}
\delta_1(\alpha_1) & \dots & \delta_n(\alpha_1) \\
\multicolumn{3}{c}{\dotfill} \\
\delta_1(\alpha_{i-1}) & \dots & \delta_n(\alpha_{i-1}) \\
\underline{c}^{-1}\partial_1\frac{\triangle}{p}\underline{c}\lambda_c(\beta) & \dots & \underline{c}^{-1}\partial_n\frac{\triangle}{p}\underline{c}\lambda_c(\beta) \\
\delta_1(\alpha_{i+1}^{\triangle}) & \dots & \delta_n(\alpha_{i+1}^{\triangle}) \\
\multicolumn{3}{c}{\dotfill} \\
\delta_1(\alpha_n^{\triangle}) & \dots & \delta_n(\alpha_n^{\triangle})
\end{vmatrix}
$$

$$
\operatorname{res} = \operatorname{res}_{t_1t_2\dots t_{n-1}t_n}.
$$

С помощью равенств (1.1) и (1.2) несложно переписать ряд Φ в следующем виде.

Предложение 5. *Пусть* $\alpha \in {\mathcal{H}_{\mathfrak{m}}}^n$ *и* $\beta \in \mathcal{H}_{\mathrm{c}}$. *Тогда*

$$
\Phi(\alpha,\beta) = \ell_c(\beta)D_{n+1} + \sum_{i=1}^{n}(-1)^{n-i+1}\ell(\alpha_i)D_i\,, \tag{2.5}
$$

где

$$
D_i = \operatorname{Det}\begin{vmatrix}
\delta_1(\alpha_1) & \dots & \delta_n(\alpha_1) \\
\multicolumn{3}{c}{\dotfill} \\
\delta_1(\alpha_{i-1}) & \dots & \delta_n(\alpha_{i-1}) \\
\eta_1(\alpha_{i+1}) & \dots & \eta_n(\alpha_{i+1}) \\
\multicolumn{3}{c}{\dotfill} \\
\eta_1(\alpha_n) & \dots & \eta_n(\alpha_n) \\
\underline{c}^{-1}\partial_1\frac{\triangle}{p}\underline{c}\lambda_c(\beta) & \dots & \underline{c}^{-1}\partial_n\frac{\triangle}{p}\underline{c}\lambda_c(\beta)
\end{vmatrix}.
$$

Легко видеть, что данные определения согласуются с данным в мультипликативном случае $c = 1$ в работе [35].

Следующая лемма немедленно следует из соотношений (2.4).

Лемма 2. *Спаривание* $[\cdot,\cdot]_c$ *линейно по обеим частям, то есть*

$$[\{\alpha_1,\dots,\alpha_i\alpha_i',\dots\alpha_n\},\beta]_c = [\{\alpha_1,\dots,\alpha_i,\dots\alpha_n\},\beta]_c + [\{\alpha_1,\dots,\alpha_i',\dots\alpha_n\},\beta]_c;$$
$$[\alpha,\beta_1 +_{F_c} \beta_2]_c = [\alpha,\beta_1]_c + [\alpha,\beta_2]_c;$$
$$[\alpha,[a]_c\beta]_c = a[\alpha,\beta]_c, a \in \mathbb{Z}_p$$

Далее изложены технические детали, необходимые для проверки основных свойств, но опущенные в [35]. При доказательстве нижеследующих лемм мы будем пользоваться схожей схемой, основанной на индукции по n. Нам понадобится следующее техническое определение, чтобы описать свойство ряда, которое необходимо будет поддерживать по индукции. Альтернативно можно провести доказательства, выводя явные формы рядов по ходу индукции, вместо поддержания этого технического свойства, однако такой подход усложняет выкладки.

Определение 3. Функцию $\Psi\colon \mathcal{H}_\mathfrak{m}{}^n \times \mathcal{H}_\mathfrak{c} \to \mathcal{O}_T\{\{t_1\}\}\dots\{\{t_n\}\}$ будем называть *симметрично-производной*, если она представляется в виде $\Psi = \sum_{i=1}^n \partial_i(\mu_i)$, где μ_i, в свою очередь, некоторые функции $\mu_i\colon \mathcal{H}_\mathfrak{m}{}^n \times \mathcal{H}_\mathfrak{c} \to \mathcal{O}_T\{\{t_1\}\}\dots\{\{t_n\}\}$ представимые в виде ряда от аргументов с коэффициентами из $\mathbb{Q}_p[\underline{c},\partial_1,\dots\partial_{i-1},\partial_{i+1},\dots,\partial_n,\triangle]$, причём μ_i отличается от μ_j лишь заменой оператора ∂_i на ∂_j и умножением на $(-1)^{i-j}$.

Лемма 3. *Пусть ряд* $\Psi \in \mathcal{O}_T\{\{t_1\}\}\dots\{\{t_n\}\}$ *таков, что* $\Psi\cdot\underline{c} = \sum_{i=1}^n \partial_i(\mu_i)$, *где* $\mu_i \in \mathcal{O}_T\{\{t_1\}\}\dots\{\{t_n\}\}$. *Тогда*

$$\operatorname{res}\Psi/s_c \equiv 0 \mod p^m$$

Доказательство. Заметим, что

$$\Psi/s_c = \Psi\cdot\underline{c}/s = \sum_{i=1}^n \partial_i(\mu_i)/s = \sum_{i=1}^n \partial_i(\mu_i/s) - \sum_{i=1}^n \mu_i\cdot\partial_i(1/s).$$

Вычет любой частной производной равен нулю, а $\partial_i(1/s) \equiv 0 \mod p^m$ по определению ряда s. Отсюда немедленно получаем утверждение леммы. □

Разложение всех определителей, кроме D_i, в (2.5) по i-ой строке, при некотором фиксированном i, можно перегруппировать в $n-1$-мерные варианты функции Φ. Для определенности при $i=n$ разложим каждый определитель по строке с α_n, перегруппируем слагаемые и, пользуясь соотношением (1.4), получим:

$$\Phi(\alpha_1,\ldots,\alpha_n,\beta) = -\ell(\alpha_n)D_n + \ell_c(\beta)D_n^* + \sum_{i=1}^{n}(-1)^{n-i}\eta_i(\alpha_n)\Phi_i(\alpha_1,\alpha_2,\ldots,\alpha_{n-1},\beta)\,, \tag{2.6}$$

где функции Φ_i определены так же, как функция Φ в размерности $n-1$ от переменных $t_1,\ \ldots,\ t_{i-1},\ t_{i+1},\ \ldots,\ t_n$ над кольцом $\mathcal{O}_T\{\{t_i\}\}$, и

$$D_n^* = \operatorname{Det}\begin{vmatrix} \delta_1(\alpha_1) & \ldots & \delta_n(\alpha_1) \\ \vdots & \ldots & \vdots \\ \delta_1(\alpha_{n-1}) & \ldots & \delta_n(\alpha_{n-1}) \\ \partial_1\ell(\alpha_n) & \ldots & \partial_n\ell(\alpha_n) \end{vmatrix}. \tag{2.7}$$

Следующие леммы позволят спустить спаривание с группы ${\mathcal{H}_\mathfrak{m}}^n$ до группы Милнора $K^n(\mathcal{H}_\mathfrak{m})$. Их доказательства проходят по одной схеме: индукцией по n мы выясним, что некоторая функция, заданная с помощью Φ, является симметрично-производной, и применим лемму 3, чтобы вывести из этого соотношение на спаривание $[\cdot,\cdot]_c$.

Лемма 4 (Кососимметричность)**.** *Для любых индексов* $1 \leqslant i \neq j \leqslant n$ *верно уравнение*

$$[\{\ldots,\alpha_i,\ldots,\alpha_j,\ldots\},\beta]_c = -[\{\ldots,\alpha_j,\ldots,\alpha_i,\ldots\},\beta]_c.$$

Доказательство. Не умаляя общности, фиксируем $i=1$, $j=2$. Индукцией по n докажем, что функция $\underline{c}\cdot(\Phi(\alpha_1,\alpha_2,\alpha_3,\ldots,\alpha_n,\beta)+\Phi(\alpha_2,\alpha_1,\alpha_3,\ldots,\alpha_n,\beta))$ является симметрично-производной.
База $n=2$. Обозначим $\kappa(\beta) \overset{\triangle}{=} \frac{}{p}\underline{c}\lambda_c(\beta)$. Воспользуемся представлением (2.5) для функции Φ. При сложении $\Phi(\alpha_1,\alpha_2,\beta)$ и $\Phi(\alpha_2,\alpha_1,\beta)$ слагаемые с $\ell_c(\beta)$ сократятся, так как определители при них отличаются перестановкой строк. Оставшиеся слагаемые, пользуясь соотношением (1.4), можно сгруппировать

следующим образом:

$$\underline{c}(\Phi(\alpha_1,\alpha_2,\beta)+\Phi(\alpha_2,\alpha_1,\beta)) = \\ = \ell(\alpha_1)\cdot \mathrm{Det}\begin{vmatrix}\partial_1\ell(\alpha_2) & \partial_2\ell(\alpha_2)\\ \partial_1\kappa(\beta) & \partial_2\kappa(\beta)\end{vmatrix} + \ell(\alpha_2)\cdot \mathrm{Det}\begin{vmatrix}\partial_1\ell(\alpha_1) & \partial_2\ell(\alpha_1)\\ \partial_1\kappa(\beta) & \partial_2\kappa(\beta)\end{vmatrix}\,.$$

Раскрывая определители и собирая члены перед $\partial_1\kappa(\beta)$ и $\partial_2\kappa(\beta)$, получим:

$$\begin{aligned}\underline{c}(\Phi(\alpha_1,\alpha_2,\beta)+\Phi(\alpha_2,\alpha_1,\beta)) &= \partial_1(\ell(\alpha_1)\ell(\alpha_2))\partial_2\kappa(\beta) - \partial_2(\ell(\alpha_1)\ell(\alpha_2))\partial_1\kappa(\beta) = \\ &= \partial_1(\ell(\alpha_1)\ell(\alpha_2)\partial_2\kappa(\beta)) - \ell(\alpha_1)\ell(\alpha_2)\partial_1\partial_2\kappa(\beta) - \\ &- \partial_2(\ell(\alpha_1)\ell(\alpha_2)\partial_1\kappa(\beta)) + \ell(\alpha_1)\ell(\alpha_2)\partial_1\partial_2\kappa(\beta) = \\ &= \partial_1(\ell(\alpha_1)\ell(\alpha_2)\partial_2\kappa(\beta)) - \partial_2(\ell(\alpha_1)\ell(\alpha_2)\partial_1\kappa(\beta))\,.\end{aligned}$$

Переход $n-1 \leftarrow n$. Воспользуемся разложением (2.6) для функции Φ. Аналогично базе слагаемые $-\ell(\alpha_n)D_n$ и $\ell_c(\beta)D_n^*$ сократятся при сложении $\Phi(\alpha_1,\alpha_2,\ldots,\alpha_n,\beta)$ и $\Phi(\alpha_2,\alpha_1,\ldots,\alpha_n,\beta)$.

Для каждой функции Φ_i воспользуемся предположением индукции. Пусть

$$\underline{c}(\Phi_i(\alpha_1,\alpha_2,\ldots,\alpha_{n-1},\beta)+\Phi_i(\alpha_2,\alpha_1,\ldots,\alpha_{n-1},\beta)) = \sum_{j\neq i}\partial_j(\mu_{ij})\,.$$

Разобьём все оставшиеся слагаемые на пары

$$\eta_i(\alpha_n)\cdot\partial_j(\mu_{ij}) + (-1)^{i-j}\eta_j(\alpha_n)\cdot\partial_i(\mu_{ji})\,. \tag{2.8}$$

Заметим, что в функциях μ_{ij} и μ_{ji} отсутствуют операторы ∂_i и ∂_j. В силу того, что они являются элементами представления двух одинаковых симметрично-производных функций, отличавшихся лишь заменой набора переменных, получаем, что $\mu_{ij} = (-1)^{i-j+1}\mu_{ji}$. Перепишем каждое слагаемое следующим образом

$$\eta_i(\alpha_n)\cdot\partial_j(\mu_{ij}) = \partial_j(\eta_i(\alpha_n)\cdot\mu_{ij}) - \partial_j(\eta_i(\alpha_n))\cdot\mu_{ij}\,.$$

Пользуясь полученным и тривиальным соотношением $\partial_j\eta_i(\alpha_n) = \partial_i\eta_j(\alpha_n)$, получаем после сокращения в каждой паре (2.8) представление изучаемой функции в виде суммы частных производных. Приводя слагаемые, получаем, что исходная сумма имеет вид:

$$\underline{c}(\Phi(\alpha_1,\alpha_2,\ldots,\alpha_n,\beta)+\Phi(\alpha_2,\alpha_1,\ldots,\alpha_n,\beta))=\sum_{i=1}^{n}\partial_i\left(\sum_{j\neq i}(-1)^{n-j}\eta_j(\alpha_n)\mu_{ji}\right).$$

Легко видеть, что эта функция является, таким образом, симметрично-производной и переход доказан.

Применяя теперь лемму 3, получаем кососимметричность спаривания $[\cdot,\cdot]_c$. □

Следствие 1 (Гиперболичность)**.** *Спаривание* $[\alpha_1,\ldots,\alpha_n,\beta]_c$ *обнуляется при* $\alpha_j=-\alpha_i$*:*

$$[\ldots,\alpha,\ldots,-\alpha,\ldots,\beta]_c=0\,.$$

Доказательство. Лемма 2 гарантирует линейность $[\cdot,\cdot]_c$. Применяя её с учётом того, что $-1=(-1)^{p^m}$, получаем

$$[\ldots,\alpha,\ldots,-\alpha,\ldots,\beta]_c=[\ldots,\alpha,\ldots,\alpha,\ldots,\beta]_c\,.$$

В обозначениях леммы 4 при $\alpha_i=\alpha_j=\alpha$ получаем:

$$2\cdot[\ldots,\alpha,\ldots,\alpha,\ldots,\beta]_c=0\,.$$

Учитывая нечетность p, получаем утверждение следствия. □

Лемма 5 (Соотношение Стейнберга)**.** *Спаривание* $[\alpha_1,\ldots,\alpha_n,\beta]_c$ *обнуляется при* $\alpha_j=1-\alpha_i$*:*

$$[\ldots,\alpha,\ldots,1-\alpha,\ldots,\beta]_c=0\,.$$

Доказательство. Не умаляя общности, считаем, что $i=1$, $j=2$. Индукцией по n докажем, что функция $\underline{c}\Phi(\alpha,1-\alpha,\ldots,\alpha_n,\beta)$ является симметрично-производной. При любом i:

$$\delta_i(1-\alpha)=-\alpha(1-\alpha)^{-1}\delta_i(\alpha)\,. \tag{2.9}$$

Из определения функции ℓ легко получить, что

$$\ell(1-\alpha) = -\sum_{\substack{(r,p)=1\\ r\geqslant 1}} \alpha^r/r - \sum_{r=1}^{\infty} \frac{\alpha^{pr}-\alpha^{\Delta r}}{pr}\,. \tag{2.10}$$

Стандартным образом проверяется, что ряды $(\alpha^{pr}-\alpha^{\Delta r})/pr$ имеют целые коэффициенты.

Пользуясь (1.4) получим

$$\begin{aligned}\eta_i(1-\alpha) &= \delta(1-\alpha) - \partial_i\ell(1-\alpha) = \\ &= \partial_i\left(\log(1-\alpha) - \left(1-\frac{\Delta}{p}\right)\log(1-\alpha)\right) = -\sum_{r=1}^{\infty}\partial_i\frac{\alpha^{\Delta r}}{pr}\,.\end{aligned} \tag{2.11}$$

База $n=2$. Обозначим $\kappa(\beta) = \dfrac{\Delta}{p}\underline{c}\lambda_c(\beta)$. Разложим функцию Φ по уравнению (2.5). Определитель при $\ell_c(\beta)$ равен нулю, так как его строки линейно зависимы в силу (2.9).

Оставшиеся слагаемые можно сгруппировать следующим образом:

$$\underline{c}\Phi(\alpha,1-\alpha,\beta) = \partial_1\kappa(\beta)(\ell(1-\alpha)\delta_2(\alpha)-\ell(\alpha)\eta_2(1-\alpha))-\partial_2\kappa(\beta)(\ell(1-\alpha)\delta_1(\alpha)-\ell(\alpha)\eta_1(1- \tag{2.12}$$

Рассмотрим одно из выражений в скобах и воспользуемся (2.10) и (2.11):

$$\begin{aligned}\ell(1-\alpha)\delta_i(\alpha) - \ell(\alpha)\eta_i(1-\alpha) &= \\ &= -\delta_i(\alpha)\sum_{(r,p)=1}\frac{\alpha^r}{r} - \sum_{r=1}^{\infty}\frac{\alpha^{pr}-\alpha^{\Delta r}}{pr}\delta_i(\alpha) + \ell(\alpha)\sum_{r=1}^{\infty}\partial_i\frac{\alpha^{\Delta r}}{pr} = \\ &= -\delta_i(\alpha)\sum_{(r,p)=1}\frac{\alpha^r}{r} - \sum_{r=1}^{\infty}\left(\frac{\alpha^{pr}-\alpha^{\Delta r}}{pr}\delta_i(\alpha) - \ell(\alpha)\partial_i\frac{\alpha^{\Delta r}}{pr}\right)\,.\end{aligned} \tag{2.13}$$

Несложно также установить следующие соотношения

$$\frac{\alpha^{pr}-\alpha^{\Delta r}}{pr}\delta_i(\alpha) - \ell(\alpha)\partial_i\frac{\alpha^{\Delta r}}{pr} = \partial_i\chi_r\,, \tag{2.14}$$

где ряд $\chi_r = \dfrac{\alpha^{pr} - \alpha^{\Delta r}}{p^2 r^2} - \ell(\alpha)\dfrac{\alpha^{\Delta r}}{pr}$ имеет целые коэффициенты. В свою очередь

$$\delta_i(\alpha) \sum_{(r,p)=1} \frac{\alpha^r}{r} = \partial_i \sum_{(r,p)=1} \frac{\alpha^r}{r^2} \tag{2.15}$$

и ряд справа имеет целые коэффициенты.

Комбинируя (2.13), (2.14), (2.15), получим, что правую часть (2.12) можно переписать следующим образом:

$$\begin{aligned}
\underline{c}\Phi(\alpha, 1-\alpha, \beta) = \partial_1\kappa\partial_2\mu(\alpha) - \partial_2\kappa\partial_1\mu(\alpha) = \\
= \partial_2(\mu(\alpha)\partial_1\kappa(\beta)) - \mu(\alpha)\partial_1\partial_2\kappa(\beta) - \\
- \partial_1(\mu(\alpha)\partial_2\kappa(\beta)) + \mu(\alpha)\partial_1\partial_2\kappa(\beta) = \\
= \partial_2(\mu(\alpha)\partial_1\kappa(\beta)) - \partial_1(\mu(\alpha)\partial_2\kappa(\beta))\,,
\end{aligned}$$

где $\mu(\alpha) = \sum_{r=1}^{\infty} \chi_r + \sum_{(r,p)=1} \dfrac{\alpha^r}{r^2}$. База доказана.

Переход $n-1 \leftarrow n$. Воспользуемся разложением (2.6) для функции Φ. Из соотношения (2.9) следует, что слагаемые $-\ell(\alpha_n)D_n$ и $\ell_c(\beta)D_n^*$ равны нулю, так как в определителях присутствуют пропорциональные строки. Оставшаяся часть рассуждения проходит аналогично переходу в лемме 4.

Применяя лемму 3, получаем соотношение Стейнберга для спаривания $[\cdot,\cdot]_c$. □

Лемма 6 (Символьное свойство)**.** *Спаривание* $[\alpha_1, \ldots, \alpha_n, \beta]_c$ *обнуляется, если* $\beta = \underline{c}^{p^m-1}\alpha_i$ *при некотором* i*:*

$$[\ldots, \alpha, \ldots, \underline{c}^{p^m-1}\alpha]_c = 0\,.$$

Доказательство. Не умаляя общности, фиксируем $i = 1$. Индукцией по n докажем, что функция $\underline{c}\Phi(\alpha, \ldots, \alpha_n, \underline{c}^{-1}\alpha)$ является симметрично-производной.

База $n = 1$. База представляет собой символьное свойство в случае обычного одномерного поля. Её несложно вывести, например, аналогично фундаментальному свойству спаривания в работе [35] (см. также работу [79]).

Переход $n-1 \leftarrow n$. Воспользуемся разложением (2.6) для функции Φ. Пользуясь (2.2), получим:

$$\underline{c}(\ell(\alpha_n)D_n + \ell_c(\beta)D_n^*) = \mathrm{Det}\begin{vmatrix} \delta_1(\alpha_1) & . & \delta_n(\alpha_1) \\ \vdots & . & \vdots \\ \delta_1(\alpha_{n-1}) & . & \delta_n(\alpha_{n-1}) \\ \nu_1 & \dots & \nu_n \end{vmatrix}, \tag{2.16}$$

где

$$\nu_i = \left(1 - \frac{\triangle}{p}\right) \log(1+\underline{c}\beta)\partial_i \ell(\alpha_n) - \ell(\alpha_n)\partial_i \frac{\triangle}{p}\log(1+\underline{c}\beta)\,.$$

Пользуясь тривиальным соотношением $\partial_i \log = \delta_i$, получаем

$$\nu_i = \partial_i(\left(1 - \frac{\triangle}{p}\right)\log(1+\underline{c}\beta)\cdot \ell(\alpha_n)) - \ell(\alpha_n)\delta_i(1+\underline{c}\beta)\,. \tag{2.17}$$

Учитывая (2.17), определитель в соотношении (2.16) можно разложить в сумму двух. Второй из них обнуляется

$$-\ell(\alpha_n)\mathrm{Det}\begin{vmatrix} \delta_1(\alpha_1) & . & \delta_n(\alpha_1) \\ \vdots & . & \vdots \\ \delta_1(\alpha_{n-1}) & . & \delta_n(\alpha_{n-1}) \\ \delta_1(1+\alpha_1) & \dots & \delta_n(1+\alpha_1) \end{vmatrix} = 0\,,$$

в силу пропорциональности первой и последней строки, согласно соотношению (2.9). Первый же после разложения по последней строке можно представить в виде

$$\sum_{i=1}^{n}(-1)^i\partial_i(\upsilon(\beta)\ell(\alpha_n)\overline{D}_i) - \upsilon(\beta)\ell(\alpha_n)\sum_{i=1}(-1)^i\partial_i(\overline{D}_i)\,, \tag{2.18}$$

где $\upsilon(\beta) = \left(1 - \frac{\triangle}{p}\right)\log(1+\underline{c}\beta)$ имеет целые коэффициенты и $D_i = |\delta_j(\alpha_r)|_{jr,j\neq i,r\neq i}$. Учитывая соотношение $\partial_i\delta_j = \partial_j\delta_i$ легко видеть, что $\sum_{i=1}(-1)^i\partial_i(\overline{D_i}) = 0$. Подставляя в (2.18), получаем что сумма $\underline{c}(\ell(\alpha_n)D_n + \ell_c(\beta)D_n^*)$ представляет собой особую функцию. Для оставшейся части разложения (2.6) повторяем рассуждение из перехода леммы 4.

Применяя лемму 3, получаем соотношение

$$[\ldots,\alpha,\ldots,\underline{c}^{-1}\alpha]_c = 0\,.$$

Подстановка $\alpha = \underline{c}^{p^m}\gamma$, в силу линейности спаривания по лемме 2, завершает доказательство леммы. □

Леммы 2, 4, 5 и следствие 1 позволяют $[\cdot,\cdot]_c$ индуцировать спаривание $\langle\cdot,\cdot\rangle_c$ на $K_n(\mathcal{H}_\mathfrak{m}) \times \mathcal{H}_\mathfrak{c}$. Учитывая лемму 6 получаем следующую теорему.

Теорема 3. *Спаривание*

$$\begin{aligned}\langle\cdot,\cdot\rangle_c\colon K_n(\mathcal{H}_\mathfrak{m}) \times \mathcal{H}_\mathfrak{c} &\to \mathcal{O}_T/p^m\\ \alpha,\beta &\mapsto \operatorname{res}\Phi(\alpha,\beta)\,/s_c \mod p^m,\end{aligned}$$

корректно задано и отвечает следующим свойствам:

- ***Аддитивность***

$$\begin{aligned}\langle\alpha_1\cdot\alpha_2,\beta\rangle_c &= \langle\alpha_1,\beta\rangle_c + \langle\alpha_2,\beta\rangle_c\,;\\ \langle\alpha,\beta_1 +_{F_c} \beta_2\rangle_c &= \langle\alpha,\beta_1\rangle_c + \langle\alpha,\beta_2\rangle_c\,;\\ \langle\alpha,[a]_c\beta\rangle_c &= a\,\langle\alpha,\beta\rangle_c\,, a\in\mathbb{Z}_p\,.\end{aligned}$$

- ***Символьное свойство***

$$\left\langle\{\ldots,\alpha,\ldots\},\underline{c}^{p^m-1}\alpha\right\rangle_c = 0\,.$$

Определение 4. Определим также спаривание

$$\begin{aligned}\langle\langle\cdot,\cdot\rangle\rangle_c\colon K_n(\mathcal{H}_\mathfrak{m}) \times \mathcal{H}_\mathfrak{c} &\to \mathbb{Z}_p/p^m\\ \alpha,\beta &\mapsto \operatorname{tr}\langle\alpha,\beta\rangle_c\,.\end{aligned}$$

Для спаривания $\langle\langle\cdot,\cdot\rangle\rangle_c$ также выполнена теорема 3.

2.4 Система образующих Гензеля формального модуля

Из предложения 2 о порождающих элементах группы главных единиц выводится построение системы образующих для формального модуля.

Предложение 6. *Элементы* $\varepsilon_{\theta,i} = -\theta c^{p^m-1} t_1^{i_1} t_2^{i_2} \ldots t_{n-1}^{i_{n-1}} \pi^{i_n}$, *где* $\theta \in \mathfrak{R}$, $\mathrm{LCM}(i_1, \ldots, i_n, p) = 1$, $0 \leqslant i_n \leqslant pe'_n$ *и последний отличный от нуля индекс* i_r *перед* i_n *должен быть положителен, если* $i_n = 0$ *и меньше* pe'_r *если* $i_n = pe'_n$, *вместе с элементом* $\omega_c(a)$, *где* $a \in \mathcal{O}_T$, $\mathrm{tr}\, a \not\equiv 0 \mod p$ *дают систему образующих формального модуля* $F_c(\mathfrak{M})$.

Доказательство. Достаточно применить замену $x \to 1 + cx$ и заменить формальное сложение умножением, чтобы свести эту лемму к задаче о нахождении системы образующих в группе главных единиц. □

Предложение 7. *Для описанных в предложении 6 элементов справедливо следующее:*

$$(\{t_1,t_2, \ldots ,t_{n-1},\pi\}, \varepsilon_{\theta,i})_c = 0 \qquad (\{t_1,t_2, \ldots ,t_{n-1},\pi\}, \omega_c(a))_c = [\mathrm{tr}\, a]_c \xi.$$

Доказательство. Вторая часть утверждения уже получена в предложении 4.

Первая же аналогична фундаментальному свойству классического мультипликативного спаривания Гильберта. А именно, заметим, что для спаривания Гильберта также выполнено символьное свойство:

$$(\{\ldots,\alpha,\ldots\}, c^{p^m-1}\alpha)_c = 0. \tag{2.19}$$

Действительно, рассмотрим $L = K(B)$, где B — решение уравнения $[p^m]_c(B) = c^{p^m-1}\alpha$.

$$[p^m]_c(X) = c^{-1}((1+cX)^{p^m} - 1) = d_1 X + d_2 X^2 + \ldots + d_{p^m-1} X^{p^m-1} + c^{p^m-1} X^{p^m},$$

где $d_i \in \mathcal{O}_K$. Поэтому B будет решением уравнения $X^{p^m} + c^{1-p^m} d_{p^m-1} + \ldots + p^m c^{1-p^m} X - \alpha = 0$, а α, таким образом, будет нормой в расширении L/K. Из этого следует, что символ $\{\ldots,\alpha,\ldots\}$ [так как остальные его элементы тоже принадлежат нижнему полю K] будет образом при отображении нормы

$N_{L/K}\colon K_n(L)\to K_n(K)$. А значит, соответствующий автоморфизм $\sigma_{\{\dots,\alpha,\dots\}}$ действует тривиально на поле L, откуда получаем символьное свойство.

Теперь пусть $\varepsilon_{\theta,i}=-\theta c^{p^m-1}t_1^{i_1}t_2^{i_2}\dots t_{n-1}^{i_{n-1}}\pi^{i_n}$ и пусть, скажем, i_j не кратен p. Тогда

$$(\{t_1,\dots,t_{n-1},\pi\},\varepsilon_{\theta,i})_c^{i_j}=(\{t_1,\dots,t_j^{i_j},\dots,t_{n-1},\pi\},\varepsilon_{\theta,i})_c=$$
$$=(\{t_1,\dots,-\theta t_1^{i_1}t_2^{i_2}\dots t_{n-1}^{i_{n-1}}\pi^{i_n},\dots,t_{n-1},\pi\},\varepsilon_{\theta,i})_c=0$$

Последний переход верен в силу символьного свойства, остальные следуют из аддитивности символа Гильберта и кососимметричности в группе Милнора. □

Получим теперь аналогичное тождество для формального спаривания. Аналог первого тождества будет следовать немедленно из символьного, которое уже доказано. Аналог второго даст нам следующая лемма.

Лемма 7. *Для произвольного $a\in\mathcal{O}_T$, $\varepsilon\in\mathcal{H}_{\mathfrak{m}}$ имеют место тождества:*

$$\langle\{t_1,\dots,t_n\},E_c(as_c)\rangle_c=a\,, \tag{2.20}$$
$$\langle\{t_1,\dots,\varepsilon,\dots,t_n\},E_c(as_c)\rangle_c=0\,. \tag{2.21}$$

Доказательство. Разберем эти тождества отдельно.

1. Пусть $\alpha=\{t_1,\dots,t_n\}$.

$$\langle\{t_1,\dots,t_n\},E_c(as_c)\rangle_c=\operatorname{res}(\ell_c(E_c(as_c))D_{n+1}+\sum_{i=1}^{n}(-1)^{n-i+1}\ell(t_i)D_i)/s_c=$$
$$=\operatorname{res}aD_{n+1}=\operatorname{res}a\cdot t_1^{-1}\dots t_n^{-1}=a\,,$$

так как $\ell(t_i)=0$ по определению функции ℓ.

2. Пусть $\alpha=\{t_1,\dots,\varepsilon,\dots,t_n\}$, где $\varepsilon\in\mathcal{H}_{\mathfrak{m}}$. Тогда

$$\langle\{t_1,\dots,\varepsilon,\dots,t_n\},E_c(as_c)\rangle_c=\operatorname{res}(\ell_c(E_c(as_c))D_{n+1}+\sum_{j\neq i}^{n}(-1)^{n-j+1}\ell(t_j)D_j+$$
$$+(-1)^{n-i+1}\ell(\varepsilon)D_i)/s_c=\operatorname{res}aD_{n+1}-(-1)^{n-i}\ell(\varepsilon)D_i/s_c\,.$$

Заметим, что $D_{n+1} = t_1^{-1} \dots \varepsilon^{-1}\partial_i \varepsilon \dots t_n^{-1}$, и так как ε имеет целые коэффициенты, то вычет $\operatorname{res} aD_{n+1}$ равен нулю. Считая оставшийся определитель, получаем:

$$D_i = t_1^{-1} \dots \underline{c}^{-1}\partial_i \frac{\triangle}{p} \underline{c}\lambda_c(E_c(as_c)) \dots t_n^{-1}$$

Далее аналогично рассуждению из предложения 6 [14] (см. также работу [79]) имеем

$$\partial_i \frac{\triangle}{p} \underline{c}\lambda_c(E_c(as_c))/s \equiv 0 \mod p^m\,.$$

и заключаем требуемое:

$$\langle \{t_1, \dots, \varepsilon, \dots, t_n\}, E_c(as_c) \rangle_c = 0\,.$$

□

2.5 Однозначность по второму аргументу

Лемма 8. *Пусть β_1, $\beta_2 \in \mathcal{H}_c$ — ряды такие, что $\beta_1(t_1, t_2, \dots, \pi) = \beta_2(t_1, t_2, \dots, \pi)$, тогда при любых $\alpha_1, \dots, \alpha_n \in \mathcal{H}_{\mathfrak{m}}$:*

$$\langle\langle \{\alpha_1, \alpha_2, \dots, \alpha_n\}, \beta_1 \rangle\rangle_c = \langle\langle \{\alpha_1, \alpha_2, \dots, \alpha_n\}, \beta_2 \rangle\rangle_c$$

Доказательство. Аналогично лемме 1 замечаем, что $\beta_1 -_{F_c} \beta_2 = u_c \cdot \psi$ для некоторого ряда $\psi \in \mathcal{H}_c$. Проводя рассуждение аналогичное проведенному в §3 работы [14] (см. также работы [79] и [35]), получаем сравнение

$$\left(\frac{\triangle}{p} \log(1 + \underline{c}u\psi)\right)/s \equiv \triangle\, (\log(1 + \underline{c}u\psi)/s) \mod (p^m, \deg 0)\,, \tag{2.22}$$

и сравнение

$$-\operatorname{res}(\ell(\alpha_i)\partial_j \frac{\triangle}{p} \log(1 + \underline{c}u\psi))/s \equiv \operatorname{res} \partial_j \ell(\alpha_i) \left(\frac{\triangle}{p} \log(1 + \underline{c}u\psi)\right)/s \mod p^m\,. \tag{2.23}$$

Используем разложение (2.5) для спаривания $\langle\cdot,\cdot\rangle_c$:

$$\langle\alpha,u\psi\rangle_c=\operatorname{res}\Phi(\alpha,u\psi)/s_c=\operatorname{res}(\ell_c(u\psi)D_{n+1}+\sum_{i=1}^{n}(-1)^{n-i+1}\ell(\alpha_i)D_i)/s_c\,. \quad (2.24)$$

Рассмотрим слагаемое $\operatorname{res}((-1)^{n-i+1}\ell(\alpha_i)D_i/s_c)$. Деля последнюю строку D_i на s_c, применяя к разложению по этой строке соотношения (2.23) и собирая определитель назад получим:

$$\operatorname{res}((-1)^{n-i+1}\ell(\alpha_i)D_i/s_c)\equiv\operatorname{res}\left(\frac{\triangle}{p}\log(1+\underline{c}u\psi)\right)/s\cdot\widehat{D}_i+$$
$$+\operatorname{res}((-1)^{1-i}\ell(\alpha_i)\sum_{j=1}^{n}(-1)^j\partial_jD_{i,j})\mod p^m,\text{ где}$$

$$\widehat{D}_i=\operatorname{Det}\begin{vmatrix}\delta_1(\alpha_1)&\dots&\delta_n(\alpha_1)\\ \multicolumn{3}{c}{\dots\dots\dots\dots}\\ \delta_1(\alpha_{i-1})&\dots&\delta_n(\alpha_{i-1})\\ \partial_1(\ell(\alpha_i))&\dots&\partial_n(\ell(\alpha_i))\\ \eta_1(\alpha_{i+1})&\dots&\eta_n(\alpha_{i+1})\\ \multicolumn{3}{c}{\dots\dots\dots\dots}\\ \eta_1(\alpha_n)&\dots&\eta_n(\alpha_n)\end{vmatrix}$$

$$\widehat{D}_i=\operatorname{Det}\begin{vmatrix}\delta_1(\alpha_1)&\dots&\delta_n(\alpha_1)\\ \multicolumn{3}{c}{\dots\dots\dots\dots}\\ \delta_1(\alpha_{i-1})&\dots&\delta_n(\alpha_{i-1})\\ \delta_1(\alpha_i)-\eta_1(\alpha_i)&\dots&\delta_n(\alpha_i)-\eta_n(\alpha_i)\\ \eta_1(\alpha_{i+1})&\dots&\eta_n(\alpha_{i+1})\\ \multicolumn{3}{c}{\dots\dots\dots\dots}\\ \eta_1(\alpha_n)&\dots&\eta_n(\alpha_n)\end{vmatrix}=\widetilde{D}_{i+1}-\widetilde{D}_i$$

$$\widetilde{D}_i=\operatorname{Det}\begin{vmatrix}\delta_1(\alpha_1)&\dots&\delta_n(\alpha_1)\\ \multicolumn{3}{c}{\dots\dots\dots\dots}\\ \delta_1(\alpha_{i-1})&\dots&\delta_n(\alpha_{i-1})\\ \eta_1(\alpha_i)&\dots&\eta_n(\alpha_i)\\ \multicolumn{3}{c}{\dots\dots\dots\dots}\\ \eta_1(\alpha_n)&\dots&\eta_n(\alpha_n)\end{vmatrix},$$

и $D_{i,j}$ это nj минор определителя D_i.

В силу тривиальных соотношений $\partial_j\delta_r = \partial_r\delta_j$ и $\partial_j\eta_r = \partial_r\eta_j$ для всех j, r легко видеть, что $\sum_{j=1}^n (-1)^j \partial_j D_{i,j} = 0$.

Сворачивая сумму в (2.24), получаем:

$$\langle\alpha,u\psi\rangle_c = \operatorname{res}\left(\ell(1+\underline{c}u\psi)D_{n+1} + \frac{\triangle}{p}\log(1+\underline{c}u\psi)(\widetilde{D}_{n+1}-\widetilde{D}_1)\right)/s\,.$$

Воспользуемся теперь определением ℓ и заметим, что $D_{n+1} = \widetilde{D}_{n+1}$:

$$\begin{aligned}\langle\alpha,u\psi\rangle_c &= \operatorname{res}\left(\left(1-\frac{\triangle}{p}\right)\log(1+\underline{c}u\psi)D_{n+1} + \frac{\triangle}{p}\log(1+\underline{c}u\psi)(\widetilde{D}_{n+1}-\widetilde{D}_1)\right)/s = \\ &= \operatorname{res}\left(\log(1+\underline{c}u\psi)D_{n+1} - \frac{\triangle}{p}\log(1+\underline{c}u\psi)\widetilde{D}_1\right)/s\,.\end{aligned}$$

Заметим, что

$$\begin{aligned}\widetilde{D_1} &= \operatorname{Det}(\eta_j(\alpha_i))_{ij} = \operatorname{Det}(t_j^{-1}\triangle(t_j\alpha_i^{-1}\partial_j(\alpha_i)))_{ij} = \\ &= t_1^{-1}\dots t_n^{-1}\triangle\operatorname{Det}(t_j\delta_j(\alpha_i))_{ij} = t_1^{-1}\dots t_n^{-1}\cdot\triangle(t_1\dots t_n D_{n+1})\,.\end{aligned}\tag{2.25}$$

Применяя далее соотношения (2.25) и (2.22) к уже полученному тождеству, выводим:

$$\langle\alpha,u\psi\rangle_c = \operatorname{res} t_1^{-1}\dots t_n^{-1}\cdot(1-\triangle)(\log(1+\underline{c}u\psi)\cdot t_1\dots t_n D_{n+1})$$
$$\langle\alpha,u\psi\rangle_c = (1-\triangle)d,\ \text{где } d\in T\,.$$

Значит $\operatorname{tr}\langle\alpha,u\psi\rangle_c = 0$, что и требовалось. □

2.6 Замена переменной

Лемма 9. *Рассмотрим ряды $g_1, g_2, \dots, g_n \in O_T\{\{z_1\}\}\{\{z_2\}\}\dots\{\{z_{n-1}\}\}[[z_n]]$ такие, что $\tau_i = g_i|_{z_1=t_1,\dots z_n=\pi}$ образуют систему локальных параметров в K. Тогда для любых рядов $\alpha\in K_n(\mathcal{H}_\mathfrak{m})$, $\beta\in\mathcal{H}_\mathrm{c}$:*

$$\langle\langle\alpha,\beta\rangle\rangle_{c,t} = \langle\langle\alpha(g),\beta(g)\rangle\rangle_{c,z}$$

В спаривании в правой части ряды и вычет рассматриваются от переменных z, а соответствующие ряды s'_m, u' строятся с помощью разложения ξ, ζ и c в ряды по системе локальных образующих τ_i при замене переменных $t_i \to g_i$.

Доказательство. Обозначим через $\underset{\sim}{c}$ ряд получающийся разложением c в новой системе образующих τ_i при замене переменных $t_i \to g_i$.

Для начала рассмотрим случай $\alpha = \{t_1, t_2, \dots, t_n\}$. В силу леммы 8 и предложения 6 ряд β можно заменить на формальную сумму базисных рядов вида: $-\theta c^{p^m-1} t_1^{i_1} t_2^{i_2} \dots t_{n-1}^{i_{n-1}} t_n^{i_n}$ и $E_c(as_c)$. Проверим каждый из подслучаев отдельно. В первом получим

$$\left\langle \{t_1, \dots, t_n\}, -\theta \underline{c}^{p^m-1} t_1^{i_1} \dots t_n^{i_n} \right\rangle_{c,t} = 0 = \left\langle \{g_1, \dots, g_n\}, -\theta \underset{\sim}{c}^{p^m-1} g_1^{i_1} \dots g_n^{i_n} \right\rangle_{c,z}$$

в силу символьного свойства [аналогично последней части доказательства предложения 7] и аддитивности спаривания. Во втором подслучае необходимо проверить, что

$$\langle \{t_1, \dots, t_n\}, E_c(as_c) \rangle_{c,t} = \langle \{g_1, \dots, g_n\}, E_c(as'_c) \rangle_{c,z} \ .$$

Это утверждение немедленно следует после применения к обоим частям тождества (2.20).

Далее рассмотрим элементы вида $\alpha = \{t_1, \dots, \varepsilon, \dots, t_n\}$, где $\varepsilon \in 1 + \mathcal{O}_T\{\{t_1\}\} \dots \{\{t_{i-1}\}\}[[t_i]]_1$. Рассмотрим ряды $f = t_i \cdot \varepsilon$, $h = f(g_1, \dots, g_n)$ и элемент $t'_i = f|_{\dots, t_n = \pi}$. Обозначим также через $f_{t_i}^{-1}$ такой ряд из $\mathcal{O}_T\{\{t_1\}\} \dots \{\{t_{i-1}\}\}[[t_i]]$, что $f_{t_i}^{-1}(t_1, \dots, t_{i-1}, f) = t_i$. Тогда

$$\langle \{t_1, \dots, \varepsilon, \dots, t_n\}, \beta \rangle_{c,t} = \langle \{t_1, \dots, f, \dots, t_n\}, \beta \rangle_{c,t} -_{F_c} \langle \{t_1, \dots, t_i, \dots, t_n\}, \beta \rangle_{c,t} \ ,$$

$$\begin{aligned} \langle \{g_1, \dots, \varepsilon(g), \dots, g_n\}, \beta \rangle_{c,z} = \langle \{g_1, \dots, f(g), \dots, g_n\}, \beta \rangle_{c,z} -_{F_c} \\ -_{F_c} \langle \{g_1, \dots, g_i, \dots, g_n\}, \beta \rangle_{c,z} \ , \end{aligned}$$

В силу уже доказанного ранее нам достаточно проверить равенство:

$$\langle \langle \{t_1, \dots, f, \dots, t_n\}, \beta \rangle \rangle_{c,t} = \langle \langle \{g_1, \dots, f(g), \dots, g_n\}, \beta \rangle \rangle_{c,z} \ .$$

Однако, обозначив $y_1 = t_1, \ldots, y_i = h, \ldots y_n = y_n$ и дважды воспользовавшись уже доказанным, мы можем написать:

$$\begin{aligned}
&\langle\langle\{t_1,\ldots,f,\ldots,t_n\},\beta\rangle\rangle_{c,t} = \\
&\qquad = \Big\langle\Big\langle\{y_1,\ldots,y_i,\ldots,y_n\},\beta(y_1,\ldots,f_{t_i}^{-1}(y_1,\ldots,y_n),\ldots y_n)\Big\rangle\Big\rangle_{c,y} = \\
&\quad = \Big\langle\Big\langle\{g_1,\ldots,h,\ldots,g_n\},\beta(g_1,\ldots,f_{t_i}^{-1}(g_1,\ldots,h,\ldots,g_n),\ldots g_n)\Big\rangle\Big\rangle_{c,z} = \\
&\qquad\qquad\qquad = \langle\langle\{g_1,\ldots,f(g),\ldots,g_n\},\beta(g)\rangle\rangle_{c,z}\,.
\end{aligned}$$

Утверждение леммы теперь немедленно следует из предложения 1. □

2.7 Основной результат

С помощью формального спаривания $\langle\cdot,\cdot\rangle_c$ зададим теперь числовое спаривание $\{\cdot,\cdot\}_c$.

Определение 5. Введем спаривание

$$\begin{aligned}
&\{\cdot,\cdot\}\colon K_n(K)\times F_c(\mathfrak{M})\to\langle\xi\rangle_c \\
&\{\alpha,\beta\}_c = \Big[\Big\langle\Big\langle\underline{\alpha},\underline{\beta}\Big\rangle\Big\rangle_c\Big]_c(\xi)\,.
\end{aligned}$$

Проверим теперь корректность этого определения.

Заметим, что независимость от разложения второго аргумента следует непосредственно из леммы 8. Независимость от выбора системы образующих из леммы 9. Проверим независимость от выбора разложения первого аргумента.

Лемма 10. *Пусть элементы $\alpha_1 \in K_n(\mathcal{H}_\mathfrak{m})$ и $\alpha_2 \in K_n(\mathcal{H}_\mathfrak{m})$ таковы, что $\alpha_1|_{\ldots,t_n=\pi} = \alpha_2|_{\ldots,t_n=\pi}$. Тогда для любого ряда $\beta \in \mathcal{H}_c$:*

$$\langle\langle\alpha_1,\beta\rangle\rangle_c = \langle\langle\alpha_2,\beta\rangle\rangle_c\,.$$

Доказательство. Достаточно проверить утверждение в случае, когда α_1 и α_2 элементарны в $K_n(\mathcal{H}_\mathfrak{m})$ и различаются лишь в одной координате, а именно: $\alpha_1 = \{a_1,\ldots,a_{i_1},\ldots,a_n\}$, $\alpha_2 = \{a_1,\ldots,a_{i_2},\ldots,a_n\}$.

В этом случае необходимо доказать, что для любого ряда $\beta \in \mathcal{H}_c$:

$$\langle\langle\{a_1, \ldots, a_{i_1}/a_{i_2}, \ldots, a_n\}, \beta\rangle\rangle_c = 0 .$$

В силу кососимметричности спаривания достаточно разобраться со случаем $i = n$. Далее рассмотрим именно его. Рассмотрим ряд $g = t_n \cdot a_{n_1}/a_{n_2} \in \mathcal{H}_{\mathfrak{m}}$. Для этого ряда $g(\pi) = \pi$. Применяя леммы 8 и 9, получаем:

$$\langle\langle\{a_1, \ldots, t_n\}, \beta\rangle\rangle_c = \langle\langle\{a_1, \ldots, g\}, \beta(g)\rangle\rangle_c = \\ = \langle\langle\{a_1, \ldots, g\}, \beta\rangle\rangle_c = \langle\langle\{a_1, \ldots, t_n \cdot a_{n_1}/a_{n_2}\}, \beta\rangle\rangle_c .$$

Сравнивая первое и последнее выражение в полученном равенстве, получаем требуемое:

$$\langle\langle\{a_1, \ldots, a_{n_1}/a_{n_2}\}, \beta\rangle\rangle_c = 0 .$$

□

Теорема 4. *Для любых элементов $\alpha \in K_n(K)$ и $\beta \in F_c(\mathfrak{M})$ значения спариваний $\{\cdot,\cdot\}_c$ и $(\cdot,\cdot)_c$ совпадают:*

$$\{\alpha,\beta\}_c = (\alpha,\beta)_c .$$

Доказательство. Согласно предложению 1, достаточно проверить это утверждение при $\alpha = \{t_1, \ldots, \pi\}$ и $\alpha = \{t_1, \ldots, t_{i-1}, \varepsilon, t_{i+1} \ldots, \pi\}$ где $\varepsilon \in 1 + \mathcal{O}_T\{\{t_1\}\} \ldots \{\{t_{i-1}\}\}[[t_i]]_1$ (если $i = n$, то вместо t_n в последних скобках стоит π). Кроме того, можно написать $\varepsilon = t_i'/t_i$, и:

$$\{t_1, \ldots, t_{i-1}, \varepsilon, t_{i+1} \ldots, \pi\} = \{t_1, \ldots, t_i' \ldots, \pi\} - \{t_1, \ldots, t_i \ldots, \pi\} .$$

Поэтому на самом деле достаточно проверить лишь случай $\alpha = \{t_1, \ldots, \pi\}$.

В этом случае из предложения 6 следует, что можно ограничиться рассмотрением лишь рядов $\varepsilon_{\theta,i}$ и $\omega_c(a)$, в качестве ряда β. Однако из первой части предложения (7) немедленно следует, что:

$$\{\{t_1, \ldots, \pi\}, \varepsilon_{\theta,i}\}_c = 0 = (\{t_1, \ldots, \pi\}, \varepsilon_{\theta,i})_c.$$

А из второй части предложения 7 и соотношения (2.20) получаем

$$\{\{t_1, \ldots, \pi\}, \omega_c(a)\}_c = [\operatorname{tr} a]_c(\xi) = (\{t_1, \ldots, \pi\}, \omega_c(a))_c \,.$$

$\square$

Таким образом, построенное явное спаривание совпадает со спариванием Гильберта, или, другими словами, для спаривания Гильберта получена явная формула.

Замечание. Описанный выше результат можно получить и другим методом, сведя его к результату работы [35], а именно, если одновременно рассмотреть изоморфизмы между группой F_c и мультипликативной группой над $\mathcal{O}_K$, а также между их поднятиями над $\mathcal{O}_T\{\{t_1\}\} \ldots \{\{t_{n-1}\}\}((t_n))$, то интересующее нас спаривание можно протащить через данные изоморфизмы и перейти к стандартному мультипликативному спариванию. Для полноты изложения, однако, мы провели прямое рассуждение, заодно осветив некоторые технические детали опущенные в оригинальной работе [35].

Глава 3. Комбинаторная теорема о нулях

3.1 Обобщения комбинаторной теоремы о нулях

Комбинаторная теорема о нулях Алона [44] (теорема 1) описывает, по сути, структуру многочленов, которые обнуляются на конечном декартовом произведении точек над данным полем. Стандартным методом применения теоремы к комбинаторной задаче является следующий: в предположении противного строится многочлен обнуляющийся на достаточно большом декартовом произведении, затем явным образом вычисляется коэффициент при соответствующем старшем члене, который оказывается ненулевым, и тем самым достигается требуемое противоречие. Вычисление самого коэффициента при этом подчас является трудной задачей и с ней помогает справится теорема 2. Г. Кош и Л. Роняй [90; 91] получили обобщение теоремы 1 на случай мультимножеств, вместе с некоторыми интересными приложениями. Изложенная ниже теорема 6 обобщает теорему 2 схожим образом, по сути осуществляя переход от лагранжевой интерполяции к эрмитовой интерполяции.

Для начала рассмотрим следующую абстрактную ситуацию. Пусть над некоторым полем $\mathbb{F}$ фиксированы векторные пространства $\mathfrak{V}_1, \ldots, \mathfrak{V}_n$. Для каждого векторного пространства $\mathfrak{V}_i$ зафиксируем также базис $\mathfrak{B}_i$ и рассмотрим соответствующий базис $\otimes\mathfrak{B}_i$ в тензорном произведении $\otimes\mathfrak{V}_i$. Рассмотрим теперь произвольные непустые подмножества $A_i \subseteq \mathfrak{B}_i$ с выделенными векторами $a_i \in A_i$ и линейные функционалы $\eta_i \colon \mathfrak{V}_i \to \mathbb{F}$, удовлетворяющие условиям $\eta_i(a_i) = 1$ и $\eta_i(b) = 0$ для каждого $b \in A_i \setminus \{a_i\}$. Следующая лемма в таких обозначениях является тривиальной.

Лемма 11. *Пусть тензор $F \in \otimes\mathfrak{V}_i$ таков, что: если $b_i \in \mathfrak{B}_i$ и F и имеет ненулевую координату над $\otimes b_i$, только если или $b_i = a_i$ при всех i или $b_i \in A_i \setminus \{a_i\}$ хотя бы для одного индекса i. Тогда координата F над $\otimes a_i$ равняется $(\otimes\eta_i)(F)$.*

Мы будем рассматривать следующую ситуацию:

$$\mathfrak{V}_i = \mathbb{F}[x_i], \quad \mathfrak{B}_i = \{1, x_i, x_i^2, \ldots\}, \quad A_i = \{1, x_i, \ldots, x_i^{d_i}\}, \quad a_i = x_i^{d_i}.$$

Более того мы будем считать, что значения $\eta_i \in \mathrm{Hom}(\mathfrak{V}_i,\mathbb{F})$ на многочленах $f \in \mathbb{F}[x_i]$ степени не выше d_i совпадает с коэффициентом при $x_i^{d_i}$ в f. Далее кольцо многочленов $\mathbb{F}[x_1,\dots,x_n]$, как векторное пространство над $\mathbb{F}$, отождествляется с $\otimes\mathfrak{V}_i$ естественным изоморфизмом расширяющим следующее отображение:

$$x_1^{k_1}\dots x_n^{k_n} \longleftrightarrow x_1^{k_1}\otimes\dots\otimes x_n^{k_n}, \qquad k_i \in \{0,1,2\dots\}.$$

Для нас также будет важно следующее элементарное наблюдение.

Лемма 12. *Предположим, что линейные функционалы $\vartheta_i \in \mathrm{Hom}(\mathfrak{V}_i,\mathbb{F})$ заданы в виде $\vartheta_i(f) = f^{(m_i)}(c_i)$ для некоторых элементов $c_i \in \mathbb{F}$ и неотрицательных целых чисел m_i. Тогда для любого многочлена $G \in \mathbb{F}[x_1,\dots,x_n]$,*

$$(\otimes\vartheta_i)(G) = \frac{\partial^{m_1+\dots+m_n}G}{\partial x_1^{m_1}\dots\partial x_n^{m_n}}(c_1,\dots,c_n).$$

Доказательство. Заметим, что обе части требуемого соотношения линейны по G. Таким образом достаточно доказать это соотношение в случае когда G является мономом. Рассмотрим отождествление $\mathbb{F}\otimes\dots\otimes\mathbb{F}\to\mathbb{F}$, действующее следующим образом: $\alpha_1\otimes\dots\otimes\alpha_n \mapsto \alpha_1\dots\alpha_n$. Используя данное отождествление, для произвольного монома $G = G = x_1^{k_1}\dots x_n^{k_n} \in \otimes\mathfrak{B}_i$ получаем

$$(\otimes\vartheta_i)(G) = \otimes\left(\vartheta_i(x_i^{k_i})\right) = \prod\nolimits_{i=1}^{n} k_i(k_i-1)\dots(k_i-m_i+1)\cdot\left(\otimes c_i^{k_i-m_i}\right) = \\ = \frac{\partial^{m_1+\dots+m_n}G}{\partial x_1^{m_1}\dots\partial x_n^{m_n}}(c_1,\dots,c_n).$$

□

Определение 6. Мы говорим, что моном $\prod x_i^{c_i} \in \mathbb{F}[x_1,\dots,x_n]$ мажорирует моном $\prod x_i^{d_i} \in \mathbb{F}[x_1,\dots,x_n]$, если $c_i \geqslant d_i$ для всех i и хотя бы одно из неравенств строгое.

Нас будут интересовать мономы, которые не мажорируются ни одним из мономов данного многочлена $F \in \mathbb{F}[x_1,\dots,x_n]$. Отметим, что во всяком случае все мономы степени не ниже $\deg(F)$ являются таковыми. Мы теперь получим усиление теоремы 2, с помощью вышеописанной абстрактной техники.

Теорема 5. *Пусть* $F \in \mathbb{F}[x_1, \ldots, x_n]$ *многочлен, причем ни один его моном не мажорирует моном* $M = \prod x_i^{d_i}$. *Пусть также* $C_1, \ldots, C_n$ *— произвольные подмножества* $\mathbb{F}$ *такие, что* $|C_i| = d_i + 1$ *при каждом* i. *Тогда коэффициент при мономе* M *в многочлене* F *может быть вычислен как*

$$\sum_{c_1 \in C_1} \sum_{c_2 \in C_2} \cdots \sum_{c_n \in C_n} \prod_{i=1}^{n} \kappa(C_i, c_i) F(c_1, c_2, \ldots, c_n),$$

где $\kappa(C_i, c_i) = \left(\prod_{c \in C_i \setminus \{c_i\}} (c_i - c)\right)^{-1}$. *В частности, если рассматриваемый коэффициент не равен нулю, то существует набор представителей* $c_i \in C_i$ *такой, что* $F(c_1, c_2, \ldots, c_n) \neq 0$.

Доказательство. Зададим линейные функционалы $\eta_i \in \mathrm{Hom}(\mathfrak{V}_i, \mathbb{F})$ в виде $\eta_i(f) = \sum_{c_i \in C_i} \kappa(C_i, c_i) f(c_i)$. Согласно интерполяционной формуле Лагранжа $\eta_i(f)$ равняется коэффициенту при $x_i^{d_i}$ многочлена f для произвольного $f \in \mathbb{F}[x_i]$ такого, что $\deg(f) \leq d_i$. Каждый функционал η_i является линейной комбинацией линейных функционалов вида $\vartheta_i(f) = f^{(0)}(c_i)$, и утверждение теперь элементарно следует из Лемм 11 и 12. $\square$

По аналогии с бинарной характеристической функцией обычного множества, любое конечное мультимножество C в поле $\mathbb{F}$ может быть представлено с помощью своей функции кратности $\omega : \mathbb{F} \to \mathbb{N} \cup \{0\}$. Введем также в рассмотрение носитель мультимножества C: $\mathrm{supp}(C) := \{c \in \mathbb{F} \mid \omega(c) \neq 0\}$. В дальнейшем будем писать $c \in C$ подразумевая $c \in \mathrm{supp}(C)$. Конечное объединение конечных мультимножеств можно воспринимать как сложение их функций кратности. Обобщим теперь теорему 5 на случай мультимножеств.

Теорема 6. *Пусть* $F \in \mathbb{F}[x_1, \ldots, x_n]$ *многочлен, причем ни один его моном не мажорирует моном* $M = \prod x_i^{d_i}$. *Пусть также* $C_1, \ldots, C_n$ *произвольные мультимножества в* $\mathbb{F}$ *с соответствующими функциями кратности* $\omega_1, \ldots, \omega_n$, *такие что* $|C_i| = d_i + 1$ *для каждого* i. *Потребуем также чтобы либо* $\mathrm{char}(\mathbb{F}) = 0$ *либо* $\mathrm{char}(\mathbb{F}) \geq \omega_i(c)$ *при всех* i *и* $c \in \mathbb{F}$. *Тогда коэффициент при мономе* M *у многочлена* F *может быть вычислен следующим образом*

$$[M]F = \sum_{c_1 \in C_1} \sum_{m_1 < \omega_1(c_1)} \cdots \sum_{c_n \in C_n} \sum_{m_n < \omega_n(c_n)} \prod_{i=1}^{n} \kappa(C_i, c_i, m_i) \frac{\partial^{m_1 + \cdots + m_n} F}{\partial x_1^{m_1} \ldots \partial x_n^{m_n}}(c_1, \ldots, c_n),$$

где

$$\kappa(C_i,c_i,m_i) = \frac{1}{m_i!\cdot(\omega_i(c_i)-1-m_i)!}\cdot\left(\frac{1}{\prod_{c\in C_i\setminus\{c_i\}}(x-c)^{\omega_i(c)}}\right)^{(\omega_i(c_i)-1-m_i)}\Bigg|_{x=c_i}.$$

В частности, если $[M]F\neq 0$, *то существует система представителей* $c_i\in C_i$ *с кратностями* $m_i<\omega_i(c_i)$, *такая что*

$$\frac{\partial^{m_1+\dots+m_n}F}{\partial x_1^{m_1}\dots\partial x_n^{m_n}}(c_1,\dots,c_n)\neq 0.$$

Замечание. 1. Если все функции кратности ω_i принимают лишь значения 0 и 1, то утверждение сводится к теореме 5.
2. Данный результат является обобщением результата полученного в работе [90; 91] в том же смысле, что теорема 5 является обобщением исходной теоремы Алона.

Доказательство. Теперь для построения линейных функционалов η_i мы будем использовать эрмитову интерполяцию, вместо интерполяции Лагранжа. Для $c_i\in C_i$, $0\leq m_i<\omega_i(c_i)$, обозначим через $g(C_i,c_i,m_i)\in V_i$ единственный многочлен степени не выше $|C_i|$, удовлетворяющий системе сравнений:

$$g(C_i,c_i,m_i)(x_i)\equiv(x_i-c_i)^{m_i}/m_i! \pmod{(x_i-c_i)^{\omega_i(c_i)}},$$

$$g(C_i,c_i,m_i)(x_i)\equiv 0 \pmod{(x_i-c)^{\omega_i(c)}}\quad(c\in C_i\setminus\{c_i\}).$$

Существование и единственность многочлена $g(C_i,c_i,m_i)$ гарантируется китайской теоремой об остатках. Другими словами многочлен $g(C_i,c_i,m_i)$ является единственным многочленом $g\in\mathbb{F}[x_i]$ степени не выше d_i, который удовлетворяет условиям $g^{(m_i)}(c_i)=1$ и $g^{(m')}(u)=0$ во всех иных случаях при $m'<\omega_i(u)$, $u\in\mathbb{F}$. Через $\kappa(C_i,c_i,m_i)$ обозначим коэффициент при $x_i^{d_i}$ в многочлене $g(C_i,c_i,m_i)$. Применяя как и раньше Леммы 11 и 12 к линейным функционалам $\eta_i\in\mathrm{Hom}(\mathfrak{V}_i,\mathbb{F})$ заданным как

$$\eta_i(f)=\sum_{c_i\in C_i}\sum_{m_i<\omega_i(c_i)}\kappa(C_i,c_i,m_i)f^{(m_i)}(c_i),$$

получим первую часть требуемого утверждение. Осталось вычислить коэффициенты $\kappa(C_i,c_i,m_i)$. Рассмотрим многочлен $p_i(x_i) = \prod_{c\in C_i\setminus\{c_i\}}(x_i - c)^{\omega_i(c)}$. Поделим $g(C_i,c_i,m_i)$ на $p_i(x_i)$ и воспользуемся соотношениями задающими $g(C_i,c_i,m_i)$. Получим многочлены $h_i,r_i \in \mathbb{F}[x_i]$ с $\deg(h_i) < \omega_i(c_i)$ и $\deg(r_i) \leq d_i - \omega_i(c_i)$ такие, что:

$$h_i(x_i) = \frac{g(C_i,c_i,m_i)(x_i)}{p_i(x_i)} = \frac{(x_i - c_i)^{m_i}}{m_i!p_i(x_i)} + (x_i - c_i)^{\omega_i(c_i)}\frac{r_i(x_i)}{p_i(x_i)}$$

причем $\kappa(C_i,c_i,m_i)$ будет коэффициентом при $x_i^{\omega_i(c_i)-1}$ многочлена $h_i(x_i)$. Раскладывая левую и правую часть как формальные ряды по переменной $x_i - c_i$ получаем, что $\kappa(C_i,c_i,m_i)$ это коэффициент при $(x_i - c_i)^{\omega_i(c_i)-m_i-1}$ в ряде $1/(m_i!p_i(x_i))$. Требуемый результат теперь следует из формулы Тейлора. $\square$

Другим возможным обобщением комбинаторной теоремы о нулях является переход к аффинным пространствам над базовым полем.

Теорема 7. *Пусть $A_1 \subset \mathbb{F}^{n_1}$, $\ldots$, $A_m \subset \mathbb{F}^{n_m}$ — конечные непустые множества, $x_i = (x_{i1}, \ldots, x_{in_i})$ при $1 \leqslant i \leqslant m$ и $H(x_1, x_2, \ldots, x_m)$ — многочлен от $n = n_1 + \cdots + n_m$ переменных над $\mathbb{F}$ степени $\deg H = w(A_1) + \cdots + w(A_m) - m$. Если коэффициент в H хотя бы при одном одночлене $x_1^{\alpha_1}x_2^{\alpha_2}\ldots x_m^{\alpha_m}$, $|\alpha_i| = w(A_i) - 1$, не равен нулю, то H не покрывает $A_1 \times A_2 \times \cdots \times A_m$.*

Доказательство. Индукция по m. База $m = 1$ тривиальна.
Разложим H по степеням x_m:

$$H(x_1, x_2, \ldots, x_m) = \sum_{|\alpha|\leq \deg H} H_\alpha(x_1, \ldots, x_{m-1})x_m^\alpha.$$

Зафиксируем такой мультииндекс a, что $|a| = w(A_m) - 1$ и коэффициент в H_a при некотором одночлене $x_1^{\alpha_1}x_2^{\alpha_2}\ldots x_{m-1}^{\alpha_{m-1}}$, где $|\alpha_i| = w(A_i) - 1$, не равен 0. Пусть $A_1 \times \cdots \times A_{m-1} = \{y_1, \ldots, y_s\}$. Пусть V — линейная оболочка в $\mathbb{F}^s$ всех векторов $(H_\alpha(y_1), \ldots, H_\alpha(y_s))$, $|\alpha| \geqslant w(A_m)$ (заметим, что $\deg H_\alpha < w(A_1) + \cdots + w(A_{m-1}) - (m-1)$ в этом случае). Рассмотрим два случая:
1. $(H_a(y_1), \ldots, H_a(y_s)) \in V$.
Разложение этого вектора в линейную комбинацию $(H_\alpha(y_1), \ldots, H_\alpha(y_s))$ с $|\alpha| \geqslant w(A_m)$ дает многочлен $G(x_1, \ldots, x_{m-1})$, нарушающий индукционное предположение для $m - 1$.

2. $(H_a(y_1), \ldots, H_a(y_s)) \notin V$.
Предположим, что H покрывает $A_1 \times A_2 \times \cdots \times A_m$. Рассмотрим линейный функционал $L \in (\mathbb{F}^s)^*$, обнуляющий V, но не обнуляющий $(H_a(y_1), \ldots, H_a(y_s))$. Тогда многочлен

$$G(x_m) = \sum_{|\alpha| \leqslant \deg H} L(H_\alpha(y_1), \ldots, H_\alpha(y_s)) \cdot x_m^\alpha$$

задает гиперповерхность степени меньше чем $w(A_m)$, покрывающую A_m. $\square$

Замечание. Выше изложен прямой подход к теореме 7, одна она также может быть представлена на языке лемм 11 и 12 подобно теоремам 5 и 6.

3.2 Приложения к комбинаторике

Рассмотрим семейство подмножеств циклической группы $\mathbb{Z}_{(p)} := \mathbb{Z}/p\mathbb{Z}$ порядка p и обозначим его $\mathcal{S} = \{S_{ij} \mid 1 \leq i < j \leq n\}$. Для произвольного набора подмножеств $A_1, \ldots, A_n \subseteq \mathbb{Z}_{(p)}$ рассмотрим следующее множество сумм с ограничениями:

$$\bigwedge\nolimits_{\mathcal{S}} A_i = \{a_1 + \cdots + a_n \mid a_i \in A_i,\, a_j - a_i \notin S_{ij} \text{ for } i < j\}\,.$$

В частном случае $A_i \equiv A$ и $S_{ij} \equiv \{0\}$, Дж. Диас да Сильва и Я. Хэмидон[47] показали, что

$$\left|\bigwedge\nolimits_{\mathcal{S}} A_i\right| \geq \min\{p, n|A| - n^2 + 1\}\,,$$

тем самым разрешив гипотезу Эрдёша-Гейлброна [92]. Их метод использует свойства циклических пространств дифференцирований на пространстве внешних произведений и теорию представлений симметрических групп. Более простое доказательство было получено с помощью полиномиального метода в работе [43]. Далеко идущее обобщение было получено Хоу и Суном в работе [93]. Мы теперь покажем как их результат может быть получен элементарным образом с помощью теоремы 5. В частности мы получаем ещё одно простое доказательство теоремы Диас да Сильвы-Хэмидона.

Теорема 8. *Пусть* $A_1, \ldots, A_n$ *— подмножества поля* $\mathbb{F}$ *такие, что* $|A_i| = k$ *при* $1 \le i \le n$ *и предположим, что подмножества* $S_{ij} \subseteq \mathbb{F}$ *удовлетворяют* $|S_{ij}| \le s$ *при* $1 \le i < j \le n$. *Если* $\mathrm{char}(\mathbb{F}) = 0$ *или*

$$\mathrm{char}(\mathbb{F}) > \max\left\{n\lceil s/2\rceil, n(k-1) - n(n-1)\lceil s/2\rceil\right\},$$

тогда

$$\left|\bigwedge\nolimits_{\mathcal{S}} A_i\right| \ge n(k-1) - n(n-1)\lceil s/2\rceil + 1.$$

Доказательство. Не умаляя общности можно считать, что s чётно и $|S_{ij}| = s = 2t$ выполнено для любой пары индексов $i < j$. Действительно дополнительные ограничения не могут увеличить размер итогового множества сумм, поэтому каждое $|S_{ij}|$ можно расширить вплоть до удовлетворения этим требованиям. Мы также можем считать, что $k - 1 \ge (n-1)t$. Предположим противное. Пусть множеств сумм $\bigwedge_{\mathcal{S}} A_i$ содержится в некотором множестве C размера $n(k-1) - n(n-1)t$, и рассмотрим многочлен

$$\prod_{e \in C}(x_1 + \cdots + x_n - e) \times \prod_{i<j}\left(\prod_{e \in S_{ij}}(x_j - x_i - e)\right).$$

Очевидно, что в нашем предположении этот многочлен степени $n(k-1)$ обнуляется на прямом произведении $A_1 \times \cdots \times A_n$. Согласно теореме 5 коэффициент при мономе $\prod x_i^{k-1}$ этого многочлена должен быть равен нулю. С другой стороны, этот коэффициент не изменится, если мы немного изменим многочлен в младших членах и рассмотрим преобразованный многочлен

$$F(\boldsymbol{x}) = \prod_{e=\binom{n}{2}t+1}^{n(k-1)-\binom{n}{2}t}(x_1 + \cdots + x_n - e) \times \prod_{i<j}\left(\prod_{e=-t}^{t-1}(x_j - x_i - e)\right).$$

Снова воспользуемся теоремой 5 чтобы вычислить соответствующий коэффициент многочлена $F(\boldsymbol{x})$, через его значения на множествах $C_i \equiv \{0,1,\ldots,k-1\}$. Несложно видеть, что, если $F(\boldsymbol{c}) \ne 0$ при некотором $\boldsymbol{c} \in C_1 \times \cdots \times C_n$, то

$|c_j - c_i| \geq t$ для любой пары $i < j$. Таким образом

$$\binom{n}{2}t \leq c_1 + \cdots + c_n \leq n(k-1) - \binom{n}{2}t,$$

то есть на самом деле $c_1 + \cdots + c_n = \binom{n}{2}t$ (так как иначе обнуляется первый множитель в многочлене $F(\boldsymbol{x})$), и числа $c_1, \ldots, c_n$ являются просто перестановкой чисел $0, t, 2t, \ldots, (n-1)t$. Более того это обязана быть тождественная перестановка, так как, если $c_i > c_j$ при некоторых $i < j$, то $c_i - c_j \geq t + 1$. Получаем, что вычисление коэффициента сводится к вычислению единственного ненулевого слагаемого представленного в формуле из теоремы 5, а именно:

$$\frac{F(0, t, \ldots, (n-1)t)}{\phi_1'(0)\phi_2'(t) \cdots \phi_n'((n-1)t)}.$$

После сокращений в числителе и знаменателе получаем значение

$$(-1)^{\binom{n}{2}t} \times \frac{(n(k-1) - n(n-1)t)!}{(t!)^n} \times \prod_{i=1}^{n} \frac{(it)!}{(k-1-(i-1)t)!}$$

которое не равно нулю в наших предположениях о характеристике поля. Получаем противоречие, которое завершает наше доказательство. $\square$

Указанная оценка точна и, как легко видеть, достигается на следующих множествах и соотношениях:

$$A_i \equiv \{0, 1, \ldots, k-1\},\ S_{ij} \equiv \{-t+1, -t+2, \ldots, t-1\}.$$

3.2.1 Дополнительные примеры

Аргумент приведенный в доказательстве выше легко применим также к следующему хорошо известному общему утверждению о ограниченных суммах (см. Теорему 2.1 [43]).

Теорема 9. *Пусть d_i, s_{ij} неотрицательные целые числа, и $A_1, \ldots, A_n$ и S_{ij} $(1 \leq i < j \leq n)$ — некоторые подмножества множества чисел поля $\mathbb{F}$, такие* *что* $|A_i| = d_i+1$, $|S_{ij}| = s_{ij}$. *Предположим также, что* $N = \sum d_i - \sum s_{ij} \geq 0$. *Если коэффициент при мономе* $\prod x_i^{d_i}$ *в многочлене*

$$F_0(\boldsymbol{x}) = (x_1 + \cdots + x_n)^N \prod_{i<j} (x_j - x_i)^{s_{ij}} \in \mathbb{F}[x_1, \ldots, x_n]$$

не равен нулю, то $|\bigwedge_{\mathcal{S}} A_i| > N$.

В доказательстве теоремы 8 мы использовали теорему 5 в случае $d_i \equiv k-1$, $s_{ij} \equiv 2t$, чтобы получить коэффициент $[x_1^{d_1} \ldots x_n^{d_n}]F_0$ в виде некоторого произведения. Схожий аргумент применим и в следующих случаях. Первый пример относится к результату Суня и Е, а именно теоремы 1.1 работы [94]. Нам потребуется внести лишь небольшое изменение в аргумент представленный выше. Следующие примеры предполагают обозначения теоремы 9

Пример 1. *Пусть* $d_i = k - i$, $s_{ij} \equiv 2t - 1$. *Тогда* $N = n(k-1) - n(n-1)t$ *и*

$$[x_1^{d_1} \ldots x_n^{d_n}]F_0 = (-1)^{\binom{n}{2}t} \times \frac{N!}{(t!)^n n!} \times \prod_{i=1}^{n} \frac{(it)!}{(k-1-(i-1)t)!}.$$

Доказательство. Применим теорему 5 к немного преобразованному в младших членах многочлену

$$F(\boldsymbol{x}) = \prod_{e=\binom{n}{2}t+1}^{n(k-1)-\binom{n}{2}t} (x_1 + \cdots + x_n - e) \times \prod_{i<j} \left(\prod_{e=1-t}^{t-1} (x_j - x_i - e) \right)$$

и множествам $C_i = \{0,1,\ldots,k-1\} \setminus \{jm \mid 0 \leq j < i-1\}$. Опять же $F(\boldsymbol{c}) \neq 0$ при всех $\boldsymbol{c} \in C_1 \times \cdots \times C_n$ кроме случая, когда $c_i = (i-1)t$ для каждого $1 \leq i \leq n$, и вычисления с минимальными отличиями от доказательства теоремы 8 приводят к требуемому результату. □

Следующим примером применения данного метода является теорема Алона-Натасона-Ружи [43]. Предлагаемый метод не сильно отличается от исходного доказательства авторов (что естественно, ведь его истоки лежат в близких результатах Алона), однако он использует необычное применение теоремы 5, в котором более чем одна точка $\boldsymbol{c} \in C_1 \times \cdots \times C_n$ даёт ненулевое слагаемое формулы.

Пример 2. *Пусть* d_i, $s_{ij} \equiv 1$. *Тогда* $N = d_1 + \dots + d_n - \binom{n}{2}$ *и*

$$[x_1^{d_1} \dots x_n^{d_n}]F_0 = \frac{N!}{d_1! \dots d_n!} \prod_{i<j} (d_j - d_i).$$

Доказательство. Заменим многочлен F_0 на

$$F(\boldsymbol{x}) = \prod_{e=\binom{n}{2}+1}^{d_1+\dots+d_n} (x_1 + \dots + x_n - e) \times \prod_{i<j} (x_j - x_i)$$

и на множествах $C_i = \{0,1,\dots,d_i\}$ применим теорему 5. Рассмотрим точку $\boldsymbol{c} \in C_1 \times \dots \times C_n$ с попарно различными координатами c_i. В этом случае $F(\boldsymbol{c}) \neq 0$ может выполнятся только, если $\{c_1,\dots,c_n\} = \{0,\dots,n-1\}$. То есть, имеется некоторая перестановка $\pi = \pi_{\boldsymbol{c}} \in \mathfrak{S}(n)$, такая что $c_i = \pi_{\boldsymbol{c}}(i) - 1$. Для такой точки $\boldsymbol{c}$,

$$F(\boldsymbol{c}) = (-1)^N N! \times \operatorname{sign}(\pi_{\boldsymbol{c}}) \prod\nolimits_{i<j} (j - i), \qquad \phi'(c_i) = (-1)^{d_i - c_i} c_i!(d_i - c_i)!.$$

Учитывая, что $\binom{d_i}{c_i} = 0$ при $d_i < c_i$, нам достаточно показать, что

$$\sum_{\pi \in \mathfrak{S}(n)} \operatorname{sign}(\pi) \prod_{i=1}^{n} \binom{d_i}{\pi(i) - 1} = \prod_{i<j} \frac{d_j - d_i}{j - i}.$$

Заметим теперь, что обе части требуемого тождества являются антисимметричными многочленами минимальной возможной степени $n(n-1)/2$ в переменных d_i, которые имеют одно и то же значение в точке $(d_1,\dots,d_n) = (0,\dots,n-1)$. Тем самым тождество установлено и доказательство окончено. □

Замечание. Альтернативно, более прямое доказательство можно получить следующим образом. Обозначим $x^{[k]} = x(x-1)\dots(x-k+1)$ и рассмотрим многочлены

$$F(\boldsymbol{x}) = \left(\sum_{i=1}^{n} x_i - \binom{n}{2} \right)^{[N]} \prod_{i<j} (x_j - x_i),$$

$$F^*(\boldsymbol{x}) = \sum_{k_1+\dots+k_n = d_1+\dots+d_n} \frac{N!}{\prod k_i!} \prod_{i<j} (k_j - k_i) \prod_{i=1}^{n} x_i^{[k_i]}.$$

Достаточно показать, что многочлен $F-F^*$ обнуляется на прямом произведении множеств $C_i = \{0,1,\ldots,d_i\}$, так как тогда, согласно теореме 5 $[x_1^{d_1}\ldots x_n^{d_n}](F-F^*)=0$ и, следовательно

$$[x_1^{d_1}\ldots x_n^{d_n}]F_0 = [x_1^{d_1}\ldots x_n^{d_n}]F = [x_1^{d_1}\ldots x_n^{d_n}]F^* = \frac{N!}{d_1!\ldots d_n!}\prod_{i<j}(d_j-d_i)$$

как и требуется. Во всех точках $\boldsymbol{c} \in C_1\times\cdots\times C_n$, кроме точки $\boldsymbol{c} = (d_1,\ldots,d_n)$ имеем $F(\boldsymbol{c}) = F^*(\boldsymbol{c}) = 0$. Совпадение значений в оставшейся точке следует напрямую из выбора коэффициентов в F^*. Данный аргумент можно продолжить и показать, что на самом деле $F = F^*$.

Последний рассматриваемый пример данного сорта берёт своё начало в работе Синя [95], где он представлен в виде соотношения на свободный член многочлена:

$$\mathrm{CT}\left[x_1^{-a_1}\ldots x_n^{-a_n}(x_1+\cdots+x_n)^{a_1+\cdots+a_n}\prod\nolimits_{i\neq j}(1-x_j/x_i)^{a_i}\right] = \binom{|\boldsymbol{a}|}{\boldsymbol{a}}. \tag{3.1}$$

Подробности есть также в работе [73]. Во всех предыдущих примерах вместо теоремы 5 можно было на самом деле использовать чуть менее общую теорему 2 с теми же аргументов. Здесь же мы используем всю общность теоремы 6 для значительного упрощения вычислений.

Пример 3. *Пусть* $d_i = na_i$, $s_{ij} = a_i + a_j$. *Тогда* $N = a_1+\cdots+a_n$ *и*

$$[x_1^{d_1}\ldots x_n^{d_n}]F_0 = (-1)^{\sum_{i<j}a_i}\binom{|\boldsymbol{a}|}{\boldsymbol{a}}.$$

Доказательство. Очеивдно, что в доказательстве данного тождества мы можем считать, что $\mathrm{char}(\mathbb{F}) = 0$. Фиксируем произвольное множество $B = \{b_1,\ldots,b_n\} \subset \mathbb{F}$ такое, что $b_1+\cdots+b_n = 0$. Рассмотрим мультимножества $C_1,\ldots,C_n$ с носителем $\mathrm{supp}(C_i) = B$ и функциями кратности $\omega_i(b_j) = a_i + \chi(j=i)$. Легко видеть, что $|C_i| = d_i + 1$. Применим теорему 6 к многочлену

$$F(\boldsymbol{x}) = (-1)^{\sum_{i<j}a_i}F_0(\boldsymbol{x}) = (x_1+\cdots+x_n)^{a_1+\cdots+a_n}\prod\nolimits_{i\neq j}(x_i-x_j)^{a_i}$$

и мультимножествам $C_1,\dots,C_n$. В полученной формуле для $[x_1^{d_1}\dots x_n^{d_n}]F$ окажется лишь одно ненулевое слагаемое. Действительно, предположим что

$$\frac{\partial^{m_1+\dots+m_n}F}{\partial x_1^{m_1}\dots\partial x_n^{m_n}}(c_1,\dots,c_n)\neq 0$$

в некоторой точке $\boldsymbol{c}\in C_1\times\dots\times C_n$ с кратностями $0\le m_i<\omega_i(c_i)$. Для начала покажем, что координаты c_i попарно различны. Пусть, напротив, $c_i=c_j$ при некоторых $i\neq j$. Тогда $m_i+m_j\le\omega_i(c_i)+\omega_j(c_i)\le a_i+a_j-1$. Отсюда следует, что многочлен $H:=\prod(\partial/\partial x_i)^{m_i}F$ делится на x_i-x_j, противоречие.

Таким образом $\{c_1,\dots,c_n\}=\{b_1,\dots,b_n\}$. Заметим, что $m_i\le a_i$. Если $m_i\le a_i$, то H делится на сумму $\sum x_i$ и обнуляется в рассматриваемой точке. Соответственно $m_i=a_i$ и $c_i=b_i$ при всех i. Более того все $a_1+\dots+a_n$ частных производных должны быть применены к множителю $(x_1+\dots+x_n)^{a_1+\dots+a_n}$ в F. Получаем

$$[x_1^{d_1}\dots x_n^{d_n}]F=\prod_{i=1}^{n}\kappa(C_i,b_i,a_i)\frac{\partial^{a_1+\dots+a_n}F}{\partial x_1^{a_1}\dots\partial x_n^{a_n}}(b_1,\dots,b_n)=\binom{|\boldsymbol{a}|}{\boldsymbol{a}},$$

при $\prod_{i\neq j}(b_i-b_j)^{a_i}=\prod_i\prod_{c\in B\setminus\{b_i\}}(b_i-c)^{a_i}$ □

В качестве последнего комбинаторного приложения мы рассмотрим некоторое обобщение теоремы Коши-Дэвенпорта.

Напомним, что Теорема Коши – Дэвенпорта [86] утверждает, что для непустых множеств A, B остатков по простому модулю p имеет место неравенство $|A+B|\ge\min(p,|A|+|B|-1)$. Этот результат является первым и простейшим результатом о размерах множеств сумм с ограничениями, рассмотренных выше (а именно, в нём вообще отсутствуют ограничения). Начиная с середины 1990-х, когда появился полиномиальный метод, основанный на комбинаторной теореме о нулях [43], в этом круге вопросов было сделано многое, в том числе получены результаты для множеств точек в аффинных пространствах [87] и для общих групп [88; 89]. Ниже мы получаем вариант этой теоремы для алгебраической сложности.

Отметим, что рассматриваемое ниже понятие *алгебраической сложности* множества точек аффинного пространства тесно связано с понятием алгебраической иммунности булевых функций в случае поля характеристики 2. Последнее представляет большой интерес в вопросах криптографии и теории сложности вычислений, что подтверждается текущими активными исследованиями: [96—99].

Пусть $\mathbb{F}$ — поле, A — непустое подмножество аффинного пространства $\mathbb{F}^n$.

Определение 7. Назовем *алгебраической сложностью* множества A минимальную степень гиперповерхности H, содержащей A:

$$w(A) := \inf\{\deg H \mid H \supset A, H \text{ — аффинная гиперповерхность в } \mathbb{F}^n\}.$$

Предложение 8 (Неравенство Коши – Дэвенпорта для алгебраической сложности)**.** *Пусть $p(\mathbb{F})$ — аддитивный порядок единицы в поле $\mathbb{F}$. Пусть A, $B \subset \mathbb{F}^n$ — конечные непустые подмножества. Тогда*

$$w(A+B) \geqslant \min\{p(\mathbb{F}), w(A)+w(B)-1\}.$$

Доказательство. Заметим, что при удалении точки из множества A его алгебраическая сложность уменьшается не более чем на 1. Поэтому если $w(A)+w(B) > p(\mathbb{F})+1$, существуют непустые подмножества $A' \subset A$, $B' \subset B$, такие что $w(A')+w(B') = p(\mathbb{F})+1$. Это рассуждение сводит дело к случаю $w(A)+w(B) \leq p(\mathbb{F})+1$.

Теперь предположим, что некоторый многочлен $H(z)$, $z \in \mathbb{F}^n$, степени $w(A)+w(B)-2 < p(\mathbb{F})$ обнуляется на $A+B$ (многочлен меньшей степени на что-нибудь домножим). Тогда $F(x{,}y) := H(x+y)$ обнуляется на $A \times B$. Но если $z_1^{c_1}\dots z_n^{c_n}$ — некоторый одночлен в H старшей степени, то F содержит некоторый одночлен степени $w(A)$ по x и $w(B)$ по y (коэффициент не равен 0, поскольку соответствующие биномиальные коэффициенты не равны 0 в поле $\mathbb{F}$). Это немедленно противоречит теореме 7. □

Глава 4. Соотношения на свободный член многочлена

В данной главе мы изучаем приложения комбинаторной теоремы о нулях и её обобщений к задачам нахождения свободного члена полиномов Лорана. Точнее мы занимаемся семейством соотношений типа Дайсона. Подобные соотношения тесно связаны с интегральной формулой Селберга, играющей важную роль в теории случайных матриц. Мы начинаем со смежной задачи, изученной Каделлом, затем применяем изучаемый метод для получения нового элементарного доказательства соотношения Морриса (т. е. фактически интегральной формулы Селберга) и, наконец, получаем положительный ответ на гипотезу Форрестера, причем в более общей форме, чем в оригинальной формулировке.

4.1 О соотношении Каделла

В своей работе [100] Каделл получил следующее соотношение типа Дайсона. Зафиксируем целые числа $m < n$. Для каждого натурального числа $1 \le r \le n$ и подмножества M множества $\{1,2,\dots,n\}$, можно рассмотреть следующий многочлен Лорана:

$$\mathcal{K}_{r,M}(\boldsymbol{x};\boldsymbol{a}) = \Big(1 + \sum_{v \notin M} a_v\Big) \prod_{s\in M}\left(1 - \frac{x_r}{x_s}\right)\mathcal{D}(\boldsymbol{x};\boldsymbol{a}).$$

Отметим, что $\mathcal{K}_{r,M}(\boldsymbol{x};\boldsymbol{a}) = 0$ при $r \in M$. Теорема 1 работы [100] гласит, что

$$\mathrm{CT}\left[\sum_{r=1}^{n}\sum_{|M|=m}\mathcal{K}_{r,M}(\boldsymbol{x};\boldsymbol{a})\right] = n\binom{n-1}{m}(1+|\boldsymbol{a}|)\binom{|\boldsymbol{a}|}{\boldsymbol{a}}. \tag{4.1}$$

Каделл предположил, что каждая ненулевая функция $\mathcal{K}_{r,M}(\boldsymbol{x};\boldsymbol{a})$ должна вносить одинаковый вклад в свободный член. Он сформулировал даже более общую гипотезу (см. гипотезу 2 [100]), которая была подтверждена Чжоу [101] с помощью формулы для коэффициентов полинома Дайсона (см. теорему 1.7 [102]). Каделл также предположил следующий q-аналог своей гипотезы:

Гипотеза 1 (Гипотеза 3 [100]). *Пусть* $M \subset \{1,2,\ldots,n\}$ *и* $\{r_s \mid s \in M\} \cap M = \emptyset$. *Тогда*

$$\mathrm{CT}\left[\prod_{1\le i<j\le n}\left(\frac{x_i}{x_j}\right)_{a_i^*}\left(\frac{qx_j}{x_i}\right)_{a_j^*}\right] = \frac{1-q^{1+|\boldsymbol{a}|}}{1-q^{1+\sum_{v\notin M} a_v}}\begin{bmatrix}|\boldsymbol{a}|\\ \boldsymbol{a}\end{bmatrix},$$

где $a_i^* = a_i^*(j) = a_i + \chi(j \in M, i = r_j)$ *и* $a_j^* = a_j^*(i) = a_j + \chi(i \in M, j = r_i)$.

Чжоу [101] показал, что эта гипотеза неверна уже при $n = 3$, $|M| = m = 1$, и доказал осмысленный q-аналог гипотезы Каделла. Мы не приводим его здесь в силу его технической сложности, однако подробности могут быть найдены в работе [101].

Основный результат данного параграфа заключается в доказательстве частного случая гипотезы 1, соответствующих случаю $M = \{1,\ldots,m\}$ и $r_s \equiv n$, который не следует из общего результата Чжоу [101].

Теорема 10. *Пусть* $m < n$. *Тогда*

$$\mathrm{CT}\left[\prod_{1\le i<j\le n}\left(\frac{x_i}{x_j}\right)_{a_i}\left(\frac{qx_j}{x_i}\right)_{a_j^*}\right] = \frac{1-q^{1+|\boldsymbol{a}|}}{1-q^{1+\sum_{v=m+1}^{n} a_v}}\begin{bmatrix}|\boldsymbol{a}|\\ \boldsymbol{a}\end{bmatrix},$$

где $a_n^* = a_n + \chi(i \le m)$ *и* $a_j^* = a_j$ *в противном случае.*

Доказательство. Заметим, что если $a_i = 0$ при некотором $i < n$, то мы можем опустить все множители включающие переменную x_i без изменения свободного члена. Таким образом, мы можем считать что каждое из чисел a_i, за исключением, возможно, a_n является натуральным числом. Очевидно, что интересующий нас свободный член является коэффициентом при мономе

$$\prod_{i=1}^{n} x_i^{|\boldsymbol{a}|-a_i+\chi(i\le m)}$$

в однородном многочлене

$$F(\boldsymbol{x}) = \prod_{1\le i<j\le n}\left(\prod_{k=0}^{a_i-1}(x_j - x_i q^k) \times \prod_{k=1}^{a_j^*}(x_i - x_j q^k)\right),$$

где

$$a_j^* = \begin{cases} a_j + 1 & \text{если } j = n \text{ и } i \le m,\\ a_j & \text{иначе.}\end{cases}$$

Чтобы выразить этот коэффициент мы используем теорему 5 для поля $\mathbb{F} = \mathbb{Q}(q)$. Как и ранее нам было бы удобно выбрать множества C_i таким образом, что $F(\boldsymbol{c}) = 0$ для всех точек $\boldsymbol{c} \in C_1 \times \cdots \times C_n$, кроме одной. Этого легко можно достичь следующим образом. Пусть $C_i = \{q^{\alpha_i} \mid \alpha_i \in B_i\}$, где

$$B_i = \{0,1,\ldots,|\boldsymbol{a}| - a_i + \chi(i \le m)\}.$$

Легко видеть, что множества C_i имеют требуемый размер. Предположим теперь, что $c_i = q^{\alpha_i} \in C_i$ и $F(\boldsymbol{c}) \neq 0$. Тогда все α_i различны. Более того

$$\alpha_j \ge \alpha_i + a_i + \chi(j < i) + \chi(i = n, j \le m)$$

при всех $\alpha_j > \alpha_i$. Далее рассмотрим единственную перестановку $\pi \in \mathfrak{S}_n$ такую, что

$$0 \le \alpha_{\pi(1)} < \alpha_{\pi(2)} < \cdots < \alpha_{\pi(n)} \le |\boldsymbol{a}| - a_{\pi(n)} + \chi(\pi(n) \le m).$$

Мы получаем следующую цепочку неравенств

$$|\boldsymbol{a}| - a_{\pi(n)} = \sum_{i=1}^{n-1} a_{\pi(i)} \le \sum_{i=1}^{n-1} (\alpha_{\pi(i+1)} - \alpha_{\pi(i)}) = \alpha_{\pi(n)} - \alpha_{\pi(1)} \le |\boldsymbol{a}| - a_{\pi(n)} + 1.$$

Отметим, что первое неравенство является точным, если π не тождественная перестановка, а второе — если $\pi(n) > m$. Предположим, что $\pi(n) \neq n$. Тогда во всяком случае $\pi \neq \mathrm{id}$, а значит $\pi(n) \le m$. Рассмотрим индекс i такой, что $\pi(i) = n$. Тогда $\alpha_{\pi(i+1)} - \alpha_{\pi(i)} = a_{\pi(i)} + 1$, откуда следует, что $\pi(i+1) > m$. Значит найдется индекс $i+1 \le j < n$ такой, что $\pi(j) > m$ и $\pi(j+1) \le m$. Для такого j получаем $\alpha_{\pi(j+1)} - \alpha_{\pi(j)} \ge a_{\pi(j)} + 1$, то есть

$$|\boldsymbol{a}| - a_{\pi(n)} = \sum_{i=1}^{n-1} a_{\pi(i)} \le \sum_{i=1}^{n-1} (\alpha_{\pi(i+1)} - \alpha_{\pi(i)}) - 2 \le |\boldsymbol{a}| - a_{\pi(n)} - 1,$$

что ведет к противоречию Таким образом мы выводим, что $\pi(n) = n$, следовательно $\pi = \mathrm{id}$ и $\alpha_i = a_1 + \cdots + a_{i-1}$ при всех i. Осталось лишь подставить данную точку в

$$\frac{F(c_1,c_2,\ldots,c_n)}{\phi_1'(c_1)\phi_2'(c_2)\cdots\phi_n'(c_n)},$$

и провести довольно стандартные технические вычисления. Чтобы не перегружать доказательство этими техническими подробностями мы отметим, что в работе [62] подстановка тех же самых значений в ту же формулу для

$$F(\boldsymbol{x}) = \prod_{1\le i<j\le n} \left(\prod_{k=0}^{a_i-1} (x_j - x_i q^k) \times \prod_{k=1}^{a_j} (x_i - x_j q^k) \right)$$

и $B_i = \{0,1,\ldots,|\boldsymbol{a}| - a_i\}$ приводит к q-соотношению Дайсона на свободный член $\mathrm{CT}[\mathcal{D}_q(\boldsymbol{x};\boldsymbol{a})]$. Небольшие отличия от проведенного в той работе вычисления легко проконтролировать и отмечая, что $\alpha_i + a_i = \alpha_{i+1}$, $\alpha_n + a_n = |\boldsymbol{a}|$ мы получаем, что требуемый свободный член действительно равен

$$\prod_{i=1}^{m} \frac{q^{\alpha_i} - q^{\alpha_n + a_n + 1}}{q^{\alpha_i} - q^{|a| - a_i + 1}} \begin{bmatrix} |\boldsymbol{a}| \\ \boldsymbol{a} \end{bmatrix} = \frac{1 - q^{1+|\boldsymbol{a}|-\alpha_1}}{1 - q^{1+|\boldsymbol{a}|-\alpha_{m+1}}} \begin{bmatrix} |\boldsymbol{a}| \\ \boldsymbol{a} \end{bmatrix}.$$

□

При специализации полученного соотношения в точке $q = 1$ с учетом симметричности произведения Дайсона мы получаем следующий частный случай гипотезы 2 [100], который уже сам по себе влечет (4.1).

Следствие 2. *Пусть $m < n$, $M \subset \{1,\ldots,n\}$, причем $|M| = m$ и $r \in \{1,\ldots,n\} \setminus M$. Тогда*

$$\mathrm{CT}\left[\prod_{s\in M} \left(1 - \frac{x_r}{x_s}\right) \mathcal{D}(\boldsymbol{x};\boldsymbol{a}) \right] = \frac{1 + |\boldsymbol{a}|}{1 + \sum_{v\notin M} a_v} \binom{|\boldsymbol{a}|}{\boldsymbol{a}}.$$

Напоследок заметим, что случай $m = 1$ данного следствия вместе с теоремой Цейльбергера-Брессоуда немедленно влечет результат Силлса (теорему 1.1. [103]): при $1 \le r \ne s \le n$,

$$\mathrm{CT}\left[(x_r/x_s)\mathcal{D}(\boldsymbol{x};\boldsymbol{a})\right] = \frac{-a_s}{1 + |\boldsymbol{a}| - a_s} \binom{|\boldsymbol{a}|}{\boldsymbol{a}}.$$

Вообще говоря, пользуясь формулой включений-исключений можно также получить формулу для свободного члена

$$\left(x_r^m / \textstyle\prod_{s\in M} x_s\right) \mathcal{D}(\boldsymbol{x};\boldsymbol{a}),$$

которая будет согласована с результатом теоремы 1.7 [102].

4.2 Интегральная формула Селберга

В силу равносильности интегральной формулы Селберга соотношению Морриса, нам будет достаточно доказать лишь последнее. Напомним формулировку соотношения Морриса:

$$\mathrm{CT}\left[\prod_{j=1}^{n}(1-x_j)^a(1-1/x_j)^b\mathcal{D}(\boldsymbol{x};k)\right]=\prod_{j=0}^{n-1}\frac{(a+b+kj)!(kj+k)!}{(a+kj)!(b+kj)!k!}. \tag{4.2}$$

Вводя дополнительную переменную можно превратить любой многочлен Лорана в однородный. Таким образом, чтобы найти свободный член многочлена Лорана

$$\mathcal{M}(x_0,\boldsymbol{x};a,b,k):=\prod_{j=1}^{n}\left(1-\frac{x_j}{x_0}\right)^a\left(1-\frac{x_0}{x_j}\right)^b\prod_{1\le i\ne j\le n}\left(1-\frac{x_i}{x_j}\right)^k,$$

достаточно определить коэффициент при $x_0^{na}\prod_{i=1}^n x_i^{(n-1)k+b}$ у однородного многочлена

$$\prod_{j=1}^{n}(x_0-x_j)^a(x_j-x_0)^b\times\prod_{1\le i\ne j\le n}(x_j-x_i)^k.$$

Как и ранее мы немного преобразуем этот многочлен в младших членах и рассмотрим многочлен

$$F(x_0,\boldsymbol{x})=\prod_{j=1}^{n}\prod_{e=-a}^{b-1}(x_j-x_0-e)\times\prod_{1\le i<j\le n}\prod_{e=-k}^{k-1}(x_j-x_i-e). \tag{4.3}$$

Теперь рассмотрим множества $C_i=\{0,1,\dots,(n-1)k+b\}$ при $1\le i\le n$ и мультимножество

$$C_0=\{0\}\cup\bigcup_{\ell=0}^{n-1}\{k\ell+1,k\ell+2,\dots,k\ell+a\},$$

и применим теорему 6. Отметим, что размеры выбранных множеств соответствуют условиям теоремы, кроме того при $k\ge a$ в множестве C_0 нет кратных элементов и поэтому мы могли бы обойтись теоремой 5. Рассмотрим теперь произвольный выбор $c_i \in C_i$ и $m_i < \omega_i(c_i)$. Отметим, что $m_i = 0$ при $1 \leq i \leq n$. Далее мы покажем, что

$$\frac{\partial^{m_0+\dots+m_n} F}{\partial x_0^{m_0} \dots \partial x_n^{m_n}}(c_0, \dots, c_n) = \frac{\partial^{m_0} F}{\partial x_0^{m_0}}(c_0, \dots, c_n) = 0$$

во всех таких точках, кроме одной.

Лемма 13. *Если* $c_0 \neq 0$, *то*

$$\frac{\partial^{m_0} F}{\partial x_0^{m_0}}(c_0, \dots, c_n) = 0. \tag{4.4}$$

Доказательство. Обозначим $S_\ell = \{k\ell + 1, k\ell + 2, \dots, k\ell + a\}$. Известно, что $m_0 < \omega_0(c_0)$, поэтому найдется индекс $0 \leq u \leq n - \omega_0(c_0)$ такой, что $c_0 \in S_u \cap S_{u+1} \cap \dots \cap S_{u+m_0}$. То есть

$$(u + m_0)k + 1 \leq c_0 \leq uk + a.$$

В таком случае, если c_j лежит в промежутке $[uk, (u + m_0)k + b]$ при некотором $1 \leq i \leq n$, то $c_0 - a \leq c_j \leq c_0 + b - 1$ и найдётся множитель вида $x_j - x_0 - e$ в F который обнуляется в точке $(c_0, \boldsymbol{c})$. Таким образом, если более чем m_0 таких c_i попадает в промежуток $[uk, (u + m_0)k + b]$, то соотношение (4.4) выполнено.

В противном случае или как минимум $u+1$ элемент из $c_1, \dots, c_n$ попадает в промежуток $[0, ku - 1]$, или как минимум $n - m_0 - u$ такой элемент попадает в промежуток $[(u + m_0)k + b + 1, (n - 1)k + b]$. В любом из этих случаев найдется пара индексов $1 \leq i < j \leq n$ такая, что $|c_j - c_i| < k$. Тогда найдется и множитель вида $x_j - x_i - e$ в F обнуляющийся в точке $(c_0, \boldsymbol{c})$, и опять же соотношение (4.4) выполнено. □

В силу вышеописанной леммы осталось рассмотреть лишь случай $c_0 = 0$. Имеем $\omega_0(c) = 1$ и $m_0 = 0$. Если в этом случае

$$\frac{\partial^{m_0} F}{\partial x_0^{m_0}}(c_0, \dots, c_n) = F(c_0, \boldsymbol{c}) \neq 0,$$

то $c_1, \dots, c_n \in [b, (n - 1)k + b]$ и $|c_j - c_i| \geq k$ для каждой пары $1 \leq i < j \leq n$. Следовательно числа $c_1, \dots, c_n$, должны, при некоторой перестановке совпадать с числами $b, k + b, \dots, (n - 1)k + b$. Более того, эта перестановка обязана быть тождественной, так как если $c_i > c_j$ при некоторых $i < j$, то $c_i - c_j \geq k + 1$. Осталось лишь вычислить значение выражения

$$\prod_{i=0}^{n} \kappa(C_i,c_i,0)F(c_0,\boldsymbol{c})$$

в последней возможной точке $(c_0,\boldsymbol{c}) = (0,b,k + b,\ldots,(n - 1)k + b)$. Так как $\omega_i(c_i) = 0$ при каждом i, то мы просто получаем

$$\kappa(C_i,c_i,0) = \frac{1}{\prod_{c\in C_i\setminus\{c_i\}}(c_i - c)^{\omega_i(c)}}$$

и элементарные сокращения дают нам соотношение (4.2).

Замечание. Для простоты изложения в описанном выше доказательстве по умолчанию предполагалось, что a, b, k являются натуральными числами. Однако доказательство выше несложно преобразовать, чтобы покрыть оставшиеся случаи (а именно $a = 0$, $b = 0$ или $k = 0$). Можно также заметить, что случаи $a = 0$ и $b = 0$ являются просто разнопараметрическим случаем соотношения Дайсона, а случай $k = 0$ сводится к соотношению Вандермонда.

Заменим теперь многочлен из соотношения (4.3) на многочлен

$$\prod_{j=1}^{n}\prod_{e=1}^{a}(x_0 - q^e x_j)\prod_{e=0}^{b-1}(x_j - q^e x_0) \times \prod_{1\leq i<j\leq n}\prod_{e=0}^{k-1}(x_j - q^e x_i)\prod_{e=1}^{k}(x_i - q^e x_j).$$

Также заменим каждое из мультимножеств C_i на мультимножества, которые состоят из степеней q с экспонентами из C_i, причем с теми же кратностями. Повторяя доказательство, представленное выше легко получаем следующую версию q-соотношения Морриса:

$$\mathrm{CT}\left[\prod_{j=1}^{n}(qx_j)_a(1/x_j)_b\mathcal{D}_q(\boldsymbol{x};k)\right] = \prod_{j=0}^{n-1}\frac{(q)_{a+b+kj}(q)_{kj+k}}{(q)_{a+kj}(q)_{b+kj}(q)_k}.$$

Соотношение, представленное в работе Морриса [66], выглядит несколько иначе:

$$\mathrm{CT}\left[\prod_{j=1}^{n}(x_j)_a(q/x_j)_b\mathcal{D}_q(\boldsymbol{x};k)\right] = \prod_{j=0}^{n-1}\frac{(q)_{a+b+kj}(q)_{kj+k}}{(q)_{a+kj}(q)_{b+kj}(q)_k}, \tag{4.5}$$

однако, легко видеть, что два данных выражения эквивалентны, так как все мономы степени ноль имеет одинаковые коэффициенты в многочленах Лорана $\prod_{j=1}^{n}(qx_j)_a(1/x_j)_b$ и $\prod_{j=1}^{n}(x_j)_a(q/x_j)_b$.

Гипотеза Морриса была независимо получена в работах [104] и [105] с помощью доказательства так называемой интегральной q-формулы Селберга, предложенной Аскеем [106]. Позднее более простое доказательство было получено в [107].

4.3 Матричная запись

Все соотношения на свободный член и их q-аналоги, изучаемые в данной работе могут быть сформулированы в следующем виде. Через $\boldsymbol{B} = (\beta_{ij})$ обозначим $(n+1)\times(n+1)$ матрицу со строками и столбцами, пронумерованными от 0 до n. Будем считать, что все числа в ячейках матрицы являются целыми неотрицательными и числа находящиеся на главной диагонали равны нулю. Такой матрице сопоставим многочлен Лорана

$$\mathcal{L}(x_0,\boldsymbol{x};\boldsymbol{B}) = \prod_{0\le i\ne j\le n}\left(1-\frac{x_i}{x_j}\right)^{\beta_{ij}}$$

и его q-аналог

$$\mathcal{L}_q(x_0,\boldsymbol{x};\boldsymbol{B}) = \prod_{0\le i<j\le n}\left(\frac{x_i}{x_j}\right)_{\beta_{ij}}\left(\frac{qx_j}{x_i}\right)_{\beta_{ji}}.$$

В частности, многочлены $\mathcal{D}(\boldsymbol{x};\boldsymbol{a}) = \mathcal{L}(x_0,\boldsymbol{x};\boldsymbol{B}_{\mathcal{D}})$ и $\mathcal{M}(x_0,\boldsymbol{x};a,b,k) = \mathcal{L}(x_0,\boldsymbol{x};\boldsymbol{B}_{\mathcal{M}})$ соответствующие матрицам

$$\boldsymbol{B}_{\mathcal{D}} = \left(\begin{array}{c|ccccc} 0 & 0 & 0 & 0 & \dots & 0 \\ \hline 0 & 0 & a_1 & a_1 & \dots & a_1 \\ 0 & a_2 & 0 & a_2 & \dots & a_2 \\ 0 & a_3 & a_3 & 0 & \dots & a_3 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & a_n & a_n & a_n & \dots & 0 \end{array}\right) \qquad \text{и} \qquad \boldsymbol{B}_{\mathcal{M}} = \left(\begin{array}{c|ccccc} 0 & b & b & b & \dots & b \\ \hline a & 0 & k & k & \dots & k \\ a & k & 0 & k & \dots & k \\ a & k & k & 0 & \dots & k \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a & k & k & k & \dots & 0 \end{array}\right)$$

представляют собой соответственно полиномы из соотношений Дайсона и Морриса, в то время как $\mathcal{D}_q(\boldsymbol{x};\boldsymbol{a}) = \mathcal{L}_q(x_0,\boldsymbol{x};\boldsymbol{B}_{\mathcal{D}})$ соответствует q-соотношению Морриса. Заметим, что одновременная перестановка строчек и столбцов $\boldsymbol{B}$ по одному и тому же элементу из $\mathfrak{S}_{n+1}$ никак не влияет на $\mathrm{CT}[\mathcal{L}(x_0,\boldsymbol{x};\boldsymbol{B})]$. Вообще говоря аналогичное неверно для $\mathrm{CT}[\mathcal{L}_q(x_0,\boldsymbol{x};\boldsymbol{B})]$, но как уже было отмечено при доказательстве q-соотношения Морриса в параграфе 4.2, мы всегда можем применить циклическую перестановку

$$n \to n-1 \to \cdots \to 1 \to 0 \to n$$

или её степень без изменения свободного члена.

Теорема 10 рассматривает свободный член $\mathrm{CT}[\mathcal{L}_q(x_0,\boldsymbol{x};\boldsymbol{B}_{\mathcal{K}})]$ соответствующий матрице

$$\boldsymbol{B}_{\mathcal{K}} = \left(\begin{array}{c|cccc|cccc}
0 & 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 \\ \hline
0 & 0 & a_1 & \dots & a_1 & a_1 & \dots & a_1 & a_1 \\
0 & a_2 & 0 & \dots & a_2 & a_2 & \dots & a_2 & a_2 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & a_m & a_m & \dots & 0 & a_m & \dots & a_m & a_m \\ \hline
0 & a_{m+1} & a_{m+1} & \dots & a_{m+1} & 0 & \dots & a_{m+1} & a_{m+1} \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & a_{n-1} & a_{n-1} & \dots & a_{n-1} & a_{n-1} & \dots & 0 & a_{n-1} \\
0 & a_n+1 & a_n+1 & \dots & a_n+1 & a_n & \dots & a_n & 0
\end{array}\right).$$

Применяя введённую выше циклическую перестановку к $\boldsymbol{B}_{\mathcal{K}}$, после перестановки индексов мы получаем следующее обобщение теоремы 10.

Теорема 11. *Зафиксируем произвольное целое число $r \in \{1,2,\dots,n\}$. Тогда гипотеза 1 справедлива при выборе $M = \{r+1,\dots,r+m\}$ и $r_s \equiv r$, где индексы рассматриваются по модулю n.*

Соотношение Аомото (2) и гипотеза Форрестера, на этом языке, относятся к матрицам

$$\boldsymbol{B}_{\mathcal{A}} = \left(\begin{array}{c|ccc|ccc} 0 & b & \dots & b & b & \dots & b \\ \hline a & 0 & \dots & k & k & \dots & k \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a & k & \dots & 0 & k & \dots & k \\ \hline a+1 & k & \dots & k & 0 & \dots & k \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a+1 & k & \dots & k & k & \dots & 0 \end{array}\right) \quad \text{и} \quad \boldsymbol{B}_{\mathcal{F}} = \left(\begin{array}{c|ccc|ccc} 0 & b & \dots & b & b & \dots & b \\ \hline a & 0 & \dots & k & k & \dots & k \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a & k & \dots & 0 & k & \dots & k \\ \hline a & k & \dots & k & 0 & \dots & k+1 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a & k & \dots & k & k+1 & \dots & 0 \end{array}\right)$$

где отделенными являются соответственно последние m, $n-n_0$ строк и столбцов. В первом случае мы перестроили матрицу так, чтобы вид q-аналога соответствовал нашему методу. Основной же результат работы, сформулированный в следующем параграфе, касается наложения данных матриц, при $m \geq n-n_0$. Мы получаем матрицу:

$$\boldsymbol{B}_{\mathcal{AF}} = \left(\begin{array}{c|ccc|ccc|ccc} 0 & b & \dots & b & b & \dots & b & b & \dots & b \\ \hline a & 0 & \dots & k & k & \dots & k & k & \dots & k \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a & k & \dots & 0 & k & \dots & k & k & \dots & k \\ \hline a+1 & k & \dots & k & 0 & \dots & k & k & \dots & k \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a+1 & k & \dots & k & k & \dots & 0 & k & \dots & k \\ \hline a+1 & k & \dots & k & k & \dots & k & 0 & \dots & k+1 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a+1 & k & \dots & k & k & \dots & k & k+1 & \dots & 0 \end{array}\right) \quad \begin{array}{c} 0 \\ \hline 1 \\ \vdots \\ n-m \\ \hline n-m+1 \\ \vdots \\ n_0 \\ \hline n_0+1 \\ \vdots \\ n \end{array} .$$

4.4 Гипотеза Форрестера

Перейдем к формулировке основного результата данной главы.

Теорема 12. *Пусть n — натуральное число. Для произвольных целых неотрицательных чисел a,b,k и m,$n_0 \le n \le m + n_0$, имеет место*

$$\mathrm{CT}[\mathcal{L}_q(x_0,\boldsymbol{x};\boldsymbol{B}_{\mathcal{AF}})] = \prod_{j=0}^{n-1} \frac{(q)_{a+b+kj+\chi(j>n_0)(j-n_0)+\chi(j\ge n-m)}(q)_{kj+\chi(j>n_0)(j-n_0)+k}}{(q)_{a+kj+\chi(j>n_0)(j-n_0)+\chi(j\ge n-m)}(q)_{b+kj+\chi(j>n_0)(j-n_0)}(q)_k} \times \\ \times \prod_{j=1}^{n-n_0} \frac{1-q^{(k+1)j}}{1-q^{k+1}}.$$

В случае $m = 0$, из этой теоремы следует гипотеза Бейкера и Форрестера (гипотеза 2.1 [71]), а при специализации в $q = 1$ получается соответственно оригинальная гипотеза Форрестера. Случай же $n_0 = n$ дает следующий q-аналог соотношения Аомото.

Следствие 3. *Пусть n целое положительное число. Для произвольных целых неотрицательных a,b,k и $m \le n$,*

$$\mathrm{CT}[\mathcal{L}_q(x_0,\boldsymbol{x};\boldsymbol{B}_{\mathcal{A}})] = \prod_{j=0}^{n-1} \frac{(q)_{a+b+kj+\chi(j\ge n-m)}(q)_{kj+k}}{(q)_{a+kj+\chi(j\ge n-m)}(q)_{b+kj}(q)_k}.$$

Обобщение этого последнего соотношения, которое требует дополнительного параметра связанного с b, можно найти в работе Каделла [105]. Элементарное доказательство данного обобщения представлено в работе Синя и Чжоу [108]. Заменяя k на $k+1$, мы получаем, что Теорема 12 верна для любого $m \le n$ при $n_0 = 0$.

4.4.1 Доказательство соотношения Аомото-Форрестера

Очевидно, что свободный член $\mathrm{CT}[\mathcal{L}_q(x_0,\boldsymbol{x};\boldsymbol{B})]$ равен коэффициенту при $\prod_j x_j^{B_j}$, где $B_j = \sum_i \beta_{ij}$, в многочлене

$$F_q(x_0,\boldsymbol{x};\boldsymbol{B}) := \prod_{0\le i<j\le n} \left(\prod_{t=0}^{\beta_{ij}-1} (x_j - q^t x_i) \times \prod_{t=1}^{\beta_{ji}} (x_i - q^t x_j) \right).$$

Утверждение 1. *Предположим, что* $c_i = q^{\alpha_i}$ *для некоторых целых* α_i*, таких что* $F_q(c_0,\boldsymbol{c};\boldsymbol{B}) \neq 0$. *Пусть* $j > i$. *Тогда при* $\alpha_j \geq \alpha_i$ *верно, что* $\alpha_j \geq \alpha_i + \beta_{ij}$*, обратно из* $\alpha_i > \alpha_j$ *следует, что* $\alpha_i \geq \alpha_j + \beta_{ji} + 1$. *Оба утверждения справедливы, даже если соответствующий элемент из* $\boldsymbol{B}$ *равен нулю. То же остается верно при замене* F_q *на любую из его частных производных, для которых* $m_i = m_j = 0$. □

Мы применим теорему 6 к многочлену $F = F_q(.;\boldsymbol{B}_{\mathcal{AF}})$. Аналогично разделу 4.2, мы будем считать a,b,k натуральными числами, так как именно этот случай представляет наибольший интерес. Остальные случаи несложно разобрать пользуясь аналогичными методами.

Выбор мультимножеств C_i

Пусть $\gamma_i = \beta_{in}$ при $0 \leq i < n$ и $\Delta_t = \sum_{i=0}^{t} \gamma_i$. Тогда,

$$\gamma_0 = b,\ \gamma_1 = \cdots = \gamma_{n_0} = k,\ \gamma_{n_0+1} = \cdots = \gamma_{n-1} = k+1$$

и $\beta_{ij} = \gamma_{\min\{i,j\}}$ при $1 \leq i \neq j \leq n$. Рассмотрим промежутки $I_t = [\Delta_t - \gamma_t + 1,\Delta_t] = [\Delta_{t-1} + 1,\Delta_t]$. Здесь и далее за $[u,v]$ обозначен набор целых чисел ℓ удовлетворяющих условию $u \leq \ell \leq v$. Интервалы $I_0 := [0,b],I_1 \ldots ,I_{n-1}$ попарно не пересекаются. Мультимножества C_i представим в виде $C_i = \{q^\alpha \mid \alpha \in A_i\}$, где при $1 \leq j \leq n$

$$A_j = \{0\} \cup \bigcup_{t=0}^{n-1} [\Delta_t - \gamma_{\min\{t,j\}} + 1,\Delta_t] \subseteq \bigcup_{t=0}^{n-1} I_t = [0,\Delta_{n-1}]$$

является обычным множеством, а

$$A_0 = \{0\} \cup \bigcup_{t=0}^{n-1} [\Delta_t - b + 1,\, \Delta_t - b + \beta_{t+1,0}]$$

является мультимножеством. Легко видеть, что $|C_i| = |A_i| = B_i+1$ справедливо для любого $0 \le i \le n$. Далее будет показано, что

$$\frac{\partial^{m_0+\dots+m_n} F}{\partial x_0^{m_0} \dots \partial x_n^{m_n}}(c_0,\dots,c_n) = \frac{\partial^{m_0} F}{\partial x_0^{m_0}}(c_0,\dots,c_n) = 0$$

при всех кроме одного набора $c_i \in C_i$ с кратностями $m_i < \omega_i(c_i)$, а именно при всех кроме $c_0 = 1$, $c_i = q^{\Delta_{i-1}}$ при $1 \le i \le n$, и все кратности равны нулю.

Комбинаторика

Рассмотрим произвольный вышеописанный набор и положим $c_i = q^{\alpha_i}$. Заметим, что $\omega_1(c_1) = \dots = \omega_n(c_n) = \omega_0(q^0) = 1$. Тогда утверждение выше следует из двух следующих лемм.

Лемма 14. *Пусть* $\alpha_0 = 0$. *Если* $F(c_0,c_1,\dots,c_n) \ne 0$, *тогда* $\alpha_i = \Delta_{i-1}$ *для любого* $1 \le i \le n$.

Лемма 15. *Если* $\alpha_0 \ne 0$, *то* $(\partial^{m_0} F/\partial x_0^{m_0})(c_0,\dots,c_n) = 0$.

Доказательство обеих лемм нетрудно вывести из представленного ниже следствия утверждения 1.

Лемма 16. *Предположим, что* $(\partial^{m_0} F/\partial x_0^{m_0})(c_0,\dots,c_n) \ne 0$. *Тогда для любого* $1 \le t \le n-1$ *существует не более одного индекса* $1 \le i \le n$ *такого, что* $\alpha_i \in I_t$.

Доказательство. Предположим противное, пусть есть пара индексов $1 \le i \ne j \le n$ таких, что $\alpha_i,\alpha_j \in I_t$. Пусть $\alpha_j \ge \alpha_i$, тогда из Утверждения 1 следует, что $\alpha_j - \alpha_i \ge k$. Длинна I_t равна $\gamma_t \in \{k,k+1\}$. Тогда, должно выполняться $\gamma_t = k+1$, $\alpha_i = \Delta_t - k$ и $\alpha_j = \Delta_t$. Вследствие чего, $t > n_0$, $i < j$ и $i \le n_0$. Отсюда $\Delta_t - \gamma_{\min\{t,i\}} + 1 = \Delta_t - k + 1$ и $\alpha_i \notin A_i$, противоречие. □

Доказательство леммы 14. Для любого $1 \le i \le n$ мы имеем $\alpha_i \ge \alpha_0$, следовательно $\alpha_i \ge \beta_{0i} = b$ согласно утверждению 1. Более того, $k > 0$ предполагает, что $\alpha_1,\dots,\alpha_n$ попарно различны, тогда из леммы 16 следует, что каждый из интервалов $I_0, I_1, \ldots, I_{n-1}$ содержит в точности одно из чисел α_i. Пусть $\pi \in \mathfrak{S}_n$ это единственная такая перестановка, для которой $\alpha_{\pi(1)} < \cdots < \alpha_{\pi(n)}$, тогда $\alpha_{\pi(i)} \in I_{i-1}$. Согласно Утверждению 1 мы имеем

$$\alpha_{\pi(i+1)} \geq \alpha_{\pi(i)} + \beta_{\pi(i),\pi(i+1)} + \chi(\pi(i) > \pi(i+1)).$$

В следствие чего,

$$\alpha_{\pi(n_0+1)} \geq b + kn_0 + \sum_{i=1}^{n_0} \chi(\pi(i) > \pi(i+1)) \geq \Delta_{n_0} + \sum_{i=1}^{n_0} \chi(\pi(i) > \pi(i+1)).$$

Поскольку $\alpha_{\pi(n_0+1)} \leq \Delta_{n_0}$, значит $\alpha_{\pi(1)} = b$, $\pi(1) < \cdots < \pi(n_0+1)$ и $\beta_{\pi(i),\pi(i+1)} = k$ for $1 \leq i \leq n_0$. Из чего в свою очередь следует, что $\pi(n_0) \leq n_0$, то есть $\pi(i) = i$ и $\alpha_i = \Delta_{i-1}$ при $1 \leq i \leq n_0$.

Теперь для $n_0 < i < n$ мы имеем $\pi(i), \pi(i+1) > n_0$ и таким образом $\beta_{\pi(i),\pi(i+1)} = k+1$. Ограничивая π на множество $[n_0+1, n]$ и проводя аналогичное рассуждение, начиная с $\alpha_{\pi(n_0+1)} = \Delta_{n_0}$, получаем полное доказательство леммы. □

Доказательство леммы 15. Предположим противное, пусть $(\partial^{m_0} F / \partial x_0^{m_0})(c_0, \ldots, c_n) \neq 0$. Положим $S_t = [\Delta_t - b + 1, \Delta_t - b + \beta_{t+1,0}]$. Поскольку $\alpha_0 \neq 0$ и $m_0 < \omega_0(c_0)$, значит существует индекс $0 \leq u \leq n - \omega_0(c_0)$ такой, что $\alpha_0 \in S_u \cap S_{u+1} \cap \cdots \cap S_{u+m_0}$. То есть,

$$\Delta_{u+m_0} - b + 1 \leq \alpha_0 \leq \Delta_u - b + \beta_{u+1,0}.$$

Соответственно, если α_j принадлежит промежутку

$$T_{uj} = [\Delta_u - b + \beta_{u+1,0} - \beta_{j0}, \Delta_{u+m_0}]$$

для какого-то $1 \leq j \leq n$, тогда $\alpha_0 - \beta_{j0} \leq \alpha_j \leq \alpha_0 + \beta_{0j} - 1$ и найдется член вида $x_j - q^t x_0$ или $x_0 - q^t x_j$ из F, который обнуляется в точке $(c_0, \boldsymbol{c})$. Тогда таких членов не более чем m_0. Отсюда, и из Леммы 16 следует, что максимум $n - 1 - u - m_0$ из попарно различных чисел $\alpha_1, \ldots, \alpha_n$ могут лежать в интервале $[\Delta_{u+m_0} + 1, \Delta_{n-1}]$.

Значит хотя бы $u + 1$ число из α_j удовлетворяет условию $\alpha_j \leq \Delta_u - b + \beta_{u+1,0} - \beta_{j0} - 1$. Это очевидно невозмжно, если $u + 1 \leq n - m$, так как тогда

$\Delta_u - b + \beta_{u+1,0} - \beta_{j0} - 1 \le uk - 1$ в силу $n - m \le n_0$, а с другой стороны разница между любыми двумя такими α_j хотя бы k согласно Утверждению 1. Тогда, $u \ge n - m$ и $\beta_{u+1,0} = a + 1$. Рассмотрим

$$\alpha_{\nu(1)} < \cdots < \alpha_{\nu(u+1)} \le \Delta_u - b + \beta_{u+1,0} - \beta_{\nu(u+1),0} - 1 \le \Delta_u - b.$$

Если $u \le n_0$, тогда должно имеет место $\alpha_{\nu(i)} = (i-1)k$ и $\nu(1) < \cdots < \nu(u+1)$, но это значит, что $\nu(u+1) \ge u+1 > n-m$, $\beta_{\nu(u+1),0} = a+1$, следовательно $\alpha_{\nu(u+1)} \in T_{u,\nu(u+1)}$, что не верно. Таким образом $u \ge n_0 + 1$. Легко видеть, что $\alpha_{\nu(i+1)} - \alpha_{\nu(i)} \ge \gamma_{\nu(i)}$ при $i \le u$, то есть $\alpha_{\nu(u+1)} \ge \sum_{i=1}^{u} \gamma_{\nu(i)} \ge \Delta_u - b$. Получаем, что $\sum_{i=1}^{u} \gamma_{\nu(i)} = \Delta_u - b$, это означает, что $\{\nu(1), \ldots, \nu(u)\} \supseteq \{1, \ldots, n_0\}$. В следствие этого, $\nu(u+1) \ge n_0 + 1 > n - m$, что также приводит к противоречию. $\square$

Вычисление

Осталось лишь вычислить

$$\frac{F_q(q^0, q^{\Delta_0}, \ldots, q^{\Delta_{n-1}}; \boldsymbol{B})}{\psi_0 \psi_1 \ldots \psi_n}, \tag{4.6}$$

где

$$\psi_j = \prod\nolimits_{\alpha \in A_j \setminus \{\Delta_{j-1}\}} (q^{\Delta_{j-1}} - q^{\alpha})$$

для $j = 1, \ldots n$, и в следующих обозначениях $\Delta_u^v = \gamma_u + \cdots + \gamma_v = \Delta_v - \Delta_{u-1}$,

$$\psi_0 = \prod_{t=0}^{n-1} \prod_{\alpha=\Delta_1^t+1}^{\Delta_1^t + \beta_{t+1,0}} (1 - q^{\alpha}) = \prod_{j=1}^{n} \left[\Delta_1^{j-1} + 1, \Delta_1^{j-1} + \beta_{j0}\right]_q. \tag{4.7}$$

Обозначим, $[u,v]_q := (1 - q^u) \ldots (1 - q^v) = (q)_v / (q)_{u-1}$, и вместо $[u,u]_q$ будем писать просто $[u]_q$. Как числитель, так и знаменатель в соотношении (4.6) является произведением множителей вида $\pm q^u (1 - q^v)$, где u, v некоторые неотрицательные целые числа. Точнее, собирая вместе множители схожей природы вместе мы обнаружим, что числитель является произведением множителей

$$(-1)^{\gamma_0} \times q^{1+\dots+(\gamma_0-1)} \times \left[\Delta_1^{j-1}+1,\Delta_0^{j-1}+\beta_{j0}\right]_q \quad \text{for} \quad 1 \le j \le n, \tag{4.8}$$

$$(-1)^{\gamma_i} \times q^{\Delta_{i-1}+\dots+(\Delta_{i-1}+\gamma_i-1)} \times \left[\Delta_i^{j-1}-\gamma_i+1,\Delta_i^{j-1}\right]_q \quad \text{for} \quad 1 \le i < j \le n, \tag{4.9}$$

и

$$q^{\gamma_i\Delta_{i-1}} \times \left[\Delta_i^{j-1}+1,\Delta_i^{j-1}+\gamma_i\right]_q \quad \text{for} \quad 1 \le i < j \le n. \tag{4.10}$$

В знаменателе же, кроме множителя (4.7) мы имеем

$$(-1) \times [\Delta_{j-1}]_q \times \psi_{j_<} \times \psi_{j_=} \times \psi_{j_>} \quad \text{for} \quad 1 \le j \le n, \tag{4.11}$$

где

$$\psi_{j_<} = \prod_{t=0}^{j-2} (-1)^{\gamma_t} \times q^{(\Delta_t-\gamma_t+1)+\dots+\Delta_t} \times \left[\Delta_{t+1}^{j-1},\Delta_{t+1}^{j-1}+\gamma_t-1\right]_q, \tag{4.12}$$

$$\psi_{j_=} = (-1)^{\gamma_{j-1}-1} \times q^{(\Delta_{j-1}-\gamma_{j-1}+1)+\dots+(\Delta_{j-1}-1)} \times [1,\gamma_{j-1}-1]_q, \tag{4.13}$$

и

$$\psi_{j_>} = \prod_{t=j}^{n-1} q^{\gamma_j\Delta_{j-1}} \times \left[\Delta_j^t-\gamma_j+1,\Delta_j^t\right]_q. \tag{4.14}$$

Теперь видно, что степени -1 и q сокращаются в силу элементарного соотношения

$$n\gamma_0 + \sum_{1\le i<j\le n} \gamma_i = n + \sum_{0\le t<j-1\le n-1} \gamma_t + \sum_{1\le j\le n} (\gamma_{j-1}-1)$$

и чуть менее тривиального соотношения

$$\begin{aligned} n\binom{\gamma_0}{2} + \sum_{1\le i<j\le n} \left(2\gamma_i\Delta_{i-1} + \binom{\gamma_i}{2}\right) = \\ = \sum_{0\le t<j-1\le n-1} \left(\gamma_t\Delta_t - \binom{\gamma_t}{2}\right) + \sum_{j=1}^{n} \left((\gamma_{j-1}-1)\Delta_{j-1} - \binom{\gamma_{j-1}-1}{2}\right) + \\ + \sum_{0\le j-1<t\le n-1} \gamma_j\Delta_{j-1}. \end{aligned}$$

Осталось разобраться с множителями вида $[u,v]_q$. Множители из (4.9) и (4.14) сокращаются. Множители из (4.8) и (4.7) дают

$$\prod_{j=1}^{n}\frac{(q)_{\Delta_0^{j-1}+\beta_{j0}}}{(q)_{\Delta_1^{j-1}+\beta_{j0}}}=\prod_{j=0}^{n-1}\frac{(q)_{a+b+kj+\chi(j>n_0)(j-n_0)+\chi(j\geq n-m)}}{(q)_{a+kj+\chi(j>n_0)(j-n_0)+\chi(j\geq n-m)}}. \tag{4.15}$$

Вклад остальных же множителей из (4.10) и (4.12) при подстановке $t+1=i$ представляется как

$$\begin{aligned}\prod_{1\leq i<j\leq n}\frac{\left[\Delta_i^{j-1}+1,\Delta_i^{j-1}+\gamma_i\right]_q}{\left[\Delta_i^{j-1},\Delta_i^{j-1}+\gamma_{i-1}-1\right]_q}&=\prod_{1\leq i<j\leq n}\frac{\left[\Delta_i^{j-1},\Delta_i^{j-1}+\gamma_i\right]_q\cdot\left[\Delta_i^{j-1}+\gamma_{i-1}\right]_q}{\left[\Delta_i^{j-1},\Delta_i^{j-1}+\gamma_{i-1}\right]_q\cdot\left[\Delta_i^{j-1}\right]_q}\\&=\prod_{j=2}^{n}\frac{\left[\Delta_1^{j-1},\Delta_1^{j-1}+\gamma_1\right]_q}{\left[\Delta_1^{j-1},\Delta_1^{j-1}+\gamma_0\right]_q}\times\Psi\times\prod_{1\leq i<j\leq n}\frac{\left[\Delta_{i-1}^{j-1}\right]_q}{\left[\Delta_i^{j-1}\right]_q}\\&=\prod_{j=2}^{n}\frac{(q)_{\Delta_1^{j-1}+\gamma_1}}{(q)_{\Delta_1^{j-1}+\gamma_0}}\times\Psi\times\prod_{j=2}^{n}\frac{\left[\Delta_{j-1}\right]_q}{1-q^{\gamma_{j-1}}},\end{aligned} \tag{4.16}$$

где множитель

$$\Psi=\prod_{j=n_0+2}^{n}\left[\Delta_{n_0+1}^{j-1}+\gamma_{n_0+1}\right]_q=\prod_{j=2}^{n-n_0}(1-q^{(k+1)j})$$

проявляет себя лишь при $n_0>0$. Приводя (4.16) вместе с произведением множителей $\left[\Delta_{j-1}\right]_q=1-q^{\Delta_{j-1}}$ из (4.11) и множителями $\left[1,\gamma_{j-1}-1\right]_q=(q)_{\gamma_{j-1}-1}$ из (4.13), после сдвига индексов получаем

$$\prod_{j=1}^{n-1}\frac{(q)_{\Delta_1^j+\gamma_1}}{(q)_{\Delta_1^j+\gamma_0}}\times\prod_{j=0}^{n-1}\frac{1}{(q)_{\gamma_j}}\times\left(\prod_{j=2}^{n-n_0}(1-q^{(k+1)j})\right)^{\chi(n_0>0)},$$

что в итоге даёт нам

$$\frac{(q)_{kj+\chi(j>n_0)(j-n_0)+k}}{(q)_{b+kj+\chi(j>n_0)(j-n_0)}(q)_k}\times\prod_{j=1}^{n-n_0}\frac{1-q^{(k+1)j}}{1-q^{k+1}}. \tag{4.17}$$

Объединяя результаты соотношений (4.15) и (4.17) получаем последний шаг доказательства Теоремы 12.

Замечание. Отметим, что в работе [83] приведён также альтернативный подход к доказательству Теоремы 12. Отличие состоит в том, что случай $a > k$ разбирается не с помощью использования мультимножеств и Теоремы 6, а с помощью специального рационального трюка, утверждающего, что формула для некоторых соотношений типа Дайсона обязана иметь особый вид, который имеет единственное продолжение со случая $k \geq a$ на все остальные.

Заключение

В заключение изложим краткое резюме каждой из основных глав, рассмотрим возможные направления дальнейшей работы и связанные открытые вопросы.

Явные формулы символа Гильберта. В данной главе была рассмотрена явная формула символа Гильберта для многочленной формальной группы в многомерном разнохарактеристическом поле. Явным образом были установлены корректность и основные свойства введённого спаривания и с помощью вычисления на базисе Шафаревича получено совпадение с классическим символом Гильберта. Данная глава демонстрирует, что классический подход к явным формулам для формальных групп, может быть применён, с небольшими изменениями, и в случае, когда коэффициенты формальной группы не лежат в подполе инерции основного поля. В работе был рассмотрен простейший подобный случай. Встаёт задача применения данного подхода, теперь, к другим менее элементарным группам подобного сорта.

Было бы также крайне интересно глубже изучить связь между явной формой закона взаимности и формулами представленными во второй и третьей главе работы. Возможно, есть способ получить некоторое абстрактное утверждение в большей общности, спецификациями которого, являлись бы как явная форма закона взаимности, так и различные версии комбинаторной теоремы о нулях. Наиболее подходящим на данную роль из известных автору утверждений является основной результат работы [51].

Комбинаторная теорема о нулях. Эта глава посвящена различным подходам и обобщениям комбинаторной теоремы о нулях, а также комбинаторным следствиям из них, связанным, в основном, с задачами сумм с ограничениями.

В первой части главы рассматриваются варианты комбинаторной теоремы о нулях дающие точную формулу на определённый коэффициент многочлена. Изложен абстрактный подход к подобным результатам с помощью тензоров. С его помощью вновь устанавливается результат Петрова-Карасёва в несколько более общей форме, а затем выводится версия комбинаторной теоремы о нулях для мультимножеств. Первая часть главы завершается версией комбинаторной теоремы о нулях для аффинных гиперповерхностей.

Во второй части главы данные результаты применяются для получения результатов в аддитивной комбинаторике. Здесь представлен новый подход к теореме Диаса да Сильвы-Хэмидона, теореме Алона-Натасона-Ружи, результатам Синя, Суня и Е, связанных с размерами сумм с ограничениями. Завершается данная глава новым вариантом теоремы Коши-Дэвенпорта для алгебраической сложности.

Представленные в этой главе результаты демонстрируют широкую универсальность полиномиального метода в задачах сумм с ограничениями. Естественным образом возникает вопрос о границах её применимости. Было бы интересно изучить этот вопрос детальнее, в частности, исследовать применимость комбинаторной теоремы о нулях к другим известным результатам этой области. Отметим один из этих результатов, установленный в работе [95], относительно которого автору неизвестно поддаётся ли он полиномиальному методу.

Задача. Пусть $h_r(\boldsymbol{x}) = \sum_{1\le j_1\le\dots\le j_r\le n} x_{j_1}\dots x_{j_r}$ — симметрический однородный многочлен степени r. С помощью комбинаторной теоремы о нулях установить соотношение:

$$\mathrm{CT}\left[x_1^{-ra_1}\dots x_n^{-ra_n} h_r(x_1,\dots,x_n)^{a_1+\dots+a_n}\prod\nolimits_{i\ne j}(1-x_j/x_i)^{a_i}\right] = \binom{|\boldsymbol{a}|}{\boldsymbol{a}}.$$

Чжоу [109] установил связь между суммами с ограничениями и соотношением Морриса, изучаемым в третьей главе данной работы. Другим направлением дальнейшей работы является изучение этой связи под призмой представленного полиномиального метода. Возможно это позволит перенести некоторые результаты из одной области в другую и определить границы применимости комбинаторной теоремы о нулях в каждой из областей.

Соотношения на свободный член. Данная глава применяет результаты предыдущей к задачам соотношений на свободный член, связанными с интегральной формулой Селберга. Сначала данный подход применяется для получения некоторой q-версии соотношения Каделла. Затем устанавливается соотношение Морриса, как хорошо известно, равносильное классической интегральной формуле Селберга. Далее, для технического удобства, вводится матричная запись подобных соотношений. Наконец в последней части главы устанавливается её основной результат: соотношение Аомото-Форрестера, следствиями которого, являются одновременно соотношение Аомото и гипотеза Форрестера.

Все полученные в данной главе формулы с точностью до небольших вариаций обладают схожей структурой. Интересно было бы установить для каких именно семейств матриц $\boldsymbol{B}$ представленный метод позволяет установить аналогичную формулу. Отметим, что в оригинальной работе [83] была высказана гипотеза о том, что для матриц Аомото-Форрестера условие $n \leqslant m + n_0$ может быть опущено, однако недавно с помощью прямых вычислений она была опровергнута И. В. Пышкиным и А. С. Гордеевым.

Задача. Определить семейство матриц $\boldsymbol{B}$, для которых описанное в работе применение полиномиального метода, позволяет получить замкнутую формулу, наподобие формулы Аомото-Форрестера.

Другим направлением дальнейшей работы является следующее. Рассматриваемые в данной главе соотношения тесно связаны с соотношениями Макдональда [110]. Данные соотношения были установлены И. В. Чередником [111], с помощью двойных афинных алгебр Гекке. Возникает задача получения этих соотношений в схожей данной главе манере. Скорее всего данная цель потребует обобщения комбинаторной теоремы о нулях для систем корней.

Задача. Получить соотношения Макдональда с помощью полиномиального метода.

Список литературы

1. *Шафаревич И. Р.* Общий закон взаимности // Матем. сб. — 1950. — Т. 26(68), № 1. — С. 113—146.
2. *Востоков С. В.*, *Иванов М. А.* Интегральная теорема Коши и классический закон взаимности // Учен. зап. Казан. ун-та. Сер. Физ.-матем. науки. — 2012. — Т. 154. — С. 73—82.
3. *Kummer E.* Uber die allgemeinen Reziprozitatsgesetze der Potenzreste // J. reine und angew. Math. — 1858. — Jg. 56. — S. 270–279.
4. *Artin E.*, *Hasse H.* Die beiden Erganzungssatze zum Reziprozitatsgesetz der l^n-ten Potenzreste im Korper der l^n-ten Einheitswurzeln // Abh. Mathem. Seminar, Hamburg. — 1928. — Jg. 6. — S. 146–162.
5. *Iwasawa K.* On explicit formulas for the norm residue symbol // J. Math. Soc. Japan. — 1968. — Vol. 20. — Pp. 151–164.
6. *Sen S.* On explicit reciprocity laws I, II // J. reine und angew. Math. — 1981. — Vol. 323. — Pp. 69–87.
7. *Wiles A.* Higher reciprocity laws // Ann. Math. — 1978. — Vol. 107. — Pp. 235–254.
8. *Колывагин В. А.* Формальные группы и символ норменного вычета // Изв. АН СССР, Сер. матем. — 1979. — Т. 43. — С. 1054—1120.
9. *Coleman R.* The dilogarithm and the norm residue symbol // Bull. Soc. Math. France. — 1981. — Vol. 109. — Pp. 373–402.
10. *Shalit E. de* The explicit reciprocity law in local class field theory // Duke Math. J. — 1986. — Vol. 53. — Pp. 163–176.
11. *Destrempes F.* Explicit reciprocity laws for Lubin-Tate modules // J. reine und angew. Math. — 1995. — Vol. 463. — Pp. 27–47.
12. *Benois D.* Periodes p-adiques et lois de reciprocite explicites // J. reine und angew. Math. — 1997. — T. 493. — P. 115–151.
13. *Hensel K.* Die multiplicative Dars ellung der algebraischen Zahlen fur den Bereich eines beliebigen Prin teil // Journ. fur die reine und a gew. Math. — 1916. — Jg. 136.

14. *Востоков С. В.* Явная форма закона взаимности // Изв. АН СССР, Сер. матем. — 1978. — Т. 42, № 6. — С. 1288—1321.

15. *Bruckner H.* Explizites Reziprozitatsgesetz und Anwendungen // Vorlesungen aus dem Fachbereich Mathematik der Universitat Essen. — 1979.

16. *Востоков С. В.* Норменное спаривание в формальных модулях // Изв. АН СССР, Сер. матем. — 1979. — Т. 43, № 4. — С. 765—794.

17. *Востоков С. В.* Символы на формальных модулях // Изв. АН СССР, Сер. матем. — 1981. — Т. 45, № 5. — С. 985—1014.

18. *Востоков С. В.* Символ Гильберта для формальных групп Любина-Тэйта I. // Зап. научн. семин. ЛОМИ. — 1982. — Т. 114. — С. 77—95.

19. *Востоков С. В.*, *Фесенко И. Б.* Символ Гильберта для формальных групп Любина-Тэйта II. // Зап. научн. семин. ЛОМИ. — 1983. — Т. 132. — С. 85—96.

20. *Фесенко И. Б.* Обобщенный символ Гильберта в 2-адическом случае // Вестник Ленингр. унив., матем., мех., астрон. — 1985. — Т. 18. — С. 88—91.

21. *Востоков С. В.*, *Демченко О. В.* Явная форма спаривания Гильберта для относительных формальных групп Любина–Тэйта // Зап. научн. сем. ПОМИ. — 1995. — Т. 227. — С. 41—44.

22. *Востоков С. В.*, *Бенуа Д. Г.* Норменное спаривание в формальных группах и представления Галуа // Алгебра и анализ. — 1990. — Т. 2, № 6. — С. 69—79.

23. *Востоков С. В.*, *Демченко О. В.* Явная формула спаривания Гильберта для формальных групп Хонды // Зап. научн. сем. ПОМИ. — 2000. — Т. 272. — С. 86—128.

24. *Мадунц А. И.*, *Востокова Р. П.* Формальные модули для обобщенных групп Любина–Тейта // Зап. научн. сем. ПОМИ. — 2015. — Т. 435. — С. 95—112.

25. *Абрашкин В. А.* Явные формулы для символа Гильберта формальной группы над векторами Витта // Изв. РАН., Сер. матем. — 1997. — Т. 61, № 3. — С. 3—56.

26. *Tavares Ribeiro F.* An explicit formula for the Hilbert symbol of a formal group // Annales de l'institut Fourier. — 2011. — Vol. 61, no. 1. — Pp. 261–318.

27. *Kato K.* A generalization of local class field theory by using K-groups. I. // Proc. Jap. Acad. — 1977. — Vol. 53. — Pp. 140–143.

28. *Kato K.* A generalization of local class field theory by using K-groups. II. // Proc. Jap. Acad. — 1978. — Vol. 54. — Pp. 250–255.

29. *Kato K.* A generalization of local class field theory by using K-groups. II. // J . Fac. Sci. Univ, Tokyo. — 1979. — Vol. 26. — Pp. 303–376.

30. *Kato K.* The Existence theorem for higher local class field theory. — Inst. Hautes Etudes Sci. Publ. Math., preprint, 1980.

31. *Паршин А. Н.* Поля классов и алгебраическая K-теория // Успехи мат. наук. — 1975. — Т. 30, № 1. — С. 253—254.

32. *Паршин А. Н.* К арифметике двумерных схем. I. Распределения и вычеты. // Изв. АН СССР. Сер мат. — 1976. — Т. 40. — С. 736—773.

33. *Паршин А. Н.* Абелевы накрытия арифметических схем. // Докл. АН СССР. — 1978. — Т. 243, № 4. — С. 855—858.

34. *Паршин А. Н.* Локальная теория полей классов // Тр. Матем. ин-та им. В. А. Стеклова АН СССР. — 1984. — Т. 165. — С. 143—170.

35. *Востоков С. В.* Явная конструкция теории полей классов многомерного локального поля // Изв. АН СССР. Сер. матем. — 1985. — Т. 49, № 2. — С. 283—308.

36. *Фесенко И. Б.* Теория полей классов многомерных локальных полей нулевой характеристики с полем вычетов положительной характеристики // Алгебра и анализ. — 1991. — Т. 3, № 3. — С. 649—678.

37. *Востоков С. В.* Спаривание Гильберта в полном многомерном поле // Тр. МИАН, Наука, Физматлит, М. — 1995. — Т. 208. — С. 80—92.

38. *Беккер Б. М.* Абелевы расширения полного дискретно нормированного поля конечной высоты // Алгебра и анализ. — 1991. — Т. 3, № 6. — С. 76—84.

39. *Fesenko I. B.* Abelian extensions of complete discrete valuation fields and their norm groups // Adv. Sov. Math. — 1994.

40. *Vostokov S. V.*, *Lorenz F.* Honda Groups and Explicit Pairings on the Modules of Cartier Curves // Contemp. Math. — 2002. — Vol. 300. — Pp. 143–170.

41. *Востоков С. В.*, *Лоренц Ф.* Явная формула символа Гильберта для групп Хонды в многомерном локальном поле // Матем. сб. — 2003. — Т. 194:2. — С. 3—36.

42. *Востоков С. В.*, *Афанасьева С. С.*, *Беккер Б. М.* Символ Гильберта в многомерных локальных полях для формальной группы Любина–Тейта // Зап. научн. сем. ПОМИ. — 2012. — Т. 400. — С. 20—49.

43. *Alon N.*, *Nathanson M. B.*, *Ruzsa I. Z.* The polynomial method and restricted sums of congruence classes // J. Number Theory. — 1996. — Т. 56. — С. 404—417.

44. *Alon N.* Combinatorial Nullstellensatz // Combin. Probab. Comput. — 1999. — Т. 8. — С. 7—29.

45. *Lasoń M.* A generalization of Combinatorial Nullstellensatz // Electron. J. Combin. — 2010. — Т. 17.

46. *Karasev R. N.*, *Petrov F. V.* Partitions of nonzero elements of a finite field into pairs // Israel J. Math. — 2012. — Т. 192. — С. 143—156.

47. *Dias da Silva J. A.*, *Hamidoune Y. O.* Cyclic spaces for Grassmann derivatives and additive theory // Bull. London Math. Soc. — 1994. — Т. 26. — С. 140—146.

48. *Alon N.* Additive Latin transversals // Israel J. Math. — 2000. — Т. 117. — С. 125—130.

49. *Dvir Z.* On the size of Kakeya sets in finite fields // J. the Amer. Math. Soc. — 2009. — Т. 22. — С. 1093—1097.

50. *Karasev R. N.* Residues and the Combinatorial Nullstellensatz. — 2015. — URL: arXiv:1503.08004.

51. Traces in strict Frobenius algebras and strict complete intersections / Kunz [u. a.] // Journal fur die reine und angewandte Mathematik. — 1987. — Jg. 381. — S. 181–204.

52. *Forrester P. J.* Normalization of the wavefunction for the Calogero–Sutherland model // Int. J. Mod. Phys. B. — 1995. — T. 9. — C. 1243—1261.

53. *Dyson F. J.* Statistical theory of energy levels of complex systems. I // J. Math. Phys. — 1962. — T. 3. — C. 140—156.

54. *Wilson K. G.* Proof of a conjecture by Dyson // J. Math. Phys. — 1962. — T. 3. — C. 1040—1043.

55. *Andrews G. E.* Problems and prospects for basic hypergeometric functions // Theory and Application of Special Functions. — New York : Academic Press, 1975. — C. 191—224.

56. *Kadell K. W. J.* A proof of Andrews's q-Dyson conjecture for $n = 4$ // Trans Amer. Math. Soc. — 1985. — T. 290. — C. 127—144.

57. *Stanley R. P.* The q-Dyson conjecture, generalized exponents, and the internal product of Schur functions // Combinatorics and Algebra. — Providence : Amer. Math. Soc., 1984. — C. 81—94.

58. *Stanley R. P.* The stable behavior of some characters of $\mathrm{SL}(n,\mathbb{C})$ // Lin. Multilin. Alg. — 1984. — T. 16. — C. 3—27.

59. *Zeilberger D.*, *Bressoud D. M.* A proof of Andrews' q-Dyson conjecture // Discrete Math. — 1985. — T. 54. — C. 201—224.

60. *Gessel I. M.*, *Xin G.* A short proof of the Zeilberger–Bressoud q-Dyson theorem // Proc. Amer. Math. Soc. — 2006. — T. 134. — C. 2179—2187.

61. *Cai T. W.* Macdonald symmetric functions of rectangular shapes. — URL: arXiv:1308.3821.

62. *Károlyi G.*, *Nagy Z. L.* A simple proof of the Zeilberger–Bressoud q-Dyson theorem // Trans Amer. Math. Soc. — 2014. — T. 142, № 9. — C. 3007—3011.

63. *Selberg A.* Bemerkninger om et multipelt integral // Norsk Mat. Tidsskr. — 1944. — T. 26. — C. 71—78.

64. *Ostrovsky D.* Selberg integral as a meromorphic function // Int. Math. Res. Not. IMRN. — 2013. — C. 3988—4028.

65. *Forrester P. J., O. W. S.* The importance of the Selberg integral // Bull. Amer. Math. Soc. (N. S.) — 2008. — T. 45. — C. 489—534.

66. *Morris W. G.* Constant Term Identities for Finite and Affine Root Systems: Conjectures and Theorems // Ph.D. Thesis, Univ. Wisconsin–Madison. — 1982.

67. *Anomoto K.* Jacobi polynomials associated with Selberg integrals // SIAM J. Math. Anal. — 1987. — T. 18. — C. 545—549.

68. *Anderson G. W.* A short proof of Selberg's generalized beta formula // Forum Math. — 1991. — T. 3. — C. 415—417.

69. *Dyson F. J.* A Brownian-motion model for the eigenvalues of a random matrix // J. Math. Phys. — 1962. — T. 3. — C. 1191—1198.

70. *Forrester P. J.* Log-Gases and Random Matrices // London Math. Soc. Monographs. — 2010. — T. 34.

71. *Baker T. H.*, *Forrester P. J.* Generalizations of the q-Morris constant term identity // J. Combin. Theory Ser. A. — 1998. — T. 81. — C. 69—87.

72. *Baratta W.* Some properties of Macdonald polynomials with prescribed symmetry // Kyushu J. Math. — 2010. — T. 64. — C. 323—343.

73. A unified elementary approach to the Dyson, Morris, Aomoto and Forrester constant term identities / I. M. Gessel [и др.] // J. Combin. Theory Ser. A. — 2008. — T. 115. — C. 1417—1435.

74. *Hamada S.* Proof of Baker–Forrester's constant term conjecture for the cases $N_1 = 2{,}3$ // Kyushu J. Math. — 2002. — T. 56. — C. 243—266.

75. *Kaneko J.* On Forrester's generalization of Morris constant term identity // q-series From a Contemporary Perspective. — Providence : Amer. Math. Soc., 2000. — C. 271—282.

76. *Kaneko J.* Forrester's constant term conjecture and its q-analogue // Physics and Combinatorics. — River Edge, NJ : World Sci. Publ., 2001. — C. 49—62.

77. *Kaneko J.* Forrester's conjectured constant term identity. II // Ann. Combin. — 2002. — T. 6. — C. 383—397.

78. *Kaneko J.* On Baker–Forrester's constant term conjecture // J. Ramanujan Math. Soc. — 2003. — Т. 18. — С. 349—367.

79. *Востоков С. В.*, *Волков В. В.* Явная форма символа Гильберта для многочленных формальных модулей // Алгебра и анализ. — 2014. — Т. 26, № 5. — С. 125—141.

80. *Востоков С. В.*, *Волков В. В.*, *Бондарко М. В.* Явная форма символа Гильберта для многочленных формальных модулей в многомерном локальном поле I // Зап. научн. сем. ПОМИ. — 2014. — Т. 430. — С. 53—60.

81. *Востоков С. В.*, *Волков В. В.* Явная форма символа Гильберта для многочленных формальных модулей в многомерном локальном поле II // Зап. научн. сем. ПОМИ. — 2016. — Т. 443. — С. 46—60.

82. *Волков В. В.*, *Петров Ф. В.* Некоторые обобщения теоремы Коши-Дэвенпорта // Зап. научн. сем. ПОМИ. — 2015. — Т. 432. — С. 105—110.

83. A new approach to constant term identities and Selberg-type integrals / G. Károlyi [и др.] // Advances in Mathematics. — 2015. — Т. 277. — С. 252—282.

84. *Fesenko I. B.*, *Vostokov S. V.* Local Fields and Their Extensions. — 2nd Edition. — Providence, R. I. : Amer. Math. Soc., 2002. — 345 pp.

85. *Иконникова Е. В.*, *Шавердова Е. В.* Базис Шафаревича в многомерном локальном поле // Зап. научн. семин. ПОМИ. — 2013. — Т. 413. — С. 115—133.

86. *Davenport H.* On the addition of residue classes. // J. London Math. Soc. — 1935. — Т. 10. — С. 30—32.

87. *Eliahou S.*, *Kervaire M.* Sumsets in Vector Spaces over Finite Fields. // Journal of Number Theory. — 1998. — Т. 71, № 1. — С. 12—39.

88. *Károlyi G.* Cauchy-Davenport theorem in group extensions. // L'Enseignement Mathematique. — 2005. — Т. 51. — С. 239—254.

89. *Wheeler J. P.* The Cauchy-Davenport Theorem for Finite Groups. — URL: http://arxiv.org/abs/1202.1816.

90. *Kós G.*, *Mészáros T.*, *Rónyai L.* Some extensions of Alon's Nullstellensatz // Publ. Math. Debrecen. — 2011. — Т. 79. — С. 507—519.

91. *Kós G.*, *Rónyai L.* Alon's Nullstellensatz for multisets // Combinatorica. — 2012. — Т. 32. — С. 589—605.

92. *Erd P.*, *Graham R. L.* Old and New Problems and Results in Combinatorial Number Theory // L'Enseignement Mathématique. — 1980. — С. 203—228.

93. *Hou Q. H.*, *Sun Z. W.* Restricted sums in a field // Acta Arith. — 2002. — Т. 102. — С. 239—249.

94. *Sun Z. W.*, *Yeh Y. N.* On various restricted sumsets // J. Number Theory. — 2005. — Т. 114. — С. 209—220.

95. *Xin G.* A residue theorem for Malcev–Neumann series // Adv. Appl. Math. — 2005. — Т. 35. — С. 271—293.

96. *Didier F.*, *Tillich J.-P.* Computing the Algebraic Immunity Efficiently // Fast Software Encryption: 13th International Workshop, FSE 2006, Graz, Austria, March 15-17, 2006, Revised Selected Papers. — Berlin, Heidelberg : Springer Berlin Heidelberg, 2006. — С. 359—374.

97. *Liu M.*, *Zhang Y.*, *Lin D.* Perfect Algebraic Immune Functions // Advances in Cryptology – ASIACRYPT 2012: 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings. — Berlin, Heidelberg : Springer Berlin Heidelberg, 2012. — С. 172—189.

98. Efficient Computation of Algebraic Immunity for Algebraic and Fast Algebraic Attacks / F. Armknecht [и др.] // Advances in Cryptology - EUROCRYPT 2006: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006. Proceedings. — Berlin, Heidelberg : Springer Berlin Heidelberg, 2006. — С. 147—164.

99. *Carlet C.* Algebraic Immunity of Boolean Functions // Encyclopedia of Cryptography and Security. — Boston, MA : Springer US, 2011. — С. 31—32.

100. *Kadell K. W. J.* Aomoto's machine and the Dyson constant term identity // Methods Appl. Anal. — 1998. — Т. 5. — С. 335—350.

101. *Zhou Y.* On Kadell's two conjectures for the q-Dyson product // Electron. J. Combin. — 2011. — Т. 18, № 2.

102. *Lv L.*, *Xin G.*, *Zhou Y.* A family of q-Dyson style constant term identities // J. Combin. Theory Ser. A. — 2009. — Т. 116. — С. 12—29.

103. *V. S. A.* Disturbing the Dyson conjecture, in a *generally* GOOD way // J. Combin. Theory Ser. A. — 2006. — Т. 113. — С. 1368—1380.

104. *Habsieger L.* Une q-intégrale de Selberg et Askey // SIAM J. Math. Anal. — 1988. — Т. 19. — С. 1475—1489.

105. *Kadell K. W. J.* A proof of Askey's conjectured q-analogue of Selberg's integral and a conjecture of Morris // SIAM J. Math. Anal. — 1988. — Т. 19. — С. 969—986.

106. *Askey R.* Some basic hypergeometric extensions of integrals of Selberg and Andrews // SIAM J. Math. Anal. — 1980. — Т. 11. — С. 938—951.

107. *Zeilberger D.* A Stembridge–Stanton style elementary proof of the Habsieger–Kadell q-Morris identity // Discrete Math. — 1990. — Т. 79. — С. 313—322.

108. *Xin G.*, *Zhou Y.* A Laurent series proof of the Habsieger–Kadell q-Morris identity. — URL: arXiv:1302.6642.

109. *Zhou Y.* New extensions to the sumsets with polynomial restrictions. — URL: arXiv:1202.3190.

110. *Macdonald I. G.* Some conjectures for root systems // Siam J. Math. Anal. — 1982. — Т. 13, № 6. — С. 988—1007.

111. *Cherednik I.* Double Affine Hecke Algebras and Macdonald's Conjectures // Annals of Mathematics. — 1995. — Т. 141, № 1. — С. 191—216.