О дзета-функциях
Дубна, 2023

Лекция 3, 21 июля
Дзета-функции Хассе-Вейля

Версия 24 июля 2023

Цель: направление наиболее успешных обобщений, при которых

$$\zeta = \underline{\zeta}_{\mathbb{Z}} = \underline{\zeta}_{\boxed{\mathrm{spec}(\mathbb{Z})}}$$

3.0. Об алгебраической геометрии

3.0.0. Три взгляда на её объекты. По-прежнему фиксируем *основное* $\Bbbk$: *поле* (теперь не обязательно алгебраически замкнутое, часто $\mathbb{F}_p$) или кольцо (обычно $\mathbb{Z}$).

Закрепляем букву

$$\mathbf{S}$$

за именем *переменного* объекта, который будет параметризовать рассматриваемые нами дзета-функции. Ниже обсудим выбор. (Другие популярные буквы: $\mathbf{X}$, а также $\mathbf{C}$ для кривых и снова $\mathbf{S}$ для поверхностей).

Также фиксируем нетрадиционное обозначение для множества простых чисел

$$\Pi := \{2, 3, 5, 7, \dots\}$$

.

I. Системы полиномиальных уравнений. Это – самый классический (и часто навязываемый популярными источниками) взгляд. Здесь сама система –

$$\mathbf{S} : \begin{cases} f_1 = 0 \\ f_2 = 0 \\ \dots \end{cases},$$

где $f_1, f_2, \dots \in \Bbbk[x_1, \dots, x_N]$ или, лучше $f_1, f_2, \dots \in \Bbbk[x_0 : x_1 : \dots : x_N]$.

Предполагается $\Bbbk = \overline{\Bbbk}$ и изучаются *множества*

$$\{\text{решения of } \mathbf{S}\} \subseteq \mathbf{A}_N(\Bbbk) \text{ или } \{\text{решения of } \mathbf{S}\} \subseteq \mathbf{P}_N(\Bbbk),$$

где $\mathbf{A}_N(\Bbbk) := \Bbbk^N$ и $\mathbf{P}_N(\Bbbk) := \frac{\Bbbk^{N+1} \setminus \{(0,\dots,0)\}}{\Bbbk^\times}$. Вы думаете, что знаете, что это такое. При обсуждении следующего взгляда мы это понятие определим.

II. Функторы точек. Немного обобщим понятие системы уравнений: теперь не просто $\mathbf{S} = \{f_1, f_2, \dots\}$, а

$$\mathbf{S} \subseteq \Bbbk[x_1, \dots, x_N] \text{ или } \mathbf{S} \subseteq \Bbbk[x_0 : x_1 : \dots : x_N]$$

– то есть не (обычно конечная) последовательность многочленов, а произвольное их множество. Все "=0" подразумеваются.

Основную роль в теории систем полиномиальных уравнений играет не столько само множество $\mathbf{S}$, сколько *порождённый*[1] им идеал

$$\langle \mathbf{S} \rangle \triangleleft \Bbbk[x_1, \dots, x_N] \text{ или } \mathbf{S} \triangleleft \Bbbk[x_0 : x_1 : \dots : x_N]$$

– во втором случае рассматриваются только *однородные идеалы*, то есть идеалы, *порождённые однородными многочленами.*

Теперь можно реализовать интуитивную идею о том, что
в полиномиальное уравнение в качестве значений переменных можно подставлять элементы "большего" кольца или поля, чем $\Bbbk$ *(кольцо или поле коэффициентов).* Например, рассматривать комплексные решения полиномиальных уравнений с вещественными коэффициентами.

"Большего" написано в кавычках, поскольку есть и другие случаи, когда элементы (переменного) кольца или поля $\mathbb{K}$ можно подставлять в полиномиальные уравнения с коэффициентами из $\Bbbk$. Множество таких решений будет обозначатся $\mathbf{S}(\mathbb{K})$; скоро оно будет определено точно.

Пример. $\Bbbk = \mathbb{Z}, N = 2, \mathbf{S} = \{x_0^2 + x_1^2 - 1\}$.

Множество $\mathbf{S}(\mathbb{R})$, как вы знаете, называется *окружностью*. Поэтому в данном случае множество $\mathbf{S}(\mathbb{K})$ – то есть множество $\{(\mathsf{x}, \mathsf{y}) \in \mathbb{K} \times \mathbb{K} \mid \mathsf{x}^2 + \mathsf{y}^2 = 1\}$ – принято называть *окружностью над (кольцом или полем)* $\mathbb{K}$.

Полезно подумать о множестве $\mathbf{S}(\mathbb{C})$ (топологически оно представляет собой *дважды проколотую сферу*). Определение мощностей $\#\mathbf{S}(\mathbb{F}_p)$ для всех $p \in \Pi$ – хороший теоретико-числовой вопрос; рекомендуем читателю ответить на него.

Затем предлагается подумать о *мнимых окружностях* $\mathbf{S}(\mathbb{R})$, $\mathbf{S}(\mathbb{C})$ и вычислить $\#\mathbf{S}(\mathbb{F}_p)$ для $\mathbf{S} = \{x_0^2 + x_1^2 + 1\}$.

Важное определение. $\Bbbk$-*алгеброй* называется кольцо $\mathbb{K}$ вместе с гомоморфизмом колец $\Bbbk \to \mathbb{K}$.

[1] Идеал, порождённый подмножеством кольца – это "наименьший" идеал, содержащий подмножество, иначе – *пересечение всех идеалов, содержащих подмножество.*

В случае $\Bbbk = \mathbb{Z}$ понятие $\Bbbk$-алгебры не является новым. Действительно, $\Bbbk$-алгебра – это просто кольцо, поскольку *существует единственный гомоморфизм* $\mathbb{Z} \to \mathbb{K}$ (на категорном языке $\mathbb{Z}$ – *начальный объект в категории колец*). В случае поля $\Bbbk$ понятие $\Bbbk$-алгебры может оказаться непривычным; это – векторное пространство над $\Bbbk$ вместе с *достаточно хорошим* коммутатиным умножением.

Элементы любой $\Bbbk$-алгебры можно подставлять в полиномиальные уравнения с коэффициентами из $\Bbbk$.

Наконец даём точное определение:

$$\mathbf{S}(\mathbb{K}) := \operatorname{Mor}\left(\frac{\Bbbk[x_1, \dots, x_n]}{\langle \mathbf{S} \rangle}, \mathbb{K}\right)$$

Определение функтора точек для понимающих *категорный язык*: это – функтор

$$\mathbf{S} : \Bbbk\text{-}\mathcal{ALG} \longrightarrow\!\!\!\longrightarrow \mathcal{SET} : \mathbb{K} \mapsto\!\!\!\mapsto \mathbf{S}(\mathbb{K}).$$

Здесь $\Bbbk$-$\mathcal{ALG}$ – категория $\Bbbk$-алгебр, $\mathcal{SET}$ – категория множеств.

В основном мы будем заниматься случаем $\Bbbk = \mathbb{Z}, \mathbb{K} = \mathbb{F}_q$. Забегаем вперёд: для достаточно хорошей системы $\mathbf{S}$ при почти всех $p \in \Pi$

Множество чисел $\{\#\mathbf{S}(\mathbb{F}_{p^r}) \mid r \in \mathbb{N}\}$

почти определяет *топологию многообразия* $\mathbf{S}(\mathbb{C})\}$.

III. Схемы (Гротендика). Сама буква – первая в слове **S**cheme – намекает на то, что наши $\mathbf{S}$ будут чем-то вроде *схем*.

Для знающих несколько профессиональных терминов всё коротко и ясно:

Схемы – это *окольцованные пространства, локально изоморфные спектрам коммутативных колец*.

То же самое формально и с обозначениями: для $\mathbf{X} \in\in \mathcal{TOP}$ структура схемы задаётся функтором

$$\mathbf{S} : \mathcal{OP}_{\mathbf{X}}^{\mathsf{op}} \longrightarrow\!\!\!\longrightarrow \mathcal{ANN}.$$

Здесь $\mathcal{TOP}$ – категория топологических пространств, $\mathcal{OP}_{\mathbf{X}}$ – малая категория открытых подмножеств топологического пространства $\mathbf{X}$ с морфизмами-вложениями, $\mathcal{ANN}$ – категория коммутативных колец с 1.

Требуется, чтобы

$$\forall P \in \mathbf{X}\Big[\exists \mathbf{U}_{\in \mathrm{OP}_{\mathbf{X}}}\big[\mathbf{U} \ni P\big] \wedge \big[\exists A \in \mathcal{ANN}[\mathbf{U} \simeq \operatorname{spec}(A)]\big]\Big]$$

Здесь добавилось обозначение множества $\mathrm{OP}_{\mathbf{X}}$ открытых подмножеств топологического пространства $\mathbf{X}$.

***

Остаётся определить *спектр коммутативного кольца* $A \in\in \mathcal{ANN}$.

Немотивированно:

$$\boxed{\operatorname{spec}(A) := \{\text{простые } \mathfrak{p} \triangleleft A\}}$$

Пока это функтор:

$$\mathrm{spec} : \mathcal{ANN}^{\mathsf{op}} \longrightarrow\!\!\!\longrightarrow \mathcal{SET},$$

То есть каждому кольцу сопоставлено множество, и это сопоставление уважает морфизмы. Точнее: гомоморфизму колец

$$f : A \longrightarrow B$$

сопоставляется морфизм (отображение) множеств

$$\mathrm{spec}(B) \longrightarrow \mathrm{spec}(A) : \mathfrak{q} \mapsto f^{-1\circ}(\mathfrak{q})$$

На спектрах надо ввести топологию *Зариского.*

Гротендик: ЛЮБОЕ (КОММУТАТИВНОЕ) КОЛЬЦО – КОЛЬЦО "ФУНКЦИЙ". На чём? На собственном спектре. Сначала рассмотрим примеры.

• Модель Гельфанда-Наймарка: $A = \mathcal{C}(\mathbf{X})$, где $\mathbf{X}$) – компакт.

Здесь полезно ввести *максимальный спектр* кольца[2]

$$\boxed{\mathrm{specm}(A) := \{\text{максимальные } \mathfrak{p} \triangleleft A\}}$$

и окажется, что $\mathrm{specm}(A) \approx X$ – максимальные идеалы состоят из функций, обращающихся в 0 в фиксированной точке. ПРОДУМАЙТЕ СЛУЧАЙ ОТРЕЗКА $\mathbf{X} \subset \mathbb{R}$.

• $A = \mathbb{C}[z], \mathrm{spec}(A) = \mathbb{C} \coprod \{0\}$. Снова элементы кольца естественно интерпретируются как *функции на спектре* – если проигнорировать 0. На спектре, помимо классической топологии, вводится *топология Зариского*, в которой замкнуто лишь всё множества и его конечные подмножества. Это – *самая грубая топология*, относительно которой все многочлены непрерывны.

• $A = \mathbb{Z}$. Для каждой "точки" $\mathfrak{p} \in \mathrm{spec}(A)$ строится *поле частных*[3]

$$\mathrm{ff}\left(\frac{A}{\mathfrak{p}}\right) =: \mathbb{k}_{\mathfrak{p}},$$

называемое *полем вычетов* "точки" $\mathfrak{p} \in \mathrm{spec}(A)$.

Нестандартное обозначение для $a \in A$

$$''a(\mathfrak{p})'' := \frac{a \bmod \mathfrak{p}}{1} \in \mathbb{k}_{\mathfrak{p}}$$

позволяет интерпретировать a как "функцию", у которой, правда, поле, в котором лежат её значения, у каждой точки своё. Это, однако, не мешает рассмотреть *множество нулей* функции

$$\mathrm{zer}(a) := \{\mathfrak{p} \in \mathrm{spec}(A) \mid'' a(\mathfrak{p})'' = 0\},$$

заметив, что

$$\mathrm{zer}(a) = \{\mathfrak{p} \in \mathrm{spec}(A) \mid a \in \mathfrak{p}\}.$$

На $\mathrm{spec}(A)$ вводится *самая грубая топология, в которой все эти "множества нулей" замкнуты.*

---

[2]Сопоставление $A \dashrightarrow \mathrm{specm}(A)$ интуитивно проще, чем $A \to \mathrm{spec}(A)$, но не функториально. Ср. $\mathbb{Z} \to \mathbb{Q}$.

[3]От слов fraction field.

ПОПЫТАЙТЕСЬ ИЗОБРАЗИТЬ ГРАФИК "ФУНКЦИИ" 12 НА $spec(\mathbb{Z})$.

3.0.1. Многообразия над $\overline{\mathbb{F}_p}$. Автоморфизм Фробениуса для любого $p \in \Pi$ и расширения $\mathbb{F}_{p^r} \supset \mathbb{F}_p$ имеет вид

$$\mathsf{Frob} : \mathbb{F}_{p^r} \longrightarrow \mathbb{F}_{p^r} : x \to x^p.$$

Факт. $\forall r \in \dot{\mathbb{N}}$,

$$\mathbb{F}_{p^r} = \mathrm{Fix}(\mathsf{Frob}^{p^r \circ} : \overline{\mathbb{F}_p})$$

То же свойство имеет место для многообразий. См. ниже.

3.1. Дзета-функция схемы.

Наша цель – распространить определение дзета-функции Римана

$$\zeta = \zeta_{\mathrm{spec}(\mathbb{Z})}$$

на дзета-функции произвольных схем. Это намерение естественно продолжает действия в лекции 1, когда мы ввели дзета-функции коммутативных колец, то есть аффинных схем.

3.1.0. Эйлерово произведение римановой ζ. Нам "известно" два определения римановой дзеты:

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in \mathcal{P}} \frac{1}{1 - p^{-s}}.$$

Мы перепишем их в виде суммы по всем идеалам кольца $\mathbb{Z}$

$$\zeta(s) := \sum_{\mathfrak{a} \lhd \mathbb{Z}} \frac{1}{\left(\# \frac{\mathbb{Z}}{\mathfrak{a}}\right)^s} \tag{3.1.0a}$$

и в виде произведения по простым идеалам этого кольца

$$\zeta(s) := \prod_{\mathfrak{p} \in \mathrm{spec}(\mathbb{Z})} \frac{1}{1 - \left(\# \frac{\mathbb{Z}}{\mathfrak{p}}\right)^{-s}}. \tag{3.1.0b}$$

Отметим, что мы не забыли исключить идеалы $\mathfrak{a} = \{0\}$ и $\mathfrak{p} = \{0\}$ из суммы (3.1.0a) и произведения (3.1.0b), а пользуемся введённым в лекции 1 соглашением

$$(\#\mathbb{Z})^{-s} := 0, \tag{3.1.0c}$$

психологически совместимым с трактовкой значений $\zeta(s)$ при $s \to \infty$ или же $\mathrm{Re}(s) \to \infty$.

3.1.1. Случай общей аффинной схемы. Определение (3.1.0a), очевидным образом распространяемое на аффинные схемы[4], вряд ли может быть автоматически распространено на произвольные (хотя, приложив некоторые усилия, можно было бы распространить его на *проективные спектры градуированных колец*, см. [**Манин2012**]).

[4]это обсуждалось в лекции 1

Наоборот, определение (3.1.0b) быстро приведёт нас к цели. Запишем его чуть-чуть иначе:

$$\zeta(s) := \prod_{p\in\Pi} \frac{1}{1-(\#\mathbb{F}_p)^{-s}} \tag{3.1.0b'}$$

– мы снова вернулись от простых идеалов к простым числам, чтобы использовать стандартные <u>имена</u> конечных полей, входящих в определение.

Теперь обратимся к категории схем $\mathcal{SCH}$. Для объекта $\mathbf{S} \in\in \mathcal{SCH}$ введём (не полностью стандартное) обозначение

$$\mathbf{S} =: (|\mathbf{S}|, \mathcal{O}_\mathbf{S}),$$

где $|\mathbf{S}|$ – топологическое пространство (*подложка* схемы), а $\mathcal{O}_\mathbf{S}$ – структурный пучок. Для "точки" $\mathfrak{p} \in | \mathbf{S} |$ воспользуемся более стандартными обозначениями: пользуясь произвольной окрестностью

$$U \simeq \mathrm{spec}(A) \ni P,$$

определим *локальное кольцо точки* с помощью *локализации*

$$\mathcal{O}_\mathfrak{p} := (A\setminus\mathfrak{p})^{-1}A$$

и единственный максимальный идеал в нём

$$(A\setminus\mathfrak{p})^{-1}\mathfrak{p} =: \mathfrak{m}_\mathfrak{p} \triangleleft \mathcal{O}_\mathfrak{p}.$$

Нетрудно проверить изоморфизм

$$\Bbbk_\mathfrak{p} := \frac{\mathcal{O}_\mathfrak{p}}{\mathfrak{m}_\mathfrak{p}}$$

для *локального кольца* точки, *максимального идеала* этого кольца и *поля вычетов* точки. В этих обозначениях переписываем определение римановой дзеты в последний раз:

$$\zeta(s) := \prod_{\mathfrak{p}\in\mathrm{spec}(\mathbb{Z})} \frac{1}{1-(\#\Bbbk_\mathfrak{p})^{-s}}, \tag{3.1.0b''}$$

и в таком виде определение уже автоматически распространяем на произвольную схему $\mathbf{S} \in \mathcal{SCH}$,

$$\boxed{\zeta_\mathbf{S}(s) := \prod_{P\in|\mathbf{S}|} \left(1-\frac{1}{(\#\Bbbk_P)^s}\right)^{-1}} \tag{3.1.0c}$$

Правая часть этого равенства представляет собой символическую запись довольно сложного объекта – произведение функций комплексной переменной по множеству априори произвольной мощности. Более точно это произведение следовало бы определить как *предел* по конечным подмножествам в смысле (бегло упомянутой выше) неклассической топологии на кольце $\mathrm{Dir}(\mathbb{C})$. Мы не вдаёмся в эти тонкости, поскольку в интересующих нас прежде всего случаях (когда $\mathbf{S}$ – проективное многообразие над конечным полем) всё сходится[5].

Ещё раз подчеркнём, что произведение в правой части (3.1.0c) вклад вносят

[5] В общем же случае, как отмечалось в лекции 1, даже для <u>аффинных</u> схем произведение может не сходиться нигде.

только точки схемы с <u>конечным</u> полем вычетов. За счёт этого соглашение наше определение компактнее обычно принятых в литературе.

Рекомендуется решить задачу 3.4.

В оставшейся части лекции мы в основном будем заниматься *натуральными числами* $\#\mathbf{S}(\mathbb{F}_q)$ Будет достаточно довольно поверхностного владения теорией схем – можно вникнуть в определения и первоначальные объяснения из [**Манин2012**] или [**Шафаревич2007**]. Для более глубокого освоения понятий можно рекомендовать, например, [**Vakil2017**].

Мы в основном будем работать со <u>счётными</u> множествами $\mathbf{S}(\overline{\mathbb{F}_p})$, содержащими счётные семейства <u>конечных</u> подмножеств $\{\mathbf{S}(\mathbb{F}_{p^r}) \mid r = 1, 2, \dots$

3.2. Обобщённое эйлерово произведение

3.2.0. Формальные ряды Дирихле. С точностью до обозначений мы следуем [**Kahn2018**] и вводим алгебру *формальных рядов Дирихле*

$$\mathrm{Dir}(\mathbb{k})$$

над произвольным полем $\mathbb{k}$ (реально будет фигурировать только $\mathbb{k} = \mathbb{C}$).

Алгебра $\mathrm{Dir}(\mathbb{k})$ является *мультипликативным аналогом* алгебры формальных степенных рядов $\mathbb{k}[[x]]$. Обе представляют собой частные случаи понятия *полугрупповой алгебры* $\mathbb{k}\langle \mathsf{N}\rangle$, которую мы сейчас определим.

Для разгона вдумаемся в алгебру формальных степенных рядов

$$\mathbb{k}[[x]] = \{a_0 + a_1x + a_2x^2 + \dots\}.$$

Нам придётся признать, что привычная буква x не имеет ни малейшего алгебраического смысла. Отождествим привычную запись формального ряда с последовательностью его коэффициентов

$$a_0 + a_1x + a_2x^2 + \dots \;\longleftrightarrow\; (a_0, a_1, \dots) \tag{3.2.0a}$$

Тогда *сложение* в алгебре $\mathbb{k}[[x]]$ определяется естественно,

$$(a_0, a_1, \dots) + (b_0, b_1, \dots) := (a_0 + b_0, a_1 + b_1, \dots) \tag{3.2.0b}$$

а умножение – не очень: в соответствии с "очевидной" формулой

$$(a_0+a_1x+a_2x^2+\dots)\cdot(b_0+b_1x+b_2x^2+\dots) := a_0b_0+(a_0b_1+a_1b_0)x+(a_0b_2+a_1b_1+a_2b_0)x^2+\dots$$

приходится определить

$$(a_0, a_1, a_2, \dots)\cdot(b_0, b_1, b_2, \dots) := (a_0b_0, a_0b_1+a_1b_0, a_0b_2+a_1b_1+a_2b_0, \dots). \tag{3.2.0c}$$

После перехода к однобуквенным обозначениям последовательностей

$$(n \mapsto c_n) \longleftrightarrow \boxed{c \in \mathbb{k}^{\mathbb{N}}}$$

умножение (3.2.1c) переписывается в виде

$$a * b : \boxed{n \mapsto \sum_{i+j=n} a_i b_j} \tag{3.2.0d}$$

и называется *свёрткой* (см., например, [**HirWid1955**]).

В такой форме операция свёртки обобщается на любую *коммутативную полугруппу*[6] $(\mathsf{N}, \odot)$, удовлетворяющую условию, которое мы введём с помощью функции *разложения*

$$\mathrm{decomp} : \mathsf{N} \longrightarrow \mathrm{Sub}(\mathsf{N} \times \mathsf{N}) : n \mapsto \{(i, j) \in \mathsf{N} \times \mathsf{N} \mid i \odot j = n\}.$$

Условие *конечной разложимости* заключается в том, что

$$\forall n \in \mathsf{N} \left[\#\mathrm{decomp}(n) < \infty\right]$$

(*любой элемент полугруппы представим как результат операции над не более чем конечным числом пар*). Полугруппы, удовлетворяющие этому условию, будем называть *конечно-разложимыми.*

Для любой конечно-разложимой полугруппы $(\mathsf{N}, \odot)$ на аддитивной группе $(\Bbbk^+)^{\mathsf{N}}$ определено умножение-свёртка

$$*_\odot : \Bbbk^{\mathsf{N}} \times \Bbbk^{\mathsf{N}} \longrightarrow \Bbbk^{\mathsf{N}}$$

той же формулой

$$\boxed{(a *_\odot b) : n \mapsto \sum_{i \odot j = n} a_i b_j} \tag{3.2.0e}$$

В задаче **3.1.** предлагается установить свойства введённой операции. Получаемые таким образом <u>коммутативные $\Bbbk$-алгебры</u> играют в теориях дзета-функций важную роль.

Далее будем пользоваться обозначением

$$\boxed{\dot{\mathbb{N}} := \mathbb{N} \setminus \{0\}}$$

Очевидно, аддитивная полугруппа $(\mathbb{N}, +)$ и мультипликативная полугруппа $(\dot{\mathbb{N}}, \times)$ являются конечно-разложимыми, и, следовательно, в обоих случаях определены соответствующие $\Bbbk$-алгебры Аддитивную из них мы уже идентифицировали:

$$(\Bbbk^{\mathbb{N}}, +, *_+) \cong \Bbbk[[x]].$$

Мультипликативная и была целью наших рассмотрений:

$$\boxed{\mathrm{Dir}(\Bbbk) := (\Bbbk^{\dot{\mathbb{N}}}, +, *_\times)} \tag{3.2.0f}$$

Чтобы придать смысл получившемуся умножению на множестве последовательностей $\Bbbk^{\dot{\mathbb{N}}}$, надо совершить действие, аналогичное (3.2.0*a*): сопоставить последовательности "коэффициентов" *формальный ряд Дирихле*

$$(c_1, c_2, c_3, \dots) \longleftrightarrow \frac{c_1}{1^s} + \frac{c_2}{2^s} + \frac{c_3}{3^s} + \dots$$

Надо сразу отметить, что буква s имеет не больше смысла, чем буква x при определении формальных степенных рядов. Свёртка $*_\times$, однако, становится интуитивно приемлемой:

[6] мы ненадолго прибегаем к экзотическому обозначению полугрупповой операции, поскольку более традиционные сейчас заняты

$$\left(\frac{a_1}{1^s}+\frac{a_2}{2^s}+\frac{a_3}{3^s}+\frac{a_4}{4^s}+\dots\right)\left(\frac{b_1}{1^s}+\frac{b_2}{2^s}+\frac{b_3}{3^s}+\frac{b_4}{4^s}+\dots\right)=$$
$$=\frac{a_1b_1}{1^s}+\frac{a_1b_2+a_2b_1}{2^s}+\frac{a_1b_3+a_3b_1}{2^s}+\frac{a_1b_4+a_2b_2+a_4b_1}{4^s}+\dots$$

***

В алгебрах формальных рядов Дирихле рассматривается два вида сходимости.

Первый имеет смысл при произвольном поле $\Bbbk$ – хоть и было обещано ограничиться классическим случаем $\Bbbk=\mathbb{C}$, несколько слов об этой неклассической сходимости скажем. На алгебре $\mathrm{Dir}(\Bbbk)$ вводится *топология* – слабейшая из тех, в которых *конечные ряды Дирихле всюду плотны.*

Пример. В этой топологии для любого морфизма полугрупп

$$\lambda:(\dot{\mathbb{N}},\times)\longrightarrow(\Bbbk,\times)$$

имеет место *эйлерово произведение*[7]

$$\boxed{\sum_{n=1}^{\infty}\frac{\lambda(n)}{n^s}=\prod_{p\in\mathcal{P}}\frac{1}{1-\lambda(p)p^{-s}}} \tag{3.2.0g}$$

Здесь левая часть понимается как обычный элемент алгебры $\mathrm{Dir}(\Bbbk)$, а правая – как предел конечных произведений во введённой топологии; в задачах 3.2 и 3.3 предлагается восстановить детали.

Второй вид сходимости относится к классическому случаю $\Bbbk=\mathbb{C}$. Как и в случае формальных степенных рядов, выражение $\sum_{n=1}^{\infty}\frac{a_n}{n^s}$ может определять настоящую функцию, и встают вопросы об обычных пределах ($a_n\in\mathbb{C}$)

$$\lim_{N\to\infty}\sum_{n=1}^{N}\frac{a_n}{n^s} \tag{3.2.0h}$$

при всевозможных $s\in\mathbb{C}$. Мы знаем, что при $a_n\equiv 1$ сходимость имеет место на полуплоскости $\{s\in\mathbb{C}\mid \mathrm{Re}(s)>1\}$. Этот результат обобщается: *область сходимости любого ряда* (7.0.1g) *– полуплоскость* $\{s\in\mathbb{C}\mid \mathrm{Re}(s)>\rho\}$ *при подходящем* $\rho\in(\mathbb{R}\coprod\{\pm\infty\})$.

См. [**Серр1972**]. Мы не вдаёмся в детали, поскольку в интересующих нас случаях сходимость рядов будет следовать из очень простых соображений.

3.2.1. Разложение по простым. В полной общности для произвольного *семейства* схем $\mathbf{S}_i$, параметризованного индексами $i\in I$ из произвольного множества, формула гласит

$$\zeta_{\coprod_{i\in I}\mathbf{S}_i}=\prod_{i\in I}\zeta_{\mathbf{S}_i}, \tag{3.2.1a}$$

[7] обратите внимание на то, что рассматриваются морфизмы именно в *полугруппу* $(\Bbbk,\times)$, а не в *моноид* $(\dot{\Bbbk},\times)$: функция λ вполне может принимать нулевые значения.

см. [**Kahn2018**]. Мы, однако, будем работать лишь с простейшей версией этой формулы. А именно, для "абсолютной" схемы $\mathbf{S}$ вспомним о морфизме, который НИКАК НЕ ОБОЗНАЧАЕТСЯ в силу своей единственности:

$$\mathbf{S} \longrightarrow \mathrm{spec}(\mathbb{Z}). \tag{3.2.1b}$$

К этому морфизму для каждого простого $p \in \Pi$ примыкает (тоже никак не обозначаемый) морфизм

$$\mathrm{spec}(\mathbb{F}_p) \longrightarrow \mathrm{spec}(\mathbb{Z}). \tag{3.2.1c)$_p$}$$

Морфизмы (3.2.1b) и (3.2.1c)$_p$ позволяют определить *расслоённые произведения*, для которых мы позволим себе использовать краткие обозначения

$$\mathbf{S}_p := \mathbf{S} \times_{\mathrm{spec}(\mathbb{Z})} \mathrm{spec}(\mathbb{F}_p). \tag{3.2.1d)$_p$}$$

(Выше было принято другое обозначение того же самого объекта, а именно $\mathbf{S}_p = \mathbf{S}(\mathbb{F}_p)$, но это не должно нас смущать). Теперь схема $\mathbf{S}$ распадается в несвязное объединение

$$\mathbf{S} = \coprod_{p \in \mathcal{P}} \mathbf{S}_p, \tag{3.2.1e}$$

и формула (3.2.1a) может быть переписана в более реалистическом виде

$$\boxed{\zeta_{\mathbf{S}}(s) = \prod_{p \in \mathcal{P}} \zeta_{\mathbf{S}_p}(s)} \tag{3.2.1f}$$

В оставшейся части лекции мы в основном будем заниматься отдельными сомножителями правой части равенства (3.2.1f).

3.2.3. Формула Шмидта[8]**.** Далее от произвольных схем $\mathbf{S}$ мы переходим к *проективным многообразиям*: для $p \in \Pi$ рассматриваем

$$\mathbf{V} \subset \mathbf{P}_N(\overline{\mathbb{F}_p}).$$

Это – проективное многообразие над алгебраически замкнутым полем, и к нему применимы все конструкции и результаты "обычной" алгебраической геометрии. Однако оно задаётся конечным множеством полиномиальных уравнений, и все эти коэффициенты лежат в некотором конечном расширении

$$\mathbb{F}_q \supseteq \mathbb{F}_p,$$

[8]Согласно [**Kahn2018**], для кривых формула была впервые получена в [**Schmidt1931**].

и принято *наивно* говорить, что *многообразие* $\mathbf{V}$ *определено над* $\mathbb{F}_q$. Мы, однако, не будем принимать это определение за окончательное, поскольку нежелательно вводить фундаментальные понятия арифметической геометрии на основе таких случайно выбираемых объектов, как *коэффициенты уравнений*, определяющих многообразие – главный вклад наивного определения заключается в том, что каждое проективное многообразие над $\overline{\mathbb{F}_p}$ определено над <u>каким-то</u> конечным полем.

Здесь мы забываем о простом числе p, вводим переобозначение

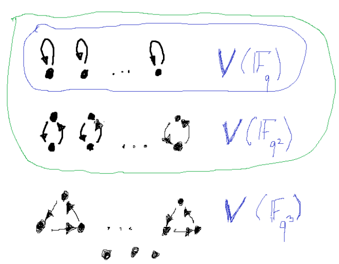
$$\overline{\mathbb{F}_p} = \overline{\mathbb{F}_q}$$

и слегка разгружаем обозначение для автоморфизма Фробениуса

$$\boxed{\mathsf{Frob} : \mathbf{P}_N(\overline{\mathbb{F}_q}) \longrightarrow \mathbf{P}_N(\overline{\mathbb{F}_q}) : (x_0 : \cdots : x_N) \mapsto (x_0^q : \cdots : x_N^q)}$$

До конца этой лекции структура $\mathbf{V}$ как алгебраического многообразия не будет играть никакой роли (в частности, не будет фигурировать пучок $\mathcal{O}_{\mathbf{V}}$). Вместо этого $\mathbf{V}$ будет рассматриваться как Frob-*инвариантное подмножество* проективного пространства $\overline{\mathbb{F}_p}$; иначе говоря, мы будем изучать *динамическую систему*

$$\mathsf{Frob} : \mathbf{V} \longrightarrow \mathbf{V}.$$



Переход к дзета-функциям требует ещё одного, последнего уточнения. В формуле (3.1.0), на основе которой мы ввели общее понятие дзета-функции, фигурирует порядок поля вычетов $\#\Bbbk_P$. Это – удобное понятие в контексте общей теории схем, но при переходе к геометрии над алгебраически замкнутым полем оно теряет смысл – поля вычетов становятся бесконечными.

Мы выйдем из этого затруднения простейшим способом, объявив для каждого $P \in \mathbf{V}$

$$\boxed{\#\Bbbk_P := q^{\#\left(\langle \mathsf{Frob}\rangle \cdot P\right)}} \tag{3.2.3a}$$

Лемма. *Для любого* $n \in \mathbb{N}_{>0}$ *имеет место равенство*

$$\#\mathbf{V}(\mathbb{F}_{q^n}) = \sum_{d|n} \sum_{\substack{P \in \mathbf{V}: \\ \#\left(\langle \mathsf{Frob}\rangle \cdot P\right) = d}} d \tag{3.2.3b}$$

Доказательство. Формула представляет собой разложение по орбитам Фробениуса конечного множества $\mathbf{V}(\mathbb{F}_{q^n})$. Учтены включения $\mathbb{F}_{q^d} \subseteq \mathbb{F}_{q^n}$ при всех $d|n$.■

Теорема. *Для любого проективного многообразия* $\mathbf{V} \subseteq \mathbf{P}_N(\overline{\mathbb{F}_q})$ *имеет место равенство*

$$\boxed{\zeta_{\mathbf{V}}(s) = \exp \sum_{n=1}^{\infty} \#\mathbf{V}(\mathbb{F}_{q^n}) \frac{q^{-ns}}{n}} \qquad (3.2.3c)$$

Доказательство. Цепочка тождественных преобразований:

$$\log \mathrm{LHS}(7.1.1c) = \log \zeta_{\mathbf{V}}(s) =_{(7.0.2d),(7.1.1a)}$$

$$= -\sum_{P \in \mathbf{V}} \log \left(1 - \frac{1}{q^{-\#\left(\langle \mathsf{Frob} \rangle \cdot P\right) \cdot s}} \right) =_{\text{разлагаем логарифм в ряд}} \sum_{P \in \mathbf{V}} \sum_{m=1}^{\infty} \frac{q^{-\#\left(\langle \mathsf{Frob} \rangle \cdot P\right) ms}}{m} =$$

$$= \sum_{m=1}^{\infty} \sum_{d=1}^{\infty} \sum_{\substack{P \in \mathbf{V}: \\ \#\left(\langle \mathsf{Frob} \rangle \cdot P\right) = d}} \frac{q^{-dms}}{m} = \sum_{m=1}^{\infty} \sum_{d=1}^{\infty} \sum_{\substack{P \in \mathbf{V}: \\ \#\left(\langle \mathsf{Frob} \rangle \cdot P\right) = d}} d \cdot \frac{q^{-dms}}{dm} =_{dm =: n}$$

$$= \sum_{n=1}^{\infty} \sum_{d \mid n} \sum_{\substack{P \in \mathbf{V}: \\ \#\left(\langle \mathsf{Frob} \rangle \cdot P\right) = d}} d \cdot \frac{q^{-ns}}{n} =_{(7.1.1b)} \sum_{n=1}^{\infty} \#\mathbf{V}(\mathbb{F}_{q^n}) \frac{q^{-ns}}{n} = \log \mathrm{RHS}(7.1.1c) \blacksquare$$

3.2.4. Главное переобозначение

$$\boxed{t := q^{-s}} \qquad (3.2.4a)$$

Вводится

$$\mathrm{Z}_{\mathbf{V}}(t) := \zeta_{\mathbf{V}}(-\log_q t). \qquad (3.2.4a)$$

Если функции $s \mapsto \zeta_{\mathbf{V}}(s)$ – с аналитической точки зрения не вполне традиционные объект, то гораздо понятнее

$$\mathrm{Z}_{\mathbf{V}}(t) =_{(7.1.1c),(7.1.1e)} \exp \sum_{n=1}^{\infty} \#\mathbf{V}(\mathbb{F}_{q^n}) \frac{t^n}{n} =$$

$$= 1 + \left(\#\mathbf{V}(\mathbb{F}_q) t + \#\mathbf{V}(\mathbb{F}_{q^2}) \frac{t^2}{2} + \dots \right) + \frac{\left(\#\mathbf{V}(\mathbb{F}_q) t + \#\mathbf{V}(\mathbb{F}_{q^2}) \frac{t^2}{2} + \dots \right)^2}{2!} + \dots,$$

откуда видно, что

$$\mathrm{Z}_{\mathbf{V}} \in \mathbb{Q}[[t]].$$

Нетрудно показать, что при любом $\mathbf{V}$ этот ряд имеет положительный радиус сходимости. Более того, будет сформулирована одна из *гипотез Вейля*, согласно которой

$$\mathrm{Z}_{\mathbf{V}} \in \mathbb{Q}(t).$$

Приведённая выше формула будет нашей основной:

$$\boxed{\boxed{\mathrm{Z}_{\mathbf{V}}(t) = \exp \sum_{n=1}^{\infty} \#\mathbf{V}(\mathbb{F}_{q^n}) \frac{t^n}{n}}} \qquad (3.2.4b)$$

3.3. Примеры

3.3.0. Проективные пространства $\mathbf{P}_N$. Как нетрудно понять,

$$\#\mathbf{P}_N(\mathbb{F}_{q^n}) = 1 + q^n + q^{2n} + \cdots + q^{Nn}. \qquad (3.3.0a)$$

Поэтому

$$\mathrm{Z}_{\mathbf{P}_N}(t) =_{(7.1.1f)} \exp \sum_{n=1}^{\infty} \#\mathbf{P}_N(\mathbb{F}_{q^n}) \frac{t^n}{n} =_{(7.2.0a)} \exp \sum_{n=1}^{\infty} \sum_{i=0}^{N} q^{ni} \frac{t^n}{n} =$$

$$= \exp \sum_{i=0}^{N} \sum_{n=1}^{\infty} \frac{(q^i t)^n}{n} = \prod_{i=0}^{N} \exp \sum_{n=1}^{\infty} \frac{(q^i t)^n}{n} = \prod_{i=0}^{N} \exp \log \frac{1}{1 - q^i t} = \frac{1}{(1-t)(1-qt)\dots(1-q^N t)}.$$

Итак,

$$\boxed{\mathrm{Z}_{\mathbf{P}_N}(t) = \frac{1}{(1-t)(1-qt)\dots(1-q^N t)}} \qquad (3.3.0b)$$

В остальных примерах размерности будут ограничены.

3.2.1. Грассманиан $\mathbf{Gr}\binom{4}{2}$. Как мы знаем из моих дубнинских лекций "Когда 1=0",

$$\#\mathbf{Gr}\binom{4}{2}(\mathbb{F}_q) = (1 + q + q^2)(1 + q^2) = 1 + q + 2q^2 + q^3 + q^4,$$

откуда

$$\#\mathbf{Gr}\binom{4}{2}(\mathbb{F}_{q^n}) = 1 + q^n + 2q^{2n} + q^{3n} + q^{4n}. \qquad (3.2.1a)$$

Поэтому

$$\mathrm{Z}_{\mathbf{Gr}\binom{4}{2}}(t) =_{(7.1.1f)} \exp \sum_{n=1}^{\infty} \#\mathbf{Gr}\binom{4}{2}(\mathbb{F}_{q^n}) \frac{t^n}{n} =_{(3.2.1a)}$$

$$= \exp \sum_{n=1}^{\infty} \left(1 + q^n + 2q^{2n} + q^{3n} + q^{4n}\right) \frac{t^n}{n} =$$

$$= \exp \sum_{n=1}^{\infty} \frac{t^n}{n} \cdot \exp \sum_{n=1}^{\infty} q^n \frac{t^n}{n} \cdot \exp \sum_{n=1}^{\infty} 2q^{2n} \frac{t^n}{n} \cdot \exp \sum_{n=1}^{\infty} q^{3n} \frac{t^n}{n} \cdot \exp \sum_{n=1}^{\infty} q^{4n} \frac{t^n}{n} =$$

$$= \exp \sum_{n=1}^{\infty} \frac{t^n}{n} \cdot \exp \sum_{n=1}^{\infty} \frac{(qt)^n}{n} \cdot \left(\exp \sum_{n=1}^{\infty} \frac{(q^2 t)^n}{n} \right)^2 \cdot \exp \sum_{n=1}^{\infty} \frac{(q^3 t)^n}{n} \cdot \exp \sum_{n=1}^{\infty} \frac{(q^4 t)^n}{n} =$$

$$= \frac{1}{(1-t)(1-qt)\big(1-q^2 t\big)^2 (1-q^3 t)(1-q^4 t)}.$$

Таким образом,

$$\boxed{\mathrm{Z}_{\mathbf{Gr}\binom{4}{2}}(t) = \frac{1}{(1-t)(1-qt)\big(1-q^2 t\big)^2 (1-q^3 t)(1-q^4 t)}} = \frac{1}{1-q^2 t} \mathrm{Z}(\mathbf{P}_4) \quad (3.2.1b)$$

Формула напоминает о *рациональности* грассманианов.

3.2.2. Рациональные поверхности. Дзета-функцию проективной плоскости мы знаем: согласно (3.2.0b),

$$\boxed{\mathrm{Z}_{\mathbf{P}_2}(t) = \frac{1}{(1-t)(1-qt)(1-q^2t)}} \tag{3.2.2a}$$

Квадрика в $\mathbf{P}_3$ изоморфна *произведению двух прямых.* Поскольку

$$\#\big(\mathbf{P}_1(\mathbb{F}_{q^n}) \times \mathbf{P}_1(\mathbb{F}_{q^n})\big) = (1+q^n)^2, \tag{3.2.2b}$$

имеем

$$\mathrm{Z}_{\mathbf{P}_1\times\mathbf{P}_1}(t) =_{(7.1.1f)} \exp\sum_{n=1}^{\infty}(1+q^n)^2\frac{t^n}{n} = \exp\sum_{n=1}^{\infty}(1+2q^n+q^{2n})\frac{t^n}{n} =$$

$$= \frac{1}{(1-t)(1-qt)^2(1-q^2t)}.$$

Таким образом,

$$\boxed{\mathrm{Z}_{\mathbf{P}_1\times\mathbf{P}_1}(t) = \frac{1}{(1-t)(1-qt)^2(1-q^2t)}} \tag{3.2.2c}$$

Раздутие точки на алгебраической поверхности – фундаментальная операция бирациональной геометрии. С точки зрения подсчёта точек над конечным полем, она весьма проста: раздуваемая одна точка заменяется на проективную прямую.

Бирациональные взаимоотношения между плоскостью и квадрикой хорошо известны (см. [**Шафаревич2007**]). Квадрика получится, если раздуть две точки $A, B \in \mathbf{P}_2$ и на полученной поверхности

$$\sigma : \widehat{\widehat{\mathbf{P}_2}} \longrightarrow \mathbf{P}_2$$

стянуть прообраз прямой, проходящей через A и B.

Проверить формулу (3.2.2c) с помощью описанной процедуры предлагается в задаче **3.5.**

Поработать с дзета-функциями *кубических поверхностей* предлагается в задачах **3.6** и **3.7*.**

Список литературы

[**Hardy1922**] G. H. Hardy, *A new proof of the functional equation for the Zeta-function.* Mathematica Scandinavica, Matematisk Tidsskrift. B(1922), pp. 71-73.

[**HirWid1955**] I. I. Hirschman and D. V. Widder, *The Convolution Transform.* Princeton University Press, 1955.

[**Kahn2018**] Bruno Kahn, *Fonctions zêta et L de variétés et de motifs.* Calgage & Mounet, 2018.

[**Kolm1923**] A. Kolmogoroff, *Une série de Fourier-Lebesque divergente presgue partout.* Fund. Math., 1923, 4, p. 324—328.

[**Osgood2019**] Brad G. Osgood, *Lectures on the Fourier Transform and Its Applications.* American Mathematical Soc., 2019.

[**Schmidt1931**] Friedrich Karl Schmidt, *Analytische Zahlentheorie in Körpern der Charakteristik p.* Mathematische Zeitschrift volume 33, p. 1–32(1931).

[**Vakil2017**] Ravi Vakil, *THE RISING SEA. Foundations of Algebraic Geometry.* math216.wordpress.com. (электронное издание).

[**Venk2015**] Akshay Venkatesh, *The analytic class number formula and L- functions.* Lecture notes, 2015 (доступны в сети).

[**БорШаф1985**] З.И. Боревич, И.Р. Шафаревич, *Теория чисел.* М.: Наука, 1985.

[**Зиг1965**] А. Зигмунд, *Тригонометрические ряды.* М.: "Мир", 1965.

[**Мен1942**] Д. Е. Меньшов, *Sur la convergence uniforme des séries de Fourier.* Математический сборник. — 1942. — Т. 11(53), вып. 1-2. — С. 67 — 96.

[**ИскШаф1989**] В.А. Исковских, И.Р. Шафаревич, *Алгебраические поверхности.* Алгебраическая геометрия – 2, Итоги науки и техн. Сер. Соврем. пробл. мат. Фундам. направления, 35, ВИНИТИ, М., 1989, 131–263.

[**КолФом1976**] А.Н. Колмогоров, С.В. Фомин, *Элементы теории функций и функционального анализа.* М.: "Наука", 1976.

[**КосФав2004**] Костомаров Д. П., Фаворский А. П. , *Вводные лекции по численным методам.* М.: Логос, 2004.

[**ЛавШаб1987**] М.А. Лаврентьев, Б.В. Шабат, *Методы теории функций комплексного переменного.* М.: "Наука", 1987.

[**Манин1972**] Ю.И. Манин, *Кубические формы: алгебра, геометрия, арифметика.* Москва: Наука, 1972.

[**Манин2012**] Ю.И. Манин, *Введение в теорию схем и квантовые группы.* МЦНМО, 2012.

[**Мачис2013**] Ю. Ю. Мачис, *О константе Эйлера–Маскерони.* Матем. заметки, 2013, том 94, выпуск 5, 695–701.

[**Серр1972**] Ж-П. Серр, *Курс арифметики.* М.,"Мир", 1972.

[**Титчмарш2010**] Э.Ч. Титчмарш, *Дзета-функция Римана.* УРСС, 2010.

[**Шафаревич2007**] И.Р. Шафаревич, *Основы алгебраической геометрии.* МЦНМО, 2007.