РОССИЙСКАЯ АКАДЕМИЯ НАУК

МАТЕМАТИЧЕСКИЙ ИНСТИТУТ ИМ. В. А. СТЕКЛОВА РАН

СОВРЕМЕННЫЕ ПРОБЛЕМЫ МАТЕМАТИКИ

Выпуск 2

Издание выходит с 2003 года

В. С. Владимиров

Таблицы интегралов комплекснозначных функций p-адических аргументов

Москва
2003

УДК 512.625.5
ББК (В)22.161.1
В57

Владимиров В. С.

В57 Таблицы интегралов комплекснозначных функций p-адических аргументов / В. С. Владимиров. — М.: МИАН, 2003. — 90 стр. — (Современные проблемы математики / Математический институт им. В. А. Стеклова (МИАН); вып. 2.)

ISBN 5-98419-001-X

ISBN 5-98419-001-X

Часть I. Краткие сведения из p-адического анализа

Всюду впредь, если это не оговорено особо, будем предполагать, что p пробегает все простые числа, $p = 2, 3, 5, \ldots, 137, \ldots$, а γ пробегает все целые (рациональные) числа, $\gamma = 0, \pm 1, \pm 2, \ldots$, $\gamma \in Z$; через Z_+ будем обозначать множество натуральных чисел $\gamma = 1, 2, \ldots$. Если $\mathbb{K}$ – некоторое поле (или кольцо), то через $\mathbb{K}^\times$ будем обозначать его мультипликативную группу.

§ 1. Поле p-адических чисел $\mathbb{Q}_p$

Обозначим: $\mathbb{Q}$ – поле рациональных чисел, $\mathbb{R}$ – поле вещественных чисел, $\mathbb{C}$ – поле комплексных чисел.

Пусть p – простое число. Любое рациональное число $x \neq 0$ однозначно представляется в виде

$$x = \pm p^\gamma \frac{a}{b},$$

где $\gamma \in Z$ и a, b – натуральные числа, не делящиеся на p и не имеющие общих множителей. *p-Адическая норма* $|x|_p$ числа $x \in \mathbb{Q}$ определяется равенствами

$$|x|_p = p^{-\gamma}, \qquad x \neq 0, \qquad |0|_p = 0.$$

Пополнение поля $\mathbb{Q}$ по норме $|\cdot|_p$ дает *поле p-адических чисел* $\mathbb{Q}_p$.

Каноническая форма произвольного p-адического числа $x \neq 0$ есть

$$x = p^\gamma (x_0 + x_1 p + x_2 p^2 + \cdots), \tag{1.1}$$

где $\gamma = \gamma(x) \in Z$, $x_j = 0, 1, \ldots, p-1$, $x_0 \neq 0$, $j = 0, 1, \ldots$; при этом $|x|_p = p^{-\gamma}$. Число $-\gamma$ называется *порядком* числа x и обозначается $\operatorname{ord} x$, $\operatorname{ord} x = -\gamma(x)$, $\operatorname{ord} 0 = -\infty$.

Работа выполнена при частичной финансовой поддержке РФФИ, гранты 96-01-01008 и 96-15-96131.

Норма $|\cdot|_p$ обладает следующими характерными свойствами:

$$\begin{aligned} &1) \quad |x|_p \geqslant 0, \qquad |x|_p = 0 \leftrightarrow x = 0, \\ &2) \quad |xy|_p = |x|_p |y|_p, \\ &3) \quad |x+y|_p \leqslant \max(|x|_p, |y|_p). \end{aligned} \tag{1.2}$$

Кроме того,

$$\begin{aligned} &3') \quad |x+y|_p = \max(|x|_p, |y|_p), \qquad |x|_p \neq |y|_p, \\ &3'') \quad |x+y|_p \leqslant |2x|_p, \qquad |x|_p = |y|_p. \end{aligned}$$

Таким образом, в силу (1.2), норма $|\cdot|_p$ *неархимедова*, а пространство $\mathbb{Q}_p$ – *ультраметрическое.*

Обозначим:

$$B_\gamma(a) = [x \in \mathbb{Q}_p : |x-a|_p \leqslant p^\gamma]$$

– *диск* с центром в точке $a \in \mathbb{Q}_p$ радиуса p^γ, $B_\gamma = B_\gamma(0)$;

$$S_\gamma(a) = [x \in \mathbb{Q}_p : |x-a|_p = p^\gamma]$$

– *окружность* с центром в точке $a \in \mathbb{Q}_p$ радиуса p^γ, $S_\gamma = S_\gamma(0)$.

Очевидные соотношения:

$$B_\gamma(a) = \bigcup_{\gamma' \leqslant \gamma} S_{\gamma'}(a), \qquad S_\gamma(a) = B_\gamma(a) \setminus B_{\gamma-1}(a),$$

$$\mathbb{Q}_p = \bigcup_{\gamma \in Z} B_\gamma(a), \qquad \mathbb{Q}_p^\times = \bigcup_{\gamma \in Z} S_\gamma(a).$$

Геометрия пространства $\mathbb{Q}_p$ весьма необычна: все треугольники в нем равнобедренные; всякая точка диска является его центром, диск не имеет границы, диск есть объединение конечного числа непересекающихся дисков меньшего радиуса; если два диска пересекаются, то один из них содержится в другом; диск есть открытый компакт.

Множество поля $\mathbb{Q}_p$, которое является открытым и замкнутым, называется *клопен* (clopen).

Обозначим: $Z_p = B_0$ – максимальное компактное подкольцо поля $\mathbb{Q}_p$ (кольцо целых p-адических чисел); мультипликативная группа $Z_p^\times = S_0$ кольца Z_p – это группа единиц поля $\mathbb{Q}_p$; $I_p = pZ_p = B_{-1}$ – максимальный идеал кольца Z_p.

Классы вычетов Z_p/I_p образуют конечное поле, изоморфное классу вычетов по модулю p: $\{0, 1, \dots, p-1\}$.

Введем специальные множества:

$$G_p = [x \in \mathbb{Q}_p : |x|_p \leqslant |2p|_p];$$
$$J_p = [x \in Z_p^\times : 1 - x \in G_p],$$

J_p – мультипликативная группа;

$$S_{\gamma,k_0k_1\dots k_n} = [x \in S_\gamma : x_0 = k_0, x_1 = k_1, \dots, x_n = k_n],$$
$$S_\gamma^{k_0k_1\dots k_n} = [x \in S_\gamma : x_0 \neq k_0, x_1 \neq k_1, \dots, x_n \neq k_n],$$

где $k_j = 0, 1, \dots, p-1,\ \ k_0 \neq 0,\ \ j = 1, 2, \dots, n$.

Введенные множества – открытые компакты в $\mathbb{Q}_p$.

Дробная часть $\{x\}_p$ числа $x \in \mathbb{Q}_p$:

$$\{x\}_p = 0, \quad \text{если} \quad \gamma(x) \geqslant 0,$$

и

$$\{x\}_p = p^\gamma(x_0 + x_1p + \dots + x_{-\gamma-1}p^{-\gamma-1}), \quad \text{если} \quad \gamma(x) \leqslant -1. \tag{1.3}$$

Мультипликативную *группу квадратов* p-адических чисел обозначим через $\mathbb{Q}_p^{\times 2}$.

Для того чтобы число $x \in \mathbb{Q}_p^\times$ *принадлежало* $\mathbb{Q}_p^{\times 2}$, *необходимо и достаточно, чтобы* $\gamma(x)$ *было четным и*

$$\begin{cases} \left(\dfrac{x_0}{p}\right) = 1, & p \neq 2; \\ x_1 = x_2 = 0, & p = 2. \end{cases}$$

Здесь

$$\left(\frac{a}{p}\right), \qquad a \in Z, \quad a \not\equiv 0 \pmod p,$$

– *символ Лежандра*, равный 1 или -1 в зависимости от того, является ли число x квадратичным вычетом или невычетом по модулю p.

Таким образом, группа $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$ состоит из четырех элементов $(1, \epsilon, -p, \epsilon p)$, где ϵ – любая единица поля $\mathbb{Q}_p$, не являющаяся квадратом в $\mathbb{Q}_p$, при $p \neq 2$, и из восьми элементов $\{1, 2, 3, 5, 6, 7, 10, 14\}$ при $p = 2$.

§ 2. Некоторые функции на $\mathbb{Q}_p$

Характеры поля $\mathbb{Q}_p$. Пусть $\chi(x)$ – *аддитивный характер поля* $\mathbb{Q}_p$:

$$\chi(x+y)=\chi(x)\chi(y), \qquad |\chi(x)|=1, \quad x,y\in\mathbb{Q}_p. \tag{2.1}$$

Стандартный аддитивный характер поля $\mathbb{Q}_p$ имеет вид

$$\chi_p(x)=\exp(2\pi i\{x\}_p), \tag{2.2}$$

где $\{x\}_p$ – дробная часть $x\in\mathbb{Q}_p$, определенная формулой (1.3).

Общий вид аддитивного характера поля $\mathbb{Q}_p$:

$$\chi(x)=\chi_p(\xi x)=\exp(2\pi i\{\xi x\}_p) \tag{2.3}$$

при некотором $\xi\in\mathbb{Q}_p$.

Пусть $\pi(x)$ – *мультипликативный характер* поля $\mathbb{Q}_p$:

$$\pi(xy)=\pi(x)\pi(y), \qquad |\pi(x)|=1, \quad x,y\in\mathbb{Q}_p^\times. \tag{2.4}$$

Общий вид мультипликативного характера поля $\mathbb{Q}_p$:

$$\pi(x)=\pi_{i\alpha,\theta}(x)=|x|_p^{i\alpha}\theta(x), \qquad x\in\mathbb{Q}_p^\times, \tag{2.5}$$

где $\alpha\in\mathbb{R}$ определяется равенством $\pi(p)=p^{-i\alpha}$ и $\theta(t)$, $t\in Z_p^\times$, – характер компактной группы $Z_p^\times$, нормированный условием $\theta(p)=1$. (Множество последних счетно и дискретно.)

Если условие унитарности $|\pi(x)|=1$ в (2.4) не выполнено, то функция $\pi(x)$ есть *представление* группы $\mathbb{Q}_p^\times$ в $\mathbb{C}$, и ее общий вид дается формулой (2.5), в которой $i\alpha$ – уже любое комплексное число,

$$\pi_{\alpha,\theta}(x)=|x|_p^{\alpha-1}\theta(x), \qquad x\in\mathbb{Q}_p^\times, \quad \alpha\in\mathbb{C}. \tag{2.5$'$}$$

Такие функции называются *квазихарактерами*. Квазихарактер $\pi(x)=|x|_p^{\alpha-1}$, для которого $\theta=1$, называется *главным*.

Пусть $d\notin\mathbb{Q}_p^{\times 2}$. Без ограничения общности можно считать, что d свободно от квадратов p-адических чисел, т. е. имеет один из перечисленных в § 1 видов: $p,\epsilon,p\epsilon$, $|\epsilon|_p=1$, $\epsilon\notin\mathbb{Q}_p^{\times 2}$ при $p\neq 2$ и $2,3,5,6,7,10,14$ при $p=2$.

Множество p-адических чисел из $\mathbb{Q}_p^\times$, представимых в виде $\alpha^2-d\beta^2$, $\alpha,\beta\in\mathbb{Q}_p$, обозначим $\mathbb{Q}_p^\times(d)$; $\mathbb{Q}_p^\times(d)$ – мультипликативная группа.

Символ Гильберта $\left(\frac{x,y}{p}\right)$, $x,y \in \mathbb{Q}_p^\times$, по определению равен 1 или -1 в зависимости от того, представляет ли форма $x\alpha^2 + y\beta^2 - \gamma^2$ нетривиально нуль в $\mathbb{Q}_p$ или нет.

Символ Гильберта обладает следующими очевидными свойствами [12]:

$$\left(\frac{x,y}{p}\right) = \left(\frac{y,x}{p}\right), \quad \left(\frac{x,-x}{p}\right) = 1, \quad \left(\frac{x,yz}{p}\right) = \left(\frac{x,y}{p}\right)\left(\frac{x,z}{p}\right)$$

и, кроме того,

$$\left(\frac{p,\epsilon}{p}\right) = \left(\frac{\epsilon_0}{p}\right), \qquad \left(\frac{\epsilon,\eta}{p}\right) = 1, \qquad p \neq 2;$$
$$\left(\frac{2,\epsilon}{2}\right) = (-1)^{(\epsilon^2-1)/2}, \quad \left(\frac{\epsilon,\eta}{2}\right) = (-1)^{(\epsilon-1)(\eta-1)/4}, \quad p = 2.$$

Здесь ϵ и η – любые единицы поля $\mathbb{Q}_p$.

Отсюда следует критерий того, что p-адическое число x принадлежит $\mathbb{Q}_p^\times(d)$ при $p \neq 2$: *для того чтобы* $x \in \mathbb{Q}_p^\times(d)$, *необходимо и достаточно*: *при* $d = \epsilon$ $\gamma(x)$ – *четное*; *при* $d = p$ $\gamma(x)$ – *четное и* $(x_0/p) = 1$ *или* $\gamma(x)$ – *нечетное и* $(-x_0/p) = 1$; *при* $D = p\epsilon$ $\gamma(x)$ – *четное и* $(x_0/p) = 1$ *или* $\gamma(x)$ – *нечетное и* $(-x_0/p) = -1$. (Аналогичный критерий имеет место и при $p = 2$.)

Отсюда выводим: *группа* $\mathbb{Q}_p^\times/\mathbb{Q}_p^\times(d)$ *изоморфна группе* $(1,-1)$ *и функция*

$$\operatorname{sgn}_{p,d} x = \begin{cases} 1, & x \in \mathbb{Q}_p^\times(d), \\ -1, & x \notin \mathbb{Q}_p^\times(d) \end{cases} \tag{2.6}$$

есть мультипликативный характер группы $\mathbb{Q}_p^\times$ (*поля* $\mathbb{Q}_p$).

Непосредственно из определений следует

$$\operatorname{sgn}_{p,d} x = \left(\frac{x,-dx}{p}\right), \qquad x \in \mathbb{Q}_p^\times, \qquad d \notin \mathbb{Q}_p^{\times 2}.$$

(Отметим, что всегда $\left(\frac{x,-dx}{p}\right) = 1$, если $d \in \mathbb{Q}_p^{\times 2}$.)

λ_p-функция поля $\mathbb{Q}_p$ определяется следующим образом [1], [2], [13], [14]:

$$\lambda_p(x)=\begin{cases}1, & \gamma(x)=2k, \quad p\ne 2,\\ \sqrt{\left(\dfrac{-1}{p}\right)}\left(\dfrac{x_0}{p}\right), & \gamma(x)=2k+1, \quad p\ne 2,\\ \exp[\pi i(1/4+x_1)], & \gamma(x)=2k, \quad p=2,\\ \exp[\pi i(1/4+x_1/2+x_2)], & \gamma(x)=2k+1, \quad p=2.\end{cases}$$

Свойства функции $\lambda_p\colon \mathbb{Q}_p^\times\to\mathbb{C}$:

$$\begin{gathered}|\lambda_p(x)|=1,\\ \lambda_p(x)\lambda_p(-x)=1,\\ \lambda_p(x)=\lambda_p(y), \qquad xy\in\mathbb{Q}_p^{\times 2},\\ \frac{\lambda_p(x)\lambda_p(y)}{\lambda_p(x+y)}=\lambda_p\left(\frac{xy}{x+y}\right),\\ \lambda_p(x)\lambda_p(y)=\left(\frac{x,y}{p}\right)\lambda_p(xy)\lambda_p(1).\end{gathered}\tag{2.7}$$

Полагая в (2.7) $y=-dx$ и пользуясь формулой (2.6), получим соотношение [13]

$$\operatorname{sgn}_{p,d}x=\lambda_p(x)\lambda_p(-dx)\lambda_p(d)\lambda_p(-1), x\in\mathbb{Q}_p^\times, \quad d\notin\mathbb{Q}_p^{\times 2}.\tag{2.8}$$

Отметим следующую формулу [13]:

$$\operatorname{sgn}_{p,d}x=\begin{cases}\left(\dfrac{x_0}{p}\right)^{\gamma(d)}\left(\dfrac{d_0}{p}\right)^{\gamma(x)}\left(\dfrac{-1}{p}\right)^{\gamma(x)\gamma(d)}, & p\ne 2,\\ (-1)^{d_1x_1+(d_1+d_2)\gamma(x)+(x_1+x_2)\gamma(d)}, & p=2.\end{cases}\tag{2.9}$$

В частности, при $d\equiv 3 \pmod 4$ имеем [14]:

$$\operatorname{sgn}_{p,d}x=\begin{cases}1, & \left(\dfrac{d}{p}\right)=1, \quad p\ne d, \quad p\ne 2,\\ (-1)^{\gamma(x)}, & \left(\dfrac{d}{p}\right)=-1, \quad p\ne d, \quad p\ne 2,\\ \left(\dfrac{x_0}{p}\right)(-1)^{\gamma(x)}, & p=d,\\ (-1)^{x_1}, & p=2, \quad d\equiv 7 \pmod 8,\\ (-1)^{x_1+\gamma(x)}, & p=2, \quad d\equiv 3 \pmod 8.\end{cases}$$

Справедливы следующие равенства при $x, y \in \mathbb{Q}_p^\times$:

$$|x|_\infty \prod_{p=2}^{\infty} |x|_p = 1, \qquad |x|_\infty = |x|, \tag{2.10}$$

$$\chi_\infty(x) \prod_{p=2}^{\infty} \chi_p(x) = 1, \qquad \chi_\infty(x) = \exp(-2\pi i x), \tag{2.11}$$

$$\lambda_\infty(x) \prod_{p=2}^{\infty} \lambda_p(x) = 1, \qquad \lambda_\infty(x) = \exp(-i\pi/4 \operatorname{sgn} x), \tag{2.12}$$

$$\left(\frac{x,y}{\infty}\right) \prod_{p=2}^{\infty} \left(\frac{x,y}{p}\right) = 1, \tag{2.13}$$

где

$$\left(\frac{x,y}{\infty}\right) = \begin{cases} -1, & x<0, \quad y<0, \\ 1 & \text{в противном случае,} \end{cases}$$

$$\operatorname{sgn}_{\infty,d} x \prod_{p=2}^{\infty} \operatorname{sgn}_{p,d} x = 1, \tag{2.14}$$

$$\operatorname{sgn}_{\infty,d} x = \begin{cases} \operatorname{sgn} x, & d<0, \\ 1, & d>0. \end{cases}$$

Бесконечные произведения в формулах (2.10)–(2.14) сходятся для всех рациональных значений x и y, поскольку лишь конечное число множителей в них отлично от 1. Такого типа формулы называются *адельными*.

Обозначаем: $\Omega(|x|_p)$ – характеристическую функцию диска B_0 (так что $\Omega(t) = 1$, если $0 \leqslant t \leqslant 1$ и $\Omega(t) = 0$, если $t > 1$); $\delta(|x|_p - p^\gamma)$ – характеристическую функцию окружности S_γ; $\delta(x_\ell - k)$ – характеристическую функцию множества $[x \in \mathbb{Q}_p : x_\ell = k]$, $k = 1, 2, \ldots, p-1$ при $\ell = 0$ и $k = 0, 1, \ldots, p-1$ при $\ell = 1, 2, \ldots$.

§ 3. Аналитические функции

Пусть $\mathscr{O}$ – открытое множество в $\mathbb{Q}_p$. Функция $f\colon \mathscr{O} \to \mathbb{Q}_p$ называется *аналитической* в $\mathscr{O}$, если для любой точки $a \in \mathscr{O}$ существует такое $\gamma \in Z$, что в диске $B_\gamma(a)$ она представляется сходящимся

степенным рядом

$$f(x) = \sum_{k=0}^{\infty} c_k (x-a)^k. \tag{3.1}$$

Радиус сходимости $r = r(f)$ ряда (3.1) есть

$$r = p^{\sigma},$$
$$\sigma = -\frac{1}{\ln p} \limsup_{n\to\infty} \frac{1}{n} \ln |f_n|_p,$$

где

$$f_n(x) = \sum_{k=0}^{n} c_k (x-a)^k.$$

Ряд (3.1) сходится тогда, и только тогда, когда сходится ряд

$$\sum_{k=0}^{\infty} |c_k| p^{\gamma k}, \qquad \gamma = \gamma(x-a),$$

и его можно дифференцировать почленно в $B_\gamma(a)$ бесконечное число раз

$$f^{(n)}(x) = \sum_{k=n}^{\infty} k(k-1)\cdots(k-n+1) c_k (x-a)^{k-n}, \qquad n = 1, 2, \ldots, \tag{3.2}$$

причем

$$c_k = \frac{f^{(k)}(a)}{k!}, \qquad k = 0, 1, \ldots. \tag{3.3}$$

При каждом дифференцировании ряда (3.1) радиус сходимости продифференцированного ряда (3.2) может разве лишь увеличиться.

Функции e^x, $\ln x$, $\sin x$, $\cos x$, $\operatorname{tg} x$, $\arcsin x$, $\operatorname{arctg} x$ аналитические, они определяются следующими рядами:

$$e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!}, \qquad x \in G_p, \tag{3.4}$$

$$\ln x = \ln[1-(1-x)], \qquad x \in J_p,$$

$$\ln x = -\sum_{k=1}^{\infty} \frac{x^k}{k}, \qquad x \in G_p, \tag{3.5}$$

$$\sin x = \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k+1)!}\, x^{2k+1}, \qquad x \in G_p, \tag{3.6}$$

$$\cos x = \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k)!}\, x^{2k}, \qquad x \in G_p, \tag{3.7}$$

$$\operatorname{tg} x = \frac{\sin x}{\cos x}, \qquad x \in G_p, \tag{3.8}$$

$$\arcsin x = \sum_{k=0}^{\infty} \frac{(2k)!}{2^{2k}(k!)^2(2k+1)}\, x^{2k+1}, \qquad x \in G_p, \tag{3.9}$$

$$\operatorname{arctg} x = \sum_{k=0}^{\infty} \frac{(-1)^k}{2k+1}\, x^{2k+1}, \qquad x \in G_p. \tag{3.10}$$

Справедливы соотношения:

$$(e^x)' = e^x, \qquad e^x e^y = e^{x+y}, \qquad x, y \in G_p, \tag{3.11}$$

$$|e^x|_p = 1, \qquad |e^x - 1|_p = |x|_p, \qquad x \in G_p, \tag{3.12}$$

$$\ln(xy) = \ln x + \ln y, \qquad x, y \in G_p, \tag{3.13}$$

$$|\ln(1+x)|_p = |x|_p, \qquad x \in G_p, \tag{3.14}$$

$$\ln e^x = x, \quad x \in G_p; \qquad e^{\ln x} = x, \qquad x \in J_p. \tag{3.15}$$

Функция e^x реализует аналитический диффеоморфизм аддитивной группы G_p на мультипликативную группу J_p. Обратное отображение осуществляется функцией $\ln x$.

Справедливы все формулы классической тригонометрии. Их доказательство легко следует из формального соотношения

$$e^{ix} = \cos x + i \sin x, \qquad x \in G_p, \tag{3.16}$$

где символ e^{ix} определяется рядом (3.3) при условии, что $i^2 = -1$.

В частности,

$$\sin^2 x + \cos^2 x = 1, \qquad x \in G_p, \tag{3.17}$$

$$e^{\theta x} = \cos x + \theta \sin x, \qquad x \in G_p, \quad \theta^2 = -1, \quad \theta \in \mathbb{Q}_p \tag{3.18}$$

(последнее возможно лишь при $p \equiv 1 \pmod 4$).

Функции $\sin x$ и $\operatorname{tg} x$ реализуют аналитические изоморфизмы группы G_p на G_p; обратные отображения даются функциями $\arcsin x$ и $\operatorname{arctg} x$ соответственно.

§ 4. Мера Хаара на $\mathbb{Q}_p$

Так как $\mathbb{Q}_p$ есть коммутативная группа по сложению, то на ней существует единственная (с точностью до множителя) инвариантная мера, – мера Хаара, – которую мы обозначим через $d_p x$:

$$d_p(x+a) = d_p x, \quad a \in \mathbb{Q}_p; \qquad d_p(ax) = |a|_p d_p x, \quad a \in \mathbb{Q}_p^\times.$$

Нормируем меру dx условием

$$\int_{Z_p} d_p x = 1. \tag{4.1}$$

Нормированная мера Хаара $d_p^\times x$ на $\mathbb{Q}_p^\times$ есть

$$d_p^\times x = (1-p^{-1})^{-1} \frac{d_p x}{|x|_p}, \qquad d_p^\times(ax) = d_p^\times x, \qquad a, x \in \mathbb{Q}_p^\times, \tag{4.2}$$

так что

$$\int_{Z_p^\times} d_p^\times x = 1.$$

Пусть $M \subset \mathbb{Q}_p$ – измеримое по мере Хаара множество. Интеграл функции $f\colon M \to \mathbb{C}$ по множеству M будем записывать в виде

$$\int_M f(x)\, d_p x, \qquad \int f(x) = \int_{\mathbb{Q}_p} f(x)\, d_p x.$$

Пусть $1 \leqslant q \leqslant \infty$. Множество функций $f\colon \mathbb{Q}_p \to \mathbb{C}$, для которых $f(x) = 0$, $x \notin M$, и

$$\|f\|_q = \left[\int_M |f(x)|^q\, d_p x\right]^{1/q} < \infty, \qquad \text{если } q < \infty,$$

$$\|f\|_\infty = \operatorname*{vrai\,sup}_{x \in M} |f(x)| < \infty, \qquad \text{если } q = \infty,$$

обозначим через $\mathscr{L}^q(M)$, $\mathscr{L}^q = \mathscr{L}^q(\mathbb{Q}_p)$. Если $\mathscr{O}$ – открытое множество в $\mathbb{Q}_p$, то множество функций $f\colon \mathscr{O} \to \mathbb{C}$, для которых для любого компакта $K \subset \mathscr{O}$ $f \in \mathscr{L}^q(K)$, обозначим через $\mathscr{L}^q_{\mathrm{loc}}(\mathscr{O})$, $\mathscr{L}^q_{\mathrm{loc}} = \mathscr{L}^q_{\mathrm{loc}}(\mathbb{Q}_p)$.

Функции из множества $\mathscr{L}^1_{\mathrm{loc}}(\mathscr{O})$ называются *локально-интегрируемыми в* $\mathscr{O}$.

Пусть функция $f \in \mathscr{L}^1_{\mathrm{loc}}(\mathbb{Q}_p^\times)$. (*Несобственным*) *интегралом* функции f по $\mathbb{Q}_p$,

$$\int f(x)\,d_px = \sum_{\gamma=-\infty}^{\infty} \int_{S_\gamma} f(x)\,d_px,$$

называется предел (если он существует)

$$\lim_{N,M\to\infty} \int_{B_N \setminus B_{-M-1}} = \lim_{N,M\to\infty} \sum_{\gamma=-M}^{N} \int_{S_\gamma} f(x)\,dx.$$

Пример. Интеграл

$$\int_{Z_p} |x|^{\alpha-1}\,d_px = \frac{1-p^{-1}}{1-p^{-\alpha}} \tag{4.3}$$

существует при $\operatorname{Re}\alpha > 0$.

Формула замены переменных в интеграле: *если* $x(y)$ *– аналитический диффеоморфизм открыто-замкнутого множества* $D' \subset \mathbb{Q}_p$ *на* $D \subset \mathbb{Q}_p$, *причем* $x'(y) \neq 0$, $y \in D'$, *то для любой* $f \in \mathscr{L}^1(D)$ *справедлива формула*

$$\int_D f(x)\,dx_p = \int_{D'} f(x(y))|x'(y)|_p\,d_py. \tag{4.4}$$

Пример. Пусть $x = (py)^{-1}$, $d_px = p|y|_p^{-2}\,d_py$. Тогда в силу (3.4) имеем

$$\int_{|x|_p>1} |x|_p^{\alpha-1}\,d_px = p^\alpha \int_{Z_p} |y|_p^{-\alpha-1}\,d_py = \frac{1-p^{-1}}{p^{-\alpha}-1}, \qquad \operatorname{Re}\alpha < 0.$$

Пример. Для дробно-линейного преобразования

$$x = \frac{ay+b}{cy+d}, \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(\mathbb{Q}_p, 2),$$

$$d_px = \frac{|ad-dc|_p}{|cx+d|_p^2}\,d_py.$$

§ 5. n-мерное пространство $\mathbb{Q}_p^n$

Пространство $\mathbb{Q}_p^n = \mathbb{Q}_p \times \mathbb{Q}_p \times \cdots \times \mathbb{Q}_p$ (n раз) состоит из точек $x = (x_1, x_2, \ldots, x_n)$, $x_j \in \mathbb{Q}_p$, $j = 1, 2, \ldots, n$, снабженных нормой

$$|x|_p = \max_{1 \leqslant j \leqslant n} |x_j|_p. \tag{5.1}$$

Эта норма обладает свойствами 1)–3) § 1, так что пространство $\mathbb{Q}_p^n$ ультраметрическое (неархимедово).

Скалярное произведение

$$(x, y) = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n, \qquad x, y \in \mathbb{Q}_p^n,$$

удовлетворяет неравенству

$$|(x, y)|_p \leqslant |x|_p |y|_p, \qquad x, y \in \mathbb{Q}_p^n.$$

Меру Хаара на $\mathbb{Q}_p^n$ обозначаем $d_p^n x = d_p x_1 d_p x_2 \cdots d_p x_n$, $d_p^1 x_1 = d_p x$,

$$d_p^n(x + a) = d_p^n x, \quad a \in \mathbb{Q}_p^n, \qquad d_p^n(Ax) = |\det A|_p \, d_p^n x,$$

где $x \to Ax$ – линейный изоморфизм $\mathbb{Q}_p^n$ на $\mathbb{Q}_p^n$ ($\det A \neq 0$).

Впредь условимся в интегралах по всему пространству $\mathbb{Q}_p^n$ опускать область интегрирования,

$$\int_{\mathbb{Q}_p^n} f(x) \, d_p^n x = \int f(x) \, d_p^n x.$$

Пространства функций $\mathscr{L}^q(M)$ и $\mathscr{L}^q_{\mathrm{loc}}(\mathscr{O})$, $M, \mathscr{O} \in \mathbb{Q}_p^n$, определяются аналогично случаю $n = 1$ (см. § 4).

Как и в случае $n = 1$, с помощью введенной нормы, определяем: $B_\gamma^n(a)$ – шар радиуса p^γ с центром в точке $a \in \mathbb{Q}_p^n$ и $S_\gamma^n(a)$ – сфера радиуса p^γ с центром в точке a; $B_\gamma^n(0) = B_\gamma^n$, $B_\gamma^1(a) = B_\gamma(a)$, $S_\gamma^n(0) = S_\gamma^n$, $S_\gamma^1(a) = S_\gamma(a)$,

$$B_\gamma^n(a) = B_\gamma(a_1) \times B_\gamma(a_2) \times \cdots \times B_\gamma(a_n).$$

Теорема Фубини. *Если функция $f\colon \mathbb{Q}_p^{n+m} \to \mathbb{C}$ такова, что повторный интеграл*

$$\int \left[\int |f(x, y)| \, d_p^m y \right] d_p^n x$$

существует, то $f \in \mathscr{L}^1(\mathbb{Q}_p^{n+m})$ *и справедливы равенства*

$$\int \left[\int f(x,y)\, d_p^m y \right] d_p^n x = \int f(x,y)\, d_p^n x\, d_p^m y = \int \left[\int f(x,y)\, d_p^n x \right] d_p^m y. \tag{5.2}$$

Замена переменных. *Если* $x = x(y)$ *– аналитический диффеоморфизм открыто-замкнутого множества* $D' \subset \mathbb{Q}_p^n$ *на множество* $D \subset \mathbb{Q}_p^n$, *причем*

$$\det \frac{\partial x(y)}{\partial y} = \det\left(\frac{\partial x_k}{\partial y_j} \right) \neq 0, \qquad y \in D',$$

то для любой $f \in \mathscr{L}^1(D)$ *справедливо равенство*

$$\int_D f(x)\, d_p^n x = \int_{D'} f(x(y)) \left| \det \frac{\partial x(y)}{\partial y} \right|_p d_p^n y. \tag{5.3}$$

Теорема Лебега (о предельном переходе под знаком интеграла). *Если последовательность* f_k, $k \to \infty$, *функций* $f_k \in \mathscr{L}^1$ *сходится почти всюду к функции* $f(x)$ *и существует функция* $\psi \in \mathscr{L}^1$ *такая, что*

$$|f_k(x)| \leqslant \psi(x) \quad \text{при почти всех } x \in \mathbb{Q}_p^n,$$

то справедливо равенство

$$\lim_{k\to\infty} \int f_k(x)\, d_p^n x = \int f(x)\, d_p^n x.$$

§ 6. Обобщенные функции на $\mathbb{Q}_p^n$

Пусть $\mathscr{O}$ – открытое множество в $\mathbb{Q}_p^n$. Функция $\varphi\colon \mathscr{O} \to \mathbb{C}$ называется *локально-постоянной* в $\mathscr{O}$, если для любой точки $x \in \mathscr{O}$ существует такое $\gamma \in Z$, что

$$\varphi(x + x') = \varphi(x), \qquad x' \in B_\gamma^n, \quad x \in \mathscr{O}.$$

Множество локально-постоянных функций в $\mathcal{O}$ обозначим через $\mathcal{E}(\mathcal{O})$; $\mathcal{E} = \mathcal{E}(\mathbb{Q}_p^n)$. Всякая функция $\varphi \in \mathcal{E}(\mathcal{O})$ непрерывна в $\mathcal{O}$. Ее носитель, – замыкание множества тех точек $x \in \mathcal{O}$, для которых $\varphi(x) \neq 0$, – будем обозначать $\operatorname{spt}\varphi$.

Примеры.

$$|x|_p \in \mathcal{E}(\mathbb{Q}_p^n \setminus \{0\}),$$
$$\chi_p((\xi, x)) \in \mathcal{E}, \qquad \xi \in \mathbb{Q}_p^n.$$

Функция $\varphi \in \mathcal{E}(\mathcal{O})$ называется *основной* в $\mathcal{O}$ (функцией Брюа–Шварца), если ее носитель есть компакт в $\mathcal{O}$. Множество основных функций в $\mathcal{O}$ обозначим $\mathcal{S}(\mathcal{O})$; $\mathcal{S} = \mathcal{S}(\mathbb{Q}_p^n)$. Всякая функция $\varphi \in \mathcal{S}(\mathcal{O})$ равномерно локально-постоянна в $\mathcal{O}$.

Примеры.

$$\Omega_k(x) = \Omega(p^{-k}|x|_p) \in \mathcal{S}, \qquad k \in Z, \tag{6.1}$$
$$\Delta_k(x) = p^k\Omega(p^k|x|_p) \in \mathcal{S}, \qquad k \in Z, \tag{6.2}$$
$$|x|_p\Omega(|x|_p) \in \mathcal{S}(\mathbb{Q}_p^n \setminus \{0\}),$$

$$\chi_p((\xi, x))\Omega(|x|_p) \in \mathcal{S}, \qquad \xi \in \mathbb{Q}_p^n,$$
$$\delta(|x|_p - p^\gamma) \in \mathcal{S}(S_\gamma), \qquad \gamma \in Z,$$
$$\delta(|x|_p - p^\gamma)\delta(x_0 - k) \in \mathcal{S}(S_\gamma), \qquad k = 1, 2, \ldots, p-1, \quad \gamma \in Z.$$

Если K – открытый компакт в $\mathbb{Q}_p^n$, то $\theta_K \in \mathcal{S}(K)$. Здесь θ_M – характеристическая функция множества $M \subset \mathbb{Q}_p^n$: $\theta_M(x) = 1$, $x \in M$, $\theta_M(x) = 0$, $x \notin M$.

Сходимость в $\mathcal{S}(\mathcal{O})$,

$$\varphi_k \to 0, \quad k \to \infty \quad \text{в } \mathcal{S}(\mathcal{O}),$$

обозначает:

(i) существует компакт $K \subset \mathcal{O}$, не зависящий от k и такой, что $\operatorname{spt}\varphi_k \in K$ при всех k;

(ii) существует $\gamma \in Z$, не зависящее ни от k, ни от x, такое что

$$\varphi_k(x + x') = \varphi_k(x), \qquad x' \in B_\gamma^n, \quad x \in K;$$

(iii) $\varphi_k(x) \rightrightarrows 0$, $x \in K$, $k \to \infty$.

Обобщенной функцией в $\mathscr{O}$ называется всякий линейный непрерывный функционал $f\colon \varphi \to (f,\varphi)$ на $\mathscr{S}(\mathscr{O})$. Множество всех обобщенных функций в $\mathscr{O}$ обозначим $\mathscr{S}'(\mathscr{O})$; $\mathscr{S}' = \mathscr{S}'(\mathbb{Q}_p^n)$.

Сходимость в $\mathscr{S}'(\mathscr{O})$,

$$f_k \to 0, \qquad k \to \infty \quad \text{в } \mathscr{S}'(\mathscr{O}),$$

определяется как слабая сходимость функционалов из $\mathscr{S}'(\mathscr{O})$, т. е.

$$(f_k,\varphi) \to 0, \qquad k \to \infty, \quad \varphi \in \mathscr{S}(\mathscr{O}).$$

Всякий линейный на $\mathscr{S}(\mathscr{O})$ *функционал* f *непрерывен на* $\mathscr{S}(\mathscr{O})$, *т. е.* $f \in \mathscr{S}'(\mathscr{O})$.

В открытом множестве $\mathscr{O}$ существует "*разложение единицы*" с функциями из $\mathscr{S}(\mathscr{O})$, а именно: если

$$\mathscr{O} = \bigcup_{k=1}^{\infty} G_k, \qquad G_k \cap G_j = \varnothing, \quad k \neq j,$$

где G_k, $k = 1,2,\ldots,$ – клопен компакты, то

$$\sum_{k=1}^{\infty} \theta_{G_k}(x) = 1, \qquad x \in \mathscr{O}. \tag{6.3}$$

Обобщенная функция f из $\mathscr{S}'(\mathscr{O})$ *обращается в нуль в открытом множестве* $\mathscr{O}' \subset \mathscr{O}$, если $(f,\varphi) = 0$, $\varphi \in \mathscr{S}(\mathscr{O})'$; при этом пишем: $f(x) = 0$, $x \in \mathscr{O}'$. Обобщенные функции f и g из $\mathscr{S}'(\mathscr{O})$ *совпадают (равны) в* $\mathscr{O}' \subset \mathscr{O}$, $f = g$ в $\mathscr{O}'$, если $f(x) - g(x) = 0$, $x \in \mathscr{O}'$. Наибольшее открытое множество, в котором обращается в нуль $f \in \mathscr{S}'(\mathscr{O})$, называется *нулевым множеством* f и оно обозначается $\mathscr{O}_f \subset \mathscr{O}$. Замкнутое в $\mathscr{O}$ множество $\mathscr{O} \setminus \mathscr{O}_f$ называется *носителем* f и обозначается $\operatorname{spt} f$, $\operatorname{spt} f = \mathscr{O} \setminus \mathscr{O}_f$.

Множество обобщенных функций с компактным носителем в $\mathscr{O}$ обозначим через $\mathscr{E}'(\mathscr{O})$, $\mathscr{E}' = \mathscr{E}'(\mathbb{Q}_p^n)$; $\mathscr{E}'(\mathscr{O})$ – сильно сопряженное пространство к $\mathscr{E}(\mathscr{O})$.

Пример. *δ-Функция*

$$(\delta,\varphi) = \varphi(0), \qquad \operatorname{spt}\delta = \{0\}. \tag{6.4}$$

Обратно, всякая $f \in \mathscr{S}'$, $\operatorname{spt} f = \{0\}$, имеет вид

$$f = C\delta, \tag{6.5}$$

где $C \neq 0$ – произвольная постоянная.

Последовательность $\{\delta_k, k \to \infty\}$ функций $\delta_k(x)$ из $\mathscr{S}$ называется δ-*образной*, если она ограничена в $\mathscr{L}^1$ и для любого $\gamma \in Z$

$$\int_{B_\gamma^n} \delta_k(x)\, d_p^n x \to 1, \qquad \int_{\mathbb{Q}_p^n \setminus B_\gamma^n} |\delta_k(x)|\, d_p^n x \to 0, \qquad k \to \infty.$$

Таким образом,

$$\delta_k \to \delta, \quad k \to \infty \quad \text{в } \mathscr{S}'. \tag{6.6}$$

Последовательность $\{\omega_k, k \to \infty\}$ функций $\omega_k(x)$ из $\mathscr{S}$ называется 1-*образной*, если она есть преобразование Фурье (см. ниже § 7) некоторой δ-образной последовательности $\{\delta_k, k \to \infty\}$.

1-Образная последовательность обладает свойствами: ограничена в $\mathscr{L}^\infty$ и для любого $\gamma \in Z$

$$\omega_k(x) \Rightarrow 1, \qquad x \in B_\gamma^n, \quad k \to \infty.$$

Таким образом,

$$\omega_k \to 1, \quad k \to \infty \quad \text{в } \mathscr{S}'. \tag{6.7}$$

Если $f \in \mathscr{L}^1_{\mathrm{loc}}(\mathscr{O})$, то $f \in \mathscr{S}'(\mathscr{O})$, причем

$$(f, \varphi) = \int f(x)\varphi(x)\, d_p^n x, \qquad \varphi \in \mathscr{S}(\mathscr{O}). \tag{6.8}$$

Обобщенные функции типа (6.8) называются *регулярными в* $\mathscr{O}$; остальные обобщенные функции называются *сингулярными*. δ-Функция сингулярна в $\mathbb{Q}_p^n$ и регулярна в $\mathbb{Q}_p^n \setminus \{0\}$.

Пусть $0 \in \mathscr{O}$. Если $f \in \mathscr{S}'(\mathscr{O} \setminus \{0\})$, то она допускает *продолжение* (*регуляризацию*) $f_1 \in \mathscr{S}'(\mathscr{O})$ на $\mathscr{O}$, и все ее регуляризации, $\operatorname{reg} f$, задаются формулой

$$\operatorname{reg} f = f_1 + C\delta, \tag{6.9}$$

где C – произвольная постоянная, а f_1 можно взять в виде

$$(f_1, \varphi) = (f, \varphi - \Omega_\gamma \varphi(0)), \qquad \varphi \in \mathscr{S}(\mathscr{O}),$$

причем $\gamma \in Z$ таково, что $B_\gamma^n \subset \mathscr{O}$. Заметим, что этот факт не имеет места для обобщенных функций вещественных аргументов! Примером такой f является функция $f(x) = \exp(x^{-1})$.

Для $f = |x|_p^{-1}$ в качестве регуляризации можно взять функционал

$$\big(\operatorname{reg}|x|_p^{-1}, \varphi\big) = \int |x|_p^{-1}[\varphi(x) - \Omega(|x|_p)\varphi(0)]\, d_p^n x, \qquad \varphi \in \mathscr{S}.$$

Обобщенная функция $\operatorname{reg}|x|_p^{-1}$ является другим примером сингулярной обобщенной функции в $\mathbb{Q}_p^n$.

Произведение обобщенной функции $f \in \mathscr{S}'(\mathscr{O})$ на функцию $a \in \mathscr{E}(\mathscr{O})$ определяется формулой

$$(af, \varphi) = (f, a\varphi), \qquad \varphi \in \mathscr{S}(\mathscr{O}), \quad af \in \mathscr{S}'(\mathscr{O}). \tag{6.10}$$

Примеры. Если $a \in \mathscr{E}$, то

$$a(x)\,\delta(x) = a(0)\,\delta(x).$$

Если $f \in \mathscr{L}^1_{\mathrm{loc}}(\mathscr{O})$, то af совпадает с обычным произведением функций $a(x)$ и $f(x)$.

Если $f \in \mathscr{S}'(\mathscr{O})$ и $\operatorname{spt} f$ – открыто-замкнутое множество в $\mathscr{O}$, то

$$f(x) = \theta_{\operatorname{spt} f}(x) f(x). \tag{6.11}$$

Наконец, если $f \in \mathscr{S}'$, то

$$\omega_k f \to f, \quad k \to \infty \quad \text{в } \mathscr{S}', \tag{6.12}$$

где $\{\omega_k, k \to \infty\}$ – любая 1-образная последовательность.

В $\mathscr{S}'(\mathscr{O})$ справедлива *теорема о "кусочном склеивании"*. Пусть задан набор обобщенных функций $f_k \in \mathscr{S}'(G_k)$, $k = 1, 2, \ldots$, где G_k – открыто-замкнутые компакты, причем $G_k \cap G_j = \varnothing$, $k \neq j$. Тогда существует (единственная) обобщенная функция $f \in \mathscr{S}'(\mathscr{O})$, где $\mathscr{O} = \bigcup_{k \geqslant 1} G_k$, такая что $f = f_k$ в G_k, $k = 1, 2, \ldots$.

Теорема о "ядре". *Пусть $\varphi \to A(\varphi)$ – линейное отображение $\mathscr{S}(\mathscr{O})$, $\mathscr{O} \in \mathbb{Q}_p^n$, в $\mathscr{S}'(\mathscr{O}')$, $\mathscr{O}' \in \mathbb{Q}_p^m$. Тогда существует (единственная) обобщенная функция $f \in \mathscr{S}'(\mathscr{O} \times \mathscr{O}')$ такая, что*

$$\big(A(\varphi), \psi\big) = \big(f, \varphi(x)\psi(y)\big), \qquad \varphi \in \mathscr{S}(\mathscr{O}), \quad \psi \in \mathscr{S}(\mathscr{O}').$$

Пространства $\mathscr{S}(\mathscr{O})$ и $\mathscr{S}'(\mathscr{O})$ – полные, рефлексивные и ядерные; $\mathscr{S}(\mathscr{O})$ плотно в $\mathscr{S}'(\mathscr{O})$.

Линейная замена переменных $y = Ax + b$, $\det A \neq 0$, переводит обобщенную функцию $f(y)$ из $\mathscr{S}'(\mathscr{O}')$ в обобщенную функцию $f(Ax+b)$ из $\mathscr{S}'(\mathscr{O})$ по формуле

$$\big(f(Ax+b),\varphi\big) = \frac{1}{|\det A|_p}\,\big(f(y),\varphi(A^{-1}(y-b))\big), \quad \varphi \in \mathscr{S}(\mathscr{O}). \tag{6.13}$$

Примеры. $\delta(x) = \delta(-x)$, $\quad (\delta(x-x_0),\varphi) = \varphi(x_0)$.

Прямое произведение $f(x) \times g(y)$ обобщенных функций $f \in \mathscr{S}'(\mathscr{O}_1)$, $\mathscr{O}_1 \subset \mathbb{Q}_p^n$, и $g \in \mathscr{S}'(\mathscr{O}_2)$, $\mathscr{O}_2 \subset \mathbb{Q}_p^m$, определяется формулой

$$(f(x)\times g(y),\varphi) = \big(f(x),(g(y),\varphi(x,y))\big), \qquad \varphi \in \mathscr{S}(\mathscr{O}_1\times\mathscr{O}_2).$$

Прямое произведение *коммутативно*, так что

$$f(x)\times g(y) = g(y)\times f(x) \in \mathscr{S}'(\mathscr{O}_1\times\mathscr{O}_2). \tag{6.14}$$

При $g = 1$ формула (6.14) принимает вид

$$\big(f(x),\int_{\mathscr{O}_2}\varphi(x,y)\,d^m y\big) = \int_{\mathscr{O}_2}\big(f(x),\varphi(x,y)\big)\,d^m y, \qquad f\in\mathscr{S}'(\mathscr{O}_1),\quad \varphi\in\mathscr{S}(\mathscr{O}_1\times\mathscr{O}_2) \tag{6.15}$$

(обобщение теоремы Фубини, см. § 5).

Свертка $f * g$ обобщенных функций $f \in \mathscr{E}$, $\operatorname{spt} f \in B_N^n$, и $g \in \mathscr{S}'$ определяется равенством

$$(f*g,\varphi) = \big(f(x)\times g(y),\Omega_N(x)\varphi(x+y)\big), \qquad \varphi\in\mathscr{S}. \tag{6.16}$$

На основе этого определяется свертка обобщенных функций f и g из $\mathscr{S}'$

$$(f*g,\varphi) = \lim_{k\to\infty}\big(f(x)\times g(y),\Omega_k(x)\varphi(x+y)\big) = \lim_{k\to\infty}\big((\Omega_k f)*g,\varphi\big),$$

если предел существует для любых $\varphi \in \mathscr{S}$, так что $f * g \in \mathscr{S}'$.

Если свертка $f * g$ существует, то существует и свертка $g * f$, и они равны (*коммутативность свертки*),

$$f*g = g*f. \tag{6.17}$$

Примеры. Если $f \in \mathscr{S}'$, то

$$f*\delta = \delta*f = f. \tag{6.18}$$

Если $f \in \mathscr{S}'$ и $\psi \in \mathscr{S}$, то свертка $f * \psi$ – локально-постоянная функция в $\mathbb{Q}_p^n$, причем

$$(f * \psi)(x) = (f(y), \psi(x-y)), \qquad x \in \mathbb{Q}_p^n. \tag{6.19}$$

Если $\{\delta_k, k \to \infty\}$ – δ-образная последовательность, то

$$f * \delta_k \to f, \quad k \to \infty \quad \text{в } \mathscr{S}', \qquad f \in \mathscr{S}'. \tag{6.20}$$

Если $f, g \in \mathscr{L}^1_{\mathrm{loc}}$ и существует функция $q \in \mathscr{L}^1_{\mathrm{loc}}$ такая, что

$$\int_{B_k} f(x-y)g(y)\, d_p^n y \to q(x), \quad k \to \infty \quad \text{в } \mathscr{S}',$$

то

$$f * g = q(x). \tag{6.21}$$

Если $f \in \mathscr{S}'$ и свертка $f * 1$ существует, то она постоянная. Эту постоянную назовем *интегралом* обобщенной функции f по всему пространству $\mathbb{Q}_p^n$, и обозначим

$$G\!\int f(x)\, d_p^n x = f * 1. \tag{6.22}$$

Это определение эквивалентно следующему:

$$G\!\int f(x)\, d_p^n x = \lim_{k\to\infty} (f, \Omega_k), \tag{6.23}$$

если предел существует.

Если $f \in \mathscr{S}'$ и $\operatorname{spt} f \subset D$, где D – открыто-замкнутое множество в $\mathbb{Q}_p^n$, то $f = \theta_D f$, и интеграл (6.22) будем обозначать так:

$$G\!\int_D f(x)\, d_p^n x.$$

В частности, если $f \in \mathscr{S}'$ и $\varphi \in \mathscr{S}$, $\operatorname{spt}\varphi \subset B_\gamma^n$, то

$$G\!\int_{B_\gamma^n} f(x)\varphi(x)\, d_p^n x = (f, \varphi). \tag{6.24}$$

Если $f \in \mathscr{S}'$, $\operatorname{spt} f \subset B_\gamma^n$, то

$$G\!\int_{B_\gamma^n} f(x)\, d_p^n x = (f, \Omega_\gamma). \tag{6.25}$$

Введенное понятие интеграла обобщенной функции является расширением понятия интеграла по мере Хаара (см. §§ 1 и 4).

Пример.

$$G\!\!\int \delta(x)\, d_p x = 1.$$

Умножение обобщенных функций. Пусть $f, g \in \mathscr{S}'$. *Произведением* $f \cdot g$ назовем функционал, определяемый равенством

$$f \cdot g = \lim_{k\to\infty} (f * \Delta_k) g,$$

если предел существует в $\mathscr{S}'$, и тогда $f \cdot g \in \mathscr{S}'$.

Если произведение $f \cdot g$ существует, то существует и произведение $g \cdot f$, и они равны (*коммутативность произведения*):

$$f \cdot g = g \cdot f. \tag{6.26}$$

Примеры. Если $a \in \mathscr{E}$, то

$$a \cdot f = af, \qquad a \in \mathscr{E}, \quad f \in \mathscr{S}'.$$

В частности,

$$f \cdot 1 = 1 \cdot f = f, \qquad f \in \mathscr{S}',$$
$$a(x) \cdot \delta(x) = a(0)\, \delta(x),$$
$$|x|_p^\alpha \cdot \delta(x) = 0, \quad \alpha > 0, \qquad |x|_p \cdot \operatorname{reg} |x|_p^{-1} = 1. \tag{6.27}$$

Как и в вещественном случае возникает вопрос: нельзя ли определить произведение любых обобщенных функций так, чтобы оно было ассоциативным и коммутативным? Ответ отрицательный. Известный пример Л. Шварца в p-адическом случае выглядит так: если бы такое произведение существовало, то в силу (6.27) мы имели бы следующую противоречивую цепочку равенств:

$$\begin{aligned} 0 &= 0 \cdot \operatorname{reg} |x|_p^{-1} = (|x|_p \cdot \delta(x)) \cdot \operatorname{reg} |x|_p^{-1} \\ &= \delta(x) \cdot (|x|_p \cdot \operatorname{reg} |x|_p^{-1}) = \delta(x) \cdot 1 = \delta(x). \end{aligned}$$

§ 7. Преобразование Фурье

Пусть $\varphi \in \mathscr{S}$. *Преобразование Фурье* $\widetilde{\varphi} = F[\varphi]$ определяется формулой

$$\widetilde{\varphi}(\xi) = \int \varphi(x)\chi_p((\xi,x))\,d_p^n x, \qquad x \in \mathbb{Q}_p^n.$$

Преобразование Фурье – линейный изоморфизм $\mathscr{S}$ на $\mathscr{S}$, справедлива *формула обращения* преобразования Фурье

$$\varphi(x) = \int \widetilde{\varphi}(\xi)\chi_p(-(x,\xi))\,d_p^n \xi, \qquad \varphi \in \mathscr{S}.$$

Пример.

$$\widetilde{\Omega}_k = \Delta_k, \qquad \widetilde{\Delta}_k = \Omega_k, \qquad k \in Z. \tag{7.1}$$

Преобразование Фурье $\widetilde{f} = F[f]$ обобщенной функции $f \in \mathscr{S}'$ определяется формулой

$$(\widetilde{f},\varphi) = (f,\widetilde{\varphi}), \qquad \varphi \in \mathscr{S},$$

так что $\widetilde{f} \in \mathscr{S}'$.

Преобразование Фурье $f \to \widetilde{f}$ – линейный изоморфизм $\mathscr{S}'$ на $\mathscr{S}'$, и справедлива формула обращения

$$f = F^{-1}[\widetilde{f}\,] = F[\check{\widetilde{f}}], \qquad f \in \mathscr{S}',$$

где $\check{f}(x) = f(-x)$.

Примеры.

$$\widetilde{\delta} = 1, \qquad \widetilde{1} = \delta; \tag{7.2}$$

$$F[f(Ax+b)] = |\det A|_p^{-1}\chi_p\big(-(A^{-1}b,\xi)\big)F[f(A^{-1}\xi)], \quad \det A \neq 0. \tag{7.3}$$

В частности,

$$F[f(x-b)] = \chi_p((b,\xi))F[f(\xi)]; \tag{7.4}$$

$$\widetilde{\check{f}} = \check{\widetilde{f}}. \tag{7.5}$$

Если $f \in \mathscr{L}^1$, то

$$\widetilde{f}(\xi) = \int f(x)\chi_p((\xi,x))\,d^n x, \tag{7.6}$$

причем $\widetilde{f}$ непрерывна в $\mathbb{Q}_p^n$ и $\widetilde{f}(\xi) \to 0$, $|\xi|_p \to \infty$ (аналог *теоремы Римана–Лебега*).

Если $f \in \mathscr{L}^1_{\mathrm{loc}}$ и существует такая $q \in \mathscr{L}^1_{\mathrm{loc}}$, что

$$\int_{B_k^n} f(x)\chi_p((\xi,x))\,d_p^n x \to q(\xi), \qquad k \to \infty \quad \text{в } \mathscr{S}',$$

то

$$\widetilde{f} = q. \tag{7.7}$$

Если $f \in \mathscr{S}'$, $\operatorname{spt} f \subset B_\gamma^n$, то

$$\widetilde{f}(\xi) = \big(f(x), \Omega_\gamma(x)\chi_p((\xi,x))\big). \tag{7.8}$$

Если $f \in \mathscr{L}^2$, то

$$\int_{B_k^n} f(x)\chi_p((\xi,x))\,d_p^n x \to \widetilde{f}(\xi), \qquad k \to \infty \quad \text{в } \mathscr{L}^2. \tag{7.9}$$

Оператор $f \to \widetilde{f}$ – унитарный в $\mathscr{L}^2$, так что справедливо равенство *Парсеваля–Стеклова*

$$\|f\| = \|\widetilde{f}\|, \qquad f \in \mathscr{L}^2, \tag{7.10}$$

где норма $\|f\| = \|f\|_2 = (f,f)^{1/2}$ определена в § 4 и *скалярное произведение* (f,g) в $\mathscr{L}^2$ равно

$$(f,g) = \int f(x)\bar{g}(x)\,d_p^n x, \qquad f,g \in \mathscr{L}^2.$$

Справедливо *неравенство Коши–Буняковского*

$$|(f,g)| \leqslant \|f\|\,\|g\|, \qquad f,g \in \mathscr{L}^2.$$

Если $f \in \mathscr{L}^2$, то

$$\lim_{k\to\infty} p^{-k/2} \int_{B_k} |f(x)|\,d_p^n x = 0. \tag{7.11}$$

Теорема. *Пусть $f, g \in \mathscr{S}'$. Свертка $f * g$ существует тогда и только тогда, когда существует произведение $\widetilde{f} \cdot \widetilde{g}$, и справедливы равенства*

$$\widetilde{f * g} = \widetilde{f} \cdot \widetilde{g}, \qquad \widetilde{f \cdot g} = \widetilde{f} * \widetilde{g}. \tag{7.12}$$

Отметим следующие полезные формулы

$$\int_{S_\gamma^n} \chi_p((x,\xi))\, d_p^n x = (1-p^{-n})p^{\gamma n}\Omega(p^\gamma|\xi|_p) - q^{(k-1)n}\delta(|\xi|_p - p^{1-\gamma}), \tag{7.13}$$

откуда

$$\int_{B_\gamma^n} \chi_p((x,\xi))\, d_p^n x = p^{\gamma n}\Omega(p^\gamma|\xi|_p). \tag{7.14}$$

Гауссовым интегралом $G_p(a;\xi)$ называется преобразование Фурье функции $\chi_p(ax^2)$, $a \in \mathbb{Q}_p^\times$, $p = \infty, 2, 3, 5, \ldots$,

$$G_p(a,\xi) = \int \chi_p(ax^2 + \xi x)\, d_p x = \lambda_p(a)|2a|_p^{-1/2}\chi_p\Big(-\frac{\xi^2}{4a}\Big). \tag{7.15}$$

Справедлива следующая адельная формула

$$G_\infty(a;\xi)\prod_{p=2}^{\infty} G_p(a;\xi) = 1, \qquad a \in \mathbb{Q}^\times, \quad \xi \in \mathbb{Q}, \tag{7.16}$$

вытекающая из адельных формул (2.10)–(2.12).

§ 8. Однородные обобщенные функции

Пусть $\pi(x) = \pi_{\alpha,\theta}(x) = |x|_p^{\alpha-1}\theta(x)$ – квазихарактер поля $\mathbb{Q}_p$ (см. (2.5′)). Обобщенная функция $f \in \mathscr{S}'$ называется *однородной* относительно $\pi_{\alpha,\theta}$, если

$$f(tx) = \pi_{\alpha,\theta}(t)f(x), \qquad t \in \mathbb{Q}_p^\times, \quad x \in \mathbb{Q}_p^\times. \tag{8.1}$$

Однородные обобщенные функции относительно главного квазихарактера

$$\pi_{\alpha,1}(x) = |x|_p^{\alpha-1}$$

называются однородными *степени однородности* $\alpha - 1$.

Квазихарактер $\pi_{\alpha,\theta}(x)$ определяет однородную относительно себя обобщенную функцию $\pi_{\alpha,\theta}$ по формуле

$$(\pi_{\alpha,\theta},\varphi)=\int|x|_p^{\alpha-1}\theta(x)\varphi(x)\,d_px,\qquad\varphi\in\mathscr{S}. \tag{8.2}$$

Обобщенная функция $\pi_{\alpha,\theta}$ при $\theta\neq 1$ – целая по α; при $\theta=1$ она голоморфна по α всюду за исключением простых полюсов

$$\alpha_k=\frac{2k\pi i}{\ln p},\qquad k\in Z,$$

с вычетом $\big((1-p^{-1})/\ln p\big)\,\delta(x)$.

Отметим, что обобщенная функция $|x|_p^{\alpha-1}$, заданная в области $\operatorname{Re}\alpha>0$ формулой (8.2), аналитически продолжается из этой области в область $\operatorname{Re}\alpha\leqslant 0,\ \alpha\neq\alpha_k,\ k\in Z$ по формуле

$$\begin{aligned}\big(|x|_p^{\alpha-1},\varphi\big)&=\big(1-p^{-\alpha}\big)^{-1}\int|x|_p^{\alpha-1}\left[\varphi(x)-\varphi\left(\frac{x}{p}\right)\right]d_px\\&=\int|x|_p^{\alpha-1}[\varphi(x)-\varphi(0)]\,d_px,\qquad\varphi\in\mathscr{S},\end{aligned} \tag{8.3}$$

поскольку

$$\int|x|_p^{\alpha-1}=0,\qquad\alpha\neq\alpha_k,\quad k\in Z. \tag{8.3$'$}$$

При $\alpha=\alpha_k,\ k\in Z$, квазихарактеру $\pi_{0,1}(x)=|x|_p^{-1}$ соответствует обобщенная функция $\delta(x)$ степени однородности -1; обратно, всякая однородная обобщенная функция $f\in\mathscr{S}'$ степени однородности -1 имеет вид $f(x)=C\delta(x)$, где C – некоторая постоянная.

Преобразование Фурье $\pi_{\alpha,\theta}$ есть однородная обобщенная функция $\widetilde{\pi}_{\alpha,\theta}$ относительно квазихарактера

$$\pi_{\alpha,\theta}^{-1}(\xi)|\xi|_p^{-1}=|\xi|_p^{-\alpha}\bar{\theta}(\xi)=\pi_{1-\alpha,\bar{\theta}}(\xi), \tag{8.4}$$

так что

$$\widetilde{\pi}_{\alpha,\theta}=\Gamma_p(\pi_{\alpha,\theta})\pi_{1-\alpha,\bar{\theta}}. \tag{8.5}$$

Здесь $\Gamma_p(\pi_{\alpha,\theta})$ – *гамма-функция* поля $\mathbb{Q}_p$, соответствующая квазихарактеру $\pi_{\alpha,\theta}(x)$,

$$\Gamma_p(\pi_{\alpha,\theta})=\widetilde{\pi}_{\alpha,\theta}(1)=\int|x|_p^{\alpha-1}\theta(x)\chi_p(x)\,d_px. \tag{8.6}$$

В частности, при $\theta = 1$, обозначая

$$\Gamma_p(\alpha) = \Gamma_p\big(|x|_p^{\alpha-1}\big),$$

для гамма-функции $\Gamma_p(\alpha)$ главного квазихарактера $|x|_p^{\alpha-1}$ получим представление

$$\Gamma_p(\alpha) = \int |x|_p^{\alpha-1}\chi_p(x)\,d_px = \frac{1-p^{\alpha-1}}{1-p^{-\alpha}}\,, \qquad \alpha \neq \alpha_k, \quad k \in Z. \tag{8.7}$$

Для $\epsilon \notin \mathbb{Q}_p^{\times 2}$, $|\epsilon|_p = 1$, $p \neq 2$

$$\theta(x) = \operatorname{sgn}_\epsilon x = |x|_p^{\pi i/\ln p} = (-1)^{\gamma(x)},$$

и обозначим

$$\widetilde{\Gamma}_p(\alpha) = \Gamma_p(|x|_p^{\alpha-1}\operatorname{sgn}_\epsilon x).$$

Для $\widetilde{\Gamma}_p$-функции из (8.7) следует выражение

$$\widetilde{\Gamma}_p(\alpha) = \Gamma_p\left(\alpha + \frac{\pi i}{\ln p}\right) = \frac{1+p^{\alpha-1}}{1+p^{-\alpha}}\,, \qquad \alpha \neq \alpha_k + \frac{\pi i}{\ln p}\,, \quad k \in Z. \tag{8.8}$$

Отметим, в частности, формулы для гамма-функций при $d = -1$ (ср. § 3),

$$\Gamma_p\big(\operatorname{sgn}_{p,-1}x|x|_p^{\alpha-1}\big) = \begin{cases} \Gamma_p(\alpha) = \dfrac{1-p^{\alpha-1}}{1-p^{-\alpha}}\,, & p \equiv 1 \pmod 4, \\ \widetilde{\Gamma}_p(\alpha) = \dfrac{1+p^{\alpha-1}}{1+p^{-\alpha}}\,, & p \equiv 3 \pmod 4, \\ 2i4^{\alpha-1}, & p = 2. \end{cases}$$

Справедливо равенство

$$\Gamma_p(\pi_{\alpha,\theta})\,\Gamma_p(\pi_{1-\alpha,\bar\theta}) = \theta(-1). \tag{8.9}$$

В частности,

$$\Gamma_p(\alpha)\,\Gamma_p(1-\alpha) = 1. \tag{8.10}$$

Свертка однородных обобщенных функций $\pi_{\alpha,\theta}$ и $\pi_{\beta,\theta'}$ существует и является однородной обобщенной функцией относительно квазихарактера

$$\pi_{\alpha,\theta}(x)\pi_{\beta,\theta'}(x)|x|_p^{-1} = \pi_{\alpha+\beta,\theta\theta'}(x)$$

и стало быть

$$\pi_{\alpha,\theta} * \pi_{\beta,\theta'} = B_p(\pi_{\alpha,\theta}, \pi_{\beta,\theta'})\pi_{\alpha+\beta,\theta\theta'}. \tag{8.11}$$

Здесь $B_p\big(\pi_{\alpha,\theta}, \pi_{\beta,\theta'}\big)$ – *бета-функция* поля $\mathbb{Q}_p$, соответствующая квазихарактерам $\pi_{\alpha,\theta}$ и $\pi_{\beta,\theta'}$,

$$\begin{aligned} B_p\big(\pi_{\alpha,\theta}, \pi_{\beta,\theta'}\big) &= \big(\pi_{\alpha,\theta} * \pi_{\beta,\theta'}\big)(1) = \frac{\Gamma_p(\pi_{\alpha,\theta})\,\Gamma_p(\pi_{\beta,\theta'})}{\Gamma_p(\pi_{\alpha+\beta,\theta\theta'})} \\ &= \Gamma_p\big(\pi_{\alpha,\theta}\big)\,\Gamma_p(\pi_{\beta,\theta'})\,\Gamma_p\big(\pi_{\gamma,\theta''}\big)\theta''(-1), \\ &\qquad \alpha+\beta+\gamma = 1, \quad \theta\theta'\theta'' = 1. \end{aligned} \tag{8.12}$$

В частности, для главных квазихарактеров (при $\theta = \theta' = 1$) формула (8.12) превращается в такую

$$B_p(\alpha,\beta) = \Gamma_p(\alpha)\,\Gamma_p(\beta)\,\Gamma_p(\gamma), \qquad \alpha+\beta+\gamma = 1, \tag{8.13}$$

где обозначено

$$B_p(\alpha,\beta) = B_p\big(|x|_p^{\alpha-1}, |x|_p^{\beta-1}\big).$$

Отметим другое симметричное выражение для бета-функции $B_p(\alpha,\beta)$ [27]:

$$\begin{aligned} B_p(\alpha,\beta) = (1-p^{-1})\big[&(1-p^{-\alpha})^{-1} + (1-p^{-\beta})^{-1} \\ &+ (1-p^{-\gamma})^{-1} - 1\big] - 1, \qquad \alpha+\beta+\gamma = 1. \end{aligned} \tag{8.14}$$

Если ввести аналоги гамма- и бета-функций Эйлера:

$$\gamma_p(\alpha) = \int_{Z_p} |x|_p^{\alpha-1}\chi_p(x)\,d_px = \frac{1-p^{-1}}{1-p^{-\alpha}}\,,$$

$$b_p(\alpha,\beta) = \int_{Z_p} |x|_p^{\alpha-1}|1-x|_p^{\beta-1}\,d_px = \gamma_p(\alpha) + \gamma_p(\beta) - 1,$$

то равенство (8.14) примет вид

$$\begin{gathered} B_p(\alpha,\beta) = \frac{1}{2}\,b_p(\alpha,\beta) + \frac{1}{2}\,b_p(\alpha,\gamma) + \frac{1}{2}\,b_p(\beta,\gamma) + \frac{1}{p} - \frac{1}{2}\,, \\ \alpha+\beta+\gamma = 1. \end{gathered} \tag{8.15}$$

Рангом $\rho(\theta)$ характера θ называется такое целое число $k \geqslant 0$, что $\theta(t) = 1$ при $|1-t|_p \leqslant p^{-k}$, $t \in Z_p$, и $\theta(t) \neq 1$ при $|1-t|_p = p^{1-k}$,

$t \in Z_p$. Ясно, что нулевой ранг имеет только главный характер $\theta(x) \equiv 1$.

Для характеров ранга $k \geqslant 1$ справедливы формулы [11]:

$$\Gamma_p(\pi_{\alpha,\theta}) = p^{\alpha k} a_{p,k}(\theta), \tag{8.16}$$

$$a_{p,\gamma}(\theta) = \int_{S_0} \theta(t)\chi_p(p^{-\gamma}t)\, d_p t, \qquad \gamma \geqslant 1, \tag{8.17}$$

$$a_{p,\gamma}(\theta) = 0, \quad \gamma \neq k, \quad |a_{p,k}(\theta)| = p^{-k/2}, \tag{8.18}$$

$$a_{p,k}(\theta)\, a_{p,k}(\bar{\theta}) = p^{-k}\theta(-1), \tag{8.19}$$

$$\int_{S_k} \theta(p^k x)\chi_p(\xi x)\, d_p x = p^k a_{p,k}(\theta)\, \bar{\theta}(\xi)\, \delta(|\xi|_p - 1), \tag{8.20}$$

$$\Gamma_p(\pi_{\alpha,\theta})\, \Gamma_p(\pi_{\alpha,\theta}^{-1}) = p^k\theta(-1), \tag{8.21}$$

$$\Gamma_p(\pi_{\alpha+1,\theta}) = p^k \Gamma_p(\pi_{\alpha,\theta}). \tag{8.22}$$

Примеры. Ранг характера

$$\operatorname*{sgn}_{p,d} x, \qquad |d|_p = \frac{1}{p}\,, \quad p \neq 2, \tag{8.23}$$

равен 1. Поэтому в силу (8.16) и (8.19)

$$\Gamma_p(\pi_{\alpha,\theta}) = \pm p^{\alpha-1/2}\sqrt{\operatorname{sgn}_{p,d}(-1)}\,. \tag{8.24}$$

Например:

$$\begin{aligned}
\Gamma_3\big(|x|_3^{\alpha-1}\operatorname{sgn}_{3,3} x\big) &= -i3^{\alpha-1/2},\\
\Gamma_2\big(|x|_2^{\alpha-1}\operatorname{sgn}_{2,-1} x\big) &= 2i4^{\alpha-1},\\
\Gamma_2\big(|x|_2^{\alpha-1}\operatorname{sgn}_{2,7} x\big) &= 2i4^{\alpha-1},\\
\Gamma_2\big(|x|_2^{\alpha-1}\operatorname{sgn}_{2,3} x\big) &= 2i4^{\alpha-1}.
\end{aligned}$$

Оператор (8.2)

$$\varphi \to (\pi_{\alpha,\theta}, \varphi) \equiv M^{\pi}[\varphi]$$

называется *преобразованием Меллина функции* $\varphi \in \mathscr{S}$ *относительно квазихарактера* $\pi_{\alpha,\theta}(x)$. При $\theta = 1$ функция $M^{|x|_p^{\alpha-1}}[\varphi] \equiv$

$M^\alpha[\varphi]$ называется просто преобразованием Меллина функции $\varphi \in \mathscr{S}$. В силу (8.3) его можно записать в следующем виде

$$M^\alpha[\varphi] = (1-p^{-\alpha})^{-1} \int |x|_p^{\alpha-1} \left[\varphi(x) - \varphi\left(\frac{x}{p}\right)\right] d_p x,$$
$$\alpha \neq \alpha_k, \quad k \in Z.$$

В силу (8.2) и (8.5) имеет место следующее равенство

$$M^\pi[\widehat{\varphi}] = \Gamma_p(\pi_{\alpha,\theta}) M^{\widetilde{\pi}}[\varphi], \qquad \varphi \in \mathscr{S}. \tag{8.25}$$

При $\theta = 1$ формула (8.25) принимает вид

$$M^\alpha[\widehat{\varphi}] = \Gamma_p(\alpha) M^{1-\alpha}[\varphi]. \tag{8.25$'$}$$

Преобразование Меллина $Z_p^\times$-инвариантных (обобщенных) функций и его обращение. Функция $\varphi \in \mathscr{S}(\mathbb{Q}_p^\times)$ называется $Z_p^\times$-*инвариантной*, если $\varphi(x) = \varphi(t|x|_p)$, $t \in Z_p^\times$, $x \in \mathbb{Q}_p^\times$, или, другими словами,

$$\varphi(x) = (1-p^{-1})^{-1} \int_{Z_p^\times} \varphi(t|x|_p)\, d_p t \equiv S[\varphi](|x|_p).$$

Всякая $Z_p^\times$-инвариантная функция $\varphi \in \mathscr{S}(\mathbb{Q}_p^\times)$ однозначно представляется в виде

$$\varphi(x) = \sum_\gamma \varphi_\gamma \delta(|x|_p - p^\gamma), \qquad \varphi_\gamma = \varphi(p^\gamma) = S[\varphi](p^\gamma).$$

Поэтому подпространство пространства $\mathscr{S}(\mathbb{Q}_p^\times)$, состоящее из $Z_p^\times$-инвариантных функций, изоморфно пространству финитных последовательностей $\{\varphi_\gamma,\, \gamma \in N\}$, где N – ограниченное подмножество Z.

Обобщенная функция $f \in \mathscr{S}(\mathbb{Q}_p^\times)$ называется $Z_p^\times$-*инвариантной*, если

$$(f, \varphi) = \big(f(x), S[\varphi](|x|_p)\big), \qquad \varphi \in \mathscr{S}(\mathbb{Q}_p^\times).$$

Всякая $Z_p^\times$-инвариантная обобщенная функция $\varphi \in \mathscr{S}'(\mathbb{Q}_p^\times)$ однозначно представляется в виде

$$f(x) = \sum_\gamma f_\gamma \delta\big(|x|_p - p^\gamma\big), \quad f_\gamma = \big(1-p^{-1}\big)^{-1} p^{-\gamma} \big(f(x), \delta(|x|_p - p^\gamma)\big),$$

так что подпространство пространства $\mathscr{S}'(\mathbb{Q}_p^\times)$, состоящее из $Z_p^\times$-инвариантных обобщенных функций, изоморфно пространству последовательностей $\{f_\gamma, \gamma \in Z\}$.

Если $\varphi \in \mathscr{S}(\mathbb{Q}_p^\times)$ есть $Z_p^\times$-инвариантная функция, то ее преобразование Меллина

$$M^\alpha[\varphi] = \int |x|^{\alpha-1} S[\varphi](|x|_p)\, d_p x = (1-p^{-1}) \sum_{\gamma \in M} \varphi_\gamma p^{\alpha\gamma}$$

есть целая функция α и справедлива формула обращения [30]

$$\varphi(x) = \frac{\ln p}{2\pi i (1-p^{-1})} \int_{\sigma - i\pi/\ln p}^{\sigma + i\pi/\ln p} M^\alpha[\varphi] |x|_p^{-\alpha}\, d\alpha. \tag{8.26}$$

Формула (8.26) распространяется и на $Z_p^\times$-инвариантные обобщенные функции f из $\mathscr{S}'(\mathbb{Q}_p^\times)$, удовлетворяющие условию

$$\sum_{\gamma \in Z} |f_\gamma| p^{c\gamma} < \infty$$

при некотором c. Ее преобразование Меллина

$$M^\alpha[f] = \big(f(x), |x|_p^{\alpha-1}\big) = \big(1-p^{-1}\big) \sum_{\gamma \in Z} f_\gamma p^{\gamma\alpha}$$

есть голоморфная функция α в полуплоскости $\operatorname{Re}\alpha < c$ и справедлива формула обращения (8.26) для f, причем интеграл (8.26) не зависит от $\sigma < c$.

Пространство $\mathbb{Q}_p^n$. Ограничимся случаем главного квазихарактера $|x|_p^\alpha$. Обобщенная функция $|x|_p^{\alpha-n}$ – однородная степени однородности $\alpha - n$, голоморфна по α всюду за исключением простых полюсов $\alpha_k = 2k\pi i/\ln p$, $k \in Z$, с вычетом $\big((1-p^{-n})/(\ln p)\big)\, \delta(x)$; справедлива формула преобразования Фурье [17], [18]

$$\widetilde{|x|_p^{\alpha-n}} = \Gamma_p^{(n)}(\alpha) |\xi|_p^{-\alpha}, \qquad \alpha \neq \alpha_k, \quad k \in Z, \tag{8.27}$$

где $\Gamma_p^{(n)}$ – гамма-функция векторного пространства $\mathbb{Q}_p^n$ ($\Gamma_p^{(1)} = \Gamma_p$),

$$\Gamma_p^{(n)}(\alpha) = \int |x|_p^{\alpha-n} \chi_p(x_1)\, d_p^n x = \frac{1-p^{\alpha-n}}{1-p^{-\alpha}}, \quad \alpha \neq \alpha_k, \quad k \in Z, \tag{8.28}$$

$$\Gamma_p^{(n)}(\alpha)\, \Gamma_p^{(n)}(n-\alpha) = 1, \tag{8.29}$$

$$\Gamma_p^{(n)}(\alpha) = (-1)^{n-1} p^{(n-1)(n/2-\alpha)} \prod_{k=1}^{n-1} \Gamma_p(\alpha - k). \tag{8.30}$$

Бета-функция $B_p^{(n)}$ пространства $\mathbb{Q}_p^n$ определяется аналогично (8.11) ($B_p^{(1)} = B_p$) равенством

$$|x|_p^{\alpha-n} * |x|_p^{\beta-n} = B_p^{(n)}(\alpha,\beta)|x|_p^{\alpha+\beta-n}, \tag{8.31}$$

$$B_p^{(n)}(\alpha,\beta) = \Gamma_p^{(n)}(\alpha)\, \Gamma_p^{(n)}(\beta)\, \Gamma_p^{(n)}(\gamma), \qquad \alpha+\beta+\gamma = n. \tag{8.32}$$

Адельные формулы для гамма- и бета-функций. Для гамма-функций справедлива следующая адельная формула [1], [7]

$$\Gamma_\infty(\alpha) \operatorname{reg} \prod_{p=2}^{\infty} \Gamma_p(\alpha) = 1, \qquad \alpha \neq 0, 1, \tag{8.33}$$

где Γ_∞ – гамма-функция поля $\mathbb{R}$,

$$\begin{aligned} \Gamma_\infty(\alpha) &= \int |x|_p^{\alpha-1} \exp(-2\pi i x)\, dx \\ &= 2(2\pi)^{-\alpha} \cos\frac{\pi\alpha}{2}\, \Gamma(\alpha) = \frac{\zeta(1-\alpha)}{\zeta(\alpha)}, \end{aligned} \tag{8.34}$$

где Γ – гамма-функция Эйлера и ζ – дзета-функция Римана,

$$\zeta(\alpha) = \sum_{n=1}^{\infty} n^{-\alpha} = \prod_{p=2}^{\infty} (1-p^{-\alpha})^{-1}. \tag{8.34$'$}$$

Регуляризация расходящегося бесконечного произведения в (8.33) определяется с помощью формулы

$$\prod_{p=2}^{P} \Gamma_p(\alpha)\, \mathrm{AC} \prod_{p=P_1}^{\infty} \frac{1}{(1-p^{-\alpha})} = \frac{\zeta(\alpha)}{\zeta(1-\alpha)}\, \mathrm{AC} \prod_{p=P_1}^{\infty} \frac{1}{(1-p^{\alpha-1})}, \qquad P = \infty, 2, 3, 5, \ldots, \tag{8.35}$$

вытекающей из общей формулы Тейта. Здесь P_1 – простое число, следующее за простым числом P; $\operatorname{AC} f(\alpha)$ – аналитическое продолжение по α функции $f(\alpha)$, голоморфной в некоторой области комплексной плоскости переменной α.

Переходя в (8.35) к пределу при $P \to \infty$ в полуплоскости $\operatorname{Re}\alpha < 0$, обозначая

$$\operatorname{reg}\prod_{p=2}^{\infty}\Gamma_p(\alpha) = \lim_{P\to\infty}\prod_{p=2}^{P}\Gamma_p(\alpha)\operatorname{AC}\prod_{p=P_1}^{\infty}\frac{1}{(1-p^{-\alpha})}$$

и пользуясь равенством (8.34), получим адельную формулу (8.33). При $\operatorname{Re}\alpha \leqslant 0$ $\operatorname{reg}\prod\Gamma_p(\alpha)$ определяется из формулы (8.33) как аналитическое (мероморфное) продолжение по α.

Аналогичная адельная формула справедлива и для бета-функций:

$$B_\infty(\alpha,\beta)\operatorname{reg}\prod_{p=2}^{\infty}B_p(\alpha,\beta) = 1, \tag{8.36}$$

где

$$B_\infty(\alpha,\beta) = \Gamma_\infty(\alpha)\,\Gamma_\infty(\beta)\,\Gamma_\infty(\gamma), \qquad \alpha+\beta+\gamma = 1, \tag{8.37}$$

– бета-функция поля $\mathbb{R}$ и, в соответствии с (8.13),

$$\operatorname{reg}\prod_{p=2}^{\infty}B_p(\alpha,\beta) = \prod_{x=\alpha,\beta,\gamma}\operatorname{reg}\prod_{p=2}^{\infty}\Gamma_p(x). \tag{8.38}$$

Отметим другие симметричные выражения для B_∞:

$$\begin{aligned} B_\infty(\alpha,\beta) &= B(\alpha,\beta)+B(\alpha,\gamma)+B(\beta,\gamma)\\ &= \frac{\Gamma(\alpha)\Gamma(\beta)}{\Gamma(\alpha+\beta)}+\frac{\Gamma(\alpha)\Gamma(\gamma)}{\Gamma(\alpha+\gamma)}+\frac{\Gamma(\beta)\Gamma(\gamma)}{\Gamma(\beta+\gamma)}\\ &= \frac{4}{\pi}\prod_{x=\alpha,\beta,\gamma}\Gamma(x)\cos\frac{\pi x}{2} = \prod_{x=\alpha,\beta,\gamma}\frac{\zeta(1-x)}{\zeta(x)}\,. \end{aligned} \tag{8.39}$$

Адельная формула для дзета-функции Римана $\zeta(\alpha)$ (см. (8.34′)). Функция $\zeta(\alpha)$ удовлетворяет функциональному соотношению

$$\pi^{-\alpha/2}\Gamma\left(\frac{\alpha}{2}\right)\zeta(\alpha) = \pi^{-(\alpha-1)/2}\Gamma\left(\frac{1-\alpha}{2}\right)\zeta(1-\alpha). \tag{8.40}$$

Обозначим:

$$\zeta_\infty(\alpha) = \int e^{-\pi x^2} |x|^{\alpha-1}\, dx = \pi^{-\alpha/2}\Gamma\left(\frac{\alpha}{2}\right), \tag{8.41}$$

$$\zeta_p(\alpha) = \frac{1}{1-p^{-1}} \int_{Z_p} |x|_p^{\alpha-1}\, d_p x = \frac{1}{1-p^{-\alpha}}\,, \tag{8.42}$$

$$\zeta_A(\alpha) = \zeta_\infty(\alpha)\zeta(\alpha). \tag{8.43}$$

Тогда будут справедливы следующие формулы:

$$\zeta_A(\alpha) = \zeta_A(1-\alpha), \qquad \text{(ср. (8.40))}, \tag{8.44}$$

$$\Gamma_\infty(\alpha) = \frac{\zeta_\infty(\alpha)}{\zeta_\infty(1-\alpha)} = \frac{\zeta(1-\alpha)}{\zeta(\alpha)}\,, \quad \text{(ср. (8.34))}, \tag{8.45}$$

$$\zeta_\infty(\alpha) \prod_{p=2}^{\infty} \zeta_p(\alpha) = \zeta_A(\alpha), \qquad \text{(ср. (8.43))}. \tag{8.46}$$

Формула (8.46) по существу есть адельная формула для дзета-функции Римана.

§ 9. Квадратичные расширения поля $\mathbb{Q}_p$

Пусть p-адическое число $d \notin \mathbb{Q}_p^{\times 2}$. *Квадратичным расширением* поля $\mathbb{Q}_p$ является поле $\mathbb{Q}_p(\sqrt{d}\,) = \mathbb{Q}_p + \sqrt{d}\,\mathbb{Q}_p$. Опишем все неизоморфные поля $\mathbb{Q}_p(\sqrt{d}\,)$. В силу сказанного в § 1, достаточно рассмотреть целые рациональные числа d, свободные от квадратов, т. е. $d = \pm p_1 p_2 \cdots p_n,\ d \neq 1$, где $p_1, p_2, \ldots, p_n$ – различные простые числа.

Возможны следующие случаи:

$p \neq 2,\ p_1, \ldots, p_n,$ $\quad \left(\dfrac{d}{p}\right) = 1,$ $\quad \mathbb{Q}_p\big(\sqrt{d}\,\big) \sim \mathbb{Q}_p;$

$p \neq 2,\ p_1, \ldots, p_n,$ $\quad \left(\dfrac{d}{p}\right) = -1,$ $\quad \mathbb{Q}_p(\sqrt{d}\,) \sim \mathbb{Q}_p(\sqrt{\epsilon}\,),$ $\epsilon \notin \mathbb{Q}_p^{\times 2},\quad |\epsilon|_p = 1;$

$p \neq 2,\ p = p_i,$ $\quad \left(\dfrac{d/p_i}{p}\right) = 1,$ $\quad \mathbb{Q}_p(\sqrt{d}\,) \sim \mathbb{Q}_p(\sqrt{p}\,);$

$p \neq 2,\ p = p_i,$ $\quad \left(\dfrac{d/p_i}{p}\right) = -1,$ $\quad \mathbb{Q}_p(\sqrt{d}\,) \sim \mathbb{Q}_p(\sqrt{p\epsilon}\,),$ $\epsilon \notin \mathbb{Q}_p^{\times 2},\quad |\epsilon|_p = 1;$

$p=2,\qquad d\equiv 3,5,7 \pmod 8,\qquad \mathbb{Q}_2(\sqrt{d}\,)\sim\mathbb{Q}_2(\sqrt{\epsilon}\,),\quad \epsilon=3,5,7$ соотв.;

$p=2,\qquad d/2\equiv 1,3,5,7 \pmod 8,\qquad \mathbb{Q}_2(\sqrt{d}\,)\sim\mathbb{Q}_2(\sqrt{2\epsilon}\,),\quad \epsilon=1,3,5,7$ соотв.

Отметим, что $\mathbb{Q}_p(\sqrt{d}\,)$ есть замыкание поля $\mathbb{Q}(\sqrt{d}\,)=\mathbb{Q}+\sqrt{d}\,\mathbb{Q}$ по метрике $\sqrt{|z\bar z|_p}$, где $z=x+\sqrt{d}\,y,\ \bar z=x-\sqrt{d}\,y,\ z\bar z=x^2-dy^2$, $x,y\in\mathbb{Q}$.

Меру Хаара d_pz поля $\mathbb{Q}_p(\sqrt{d}\,)$ выберем в виде

$$d_pz=\frac{1}{\delta}\,d_px\,d_py,\qquad z=x+\sqrt{d}\,y,\qquad x,y\in\mathbb{Q}_p, \tag{9.1}$$

где $\delta=\delta_{p,d}=2$, если $p=2,\ d\equiv 5 \pmod 8$ и $\delta=1$ в остальных случаях. Мера d_pz нормирована условием (см. [6])

$$\int_{B_0^2} d_pz=1,\qquad B_0^2=[z\in\mathbb{Q}_p(\sqrt{d}\,):|z\bar z|_p\leqslant 1]. \tag{9.2}$$

Имеет место равенство

$$d_p(az)=|a\bar a|_p\,d_pz,\qquad a\in\mathbb{Q}_p^\times(\sqrt{d}\,). \tag{9.3}$$

Величина $|a\bar a|_p$ называется *модулем автоморфизма* $z\to az$ поля $\mathbb{Q}_p(\sqrt{d}\,)$.

Максимальное компактное подкольцо $Z_p(\sqrt{d}\,)$ поля $\mathbb{Q}_p(\sqrt{d}\,)$ есть

$$Z_p(\sqrt{d}\,)=[z\in\mathbb{Q}_p(\sqrt{d}\,):|z\bar z|_p\leqslant 1],\qquad Z_p(\sqrt{d}\,)=B_0^2;$$

его мультипликативная подгруппа есть

$$Z_p^\times(\sqrt{d}\,)=[z\in\mathbb{Q}_p(\sqrt{d}\,):|z\bar z|_p=1];$$

его максимальный идеал есть

$$I_p(\sqrt{d}\,)=[z\in\mathbb{Q}_p(\sqrt{d}\,):|z\bar z|_p<1].$$

Классы вычетов $Z_p(\sqrt{d}\,)/I_p(\sqrt{d}\,)$ образуют конечное поле характеристики p, называемое *полем вычетов*; число его элементов $q=q_{p,d}$ (равное p или p^2) называется *модулем поля* $\mathbb{Q}_p(\sqrt{d}\,)$. Для

конкретных случаев имеем: при $p = 2$, $d \equiv 5 \pmod 8$, $q = 4$, поле вычетов $\{0, 1, 1/2 \pm \sqrt{5}/2\}$; при $d \not\equiv 5 \pmod 8$, $q = 2$ поле вычетов $\{0, 1\}$; при $p \neq 2$, $|d|_p = 1$, $q = p^2$ поля вычетов $\{k + \sqrt{d}j,\ k, j = 0, 1, \dots, p-1\}$; при $|d|_p = 1/p$, $q = p$ поле вычетов $\{0, 1, \dots, p-1\}$.

Ранг аддитивного характера $\chi_p(z + \bar{z})$ есть наибольшее целое число $r \geqslant 0$, для которого

$$\chi_p(z + \bar{z}) \equiv 1, \qquad |z\bar{z}|_p \leqslant q^r \qquad \Big(q^{-r/2} = \delta\sqrt{|4d|_p}\Big). \tag{9.4}$$

В частности,

$$\begin{cases} r = 0, & |d|_p = 1, \quad p \neq 2 \text{ или } d \equiv 5 \pmod 8,\ p = 2; \\ r = 1, & |d|_p = \dfrac{1}{p}, \quad p \neq 2; \\ r = 2, & d \equiv 3, 7 \pmod 8, \quad p = 2; \\ r = 3, & |d|_2 = \dfrac{1}{2}, \quad p = 2. \end{cases}$$

Преобразование Фурье $\widetilde{\varphi}(\zeta)$, $\zeta = \xi + \sqrt{d}\,\eta$, основной функции $\varphi(z) \equiv \varphi(x, y)$ из $\mathscr{S}(\mathbb{Q}_p(\sqrt{d}\,)) \sim \mathscr{S}(\mathbb{Q}_p^2)$ определим формулой

$$\begin{aligned} \widetilde{\varphi}(\zeta) &= \delta\sqrt{|4d|_p} \int \varphi(z)\chi_p(z\zeta + \bar{z}\bar{\zeta}\,)\, d_p z \\ &= \sqrt{|4d|_p} \int \varphi(x, y)\chi_p(2x\xi + 2dy\eta)\, d_p x\, d_p y. \end{aligned}$$

Обратное преобразование Фурье выражается равенством

$$\varphi(z) = \delta\sqrt{|4d|_p} \int \widetilde{\varphi}(\zeta)\xi_p(-z\zeta - \bar{z}\bar{\zeta}\,)\, d_p\zeta.$$

Таким образом, мера $\delta\sqrt{|4d|_p}\, d_p z$ самодвойственна относительно характера $\chi_p(z + \bar{z})$.

Обобщенная функция

$$|z\bar{z}|_p^{\alpha-1} = |x^2 - dy^2|_p^{\alpha-1}$$

определяется равенством (см. § 8)

$$\begin{aligned} \big(|z\bar{z}|_p^{\alpha-1}, \varphi\big) = &\int_{|z\bar{z}|_p \leqslant 1} |z\bar{z}|_p^{\alpha-1}[\varphi(z) - \varphi(0)]\, d_p z + \int_{|z\bar{z}|_p > 1} |z\bar{z}|_p^{\alpha-1}\, d_p z \\ &+ \varphi(0)\frac{1 - q^{-1}}{1 - q^{-\alpha}}, \qquad \varphi \in \mathscr{S}\big(\mathbb{Q}_p(\sqrt{d}\,)\big), \end{aligned}$$

или эквивалентно,

$$\big(|z\bar z|_p^{\alpha-1},\varphi\big)=\int|z\bar z|_p^{\alpha-1}[\varphi(z)-\varphi(0)]\,d_pz,\qquad \varphi\in\mathscr{S}\big(\mathbb{Q}_p(\sqrt{d}\,)\big).$$

Здесь мы использовали формулы:

$$\int_{B_0^2}|z\bar z|_p^{\alpha-1}\,d_pz=\frac{1-q^{-1}}{1-q^{-\alpha}}\,,\qquad \alpha\neq\alpha_k,\quad k\in Z,\tag{9.5}$$

$$\int|z\bar z|_p^{\alpha-1}\,d_pz=0,\qquad \alpha\neq\alpha_k,\quad k\in Z,\tag{9.6}$$

где

$$\alpha_k=\frac{2k\pi i}{\ln q}\,,\qquad k\in Z.\tag{9.7}$$

Обобщенная функция $|z\bar z|_p^{\alpha-1}$ (степени однородности $2\alpha-2$) голоморфна по α всюду за исключением простых полюсов $\alpha=\alpha_k$, $k\in Z$ (см. (9.6)), с вычетом $\big((q-1)/(q\ln q)\big)\delta(x,y)$.

Справедлива формула преобразования Фурье [6]

$$F\big[|z\bar z|_p^{\alpha-1}\big]=\Gamma_{p,d}(\alpha)|\zeta\bar\zeta|_p^{-\alpha},\qquad \alpha\neq\alpha_k,\quad k\in Z,\tag{9.8}$$

где

$$\Gamma_{p,d}(\alpha)=\delta\sqrt{|4d|_p}\int|z\bar z|_p^{\alpha-1}\xi_p(z+\bar z)\,d_pz=\rho_{p,d}(\alpha)\,\Gamma_q(\alpha)\tag{9.9}$$

– гамма-функция поля $\mathbb{Q}_p(\sqrt{d}\,)$,

$$\Gamma_q(\alpha)=\frac{1-q^{\alpha-1}}{1-q^{-\alpha}}\tag{9.10}$$

– *приведенная гамма-функция* поля $\mathbb{Q}_p(\sqrt{d}\,)$.

Из (9.8)–(9.10) вытекает следующее соотношение для гамма-функции поля $\mathbb{Q}_p(\sqrt{d}\,)$:

$$\Gamma_{p,d}(\alpha)\,\Gamma_{p,d}(1-\alpha)=1.\tag{9.11}$$

Бета-функция поля $\mathbb{Q}_p(\sqrt{d}\,)$ вводится аналогично § 8. Свертка $|z\bar z|_p^{\alpha-1}*|z\bar z|_p^{\beta-1}$ существует для всех комплексных (α,β) из трубчатой области $\operatorname{Re}\alpha>0$, $\operatorname{Re}\beta>0$, $\operatorname{Re}(\alpha+\beta)<1$ и выражается интегралом

$$\begin{aligned}|z\bar z|_p^{\alpha-1}*|z\bar z|_p^{\beta-1}&=\int|\zeta\bar\zeta|_p^{\alpha-1}|(z-\zeta)(\bar z-\bar\zeta)|_p^{\beta-1}\,d_p\zeta\\&=B_{p,d}(\alpha,\beta)|z\bar z|_p^{\alpha+\beta-1},\end{aligned}\tag{9.12}$$

где $B_{p,d}$ – бета-функция поля $\mathbb{Q}_p(\sqrt{d}\,)$ [11]:

$$B_{p,d}(\alpha,\beta) = \int |\zeta\bar{\zeta}|_p^{\alpha-1}|(1-\zeta)(1-\bar{\zeta})|_p^{\beta-1}\,d_p\zeta$$
$$= \frac{\Gamma_{p,d}(\alpha)\,\Gamma_{p,d}(\beta)}{\delta\sqrt{|4d|_p}\,\Gamma_{p,d}(\alpha+\beta)}\,. \tag{9.13}$$

Из равенств (9.9)–(9.13) следуют такие симметричные выражения для бета-функции:

$$B_{p,d}(\alpha,\beta) = \frac{1}{\delta\sqrt{|4d|_p}}\,\Gamma_{p,d}(\alpha)\,\Gamma_{p,d}(\beta)\,\Gamma_{p,d}(\gamma)$$
$$= B_q(\alpha,\beta) = \Gamma_q\,(\alpha)\,\Gamma_q(\beta)\,\Gamma_q(\gamma), \tag{9.14}$$
$$\alpha+\beta+\gamma = 1, \quad (\alpha,\beta) \neq (\alpha_k,\alpha_j), \quad (k,j) \in Z^2.$$

Отметим, что равенства (9.12)–(9.14) справедливы при всех (α,β) таких, что $(\alpha,\beta) \neq (\alpha_k,\alpha_j)$, $(k,j) \in Z^2$.

Назовем *верхней* (*нижней*) *полуплоскостью* поля $\mathbb{Q}_p(\sqrt{d}\,)$ совокупность точек $z = x+\sqrt{d}\,y$, для которых $\operatorname{sgn}_{p,d} y = 1$ (соответственно $\operatorname{sgn}_{p,d} y = -1$).

Введем обобщенные функции $(x \pm \sqrt{d}\,0)^{-1}$ как преобразование Фурье функций

$$\theta_d^{\pm}(\xi) = \frac{1}{2}\,(1 \pm \operatorname{sgn}_{p,d}\xi), \qquad \big(x \pm \sqrt{d}\,0\big)^{-1} = \widetilde{\theta}_d^{\pm}(x). \tag{9.15}$$

Справедливы равенства [11]

$$F\big[\theta_d^{\pm}\big](x) = \big(x \pm \sqrt{d}\,0\big)^{-1} = \frac{1}{2}\,\delta(x) + C_{p,d}\,\frac{\operatorname{sgn}_{p,d} x}{|x|_p}\,, \qquad p \neq 2, \tag{9.16}$$

аналогичные формулам Сохоцкого (для поля $\mathbb{R}$). Здесь обобщенная функция $(\operatorname{sgn}_{p,d} x)/|x|_p$ и число $C_{p,d}$ определяются равенствами

$$\left(\frac{\operatorname{sgn}_{p,d} x}{|x|_p}\,,\varphi\right) = \int \frac{\operatorname{sgn}_{p,d} x}{|x|_p}\,\varphi(x)\,d_p x, \qquad \varphi \in \mathscr{S}, \tag{9.17}$$

$$C_{p,d} = \begin{cases} \sqrt{\dfrac{p}{p+1}}\,, & \text{если } |d|_p = 1, \\ \pm\dfrac{1}{2}\sqrt{p\,\operatorname{sgn}_{p,d}(-1)}\,, & \text{если } |d|_p = \dfrac{1}{p}\,. \end{cases}$$

Для Γ_q-функций справедливы следующие адельные формулы [6]

$$\Gamma_\infty^2(\alpha)\operatorname{reg}\prod_{p=2}^{\infty}\Gamma_q^\nu(\alpha)=D^{1/2-\alpha},\qquad d>0, \tag{9.18}$$

$$\Gamma_\omega(\alpha)\operatorname{reg}\prod_{p=2}^{\infty}\Gamma_q^\nu(\alpha)=|D|^{1/2-\alpha},\qquad d<0, \tag{9.18$'$}$$

где Γ_∞ и Γ_ω – гамма-функции полей $\mathbb{R}$ и $\mathbb{C}$ соответственно;

$$\begin{aligned}\Gamma_\omega(\alpha)&=2\int|z\bar z|^{\alpha-1}\exp(-4\pi ix)\,dx\,dy=(2\pi)^{1-2\alpha}\frac{\Gamma(\alpha)}{\Gamma(1-\alpha)}\\&=2(2\pi)^{-2\alpha}\Gamma^2(\alpha)\sin\pi\alpha=i\Gamma_\infty(\alpha)\,\widetilde\Gamma(\alpha),\end{aligned}$$

где

$$\widetilde\Gamma(\alpha)=\int\operatorname{sgn}x|x|^{\alpha-1}\exp(-2\pi ix)\,dx=-2i(2\pi)^{-\alpha}\Gamma(\alpha)\sin\frac{\pi\alpha}{2};$$

$\nu=2$, если $d\in\mathbb{Q}_p^{\times2}$ и $\nu=1$, если $d\notin\mathbb{Q}_p^{\times2}$; D – дискриминант поля $Q(\sqrt d\,)$, равный d, если $d\equiv1\pmod4$ и равный $4d$, если $d\equiv2,3\pmod4$. (Мера Хаара поля $\mathbb{C}$ выбрана самодвойственной: $|dz\wedge d\bar z|=2\,dx\,dy$, $z=x+iy$.)

Регуляризация расходящегося бесконечного произведения в (9.18) определяется с помощью формулы (ср. (8.35))

$$\prod_{p=2}^{P}\Gamma_q^\nu(\alpha)\,\mathrm{AC}\prod_{p=P_1}^{\infty}(1-q^{-\alpha})^{-\nu}=\frac{\zeta_d(\alpha)}{\zeta_d(1-\alpha)}\,\mathrm{AC}\prod_{p=P_1}^{\infty}(1-q^{-\alpha})^{-\nu},$$
$$P=\infty,2,3,5,\dots, \tag{9.19}$$

вытекающей из общей формулы Тейта. Здесь ζ_d – дзета-функция Дедекинда поля $\mathbb{Q}(\sqrt d\,)$,

$$\zeta_d(\alpha)=\prod_{p=2}^{\infty}(1-q^{-\alpha})^{-\nu}.$$

Дзета-функция Дедекинда удовлетворяет соотношению (ср. (8.40))

$$(2\pi)^{1-\alpha}\Gamma(\alpha)\zeta_d(\alpha)=(2\pi)^{\alpha}\Gamma(1-\alpha)\zeta_d(1-\alpha)|D|^{1/2-\alpha},$$

которое эквивалентно соотношению (ср. (8.46))

$$\zeta_{A_d}(\alpha) = \zeta_{A_d}(1-\alpha)|D|^{1/2-\alpha},$$

где обозначено

$$\zeta_{A_d}(\alpha) = (2\pi)^{1-\alpha}\Gamma(\alpha)\zeta_d(\alpha).$$

Переходя в (9.19) к пределу при $P \to \infty$, обозначая

$$\operatorname{reg}\prod_{p=2}^{\infty}\Gamma_q^{\nu}(\alpha) = \lim_{P\to\infty}\prod_{p=2}^{P}\Gamma_q^{\nu}(\alpha)\,\mathrm{AC}\prod_{p=P_1}^{\infty}(1-q^{-\alpha})^{-\nu}$$

и пользуясь равенствами

$$\Gamma_{\infty}^2(\alpha) = D^{1/2-\alpha}\frac{\zeta(1-\alpha)}{\zeta(\alpha)}, \qquad d>0, \tag{9.20}$$

$$\Gamma_{\omega}(\alpha) = |D|^{1/2-\alpha}\frac{\zeta(1-\alpha)}{\zeta(\alpha)}, \qquad d<0, \tag{9.20$'$}$$

в полуплоскости $\operatorname{Re}\alpha < 0$ получим адельные формулы (9.18). При остальных α $\operatorname{reg}\prod\Gamma_q^{-\nu}(\alpha)$ определяется из формул (9.18) как аналитическое (мероморфное) продолжение по α.

Аналогичные адельные формулы справедливы и для бета-функций

$$B_{\infty}^2(\alpha,\beta)\operatorname{reg}\prod_{p=2}^{\infty}B_q^{\nu}(\alpha,\beta) = \sqrt{D}\,, \qquad d>0, \tag{9.21}$$

$$B_{\omega}(\alpha,\beta)\operatorname{reg}\prod_{p=2}^{\infty}B_q^{\nu}(\alpha,\beta) = \sqrt{|D|}, \qquad d<0, \tag{9.21$'$}$$

где B_{∞} и B_{ω} – бета-функции полей $\mathbb{R}$ и $\mathbb{C}$ соответственно.

$$B_{\omega}(\alpha,\beta) = \Gamma_{\omega}(\alpha)\,\Gamma_{\omega}(\beta)\,\Gamma_{\omega}(\gamma), \qquad \alpha+\beta+\gamma = 1 \tag{9.22}$$

и в соответствии с формулой (9.14) (ср. (8.36))

$$\operatorname{reg}\prod_{p=2}^{\infty}B_q^{\nu}(\alpha,\beta) = \prod_{x=\alpha,\beta.\gamma}\operatorname{reg}\prod_{p=2}^{\infty}\Gamma_q^{\nu}(x).$$

Отметим другие симметричные выражения для $B_{-\omega}$:

$$B_{\omega}(\alpha,\beta) = 2\pi\prod_{x=\alpha,\beta,\gamma}\frac{\Gamma(x)}{\Gamma(1-x)} = \frac{2}{\pi^2}\prod_{x=\alpha,\beta,\gamma}\Gamma^2(x)\sin\pi x. \tag{9.23}$$

§ 10. Оператор D^α

Обобщенная функция

$$f_\alpha(x) = \frac{|x|_p^{\alpha-1}}{\Gamma_p(\alpha)}$$

голоморфна по α всюду за исключением простых полюсов $1+\alpha_k$, $\alpha_k = 2k\pi i/\ln p$, $k \in Z$, с вычетом $(1-p)/(p\ln p)\,\delta(x)$, причем $f_{\alpha_k} = \delta$ и

$$f_\alpha * f_\beta = f_{\alpha+\beta},$$
$$\alpha \neq 1+\alpha_k, \quad \beta \neq 1+\alpha_j, \quad \alpha+\beta \neq 1+\alpha_i, \quad (k,j,i) \in Z^3.$$

Пусть $\alpha \in \mathbb{R}$, $\alpha \neq -1$ и $f \in \mathscr{S}'$ таковы, что свертка $f_{-\alpha} * f$ существует в $\mathscr{S}'$. Оператор $D^\alpha f = f_{-\alpha} * f$ называется при $\alpha > 0$ оператором (дробного) *дифференцирования порядка* α, а при $\alpha < 0$ – оператором (дробного) *интегрирования порядка* $-\alpha$; при $\alpha = 0$ $D^0 f = \delta * f = f$ – тождественный оператор. Таким образом, оператор D^α – гиперсингулярный псевдодифференциальный (РДО) с символом $|\xi|_p$.

Пример. Если $\alpha = 1$ и $\varphi \in \mathscr{S}$, то

$$(D\varphi)(x) = \frac{p^2}{p+1}\int \frac{\varphi(x)-\varphi(y)}{|x-y|_p^2}\,d_p y = \int |\xi|_p \widetilde{\varphi}(\xi)\chi_p(-\xi x)\,d_p\xi. \tag{10.1}$$

Пусть $\alpha = 1$. Рассмотрим локально-интегрируемую в $\mathbb{Q}_p$ функцию

$$f_1(x) = -\frac{1-p^{-1}}{\ln p}\ln|x|_p. \tag{10.2}$$

Она обладает следующими свойствами:

$$\int f_\alpha(x)\varphi(x)\,d_p x \to \int f_1(x)\varphi(x)\,d_p x, \qquad \alpha \to 1, \tag{10.3}$$

если $\varphi \in \mathscr{S}$ удовлетворяет условию

$$\int \varphi(x)\,d_p x = 0; \tag{10.4}$$

$$\widetilde{f}_1(\xi) = \operatorname{reg}|\xi|_p^{-1} + \frac{1}{p}\,\delta(\xi), \tag{10.5}$$

где обобщенная функция $\operatorname{reg}|\xi|_p^{-1}$ определена в § 6;

$$f_1 * f_\alpha = f_{1-\alpha}, \qquad \alpha \geqslant 1. \tag{10.6}$$

Введем оператор интегрирования порядка 1, соответствующий значению $\alpha = -1$,

$$D^{-1} f = f_1 * f, \qquad f \in \mathscr{S}', \tag{10.7}$$

если свертка $f_1 * f$ существует. Тогда

$$D^{-\alpha} f \to D^{-1} f, \qquad \alpha \to 1 \quad \text{в} \ \mathscr{S}', \tag{10.8}$$

если $f \in \mathscr{E}'$ и

$$G\!\!\!\!\int f(x)\, d_p x = 0. \tag{10.9}$$

Резюмируя, получаем следующие свойства оператора D^α, $\alpha \in \mathbb{R}$:

$$D^\alpha D^\beta f = D^{\alpha+\beta} f = D^\beta D^\alpha f, \qquad f \in \mathscr{S}', \tag{10.10}$$

если $\alpha \neq -1,\ \beta \neq -1,\ \alpha+\beta \neq -1$, или $\alpha \leqslant 0,\ \beta = -1$, или $\alpha = -1$, $\beta \leqslant 0$; если f удовлетворяет условию (10.9), то равенства (10.10) справедливы при всех вещественных α и β, и $D^\alpha f$ непрерывно зависит от α в $\mathscr{S}'$.

Пример.

$$D^\alpha \chi_p(ax) = |a|_p^\alpha \chi_p(ax), \quad \alpha \in \mathbb{R}, \quad a \in \mathbb{Q}_p^\times. \tag{10.11}$$

Уравнение

$$D^\alpha \psi = g, \quad g \in \mathscr{E}', \tag{10.12}$$

разрешимо при всех $\alpha \in \mathbb{R}$, причем при $\alpha > 0$ его общее решение выражается формулой

$$\psi = D^{-\alpha} g + C, \tag{10.13}$$

где C – произвольная постоянная; при $\alpha \leqslant 0$ его решение единственно и выражается формулой (10.13) при $C = 0$.

Фундаментальное решение $\mathscr{E}(x)$ оператора D^α,

$$D^\alpha \mathscr{E}(x) = \delta(x), \quad \mathscr{E} \in \mathscr{S}', \tag{10.14}$$

вычислено в [3]. Оно равно

$$\mathscr{E}(x) = \begin{cases} \Gamma_p^{-1}(\alpha)|x|_p^{\alpha-1}, & \alpha \neq -1, \\ -\dfrac{1-p^{-1}}{\ln p}\,\ln|x|_p, & \alpha = -1. \end{cases} \tag{10.15}$$

Отметим, что фундаментальное решение существует в $\mathscr{S}'$ не для любого РДО. Например, для оператора $D_t^\alpha - D_x^\alpha$ оно не существует. Действительно, если бы решение $\mathscr{E}$ уравнения

$$(D_t^\alpha - D_x^\alpha)\,\mathscr{E}(t,x) = \delta(t,x)$$

существовало в $\mathscr{S}'$, то мы имели бы противоречивое равенство

$$(|\eta|_p^\alpha - |\xi|_p^\alpha)F[\mathscr{E}](\eta,\xi) = 1, \qquad (\eta,\xi) \in \mathbb{Q}_p^2,$$

в котором левая часть обращается в нуль в открытом множестве $|\eta|_p = |\xi|_p$ пространства $\mathbb{Q}_p^2$.

Оператор D^α при $\alpha > 0$ в открыто-замкнутом множестве G определен на тех $\psi \in \mathscr{L}^2(G)$ (см. § 4), для которых $|\xi|_p^\alpha \widetilde{\psi} \in \mathscr{L}^2$. Это множество функций называется *областью определения* оператора D^α в области G и обозначается $\mathscr{D}(D^\alpha, G)$; $\mathscr{D}(D^\alpha, \mathbb{Q}_p) = \mathscr{D}(D^\alpha)$. Справедливо равенство

$$(D^\alpha\psi, \varphi) = \int |\xi|_p^\alpha \widetilde{\psi}(\xi)\bar{\widetilde{\varphi}}(\xi)\,d_p\xi, \qquad \psi, \varphi \in \mathscr{D}(D^\alpha, G). \tag{10.16}$$

Оператор D^α в G – самосопряженный положительно-определенный, причем в силу (10.16) при всех $\psi \in \mathscr{D}(D^\alpha, G)$ имеем

$$(D^\alpha\psi, \psi) = (D^{\alpha/2}\psi, D^{\alpha/2}\psi) = \int |\xi|_p^\alpha |\psi(\xi)|^2\,d_p\xi \geqslant 0, \tag{10.17}$$

так что его спектр лежит на полуоси $\lambda \geqslant 0$.

Для оператора D^α, $\alpha > 0$, рассмотрим задачу на собственные значения

$$D^\alpha\psi = \lambda\psi, \qquad \psi \in \mathscr{D}(D^\alpha, G). \tag{10.18}$$

Теорема [1], [2]. *Спектр оператора D^α в $\mathbb{Q}_p$ состоит из счетного числа собственных значений $\lambda_N = p^{\alpha N}$, $N \in Z$, каждое из которых бесконечной кратности, и точки 0. Существует ортонормальный базис собственных функций в $\mathscr{L}^2(\mathbb{Q}_p)$ оператора D^α следующего вида*:

при $p \neq 2$

$$\psi^{\ell}_{N,j,\epsilon}(x) = p^{\frac{N+1-\ell}{2}}\delta(|x|_p - p^{\ell-N})\delta(x_0 - j)\chi_p(\epsilon_\ell p^{\ell-2N}x^2), \tag{10.19}$$
$$\ell = 2,3,\ldots, \quad j = 1,2,\ldots,p-1, \quad \epsilon_\ell = \varepsilon_0 + \varepsilon_1 p + \cdots + \varepsilon_{\ell-2}p^{\ell-2},$$
$$\varepsilon_s = 0,1,\ldots,p-1, \quad \varepsilon_0 \neq 0, \quad s = 0,1,\ldots,\ell-2;$$

$$\psi^{1}_{N,j,0}(x) = p^{\frac{N-1}{2}}\Omega(p^{N-1}|x|_p)\chi_p(jp^{-N}x), \tag{10.19$'$}$$
$$\ell = 1, \quad j = 1,2,\ldots,p-1, \quad \epsilon_\ell = 0;$$

при $p = 2$

$$\psi^{\ell}_{N,j,\epsilon_\ell}(x) = 2^{\frac{N-\ell}{2}}\delta(|x|_2 - 2^{\ell+1-N})\chi_2(\epsilon_\ell 2^{\ell-2N}x^2 + 2^{\ell-N+j}x), \tag{10.20}$$
$$\ell = 2,3,\ldots, \quad j = 0,1, \quad \epsilon_\ell = 1 + \varepsilon_1 2 + \cdots + \varepsilon_{\ell-2}2^{\ell-2},$$
$$\varepsilon_s = 0,1, \quad s = 1,2,\ldots,\ell-2;$$
$$\psi^{1}_{N,j,0}(x) = 2^{\frac{N-1}{2}}[\Omega(2^N|x - j2^{N-2}|_2) - \delta(|x - j2^{N-2}|_2 - 2^{1-N})], \tag{10.20$'$}$$
$$\ell = 1, \quad j = 0,1, \quad \epsilon_\ell = 0.$$

В [33] был найден новый, более простой, ортонормальный базис собственных функций оператора D^α, эквивалентный (10.19)–(10.20):

$$\psi_{Njn}(x) = p^{(N-1)/2}\chi_p(p-njx)\Omega(|p^{N-1}x - n|_p), \tag{10.21}$$
$$N \in Z, \quad j = 1,2,\ldots,p-1, \quad n \in \mathbb{Q}_p/Z_p,$$

соответствующих собственному значению $p^{\alpha N}$.

Теорема [4], [5]. *Если* G *– открыто-замкнутый компакт, то собственные значения* λ_k, $k = 0,1,\ldots$, *оператора* D^α, $\alpha > 0$, *в* G *– конечной кратности, а собственные функции* $\psi_k(x)$ *образуют ортонормальный базис в* $\mathscr{L}^2(G)$.

Пример. Собственные значения и ортонормальный базис собственных функций оператора D^α в B_γ, $\gamma \in Z$ [4].

При $p \neq 2$:

$$\lambda_0 = \frac{p-1}{p^{\alpha+1}-1}\, p^{\alpha(1-\gamma)}, \qquad \psi_0(x) = p^{-\gamma/2}, \qquad \text{кратность } 1;$$

$$\lambda_k = p^{\alpha(k-\gamma)}, \qquad \psi_k(x) = \psi^{\ell}_{k-\gamma,j,\epsilon_\ell}(x),$$

$$\ell = 1, 2, \ldots, k, \quad j = 1, 2, \ldots, p-1, \quad \epsilon_\ell,$$

$$\text{кратность } (p-1)p^{k-1}, \quad k = 1, 2, \ldots .$$

При $p = 2$:

$$\lambda_0 = \frac{2^{\alpha(1-\gamma)}}{2^{\alpha+1}-1}, \qquad \psi_0(x) = 2^{-\gamma/2}, \qquad \text{кратность } 1;$$

$$\lambda_1 = 2^{\alpha(1-\gamma)}, \qquad \psi_1(x) = \psi^1_{1-\gamma,0,0}(x), \qquad \text{кратность } 1;$$

$$\lambda_k = 2^{\alpha(k-\gamma)}, \quad \psi_k(x) = \psi^{\ell}_{k-\gamma,j,\epsilon_\ell}(x),$$

$$\ell = 1, 2, \ldots, k-1, \quad j = 0, 1,$$

$$\text{кратность } 2^{k-1}, \quad k = 2, 3, \ldots .$$

Пример. Собственные значения и нормированный базис собственных функций оператора D^α в S_γ, $\gamma \in Z$ [4].
При $p \neq 2$:

$$\lambda_0 = \frac{p^\alpha + p - 2}{p^{\alpha+1}-1}\, p^{\alpha(1-\gamma)}, \quad \psi_0(x) = p^{\frac{1-\gamma}{2}}\,(p-1)^{1/2}, \quad \text{кратность } 1;$$

$$\lambda_1 = p^{\alpha(1-\gamma)}, \qquad \psi_1(x) = 2^{-1/2}[\psi^1_{1-\gamma,j,0}(x) - \psi^1_{1-\gamma,j+1,0}(x)],$$

$$\text{кратность } p-2;$$

$$\lambda_k = p^{\alpha(k-\gamma)}, \qquad \psi_k(x) = \psi^k_{k-\gamma,j,\epsilon_k}(x),$$

$$j = 1, 2, \ldots, p-1, \quad \epsilon_k,$$

$$\text{кратность } (p-1)^2 p^{k-2}, \quad k = 2, 3, \ldots .$$

При $p = 2$:

$$\lambda_0 = \frac{2^{\alpha(2-\gamma)}}{2^{\alpha+1}-1}, \qquad \psi_0(x) = 2^{\frac{1-\gamma}{2}}, \qquad \text{кратность } 1;$$

$$\lambda_1 = 2^{\alpha(2-\gamma)}, \qquad \psi_1(x) = \psi^1_{1-\gamma,1,0}(x), \qquad \text{кратность } 1;$$

$$\lambda_k = 2^{\alpha(k+1-\gamma)}, \qquad \psi_k(x) = \psi^k_{k+1-\gamma,j,\epsilon_k}(x),$$

$$j = 0, 1, \quad \epsilon_k,$$

$$\text{кратность } 2^{k-1}, \quad k = 2, 3, \ldots .$$

Следует отметить, что мультипликативные характеры ранга k группы $Z_p^\times$ являются собственными функциями оператора D^α в S_0, соответствующие собственному значению λ_k [21]. С другой стороны, число линейно-независимых мультипликативных характеров ранга k группы $Z_p^\times$ вычислено (см. [30]) и оно совпадает с кратностью n_k собственного значения λ_k оператора D^α, $\alpha > 0$, в S_0 [4]. Отсюда следует такой результат:

существует ортонормальный базис собственных функций оператора D^α, $\alpha > 0$, в S_0, состоящий из всех мультипликативных характеров группы $Z_p^\times$.

С другой стороны, любой мультипликативный характер группы $Z_p^\times$ ранга k разлагается по собственным функциям $\psi_{a_k+j}(x)$, $j = 1, 2, \dots, n_k$ (при надлежащем выборе a_k [4]), т. е. разлагается по аддитивным характерам поля $\mathbb{Q}_p$.

Приведем конкретные значения для λ_k и n_k. Полагая $\gamma = 0$, получим [4]:
при $p \neq 2$

$$\lambda_0 = \frac{p^\alpha + p - 2}{p^{\alpha+1} - 1}\, p^\alpha, \qquad n_0 = 1;$$
$$\lambda_1 = p^\alpha, \quad n_1 = p - 2;$$
$$\lambda_k = p^{\alpha k}, \quad n_k = (p-1)^2 p^{k-2}, \quad k = 2, 3, \dots;$$

при $p = 2$

$$\lambda_0 = \frac{2^{2\alpha}}{2^{\alpha+1} - 1}, \qquad n_0 = 1;$$
$$\lambda_k = 2^{\alpha(k+1)}, \quad n_k = 2^{k-1}, \quad k = 1, 2, \dots .$$

Часть II. Таблицы интегралов

§ 11. Простейшие интегралы, одна переменная

$$\int_{B_0} d_p x = 1. \tag{11.1}$$

$$\int_{B_\gamma} d_p x = p^\gamma. \tag{11.2}$$

$$\int_{S_\gamma} d_p x = \left(1 - \frac{1}{p}\right) p^\gamma. \tag{11.3}$$

$$\int f(x)\, d_p x = \sum_{\gamma=-\infty}^{\infty} \int_{S_\gamma} f(x)\, d_p x. \tag{11.4}$$

$$\int_{B_\gamma} f(|x|_p)\, d_p x = \left(1 - \frac{1}{p}\right) \sum_{k=-\infty}^{\gamma} p^k f(p^k). \tag{11.5}$$

$$\int f(|x|_p)\, d_p x = \left(1 - \frac{1}{p}\right) \sum_{k=-\infty}^{\infty} p^k f(p^k). \tag{11.6}$$

$$\int_D f(x)\, d_p x = |a|_p \int_{\frac{D-b}{a}} f(ay + b)\, d_p y, \qquad a \neq 0. \tag{11.7}$$

$$\int_{S_\gamma} f(x)\, d_p x = p^{2\gamma} \int_{S_{-\gamma}} f\left(\frac{1}{y}\right) d_p y. \tag{11.8}$$

$$\int_{B_\gamma} f(x)\, d_p x = \int_{\mathbb{Q}_p \setminus B_{1-\gamma}} f\left(\frac{1}{y}\right) |y|_p^{-2}\, d_p y. \tag{11.9}$$

$$\int f(x)\, d_p x = \int f\left(\frac{1}{y}\right) |y|_p^{-2}\, d_p y. \tag{11.10}$$

$$\int f(|x|_p)\, d_p x = \int f\left(\frac{1}{|y|_p}\right) |y|_p^{-2}\, d_p y. \tag{11.11}$$

$$\int_{G_p} f(x)\, d_p x = \int_{G_p} f(\sin y)\, d_p y. \tag{11.12}$$

$$\int_{G_p} f(x)\,d_px = \int_{G_p} f(\arcsin y)\,d_py. \tag{11.13}$$

$$\int_{G_p} f(x)\,d_px = \int_{G_p} f(\operatorname{tg} y)\,d_py. \tag{11.14}$$

$$\int_{G_p} f(x)\,d_px = \int_{G_p} f(\operatorname{arctg} y)\,d_py. \tag{11.15}$$

$$\int_{G_p} f(x)\,d_px = \int_{J_p} f(\ln y)\,d_py. \tag{11.16}$$

$$\int_{J_p} f(x)\,d_px = \int_{G_p} f(\exp y)\,d_py. \tag{11.17}$$

$$\int_{B_\gamma} |x|_p^{\alpha-1}\,d_px = \frac{1-p^{-1}}{1-p^{-\alpha}}\,p^{\alpha\gamma}, \qquad \operatorname{Re}\alpha > 0. \tag{11.18}$$

$$\int_{S_0} |x-1|_p^{\alpha-1}\,d_px = \frac{p-2+p^{-\alpha}}{p(1-p^{-\alpha})}, \qquad \operatorname{Re}\alpha > 0\ [3]. \tag{11.19}$$

$$\int_{S_\gamma} |x-a|_p^{\alpha-1}\,d_px = \frac{p-2+p^{-\alpha}}{p(1-p^{-\alpha})}\,|a|_p^{\alpha}, \qquad |a|_p = p^{\gamma}, \quad \operatorname{Re}\alpha > 0. \tag{11.20}$$

$$\int_{B_\gamma} \ln|x|_p\,d_px = \left(\gamma - \frac{1}{p-1}\right) p^{\gamma}\ln p. \tag{11.21}$$

$$\int_{S_0} \ln|x-1|_p\,d_px = -\frac{\ln p}{p-1}\ [3]. \tag{11.22}$$

$$\int_{S_\gamma} \ln|x-a|_p\,d_px = \left[\left(1-\frac{1}{p}\right)\ln|a|_p - \frac{\ln p}{p-1}\right]|a|_p, \quad |a|_p = p^{\gamma}. \tag{11.23}$$

$$\int_{S_\gamma} \ln|x|_p\,d_px = \gamma\left(1-\frac{1}{p}\right)p^{\gamma}\ln p. \tag{11.24}$$

$$\int |x|_p^{\alpha-1}|1-x|_p^{\beta-1}\,d_px = B_p(\alpha,\beta),$$
$$\operatorname{Re}\alpha > 0, \quad \operatorname{Re}\beta > 0, \quad \operatorname{Re}(\alpha+\beta) < 1\ [11]. \tag{11.25}$$

$$\int |x|_p^{\alpha-1}|y-x|_p^{\beta-1}\,d_px = B_p(\alpha,\beta)|y|_p^{\alpha+\beta-1},$$
$$\operatorname{Re}\alpha>0,\quad \operatorname{Re}\beta>0,\quad \operatorname{Re}(\alpha+\beta)<1. \tag{11.26}$$

$$\int_{B_\gamma} |x^2+a^2|_p^{(\alpha-1)/2}\,d_px$$
$$= p^\gamma|a|_p^{\alpha-1},\qquad p^\gamma<|a|_p. \tag{11.27}$$

$$= \frac{1-p^{\alpha-1}}{1-p^\alpha}\,|a|_p^\alpha + \frac{1-p^{-1}}{1-p^{-\alpha}}\,p^{\alpha\gamma},$$
$$p^\gamma \geqslant |a|_p\neq 0,\quad \operatorname{Re}\alpha>0,\quad p\equiv 3\ (\mathrm{mod}\ 4)\ [9]. \tag{11.28}$$

$$= \left[1-\frac{2}{p}+\left(1-\frac{1}{p}\right)\left(\frac{2}{p^{(\alpha+1)/2}-1}-\frac{1}{1-p^{-\alpha}}\right)\right]|a|_p^\alpha$$
$$-\frac{1-p^{-1}}{1-p^{-\alpha}}\,p^{\alpha\gamma},\qquad p^\gamma\geqslant|a|_p\neq 0,\quad \operatorname{Re}\alpha>0,$$
$$p\equiv 1\ (\mathrm{mod}\ 4)\ [9]. \tag{11.29}$$

$$\int |x^2+a^2|_p^{(\alpha-1)/2}\,d_px,\qquad a\neq 0,$$
$$= \frac{1-p^{\alpha-1}}{1-p^\alpha}\,|a|_p^\alpha \qquad \operatorname{Re}\alpha<0,\quad p\equiv 3\ (\mathrm{mod}\ 4). \tag{11.30}$$

$$= \left[1-\frac{2}{p}+\left(1-\frac{1}{p}\right)\left(\frac{2}{p^{(\alpha+1)/2}-1}-\frac{1}{1-p^{-\alpha}}\right)\right]|a|_p^\alpha,$$
$$\operatorname{Re}\alpha<0,\quad p\equiv 1\ (\mathrm{mod}\ 4). \tag{11.31}$$

$$\int_{S_0} \left|1+x^2\right|_p^{\alpha-1} d_px = 1-\frac{3}{p}-2\frac{1-p^{-1}}{1-p^\alpha},$$
$$\operatorname{Re}\alpha>0,\quad p\equiv 1\ (\mathrm{mod}\ 4). \tag{11.32}$$

$$\int_{S_{\gamma,k_0}} d_px = p^{\gamma-1},\qquad k_0=1,2,\dots,p-1\ [3]. \tag{11.33}$$

$$\int_{S_\gamma^{k_0}} d_px = \left(1-\frac{2}{p}\right)p^\gamma,\qquad k_0=1,2,\dots,p-1\ [3]. \tag{11.34}$$

$$\int_{S_{\gamma,k_n}} d_px = \left(1-\frac{1}{p}\right)p^{\gamma-1},\qquad k_n=0,1,\dots,p-1,\quad n\in Z_+\ [3]. \tag{11.35}$$

$$\int_{S_\gamma^{k_n}} d_p x = \left(1-\frac{1}{p}\right)^2 p^\gamma, \qquad k_n = 0,1,\dots,p-1, \quad n \in Z_+ \text{ [3]}. \tag{11.36}$$

$$\int_{S_{\gamma,k_0k_1\dots k_n}} d_p x = p^{\gamma-n-1},$$
$$k_j = 0,1,\dots,p-1, \quad k_0 \neq 0, \quad n \in Z_+ \text{ [3]}. \tag{11.37}$$

$$\int_{S_\gamma^{k_0k_1\dots k_n}} d_p x = (1-p^{-1}-p^{-n-1})p^\gamma,$$
$$k_j = 0,1,\dots,p-1, \quad k_0 \neq 0, \quad n \in Z_+ \text{ [3]}. \tag{11.38}$$

$$\int_{\bigcap_{1\leqslant i\leqslant k}[|x-x_i|_p=1]} d_p x = 1-\frac{k}{p}, \qquad 1 \leqslant k \leqslant p, \quad |x_j-x_j|_p = 1,$$

$$i,j = 1,2,\dots,k, \quad i \neq j \text{ [17]}. \tag{11.39}$$

Пусть π – мультипликативный характер поля $\mathbb{Q}_p$ ранга $k \geqslant 1$.

$$\int_{S_\gamma} \pi(x)\, d_p x = 0 \text{ [11]}. \tag{11.40}$$

Обозначим: $V_0 = S_0$, $V_j = [x \in S_0 : |1-x|_p \leqslant p^{-j}]$, $j \in Z_+$.

$$\int_{V_j\setminus V_{j+1}} \pi(x)\, d_p x$$
$$= 0, \qquad 0 \leqslant j < k-1. \tag{11.41}$$
$$= -p^{-k}, \qquad j = k-1. \tag{11.42}$$
$$= \left(1-\frac{1}{p}\right)p^{-j}, \qquad j \geqslant k \text{ [21]}. \tag{11.43}$$

$$\int_{S_0} |1-x|_p^{\alpha-1}\pi(x)\, d_p x = \Gamma_p(\alpha)p^{-k\alpha}, \qquad \operatorname{Re}\alpha > 0 \text{ [21]}. \tag{11.44}$$

$$\int_{S_\gamma} \operatorname{sgn}_{p,\epsilon} x\, d_p x = \left(1-\frac{1}{p}\right)(-p)^\gamma,$$
$$\epsilon \notin \mathbb{Q}_p^{\times 2}, \quad |\epsilon|_p = 1, \quad p \neq 2 \text{ [11]}. \tag{11.45}$$

$$\int_{B_\gamma} \operatorname{sgn}_{p,\epsilon} x\, d_p x = \frac{p-1}{p+1}\,(-p)^\gamma,$$
$$\epsilon \notin \mathbb{Q}_p^{\times 2}, \quad |\epsilon|_p = 1, \quad p \neq 2 \text{ [11]}. \tag{11.46}$$

$$\int_{B_0} \operatorname{sgn}_{p,\epsilon} x \, d_p x$$

$$= \frac{p-1}{p+1}, \qquad \epsilon \notin \mathbb{Q}_p^{\times 2}, \quad |\epsilon|_p = 1, \quad p \neq 2 \text{ [11]}. \tag{11.47}$$

$$= \frac{1}{3}, \qquad \epsilon \equiv 5 \pmod 8, \quad p = 2, \tag{11.48}$$

$$= 0, \qquad |\epsilon|_p = \frac{1}{p}, \quad p \neq 2 \tag{11.49}$$

$$\text{или} \quad \epsilon \not\equiv 1, 5 \pmod 8, \quad p = 2 \text{ [11]}.$$

$$\int_{B_0} \theta_\epsilon^+(x) \, d_p x$$

$$= \frac{p}{p+1}, \qquad \epsilon \notin \mathbb{Q}_p^{\times 2}, \quad |\epsilon|_p = 1, \quad p \neq 2. \tag{11.50}$$

$$= \frac{2}{3}, \qquad \epsilon \equiv 5 \pmod 8, \quad p = 2. \tag{11.51}$$

$$= \frac{1}{2}, \qquad |\epsilon|_p = \frac{1}{p}, \quad p \neq 2 \tag{11.52}$$

$$\text{или} \quad \epsilon \not\equiv 1, 5 \pmod 8, \quad p = 2 \text{ [11]}.$$

$$\int_{B_0} \theta_\epsilon^-(x) \, d_p x$$

$$= \frac{1}{p+1}, \qquad \epsilon \notin \mathbb{Q}_p^{\times 2}, \quad |\epsilon|_p = 1, \quad p \neq 2. \tag{11.53}$$

$$= \frac{1}{3}, \qquad \epsilon \equiv 5 \pmod 8, \quad p = 2. \tag{11.54}$$

$$= \frac{1}{2}, \qquad |\epsilon|_p = \frac{1}{p}, \quad p \neq 2 \tag{11.55}$$

$$\text{или} \quad \epsilon \not\equiv 1, 5 \pmod 8, \quad p = 2 \text{ [11]}.$$

$$\int_{(B_0)^2} d_p x$$

$$= \frac{p}{2(p+1)}, \qquad p \neq 2. \tag{11.56}$$

$$= \frac{1}{6}, \qquad p = 2, \tag{11.57}$$

где $(B_0)^2$ – множество квадратов целых p-адических чисел Z_p.

$$\int_{\gamma(x)=2k \leqslant 0} d_p x = \frac{p}{p+1}. \tag{11.58}$$

$$\int_{\gamma(x)=2k\leqslant 0} f(|x|_p)\,d_px = \left(1-\frac{1}{p}\right)\sum_{\gamma=0}^{\infty} p^{-2\gamma} f(p^{-2\gamma}). \tag{11.59}$$

$$\int_{\gamma(x)-1=2k\leqslant 0} d_px = \frac{1}{p+1}\,. \tag{11.60}$$

$$\int_{\gamma(x)-1=2k\leqslant 0} f(|x|_p)\,d_px = \left(1-\frac{1}{p}\right)\sum_{\gamma=0}^{\infty} p^{-2\gamma-1} f(p^{-2\gamma-1}). \tag{11.61}$$

$$\int_{B_0} \lambda_p(x)|x|_p^{-1/2}\,d_px$$

$$= 1, \qquad p\neq 2\ [2]. \tag{11.62}$$

$$= 2^{-3/2}, \qquad p=2\ [2]. \tag{11.63}$$

Пусть функция f обладает свойством

$$\int_{B_0} f(x+k)\,d_px = f(k), \qquad k\in I_p,$$

где I_p множество индексов,

$$I_p = [k\in\mathbb{Q}_p : k = p^{-\gamma}(k_0+k_1+\cdots+k_{\gamma-1}p^{\gamma-1}),$$
$$k_j = 0,1,\ldots,p-1, \quad k_0\neq 0, \quad j=0,1,\ldots,\gamma-1, \quad \gamma\in Z_+.$$

$$\int_{\mathbb{Q}_p\setminus B_0} f(x)\,d_px = \sum_{k\in I_p} f(k)\ [28]. \tag{11.64}$$

$$\int_{B_{-1}\setminus B_{-2n}} \lambda_p^2(x)|x|_p^{-1}\,d_px, \qquad n\in Z_+,$$

$$= 1-\frac{1}{p}\,, \quad p\equiv 3\ (\mathrm{mod}\ 4)\ [2]. \tag{11.65}$$

$$= \left(1-\frac{1}{p}\right)(2n-1), \quad p\equiv 1\ (\mathrm{mod}\ 4)\ [2]. \tag{11.66}$$

$$\int_{B_{-2}\setminus B_{-2n}} \lambda_2^2(x)|x|_2^{-1}\,d_2x = 0, \qquad p=2, \quad n\geqslant 2\ [2]. \tag{11.67}$$

Обозначим $|(x,m)|_p = \max(|x|_p, |m|_p)$.

$$\int |(y,m)|_p^{\alpha-1}\,|(x-y,m)|_p^{\beta-1}\,d_py = B_p(\alpha,\beta)\,|(x,m)|_p^{\alpha+\beta-1}$$
$$-\Gamma_p(\alpha)\,|pm|_p^{\alpha}\,|(x,m)|_p^{\beta-1} - \Gamma_p(\beta)\,|pm|_p^{\beta}\,|(x,m)|_p^{\alpha-1},$$
$$m\neq 0,\quad \operatorname{Re}(\alpha+\beta)<1\ [17]. \tag{11.68}$$

Обозначим:

$$\mathscr{K}_t(x,y) = \lambda_p(t)\sqrt{\left|\frac{2}{t}\right|_p}\,\chi_p\!\left(\frac{2xy}{\sin t} - \frac{x^2+y^2}{\operatorname{tg} t}\right),\quad t\in G_p,\quad x,y\in\mathbb{Q}_p,$$
$$\mathscr{K}_t(x) = \lambda_p(t)\sqrt{\left|\frac{2}{t}\right|_p}\,\chi_p\!\left(-\frac{x^2}{t}\right),\qquad t\in\mathbb{Q}_p^{\times},\quad x\in\mathbb{Q}_p.$$

$$\int \mathscr{K}_t(x,y')\mathscr{K}_\tau(y',x)\,d_py' = \mathscr{K}_{t+\tau}(x,y),$$
$$t,\tau\in G_p,\quad x,y\in\mathbb{Q}_p\ [15]. \tag{11.69}$$

$$\int_{B_0}\mathscr{K}_t(x,y)\,d_py = \Omega(|x|_p),\qquad t\in G_p,\quad x\in\mathbb{Q}_p\ [15]. \tag{11.70}$$

$$\mathscr{K}_t(x,y)\to\delta(x-y),\qquad t\to 0\ \text{ в }\ \mathscr{S}'(\mathbb{Q}_p^2)\ [15]. \tag{11.71}$$

$$\int \mathscr{K}_t(x-y)\mathscr{K}_\tau(y)\,d_py = \mathscr{K}_{t+\tau}(x),\qquad t,\tau\in\mathbb{Q}_p^{\times},\quad x\in\mathbb{Q}_p\ [15]. \tag{11.72}$$

$$\mathscr{K}_t(x)\to\delta(x),\qquad t\to 0\ \text{ в }\ \mathscr{S}'\ [15]. \tag{11.73}$$

$$\int_{|x|_p\neq 1} f(|x|_p)|1-x|_p^{-1}\,d_px = (1-p^{-1})\sum_{\gamma\neq 0} f(p^\gamma)\min(1,p^\gamma). \tag{11.74}$$

§ 12. Интегралы Фурье

Интегралом Фурье называется интеграл вида

$$\int f(x)\chi_p(\xi x)\,d_px,\qquad \xi\in\mathbb{Q}_p^{\times}.$$

$$\int_{B_\gamma}\chi_p(\xi x)\,d_px = p^\gamma\Omega(p^\gamma|\xi|_p)\ [3]. \tag{12.1}$$

$$\int_{S_\gamma} \chi_p(\xi x)\, d_p x = \left(1-\frac{1}{p}\right) p^\gamma \Omega(p^\gamma |\xi|_p) - p^{\gamma-1}\delta(|\xi|_p - p^{1-\gamma}) \text{ [3]}. \tag{12.2}$$

$$\int \chi_p(\xi x)\, d_p x = 0, \qquad \xi \neq 0 \text{ [3]}. \tag{12.3}$$

$$\int_{B_\gamma} f(|x|_p)\chi_p(\xi x)\, d_p x$$

$$= \left(1-\frac{1}{p}\right) \sum_{k=-\gamma}^{\infty} p^{-k} f(p^{-k}), \qquad |\xi|_p \leqslant p^{-\gamma}. \tag{12.4}$$

$$= \left(1-\frac{1}{p}\right) |\xi|_p^{-1} \sum_{k=0}^{\infty} p^{-k} f(p^{-k}|\xi|_p^{-1}) - |\xi|_p^{-1} f(p\,|\xi|_p^{-1}), \tag{12.5}$$

$|\xi|_p > p^{-\gamma}$ [3].

$$= \int f(|x|_p)\chi_p(\xi x)\, d_p x, \qquad |\xi|_p > p^{-\gamma}. \tag{12.6}$$

$$\int f(|x|_p)\chi_p(\xi x)\, d_p x = \left(1-\frac{1}{p}\right) |\xi|_p^{-1} \sum_{k=0}^{\infty} p^{-k} f(p^{-k}|\xi|_p^{-1})$$

$$-|\xi|_p^{-1} f(p|\xi|_p^{-1}), \qquad \xi \neq 0 \text{ [3]}. \tag{12.7}$$

$$\int |x|_p^{\alpha-1}\chi_p(x)\, d_p x = \frac{1-p^{\alpha-1}}{1-p^{-\alpha}} = \Gamma_p(\alpha), \qquad \operatorname{Re}\alpha > 0 \text{ [11]}. \tag{12.8}$$

$$\int |x|_p^{\alpha-1}\chi_p(\xi x)\, d_p x = \Gamma_p(\alpha)|\xi|_p^{-\alpha}, \qquad \xi \neq 0, \quad \operatorname{Re}\alpha > 0 \text{ [11]}. \tag{12.9}$$

$$\int \ln|x|_p \chi_p(x)\, d_p x = -\left(1-\frac{1}{p}\right)^{-1} \ln p \text{ [3]}. \tag{12.10}$$

$$\int \ln|x|_p \chi_p(\xi x)\, d_p x = -\left(1-\frac{1}{p}\right)^{-1} \ln p|\xi|_p^{-1}, \qquad \xi \neq 0 \text{ [3]}. \tag{12.11}$$

$$\int \frac{\chi_p(\xi x)}{|x|_p^2 + m^2}\, d_p x, \qquad m \neq 0,$$

$$= \left(1-\frac{1}{p}\right) \sum_{k=-\infty}^{\infty} \frac{p^k}{p^{2k}+m^2}, \qquad \xi = 0. \tag{12.12}$$

$$= \left(1-\frac{1}{p}\right)\frac{|\xi|_p}{p^2+m^2|\xi|_p^2}\sum_{k=0}^{\infty} p^{-k}\frac{p^2-p^{-2k}}{p^{-2k}+m^2|\xi|_p^2}, \qquad \xi\neq 0\ [3]. \tag{12.13}$$

$$\sim \frac{p^4+p^3}{p^2+p+1}\,m^{-4}|\xi|_p^{-3}+O(|\xi|_p^{-5}), \qquad |\xi|_p\to\infty\ [3]. \tag{12.14}$$

$$\mu_t^\alpha(x)=\int \exp(-t|\xi|_p^\alpha)\chi_p(\xi x)\,d_p\xi, \qquad t>0, \quad \alpha>0$$

$$= \left(1-\frac{1}{p}\right)|x|_p^{-1}\sum_{\gamma=0}^{\infty} p^{-\gamma}\exp(-t|px|_p^{-\alpha})$$

$$\times\big(\exp[t|px|_p^{-\alpha}(1-p^{-\alpha\gamma-\alpha})]-1\big)>0\ [1],[2]. \tag{12.15}$$

$$= \sum_{n=1}^{\infty}\frac{(-t)^n}{n!}\,\Gamma_p(\alpha n+1)|\xi|_p^{-\alpha n-1}\ [1]. \tag{12.16}$$

$$\int \mu_t^\alpha(x)\,d_px=1, \qquad t>0. \tag{12.17}$$

$$\mu_t^\alpha(x)\to\delta(x), \qquad t\to 0 \ \text{ в } \ \mathscr{S}\ [1]. \tag{12.18}$$

$$\mu_t^\alpha * \mu_\tau^\alpha=\mu_{t+\tau}^\alpha, \qquad t,\tau>0\ [1]. \tag{12.19}$$

$$\int_0^\infty \mu_t^\alpha(x)\,dt=\Gamma_p^{-1}(\alpha)|x|_p^{\alpha-1}=f_\alpha(x), \tag{12.20}$$

$$\frac{\partial}{\partial t}\,\mu_p^\alpha(x)|_{t=0}=\Gamma_p(\alpha+1)|x|_p^{-\alpha-1}, \qquad \alpha>0. \tag{12.21}$$

$$|x|_p^\alpha=-\Gamma_p^{-1}(-\alpha)\int[1-\operatorname{Re}\chi_p(x\xi)]|\xi|_p^{-\alpha-1}\,d_p\xi, \tag{12.22}$$

причем

$$-\Gamma_p^{-1}(-\alpha)|\xi|_p^{-\alpha-1}\,d_p\xi>0, \qquad \alpha>0.$$

$$\int_{B_{-1}}\chi_p(a^2\operatorname{tg}\xi-x\xi)\,d_p\xi, \qquad p\neq 2\ [2],$$

$$= \frac{1}{2}\,\Omega(|px|_p), \qquad |a|_p\leqslant 1. \tag{12.23}$$

$$= \frac{1}{2}\,\delta\big(|x|_p-p^2\big)\,\delta\big(x_0-(a^2)_0\big), \qquad |a|_p=p. \tag{12.24}$$

$$= \frac{1}{2}\,\delta\big(|x|_p-|a|_p^2\big)\,\delta\big(x_0-(a^2)_0\big)\,\delta\big(x_1-(a^2)_1\big)\varphi_a(x), \quad |a|_p\geqslant p^2, \tag{12.25}$$

где $\varphi_a(x)$ – непрерывная функция.

$$\int |x|_p^{\alpha-1}|x-a|_p^{\beta-1}\chi_p(x)\,d_px, \qquad \operatorname{Re}\alpha, \operatorname{Re}\beta > 0, \quad \operatorname{Re}(\alpha+\beta) < 1,$$

$$= B_p(\alpha,\beta)|a|_p^{\alpha+\beta-1} + \Gamma_p(\alpha+\beta-1), \qquad |a|_p \leqslant 1. \tag{12.26}$$

$$= \Gamma_p(\alpha)|a|_p^{\beta-1} + \Gamma_p(\beta)|a|_p^{\alpha-1}\chi_p(a), \qquad |a|_p \geqslant p. \tag{12.27}$$

$$\int_{S_\gamma} |x-a|_p^{\alpha-1}\chi_p(x-a)\,d_px = \Gamma_p(\alpha),$$
$$|a|_p = p^\gamma, \quad \gamma \geqslant 2, \quad \operatorname{Re}\alpha > 0. \tag{12.28}$$

Пусть $n \in Z_+$ не делится на p и P – полином степени n,

$$P(x) = \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_n x^n,$$
$$|\alpha_k|_p \leqslant 1, \quad k = 1, 2, \ldots, n-1, \quad |\alpha_n|_p = 1.$$

Тогда

$$\int_{S_\gamma} \chi_p[P(x)]\,d_px$$

$$= \left(1 - \frac{1}{p}\right)p^\gamma, \qquad \gamma \leqslant 0, \quad n \in Z_+ \text{ [3]}. \tag{12.29}$$

$$= 0, \qquad \gamma = 2, 3, \ldots, \ n \in Z_+ \ \text{ или } \ \gamma = 1, \ n = 2, 3, \ldots \text{ [3]}. \tag{12.30}$$

$$= -1, \qquad \gamma = 1, \quad n = 1 \text{ [3]}. \tag{12.31}$$

$$\int_{B_\gamma} \chi_p[P(x)]\,d_px$$

$$= p^\gamma, \qquad \gamma \leqslant 0, \quad n \in Z_+, \tag{12.32}$$

$$= 1, \qquad \gamma = 2, 3, \ldots, \ n \in Z_+ \ \text{ или } \ \gamma = 1, \ n = 2, 3, \ldots. \tag{12.33}$$

$$= 0, \qquad \gamma \in Z_+, \quad n = 1. \tag{12.34}$$

$$\int \chi_p[P(x)]\,d_px$$

$$= 1, \qquad n = 2, 3, \ldots. \tag{12.35}$$

$$= 0, \qquad n = 1. \tag{12.36}$$

Пусть (комплексные) числа $\eta_1, \eta_2, \ldots, \eta_{p-1}$ таковы, что

$$\sum_{k=1}^{p-1} \eta_k = 0, \qquad p \neq 2,$$

и числа $\eta'_1, \eta'_2, \dots, \eta'_{p-1}$ взаимны к $\{\eta_k\}$,

$$\eta'_j = \sum_{k=1}^{p-1} \eta_k \exp\left(2\pi i \frac{kj}{p}\right), \qquad \sum_{j=1}^{p-1} \eta'_j = 0.$$

Тогда

$$\int_{S_\gamma} \eta_{x_0} \chi_p(\xi x)\, d_p x = p^{\gamma-1} \eta'_{\xi_0} \delta(|\xi|_p - p^{1-\gamma}) \text{ [4]}. \tag{12.37}$$

$$\int_{B_\gamma} |x|_p^{\alpha-1} \chi_p(\xi x)\, d_p x, \qquad \operatorname{Re}\alpha > 0,$$

$$= \frac{1-p-1}{1-p^{-\alpha}}\, p^{\alpha\gamma}, \qquad |\xi|_p \leqslant p^{-\gamma}. \tag{12.38}$$

$$= \Gamma_p(\alpha) |\xi|_p^{-\alpha}, \qquad |\xi|_p > p^{-\gamma} \quad \text{[1]}. \tag{12.39}$$

$$= \Gamma_p(\alpha), \qquad \xi = 1, \quad \gamma \geqslant 1 \text{ [7]}. \tag{12.40}$$

$$\int_{S_0} \delta(x_0 - k) \chi_p(\xi x)\, d_p x = p^{-1} \chi_p(k\xi) \Omega(|p\xi|_p),$$
$$k = 1, 2, \dots, p-1. \tag{12.41}$$

$$\int \delta(x_0 - k) \chi_p(\xi x)\, d_p x = |\xi|_p^{-1} \left(\frac{1}{p-1} + \chi_p(k\xi_0/p)\right),$$
$$\xi \neq 0, \quad k = 1, 2, \dots, p-1. \tag{12.42}$$

$$\int_{B_1} \chi_p[(k-\xi)x]\, d_p x = p\delta(|\xi|_p - 1)\delta(\xi_0 - k),$$
$$k = 1, 2, \dots, p-1. \tag{12.43}$$

$$\int_{S_0} \delta(x_1 - k) \chi_p(\xi x)\, d_p x = \frac{1}{p}\left(1 - \frac{1}{p}\right)\Omega(|\xi|_p) - p^{-2}\delta(|\xi|_p - p)$$
$$+ p^{-2} \frac{\chi_p(\xi) - \chi_p(p\xi)}{1 - \chi_p(\xi)}\, \chi_p(kp\xi)\delta(|\xi|_p - p^2),$$
$$k = 0, 1, \dots, p-1. \tag{12.44}$$

$$\int \delta(x_1 - k) \chi_p(\xi x)\, d_p x = |\xi|_p^{-1} \frac{\chi_p(p^{-2}|\xi|_p \xi) - \chi_p(p^{-1}\xi_0)}{1 - \chi_p(p^{-1}\xi_0)}\, \chi_p(kp^{-1}\xi_0),$$
$$\xi \neq 0, \quad p = 0, 1, \dots, p-1. \tag{12.45}$$

$$\int_{S_0}\delta(x_2-k)\chi_p(\xi x)\,d_px=\frac{1}{p}\left(1-\frac{1}{p}\right)\Omega(|\xi|_p)-p^{-2}\delta(|\xi|_p-p)$$
$$+p^{-3}\frac{\chi_p(\xi)-\chi_p(p\xi)}{1-\chi_p(\xi)}\,\frac{\chi_p(kp^2\xi)-\chi_p((k+1)p^2\xi)}{1-\chi_p(p\xi)}\,\delta(|\xi|_p-p^3),$$
$$k=0,1,\dots,p-1. \tag{12.46}$$

$$\int\delta(x_2-k)\chi_p(\xi x)\,d_px=|\xi|_p^{-1}\frac{\chi_p(p^{-3}|\xi|_p\xi)-\chi_p(p^{-2}|\xi|_p\xi)}{1-\chi_p(p^{-3}|\xi|_p\xi)}$$
$$\times\frac{\chi_p(kp^{-1}\xi_0)-\chi_p((k+1)p^{-1}\xi_0)}{1-\chi_p(p^{-2}|\xi|_p\xi)},$$
$$\xi\neq0,\quad k=0,1,\dots,p-1. \tag{12.47}$$

$$\int|x,m|_p^{\alpha-1}\chi_p(\xi x)\,d_px=\Gamma_p(\alpha)\big(|\xi|_p^{-\alpha}-|pm|_p^{\alpha}\big)\Omega(|m\xi|_p),$$
$$m\neq0,\quad \operatorname{Re}\alpha<0\ [17]. \tag{12.48}$$

$$\int|x,1|_p^{-\alpha}\chi_p(\xi x)\,d_px=\Gamma_p(1-\alpha)(|\xi|_p^{\alpha-1}-p^{\alpha-1})\Omega(|\xi|_p)\equiv J_p^{\alpha}(\xi),$$
$$\operatorname{Re}\alpha>0. \tag{12.49}$$

$$J_p^1(\xi)=\left(1-\frac{1}{p}\right)\left(1-\frac{\ln|\xi|_p}{\ln p}\right)\Omega(|\xi|_p),\qquad \alpha=1. \tag{12.50}$$

$$\int J_p^{\alpha}(\xi)J_p^{\beta}(x-\xi)\,d_p\xi=J_p^{\alpha}*J_p^{\beta}=J_p^{\alpha+\beta},\qquad \alpha,\beta\in\mathbb{C}. \tag{12.51}$$

$$\ln|x,1|_p=\int\big(1-\operatorname{Re}\chi_p(x\xi)\big)\,d\sigma(\xi)$$
$$=\ln p\sum_{\gamma=0}^{\infty}p^{\gamma}\Omega(p^{\gamma}|\xi|_p),\qquad d\sigma(\xi)\geqslant0. \tag{12.52}$$

$$\int_{B_{-1}\setminus B_{-2n}}\lambda_p^2(x)|x|_p^{-1}\chi_p(\xi x)\,d_px,\qquad n\in Z_+,$$
$$=\left(1-\frac{1}{p}\right)(2n-1),$$
$$\xi=0\ \text{ или }\ \gamma(\xi)\leqslant1,\quad p\equiv1\ (\mathrm{mod}\ 4)\ [2]. \tag{12.53}$$
$$=\left(1-\frac{1}{p}\right)(2n-\gamma(\xi))-\frac{1}{p},,$$
$$2\leqslant\gamma(\xi)\leqslant2n,\quad p\equiv1\ (\mathrm{mod}\ 4)\ [2]. \tag{12.54}$$

$$= 1 - \frac{1}{p}, \qquad \xi = 0 \ \text{ или } \ \gamma(\xi) \leqslant 1, \quad p \equiv 3 \pmod 4 \ [2]. \tag{12.55}$$

$$= \frac{1}{2}\,(-1)^{\gamma(\xi)}\left(1 + \frac{1}{p}\right) - \frac{1}{2}\left(1 - \frac{1}{p}\right), \quad 2 \leqslant \gamma(\xi) \leqslant 2n, \quad p \equiv 3 \pmod 4 \ [2]. \tag{12.56}$$

$$\int_{B_{-1}} \lambda_p^2(x)|x|_p^{-1}\chi_p(\xi x)\,d_p x$$

$$= 1 - \frac{1}{p}\,, \qquad \xi = 0 \ \text{ или } \ \gamma(\xi) \leqslant 1, \quad p \equiv 3 \pmod 4 \ [2]. \tag{12.57}$$

$$= \frac{1}{2}\,(-1)^{\gamma(\xi)}\left(1 + \frac{1}{p}\right) - \frac{1}{2}\left(1 - \frac{1}{p}\right), \quad \gamma(\xi) \geqslant 2, \quad p \equiv 3 \pmod 4 \ [2]. \tag{12.58}$$

$$\int_{B_{-2}\setminus B_{-2n}} \lambda_2^2(x)|x|_2^{-1}\chi_2(\xi x)\,d_2 x, \qquad n = 2, 3, \ldots,$$

$$= 0, \qquad \gamma(\xi) \leqslant 3 \ [2]. \tag{12.59}$$

$$= \frac{1}{4}(-1)^{\xi_1+1}, \qquad \gamma(\xi) \geqslant 4 \ [2]. \tag{12.60}$$

$$\int_{B_{-2}} \lambda_2^2(x)|x|_2^{-1}\chi_2(\xi x)\,d_2 x$$

$$= 0, \qquad \xi = 0 \ \text{ или } \ \gamma(\xi) \leqslant 3 \ [2]. \tag{12.61}$$

$$= \frac{1}{2}(-1)^{\xi_1+1}, \qquad \gamma(\xi) \geqslant 4 \ [2]. \tag{12.62}$$

$$\int \operatorname{sgn}_{p,d} x|x|_p^{\alpha-1}\chi_p(\xi x)\,d_p x, \qquad d \notin \mathbb{Q}_p^{\times 2}$$

$$= \widetilde{\Gamma}_p(\alpha)\operatorname{sgn}_{p,d}\xi|\xi|_p^{-\alpha}, \qquad |d|_p = 1, \quad \operatorname{Re}\alpha > 0 \ [11]. \tag{12.63}$$

$$= \pm p^{\alpha-1/2}\sqrt{\operatorname{sgn}_{p,d}(-1)}\,\operatorname{sgn}_{p,d}\xi|\xi|_p^{-\alpha}, \quad |d|_p = \frac{1}{p}\,, \quad \alpha \in \mathbb{C} \ [11]. \tag{12.64}$$

Пусть $\varepsilon = \pm$.

$$\int_{S_\gamma} \lambda_p(x)\chi_p(\varepsilon\xi x)\,d_p x \ [2], [29]$$

$$= p^{\gamma}\left(1 - \frac{1}{p}\right), \qquad |\xi|_p \leqslant p^{-\gamma}, \quad \gamma = 2k. \tag{12.65}$$

$$= 0, \qquad |\xi|_p \leqslant p^{-\gamma}, \quad \gamma = 2k+1. \tag{12.66}$$

$$= -p^{\gamma-1}, \qquad |\xi|_p = p^{-\gamma+1}, \quad \gamma = 2k. \tag{12.67}$$

$$= \left(\frac{\xi_0}{p}\right) p^{\gamma-1/2}, \qquad \begin{array}{l} |\xi|_p \leqslant p^{-\gamma+1}, \\ \gamma = 2k+1, \quad p \equiv 1 \pmod 4. \end{array} \tag{12.68}$$

$$= -\varepsilon\left(\frac{\xi_0}{p}\right) p^{\gamma-1/2}, \qquad \begin{array}{l} |\xi|_p \leqslant p^{-\gamma+1}, \\ \gamma = 2k+1, \quad p \equiv 3 \pmod 4. \end{array} \tag{12.69}$$

$$= 0, \qquad |\xi|_p \geqslant p^{-\gamma+2}. \tag{12.70}$$

$$\int_{S_\gamma} \lambda_2(x)\chi_2(\varepsilon\xi x)\, d_2x \text{ [20], [29]}$$

$$= 2^{\gamma-3/2}, \qquad |\xi|_2 \leqslant 2^{-\gamma}, \quad \gamma = 2k. \tag{12.71}$$

$$= 0, \qquad |\xi|_2 \leqslant 2^{-\gamma}, \quad \gamma = 2k+1. \tag{12.72}$$

$$= -2^{\gamma-3/2}, \qquad |\xi|_2 = 2^{-\gamma+1}, \quad \gamma = 2k. \tag{12.73}$$

$$= 0, \qquad |\xi|_2 = 2^{-\gamma+1}, \quad \gamma = 2k+1. \tag{12.74}$$

$$= -\varepsilon(-1)^{\xi_1} 2^{\gamma-3/2}, \qquad |\xi|_2 = 2^{-\gamma+2}, \quad \gamma = 2k. \tag{12.75}$$

$$= 0, \qquad |\xi|_2 = 2^{-\gamma+2}, \quad \gamma = 2k+1. \tag{12.76}$$

$$= 0, \qquad |\xi|_2 \geqslant 2^{-\gamma+3}, \quad \gamma = 2k. \tag{12.77}$$

$$= i^{\xi_1}(-1)^{\xi_2} 2^{\gamma-3}(1+i)(1+i\varepsilon)[1-\varepsilon(-1)^{\xi_1}], \quad |\xi|_2 = 2^{-\gamma+3}, \quad \gamma = 2k+1. \tag{12.78}$$

$$= 0, \qquad |\xi|_2 \geqslant 2^{-\gamma+4}, \quad \gamma = 2k+1. \tag{12.79}$$

$$\int_{|x|_p \geqslant 1} \lambda_p(x)|x|_p^{\alpha-1}\chi_p(\varepsilon\xi^2 x)\, d_px$$

$$= 0, \qquad |\xi|_p \geqslant p, \quad p \neq 2. \tag{12.80}$$

$$= \left(1-\frac{1}{p}\right)\frac{1-p^{2\alpha}|\xi|_p^{-2\alpha}}{1-p^{2\alpha}} + p^{\alpha-1/2}|\xi|_p^{-2\alpha}, \quad |\xi|_p \leqslant 1, \quad p \equiv 1 \pmod 4. \tag{12.81}$$

$$= \left(1-\frac{1}{p}\right)\frac{1-p^{2\alpha}|\xi|_p^{-2\alpha}}{1-p^{2\alpha}} - \varepsilon p^{\alpha-1/2}|\xi|_p^{-2\alpha}, \quad |\xi|_p \leqslant 1, \quad p \equiv 3 \pmod 4. \tag{12.82}$$

$$\int_{|x|_p \geqslant 1} \lambda_p(x)|x|_p^{-3/2}\chi_p(-\xi^2 x)\, d_px = \Omega(|\xi|_p), \qquad p \neq 2 \text{ [29]}. \tag{12.83}$$

$$\int_{|x|_2 \geqslant 4} \lambda_2(x)|x|_2^{-3/2}\chi_2(-\xi^2 x)\, d_2x = \sqrt{2}\Omega(|\xi|_2), \quad p = 2 \text{ [29]}. \tag{12.84}$$

§ 13. Гауссовы интегралы

Гауссовым интегралом называется интеграл вида

$$\int f(x)\chi_p(ax^2+bx)\,d_px, \qquad a\in\mathbb{Q}_p^\times, \quad b\in\mathbb{Q}_p.$$

Различные формулы для гауссовых интегралов встречаются в [3], [13]–[16], [20]. Наиболее полные списки их приведены в [1], [2]. Здесь

$$\epsilon=\varepsilon_0+\varepsilon_1 p+\varepsilon_2 p^2+\cdots.$$

$$\int_{S_\gamma}\chi_p\big[\epsilon(x-y)^2\big]\,d_py$$

$$=p^\gamma\chi_p(\epsilon x^2)\left[\left(1-\frac{1}{p}\right)\Omega(p^\gamma|x|_p)-\frac{1}{p}\,\delta(|x|_p-p^{1-\gamma})\right],$$
$$\gamma\leqslant 0, \quad p\neq 2. \tag{13.1}$$
$$=\delta(|x|_p-p^\gamma), \qquad \gamma\geqslant 1, \quad p\neq 2. \tag{13.2}$$
$$=2^{\gamma-1}\chi_2(\epsilon x^2)\big[\Omega(2^{\gamma-1}|x|_2)-\delta(|x|_2-2^{2-\gamma})\big],$$
$$\gamma\leqslant 0, \quad p=2. \tag{13.3}$$
$$=\big[\sqrt{2}\,\lambda_2(\epsilon)-1\big]\Omega(|x|_2)+\delta(|x|_2-2), \quad \gamma=1, \quad p=2. \tag{13.4}$$
$$=\sqrt{2}\,\lambda_2(\epsilon)\delta(|x|_2-2^\gamma), \qquad \gamma\geqslant 2, \quad p=2. \tag{13.5}$$

$$\int_{S_\gamma}\chi_p[\epsilon p(x-y)^2]\,d_py$$

$$=p^\gamma\chi_p\big(\epsilon px^2\big)\left[\left(1-\frac{1}{p}\right)\Omega\big(p^{1-\gamma}|x|_p\big)-\frac{1}{p}\,\delta\big(|x|_p-p^{2-\gamma}\big)\right],$$
$$\gamma\leqslant 0, \quad p\neq 2. \tag{13.6}$$
$$=\big[\sqrt{p}\,\lambda_p(\epsilon p)-\chi_p(\epsilon px^2)\big]\,\Omega(|px|_p), \qquad \gamma=1, \quad p\neq 2. \tag{13.7}$$
$$=\sqrt{p}\,\lambda_p(\epsilon p)\delta(|x|_p-p^\gamma), \qquad \gamma\geqslant 2, \quad p\neq 2. \tag{13.8}$$
$$=2^{\gamma-1}\chi_2(2\epsilon x^2)[\Omega(2^{\gamma-2}|x|_2)-\delta(|x|_2-2^{3-\gamma})],$$
$$\gamma\leqslant 0, \quad p=2. \tag{13.9}$$
$$=-\Omega(|x|_2)+\delta(|x|_2-2)+\lambda_2(2\epsilon)\,\delta(|x|_2-4),$$
$$\gamma=1, \quad p=2. \tag{13.10}$$
$$=2\lambda_2(2\epsilon)\,\Omega(|2x|_2), \qquad \gamma=2, \quad p=2. \tag{13.11}$$
$$=2\lambda_2(2\epsilon)\,\delta(|x|_2-2^\gamma), \qquad \gamma\geqslant 3, \quad p=2. \tag{13.12}$$

$$\int_{S_\gamma} \chi_p(ax^2+\xi x)\,d_p x$$

$$= \lambda_p(a)|2a|_p^{-1/2}\chi_p\biggl(-\frac{\xi^2}{4a}\biggr)\,\delta\biggl(\biggl|\frac{\xi}{2a}\biggr|_p - p^\gamma\biggr), \qquad |4a|_p \geqslant p^{2-2\gamma}. \tag{13.13}$$

$$= |2a|_p^{-1/2}\biggl[\lambda_p(a)\chi_p\biggl(-\frac{\xi^2}{4a}\biggr) - \frac{1}{\sqrt{p}}\biggr]\Omega\bigl(p^{1-\gamma}|\xi|_p\bigr), \quad |a|_p = p^{1-2\gamma}. \tag{13.14}$$

$$\int_{B_\gamma} \chi_p(ax^2+\xi x)\,d_p x = p^\gamma\Omega(p^\gamma|\xi|_p), \qquad |a|_p p^{2\gamma} \leqslant 1, \tag{13.15}$$

$$= \lambda_p(a)|2a|_p^{-1/2}\chi_p\biggl(-\frac{\xi^2}{4a}\biggr)\,\Omega\biggl(p^{-\gamma}\biggl|\frac{\xi}{2a}\biggr|_p\biggr), \qquad |4a|_p p^{2\gamma} > 1. \tag{13.16}$$

$$= 2^\gamma\lambda_2(a)\chi_2\biggl(-\frac{\xi^2}{4a}\biggr)\,\delta\bigl(|\xi|_2 - 2^{1-\gamma}\bigr), \qquad |a|_2 2^{2\gamma} = 2, \quad p=2. \tag{13.17}$$

$$= 2^{\gamma-1/2}\lambda_2(a)\chi_2\biggl(-\frac{\xi^2}{4a}\biggr)\,\Omega\bigl(2^\gamma|\xi|_2\bigr), \qquad |a|_2 2^{2\gamma} = 4, \quad p=2. \tag{13.18}$$

$$\int \chi_p(ax^2+\xi x)\,d_p x, \qquad a \neq 0,$$

$$= \lambda_p(a)|2a|_p^{-1/2}\chi_p\biggl(-\frac{\xi^2}{4a}\biggr). \tag{13.19}$$

$$= \chi_p\biggl(-\frac{\xi^2}{2}\biggr), \qquad a = \frac{1}{2}, \quad p \neq 2. \tag{13.20}$$

$$= \exp\biggl(\frac{i\pi}{4}\biggr)\chi_p\biggl(-\frac{\xi^2}{2}\biggr), \qquad a = \frac{1}{2}, \quad p = 2. \tag{13.21}$$

$$\int \exp\bigl(-|y|_p^2\bigr)\chi_p[a(x-y)^2]\,d_p y, \qquad a \neq 0, \quad \gamma = \gamma(a),$$

$$= |a|_p^{-1/2} S\biggl(|a|_p^{-1}, \frac{1}{p}\biggr), \qquad |x|_p\sqrt{|a|_p} \leqslant 1, \quad \gamma = 2k, \quad p \neq 2. \tag{13.22}$$

$$= \frac{1}{\sqrt{p}}\,|a|_p^{-1/2} S\biggl(\frac{1}{p}\,|a|_p^{-1}, \frac{1}{p}\biggr) + \biggl[\lambda_p(a) - \frac{1}{\sqrt{p}}\biggr]|a|_p^{-1/2}\exp(-|pa|_p^{-1}),$$
$$|x|_p\sqrt{p|a|_p} \leqslant 1, \quad \gamma = 2k+1, \quad p \neq 2. \tag{13.23}$$

$$= \lambda_p(a)|a|_p^{-1/2}\exp(-|x|_p^2) + |ax|_p^{-1}\chi_p(ax^2)\biggl[S\biggl(|ax|_p^{-2},\frac{1}{p}\biggr) - \exp(-|pax|_p^{-2})\biggr], \qquad |x|_p\sqrt{|a|_p} \geqslant \sqrt{p}, \quad p \neq 2. \tag{13.24}$$

$$= [\sqrt{2}\lambda_2(a) - 1]|a|_2^{-1/2}\exp(-|4a|_2^{-1}) + |a|_2^{-1/2}S\biggl(|a|_2^{-1},\frac{1}{2}\biggr), \quad |x|_2\sqrt{|a|_2} \leqslant 1, \quad \gamma = 2k, \quad p = 2. \tag{13.25}$$

$$= |a|_2^{-1/2}\exp(-|4a|_2^{-1}) + [\sqrt{2}\,\lambda_2(a) - 1]|a|_2^{-1/2}S\biggl(|a|_2^{-1},\frac{1}{2}\biggr), \quad |x|_2\sqrt{|a|_2} = 2, \quad \gamma = 2k, \quad p = 2. \tag{13.26}$$

$$= (2|a|_2)^{-1/2}S\biggl((2|a|_2)^{-1},\frac{1}{2}\biggr) - (2|a|_2)^{-1/2}\exp(-|2a|_2^{-1}) + \lambda_2(a)|2a|_2^{-1/2}\exp(-|8a|_2^{-1}), \quad |x|_2\sqrt{2|a|_2} \leqslant 1, \quad \gamma = 2k+1, \quad p = 2. \tag{13.27}$$

$$= |2a|_2^{-1/2}S\biggl(|2a|_2^{-1},\frac{1}{2}\biggr) + \lambda_2(a)|2a|_2^{-1/2}\exp(-|8a|_2^{-1}), \quad |x|_2\sqrt{|a|_2} = \sqrt{2}, \quad \gamma = 2k+1, \quad p = 2. \tag{13.28}$$

$$= \lambda_2(a)(2|a|_2)^{-1/2}S\biggl(|2a|_2^{-1},\frac{1}{2}\biggr), \quad |x|_2\sqrt{|a|_2} = 2\sqrt{2}, \quad \gamma = 2k+1, \quad p = 2. \tag{13.29}$$

$$= \lambda_2(a)|2a|_2^{-1/2}\exp(-|x|_2^2) + |2ax|_2^{-1}\chi_2(ax^2)\biggl[S\biggl(|2ax|_2^{-2},\frac{1}{2}\biggr) - 2\exp(-|4ax|_2^{-2})\biggr], \qquad |x|_2\sqrt{|a|_2} > 2, \quad p = 2. \tag{13.30}$$

$$\sim \frac{p^4+p^3}{p^2+p+1}\,|2ax|_p^{-3}\chi_p(ax^2) + O(|x|_p^{-5}), \qquad |x|_p \to \infty. \tag{13.31}$$

$$\sim |a|_p^{-1/2}S(|a|_p^{-1},p^{-1}) + O[|a|_p^{-1/2}\exp(-|p^2a|_p^{-1})], \quad |a|_p \to 0, \quad \gamma = 2k. \tag{13.32}$$

$$\sim (p|a|_p)^{-1/2}S((p|a|_p)^{-1},p^{-1}) + O[|a|_p^{-1/2}\exp(-|pa|_p^{-1})], \quad |a|_p \to 0, \quad \gamma = 2k+1. \tag{13.33}$$

Здесь

$$S(\alpha,q) = (1-q)\sum_{k=0}^{\infty}\frac{(-\alpha)^k}{k!(1-q^{2k+1})}\,, \qquad |q| < 1, \quad \alpha \in \mathbb{C}.$$

Эта функция удовлетворяет соотношению

$$S(\alpha q^2, q) = \frac{1}{q}\, S(\alpha, q) + \left(1 - \frac{1}{q}\right) e^{-\alpha}. \tag{13.34}$$

§ 14. Две переменные

$$\int_{B_0^2} d_p^2 x = 1. \tag{14.1}$$

$$\int_{B_\gamma^2} d_p^2 x = p^{2\gamma}. \tag{14.2}$$

$$\int_{S_\gamma^2} d_p^2 x = (1 - p^{-2})\, p^{2\gamma}. \tag{14.3}$$

$$\int_{B_\gamma^2} f(|x|_p)\, d_p^2 x = (1 - p^{-2}) \sum_{k=-\infty}^{\gamma} p^{2k} f(p^k). \tag{14.4}$$

$$\int f(|x|_p)\, d_p^2 x = (1 - p^{-2}) \sum_{k=-\infty}^{\infty} p^{2k} f(p^k). \tag{14.5}$$

$$\int_{B_\gamma^2} |x|_p^{\alpha-2}\, d_p^2 x = \frac{1 - p^{-2}}{1 - p^{-\alpha}}\, p^{\alpha\gamma}, \qquad \operatorname{Re}\alpha > 0. \tag{14.6}$$

$$\int_{S_\gamma^2} |x|_p^{\alpha-2}\, d_p^2 x = (1 - p^{-2})\, p^{\alpha\gamma}. \tag{14.7}$$

$$\int_{B_\gamma^2} |(x,x)|_p^{\alpha-1} \chi_p((\xi,x))\, d_p^2 x, \qquad \operatorname{Re}\alpha > 0, \quad |(\xi,\xi)|_p > p^{-\gamma}.$$

$$= \Gamma_p^2(\alpha) |(\xi,\xi)|_p^{-\alpha}, \qquad p \equiv 1 \pmod 4 \text{ [9]}. \tag{14.8}$$

$$= \Gamma_p(\alpha) \widetilde{\Gamma}_p(\alpha) |(\xi,\xi)|_p^{-\alpha}, \qquad p \equiv 3 \pmod 4 \text{ [9]}. \tag{14.9}$$

$$\int |(x,x)|_p^{\alpha-1} \chi_p((\xi,x))\, d_p^2 x, \qquad \operatorname{Re}\alpha > 0, \quad (\xi,\xi) \neq 0,$$

$$= \Gamma_p^2(\alpha) |(\xi,\xi)|_p^{-\alpha}, \qquad p \equiv 1 \pmod 4 \text{ [9]}. \tag{14.10}$$

$$= \Gamma_p(\alpha) \widetilde{\Gamma}_p(\alpha) |(\xi,\xi)|_p^{-\alpha}, \qquad p \equiv 3 \pmod 4 \text{ [9]}. \tag{14.11}$$

$$\int f((x,x)) \chi_p((\xi,x))\, d_p^2 x, \qquad (\xi,\xi) \neq 0,$$

$$= |(\xi,\xi)|_p^{-1}\Big[\big(1-p^{-2}\big)\sum_{\gamma=0}^{\infty} p^{-2\gamma} f\big(p^{-2\gamma}|(\xi,\xi)|_p^{-1}\big) - f\big(p^2|(\xi,\xi)|_p^{-1}\big)\Big], \qquad p\equiv 3 \pmod 4 \text{ [1]}. \tag{14.12}$$

$$= |(\xi,\xi)|_p^{-1}\Big[\Big(1-\frac{1}{p}\Big)^{-2}\sum_{\gamma=0}^{\infty}\Big(\gamma+\frac{p-3}{p-1}\Big)p^{-\gamma} f\big(p^{-\gamma}|(\xi,\xi)|_p^{-1}\big) - 2\Big(1-\frac{1}{p}\Big) f\big(p\,|(\xi,\xi)|_p^{-1}\big) + f\big(p^2|(\xi,\xi)|_p^{-1}\big)\Big], \quad p\equiv 1 \pmod 4 \text{ [1]}. \tag{14.13}$$

$$\int \frac{\chi_p((\xi,x))}{|(x,x)|_p+m^2}\,d_p^2x, \qquad m\neq 0, \quad (\xi,\xi)\neq 0,$$

$$= \frac{1-p^{-2}}{p^2+m^2|(\xi,\xi)|_p}\sum_{\gamma=0}^{\infty}\frac{p^2-p^{-2\gamma}}{1+p^\gamma m^2|(\xi,\xi)|_p}$$

$$= \sum_{\gamma=0}^{\infty}\frac{1}{1+p^{2\gamma}m^2|(\xi,\xi)|_p} - \frac{1}{p^2+p^{2\gamma}m^2|(\xi,\xi)|_p}, \quad p\equiv 3 \pmod 4 \text{ [1], [9]}. \tag{14.14}$$

$$\sim \frac{p^4}{p^2+1}\,m^{-4}|(\xi,\xi)|_p^{-2}, |(\xi,\xi)|_p\to\infty, \qquad p\equiv 3 \pmod 4 \text{ [1], [9]}. \tag{14.15}$$

$$= \Big(1-\frac{1}{p}\Big)^2\sum_{\gamma=0}^{\infty}\Big(\gamma+\frac{p-3}{p-1}\Big)\frac{1}{1+p^\gamma m^2|(\xi,\xi)|_p} - 2\Big(1-\frac{1}{p}\Big)\frac{1}{p+m^2|(\xi,\xi)|_p} + \frac{1}{p^2+m^2|(\xi,\xi)|_p}$$

$$= \sum_{\gamma=0}^{\infty}(\gamma+1)\Big(\frac{1}{1+p^\gamma m^2|(\xi,\xi)|_p} - \frac{2}{p+p^\gamma m^2|(\xi,\xi)|_p} + \frac{1}{p^2+p^\gamma m^2|(\xi,\xi)|_p}\Big), \qquad p\equiv 1 \pmod 4 \text{ [9]}. \tag{14.16}$$

$$\sim -\frac{p^4}{(p+1)^2}\,m^{-4}|(\xi,\xi)|_p^{-2}, |(\xi,\xi)|_p\to\infty, \qquad p\equiv 1 \pmod 4 \text{ [9]}. \tag{14.17}$$

$$\int |x|_p^{\alpha-1}|1-x|_p^{\beta-1}|x-y|_p^{\gamma}|y|_p^{\alpha'-1}|1-y|_p^{\beta'-1}\,d_px\,d_py$$

$$= \Gamma_p(\gamma)\int |t|_p^{2-\alpha-\beta-\alpha'-\beta'}B_p(t;\alpha,\beta)B_p(-t;\alpha',\beta')\,d_pt$$

$$
\begin{aligned}
&= B_p(\alpha,\beta)B_p(\alpha',\beta') + B_p(\alpha,\beta)B_p(\gamma,\alpha'+\beta'-1)\\
&\quad + B_p(\alpha',\beta')B_p(\gamma,\alpha+\beta-1) + B_p(\alpha+\beta-1,\alpha'+\beta'-1)\\
&\quad \times B_p(\gamma,3-\alpha-\beta-\alpha'-\beta') - B_p(\alpha,\alpha')B_p(\gamma,\alpha+\alpha')\\
&\quad - B_p(\beta,\beta')B_p(\gamma,\beta+\beta')\\
&\quad + \Gamma_p(\gamma)p^{-\gamma}\Big\{[\Gamma_p(\alpha+\beta-1)p^{1-\alpha-\beta} + B_p(\alpha,\beta)]\\
&\quad \times [\Gamma_p(\alpha'+\beta'-1)p^{1-\alpha'-\beta'} + B_p(\alpha',\beta')]\\
&\quad - [\Gamma_p(\alpha)p^{-\alpha} + \Gamma_p(\beta)p^{-\beta}][\Gamma_p(\alpha')p^{-\alpha'} + \Gamma_p(\beta')p^{-\beta'}]\Big\},\\
&\quad \operatorname{Re}\alpha>0,\ \operatorname{Re}\beta>0,\ \operatorname{Re}\gamma>0,\ \operatorname{Re}\alpha'>0,\ \operatorname{Re}\beta'>0. \qquad (14.18)
\end{aligned}
$$

Здесь

$$B_p(t;\alpha,\beta) = \int |x|_p^{\alpha-1}|t-x|_p^{\beta-1}\chi_p(x)\,d_px.$$

Ниже в формулах (14.19)–(14.29) используются обозначения для поля $\mathbb{Q}_p(\sqrt{d}\,)$, $d\notin\mathbb{Q}_p^{\times 2}$ (см. § 9). В частности (см. (9.2) и (9.6)),

$$B_\gamma^2 = [z\in\mathbb{Q}_p(\sqrt{d}\,) : |z\bar z|_p\leqslant q^\gamma]; \qquad \alpha_k = \frac{2k\pi i}{\ln q}, \quad k\in Z.$$

$$\int_{B_0^2} d_pz = 1. \qquad (14.19)$$

$$\int_{B_0^2} |z\bar z|_p^{\alpha-1}\,d_pz = \frac{1-q^{-1}}{1-q^{-\alpha}}, \qquad \operatorname{Re}\alpha>0. \qquad (14.20)$$

$$\int_{B_\gamma^2} |z\bar z|_p^{\alpha-1}\,d_pz = \frac{1-q^{-1}}{1-q^{-\alpha}}\,q^{\alpha\gamma}, \qquad \operatorname{Re}\alpha>0. \qquad (14.21)$$

$$\int_{B_0^2} f(z\bar z)\,d_pz = \frac{1}{C_{p,d}}\int_{B_0} f(x)\theta_d^+(x)\,d_px, \qquad p\neq 2\ [11], \qquad (14.22)$$

где величина $C_{p,d}$ определена в (9.16) и (9.17).

$$
\begin{aligned}
&\delta\sqrt{|4d|_p}\int |z\bar z|_p^{\alpha-1}\chi_p(z\zeta+\bar z\bar\zeta)\,d_pz, \qquad \operatorname{Re}\alpha>0,\\
&\quad = \Gamma_{p,d}(\alpha)|\zeta\bar\zeta|_p^{-\alpha}, \qquad \zeta\neq 0\ [3]. \qquad (14.23)\\
&\quad = \Gamma_{p,d}(\alpha), \qquad \zeta = 1. \qquad (14.24)
\end{aligned}
$$

$$\delta\sqrt{|4d|_p}\int_{B_\gamma^2}|z\bar z|_p^{\alpha-1}\chi_p(z+\bar z)\,d_pz=\Gamma_{p,d}(\alpha),$$
$$\operatorname{Re}\alpha>0,\quad \gamma\geqslant 1\ [3]. \tag{14.25}$$

$$\int|\zeta\bar\zeta|_p^{\alpha-1}|(z-\zeta)(\bar z-\bar\zeta)|_p^{\beta-1}\,d_p\zeta,$$
$$\operatorname{Re}\alpha>0,\quad \operatorname{Re}\beta>0,\quad \operatorname{Re}(\alpha+\beta)<1,$$
$$=B_q(\alpha,\beta)|z\bar z|_p^{\alpha+\beta-1},\qquad z\neq 0\ [3]. \tag{14.26}$$
$$=B_q(\alpha,\beta),\qquad z=1. \tag{14.27}$$

$$\int\chi_p(\xi z\bar z)\,d_pz,\qquad \xi\neq 0,\quad p\neq 2,$$
$$=\frac{\operatorname{sgn}_{p,d}\xi}{|\xi|_p},\qquad |d|_p=1,\quad d\notin\mathbb{Q}_p^{\times 2}\ [11], \tag{14.28}$$
$$=\pm\sqrt{p\operatorname{sgn}_{p,d}(-1)}\,\frac{\operatorname{sgn}_{p,d}\xi}{|\xi|_p},\qquad |d|_p=\frac{1}{p}\ [11], \tag{14.29}$$

$$\int_{B_\gamma^2}\chi_p(z\zeta+\bar z\bar\zeta)=q^\gamma\Omega(q^{\gamma-r}|\zeta\bar\zeta|_p)\ [8]. \tag{14.30}$$

§ 15. n-переменных

$$\int_{B_0^n}d_p^nx=1. \tag{15.1}$$

$$\int_{S_0^n}d_p^nx=1-p^{-n}. \tag{15.2}$$

$$\int_{B_\gamma^n}d_p^nx=p^{n\gamma}. \tag{15.3}$$

$$\int_{S_\gamma^n}d_p^nx=(1-p^{-n})p^{n\gamma}. \tag{15.4}$$

$$\int_{B_\gamma^n}f(|x|_p)\,d_p^nx=(1-p^{-n})\sum_{k=-\infty}^{\gamma}p^{nk}f(p^k). \tag{15.5}$$

$$\int f(|x|_p)\,d_p^nx=(1-p^{-n})\sum_{k=-\infty}^{\infty}p^{nk}f(p^k). \tag{15.6}$$

$$\int_{B_\gamma^n} |x|_p^{\alpha-n}\, d_p^n x = \frac{1-p^{-n}}{1-p^{-\alpha}}\, p^{\alpha\gamma}, \qquad \operatorname{Re}\alpha > 0. \tag{15.7}$$

$$\int_{S_\gamma^n} |x|_p^{\alpha-n}\, d_p^n x = (1-p^{-n})\, p^{\alpha\gamma}. \tag{15.8}$$

$$\int_{|x|_p > p^\gamma} |x|_p^{\alpha-n}\, d_p^n x = -\frac{1-p^{-n}}{1-p^{-\alpha}}\, p^{\gamma\alpha}, \qquad \operatorname{Re}\alpha < 0. \tag{15.9}$$

$$\int_{S_\gamma^n} \chi_p((\xi,x))\, d_p^n x = (1-p^{-n})\, p^{\gamma n}\Omega(p^\gamma|\xi|_p)$$
$$-p^{(\gamma-1)n}\delta(|\xi|_p - p^{1-\gamma}) \text{ [26], [3]}. \tag{15.10}$$

$$\int_{B_\gamma^n} \chi_p((\xi,x))\, d_p^n x = p^{\gamma n}\Omega(p^\gamma|\xi|_p) \text{ [26], [3]}. \tag{15.11}$$

$$\int_{B_\gamma^n} |(x,x)|_p^{\alpha-n/2}\chi_p((\xi,x))\, d_p^n x, \qquad |(\xi,\xi)|_p > p^{-\gamma}, \quad \operatorname{Re}\alpha > 0,$$
$$= \Gamma_p\left(\alpha - \frac{n}{2} + 1\right)\Gamma_p(\alpha)|(\xi,\xi)|_p^{-\alpha}, \qquad n \equiv 0 \pmod 4,$$
$$p \neq 2 \text{ или } n \equiv 2 \pmod 4, \quad p \equiv 1 \pmod 4 \text{ [10]}. \tag{15.12}$$
$$= (-1)^{\gamma((\xi,\xi))}\Gamma_p\left(\alpha - \frac{n}{2} + 1\right)\widetilde{\Gamma}_p(\alpha)|(\xi,\xi)|_p^{-\alpha},$$
$$n \equiv 2 \pmod 4, \quad p \equiv 3 \pmod 4 \text{ [10]}. \tag{15.13}$$

$$\int |(x,x)|_p^{\alpha-n/2}\chi_p((\xi,x))\, d_p^n, \qquad (\xi,\xi) \neq 0, \quad \operatorname{Re}\alpha > 0,$$
$$= \Gamma_p\left(\alpha - \frac{n}{2} + 1\right)\Gamma_p(\alpha)|(\xi,\xi)|_p^{-\alpha}, \qquad n \equiv 0 \pmod 4, \quad p \neq 2$$
$$\text{или } n \equiv 2 \pmod 4, \quad p \equiv 1 \pmod 4 \text{ [10]}. \tag{15.14}$$
$$= (-1)^{\gamma((\xi,\xi))}\Gamma_p\left(\alpha - \frac{n}{2} + 1\right)\widetilde{\Gamma}_p(\alpha)|(\xi,\xi)|_p^{-\alpha},$$
$$n \equiv 2 \pmod 4, \quad p \equiv 3 \pmod 4 \text{ [10]}. \tag{15.15}$$

$$\int_{B_\gamma^n} |x|_p^{\alpha-n}\chi_p(x_1)\, d_p^n x = \Gamma_p^{(n)}(\alpha), \qquad \operatorname{Re}\alpha > 0, \quad \gamma \geqslant 1. \tag{15.16}$$

$$\int |x|_p^{\alpha-n}\chi_p(x_1)\, d_p^n x = \Gamma_p^{(n)}(\alpha), \qquad \operatorname{Re}\alpha > 0. \tag{15.17}$$

$$\int |x|_p^{\alpha-n}\chi_p((\xi,x))\,d_p^n x = \Gamma_p^{(n)}(\alpha)|\xi|_p^{-\alpha}, \quad \operatorname{Re}\alpha > 0, \quad \xi \neq 0. \tag{15.18}$$

$$\int |x,m|_p^{\alpha-n}\chi_p((\xi,x))\,d_p^n x = \Gamma_p^{(n)}(\alpha)\big(|\xi|_p^{-\alpha} - |pm|_p^{\alpha}\big)\Omega(|m\xi|_p),$$
$$m \neq 0\ [1], [17]. \tag{15.19}$$

$$\int |x,1|_p^{-\alpha}\chi_p((\xi,x))\,d_p^n x = \Gamma_p^{(n)}(n-\alpha)\big(|\xi|_p^{\alpha-n} - p^{\alpha-n}\big)\Omega(|\xi|_p)$$
$$\equiv J_p^{\alpha}(\xi), \qquad \operatorname{Re}\alpha > n. \tag{15.20}$$

Определим функцию $J_p^{\alpha}(\xi)$ при $\operatorname{Re}\alpha \leqslant n$ как мероморфное продолжение с области $\operatorname{Re}\alpha > n$. В частности,

$$\lim_{\substack{\alpha\to n,\\ \alpha>n}} J_p^{\alpha}(\xi) = J_p^n(\xi) = (1-p^{-n})\left(1 - \frac{\ln|\xi|_p}{\ln p}\right)\Omega(|\xi|_p), \qquad \alpha = n. \tag{15.21}$$

$$\int J_p^{\alpha}(\xi)J_p^{\beta}(x-\xi)\,d_p^n\xi = J_p^{\alpha} * J_p^{\beta} = J_p^{\alpha+\beta}, \qquad \alpha,\beta \in \mathbb{C}. \tag{15.22}$$

$$\int |x|_p^{\alpha-n}|\varepsilon - x|_p^{\beta-n}\,d_p^n x = B_p^{(n)}(\alpha,\beta),$$
$$\operatorname{Re}\alpha > 0, \quad \operatorname{Re}\beta > 0, \quad \operatorname{Re}(\alpha+\beta) < n, \quad |\varepsilon|_p = 1. \tag{15.23}$$

$$\int |y|_p^{\alpha-n}|x-y|_p^{\beta-n}\,d_p^n y = B_p^{(n)}(\alpha,\beta)|x|_p^{\alpha+\beta-n},$$
$$\operatorname{Re}\alpha > 0, \quad \operatorname{Re}\beta > 0, \quad \operatorname{Re}(\alpha+\beta) < n\ [1], [17]. \tag{15.24}$$

$$\int |y,m|_p^{\alpha-n}|x-y,m|_p^{\beta-n}\,d_p^n y = B_p^{(n)}(\alpha,\beta)|x,m|_p^{\alpha+\beta-n}$$
$$- \Gamma_p^{(n)}(\alpha)|pm|_p^{\alpha}|x,m|_p^{\beta-n} - \Gamma_p^{(n)}(\alpha)|pm|_p^{\beta}|x,m|_p^{\alpha-n},$$
$$\operatorname{Re}(\alpha+\beta) < n, \quad m \neq 0\ [17]. \tag{15.25}$$

$$\int_{\mathbb{Q}_p^{n-1}} \chi_p\left\{\sum_{k=0}^{n-1}\left(\frac{2x_kx_{k+1}}{\sin t_k} - \frac{x_k^2+x_{k+1}^2}{\operatorname{tg} t_k}\right)\right\} d_px_1\,d_px_2\ldots d_px_{n-1}$$
$$= \frac{\lambda_p(T_n)}{\sqrt{|T_n|_p}}\prod_{k=0}^{n-1}\frac{\sqrt{|t_k|_p}}{\lambda_p(t_k)}\,\chi_p\left(\frac{2x_0x_n}{\sin T_n} - \frac{x^2+x_n^2}{\operatorname{tg} T_n}\right), \qquad n = 2,3,\ldots,$$
$$p \neq 2, \quad |t_k|_p \leqslant \frac{1}{p}, \quad T_n = \sum_{k=0}^{n-1} t_k\ [17]. \tag{15.26}$$

Пусть $x_i \in \mathbb{Q}_p^n,\ |x_i|_p = 1,\ i = 1, 2, \dots, k < p^n$ и $|x_i - x_j|_p = 1$, $i, j = 1, 2, \dots,\ i \neq j$. Обозначим

$$D_k^n = \big[x \in \mathbb{Q}_p^n : |x - x_i|_p = 1,\ i = 1, 2, \dots, k\big].$$

Тогда

$$\int_{D_k^n} d_p^n x = 1 - kp^{-n}, \qquad k \leqslant p^n, \quad p \neq 2 \text{ [18]}. \tag{15.27}$$

Пусть $G_k^n = \big[(x_1, x_2, \dots, x_k) \in \mathbb{Q}_p^{kn} : |x_i|_p = 1,\ |x_i - x_j|_p = 1,\ i, j = 1, 2, \dots, k,\ i \neq j\big]$. Тогда

$$\int_{G_k^n} d_p^n x_1\, d_p^n x_2 \dots d_p^n x_k = \prod_{\ell=1}^{k} (1 - \ell p^{-n}) = c_{p,k}^n,$$
$$k \leqslant p^n, \quad p \neq 2 \text{ [18]}. \tag{15.28}$$

Пусть $x_0 \in \mathbb{Q}_p^n,\ |x_0|_p = 1$ и $G_k^n(x_0) = \big[(x_1, \dots, x_k) \in \mathbb{Q}_p^{kn} : |x_i|_p = 1,\ i = 0, 1, \dots, k,\ |x_i - x_j|_p = 1,\ i, j = 0, 1, \dots, k,\ i \neq j\big]$,

$$\int_{G_k^n(x_0)} d_p^n x_1\, d_p^n x_2 \dots d_p^n x_k = \frac{1 - (k+1)p^{-n}}{1 - p^{-n}}\, c_{k,p}^n,$$
$$k + 1 \leqslant p^n, \quad p \neq 2 \text{ [18]}. \tag{15.29}$$

Интеграл Миссарова–Лернера [26], [31]. Пусть G – некоторый связный конечный граф, $V = V(G)$ и $L = L(G)$ – множества вершин и ребер его соответственно. Каждой линии $l \in L$ сопоставим комплексное число a_l и обозначим $a = \{a_l,\ l \in L\}$, и каждой вершине $v \in V$ сопоставим n-мерный p-адический вектор $x_v = (x_{v1}, x_{v2}, \dots, x_{vn}) \in \mathbb{Q}_p^n$. На множестве вершин V введем иерархию A следующим образом. Иерархия A – это семейство подмножеств множества V, таких что: 1) $V \in A$, 2) $v \in A$ для всех $v \in V$ и 3) для любой пары $V' \in A,\ V'' \in A$ либо $V' \cap V'' = \varnothing$, либо $V' \subset V''$, либо $V'' \subset V'$. Для любого $V' \in A,\ V' \neq V$, обозначим через $\theta(V')$ минимальное подмножество в A, содержащее V', но не совпадающее с ним, и пусть $K(V') = [V'' \in A : \theta(V'') = V']$. Рассматриваются только такие иерархии A, для которых

$$1 < |K(V')| \leqslant p^n, \quad V' \in A', \qquad \text{где } A' = [V' \in A : |V'| > 1].$$

Обозначим

$$a(V') = \sum_{l \in L(G(V'))} a_l, \qquad \beta(V') = a(V') + n(|V'| - 1),$$

где $L(G(V'))$ – множество ребер l графа G, начало $i(l)$ и конец $f(l)$ которых лежат в $V' \subset V = V(G)$. При условии $\beta(V') > 0$, $V' \in A'$, справедливо равенство

$$F_G(a) \equiv \int_{Z_p^{n|V|}} \prod_{l\in L} |x_{i(l)} - x_{f(l)}|_p^{a_l} \prod_{v\in V} d_p^n x_v$$
$$= p^{a(V)} \sum_A \prod_{V'\in A'} \frac{1}{p^{\beta(V')} - 1} \frac{(p^n-1)!}{(p^n - |K(V')|)!},$$

где суммирование проводится по всем иерархиям A. (Символ $|V|$ обозначает число элементов множества V.) Вычисление различных фейнмановских интегралов сводится к вычислению интеграла $F_G(a)$ [26].

§ 16. Интегралы и свертки обобщенных функций

Интегралом (см. § 6) *обобщенной функции* $f \in \mathscr{S}'(\mathscr{O})$ по открыто-замкнутому множеству $D \in \mathscr{O} \in \mathbb{Q}_p^n$ называется предел, если он существует,

$$G\!\int_D f(x)\, d_p^n x = \lim_{k\to\infty} (f\theta_D, \Omega_k).$$

Интегралы обобщенных функций содержатся также в §§ 12–15 и § 17.

$$G\!\int_{B_0^n} d_p^n x = 1. \tag{16.1}$$

$$G\!\int_{B_\gamma^n} d_p^n x = p^{\gamma n}. \tag{16.2}$$

$$G\!\int_{S_\gamma^n} d_p^n x = (1 - p^{-n})\, p^{\gamma n}. \tag{16.3}$$

$$G\!\int f(x)\, d_p^n x = \int f(x)\, d_p^n x, \qquad f \in \mathscr{L}^1. \tag{16.4}$$

$$G\!\int f(x)\, d_p^n x = \lim_{\gamma\to\infty} \int_{B_\gamma^n} f(x)\, d_p^n x, \qquad f \in \mathscr{L}^1_{\mathrm{loc}}. \tag{16.5}$$

$$G\int_D f(x)\,d_p^n x = \int_D f(x)\,d_p^n x, \qquad f \in \mathscr{L}^1(D). \tag{16.6}$$

$$G\int f(x)\,d_p^n x = \lim_{\gamma\to\infty} \int_{B_\gamma^n} f(x)\,d_p^n x, \qquad f \in \mathscr{L}^p. \tag{16.7}$$

$$G\int f(x)\,d_p^n x = (f, \Omega_N), \qquad f \in \mathscr{S}', \quad \operatorname{spt} \in B_N^n. \tag{16.8}$$

$$G\int_D f(x)\,d_p^n x = (f, \theta_D), \qquad f \in \mathscr{S}'(\mathscr{O}), \tag{16.9}$$

где D – открытый компакт в $\mathscr{O}$.

$$G\int f(x)\,d_p^n x = \lim_{\gamma\to\infty} (f, \Omega_\gamma), \qquad f \in \mathscr{S}'. \tag{16.10}$$

$$G\int \delta(x)\,d_p^n x = 1. \tag{16.11}$$

$$G\int_{S_\gamma} \pi(x)\,d_p x = 0, \qquad \pi \not\equiv 1, \quad \alpha \in \mathbb{C} \quad \text{(ср. (11.40))}. \tag{16.12}$$

$$G\int_{B_\gamma} |x|_p^{\alpha-1}\pi(x)\,d_p x = 0, \qquad \pi \not\equiv 1, \quad \alpha \in \mathbb{C}. \tag{16.13}$$

$$G\int |x|_p^{\alpha-1}\pi(x)\,d_p x = 0, \qquad \pi \not\equiv 1, \quad \alpha \in \mathbb{C}. \tag{16.14}$$

$$G\int_{B_\gamma} |x|_p^{\alpha-1}\,d_p x = \frac{1-p^{-1}}{1-p^{-\alpha}}\,p^{\alpha\gamma} \quad \text{(ср. (11.18))}. \tag{16.15}$$

$$G\int |x|_p^{\alpha-1}\,d_p x = 0, \qquad \alpha \neq \alpha_k, \quad k \in Z \quad \text{(ср. (8.3$'$))}. \tag{16.16}$$

$$G\int_{S_\gamma} |x-a|_p^{\alpha-1}\,d_p x = \frac{p-2+p^{-\alpha}}{p(1-p^{-\alpha})}\,|a|_p^\alpha, \quad |a|_p = p^\gamma \quad \text{(ср. (11.20))}. \tag{16.17}$$

$$G\int_{B_\gamma} |x^2+a^2|_p^{(\alpha-1)/2}\,d_p x = \frac{1-p^{\alpha-1}}{1-p^\alpha}\,|a|_p^\alpha + \frac{1-p^{-1}}{1-p^{-\alpha}}\,p^{\alpha\gamma}, \quad 0 \neq |a|_p \leqslant p^\gamma, \quad p \equiv 3 \pmod 4 \quad \text{(ср. (11.28))}. \tag{16.18}$$

$$G\!\int |x^2+a^2|_p^{(\alpha-1)/2}\,d_px=\frac{1-p^{\alpha-1}}{1-p^{\alpha}}\,|a|_p^{\alpha},$$
$$a\neq 0,\quad p\equiv 3\ (\mathrm{mod}\ 4)\quad (\text{ ср. (11.30)}). \tag{16.19}$$

$$G\!\int_{B_\gamma} |x^2+a^2|_p^{\alpha-1}\,d_px$$
$$=\left[1-\frac{2}{p}+\left(1-\frac{1}{p}\right)\left(\frac{2}{p^{\alpha}-1}+\frac{1}{p^{1-2\alpha}-1}\right)\right]|a|_p^{2\alpha-1}$$
$$-\left(1-\frac{1}{p}\right)\frac{p^{(2\alpha-1)\gamma}}{1-p^{2\alpha-1}}\,,$$
$$0\neq |a|_p\leqslant p^{\gamma},\quad p\equiv 1\ (\mathrm{mod}\ 4). \tag{16.20}$$

$$G\!\int |x^2+a^2|_p^{\alpha-1}\,d_px=\left[1-\frac{2}{p}+\left(1-\frac{1}{p}\right)\right.$$
$$\left.\times\left(\frac{2}{p^{\alpha}-1}+\frac{1}{p^{1-2\alpha}-1}\right)\right]|a|_p^{2\alpha-1},$$
$$a\neq 0,\quad p\equiv 1\ (\mathrm{mod}\ 4)\quad (\text{ср. (11.31)}). \tag{16.21}$$

$$G\!\int_{S_0} |x^2+1|_p^{\alpha-1}\,d_px=1-\frac{3}{p}-2\frac{1-p^{-1}}{1-p^{\alpha}}\,,$$
$$\alpha\neq\alpha_k,\quad k\in Z,\quad p\equiv 1\ (\mathrm{mod}\ 4)\quad (\text{ср. (11.32)}). \tag{16.22}$$
$$|x|_p^{\alpha-1}*|x|_p^{\beta-1}=B_p(\alpha,\beta)|x|_p^{\alpha+\beta-1}. \tag{16.23}$$

$$G\!\int |x|_p^{\alpha-1}|1-x|_p^{\beta-1}\,d_px=B_p(\alpha,\beta),$$

$$|x,m|_p^{\alpha-1}*|x,m|_p^{\beta-1}=B_p(\alpha,\beta)|x,m|_p^{\alpha+\beta-1}$$
$$-\Gamma_p(\alpha)|pm|_p^{\alpha}|x,m|_p^{\beta-1}-\Gamma_p(\beta)|pm|_p^{\beta}|x,m|_p^{\alpha-1}, \tag{16.24}$$
$$m\neq 0\quad (\text{ср. (11.68)}). \tag{16.25}$$

$$G\!\int |x,m|_p^{\alpha-1}\chi_p(\xi x)\,d_px=\Gamma_p(\alpha)(|\xi|_p^{-\alpha}-|pm|_p^{\alpha})\Omega(|m\xi|_p),$$
$$m\neq 0,\quad \alpha\in\mathbb{C}\quad (\text{см. (12.48)}). \tag{16.26}$$

$$G\!\int_{S_\gamma}\delta(x_0-k)\,d_px=p^{\gamma-1},\quad k=1,2,\ldots,p-1\ \ (\text{см. (11.33)}). \tag{16.27}$$

$$G\!\int_{S_\gamma}[1-\delta(x_0-k)]\,d_px=\left(1-\frac{2}{p}\right)p^{\gamma},$$
$$k=1,2,\ldots,p-1\quad (\text{см. (11.34)}). \tag{16.28}$$

$$G\!\!\int_{S_\gamma} \delta(x_n - k)\, d_p x = \left(1 - \frac{1}{p}\right) p^{\gamma-1},$$
$$k = 0, 1, \ldots, p-1, \quad n \in Z_+ \quad \text{(см. (11.35))}. \tag{16.29}$$

$$G\!\!\int_{S_\gamma} [1 - \delta(x_n - k)]\, d_p x = \left(1 - \frac{1}{p}\right)^2 p^{\gamma},$$
$$k = 0, 1, \ldots, p-1, \quad n \in Z_+ \quad \text{(см. (11.36))}. \tag{16.30}$$

$$G\!\!\int_{S_\gamma} \delta(x_0 - k_0) \prod_{l=1}^{n} \delta(x_l - k_l) = p^{\gamma-n-1}, \qquad k_l = 0, 1, \ldots, p-1,$$
$$k_0 \neq 0, \quad n = 0, 1, \ldots \quad \text{(см. (11.37))}. \tag{16.31}$$

$$G\!\!\int_{S_\gamma} \Big[1 - \delta(x_0 - k_0) \prod_{l=1}^{n} \delta(x_l - k_l)\Big] = (1 - p^{-1} - p^{-n-1}) p^{\gamma},$$
$$k_l = 0, 1, \ldots, p-1, \quad k_0 \neq 0, \tag{16.32}$$
$$n = 0, 1, \ldots \quad \text{(см. (11.38))}.$$

$$G\!\!\int_{S_\gamma} \left(\prod_{l=1}^{n} \delta(x_l - k_l)\right) d_p x = \left(1 - \frac{1}{p}\right) p^{\gamma-n},$$
$$k_l = 0, 1, \ldots, p-1, \quad n \in Z_+. \tag{16.33}$$

$$G\!\!\int_{S_\gamma} \Big[1 - \prod_{l=1}^{n} \delta(x_{i_l} - k_{i_l})\Big]\, d_p x = \left(1 - \frac{1}{p}\right)(1 - p^{-n})\, p^{\gamma},$$
$$k_l = 0, 1, \ldots, p-1, \quad n \in Z_+. \tag{16.34}$$

$$G\!\!\int_{S_\gamma^n} |x|_p^{\alpha-n}\, d_p^n x = \left(1 - \frac{1}{p^{-n}}\right) p^{\alpha\gamma}, \qquad \alpha \in \mathbb{C} \quad \text{(см. (15.8))}. \tag{16.35}$$

$$G\!\!\int_{B_\gamma^n} |x|_p^{\alpha-n}\, d_p^n x = \frac{1 - p^{-n}}{1 - p^{-\alpha}}\, p^{\alpha\gamma} \quad \text{(ср. (15.7))}. \tag{16.36}$$

$$G\!\!\int |x|_p^{\alpha-n}\, d_p^n x = 0, \qquad n \in Z_+. \tag{16.37}$$

$$G\!\!\int_{B_\gamma^n} |(x,x)|_p^{\alpha-n/2} \chi_p((\xi,x))\, d_p^n x, \qquad |(\xi,\xi)|_p > p^{\gamma},$$
$$= \Gamma_p\left(\alpha - \frac{n}{2} + 1\right) \Gamma_p(\alpha) |(\xi,\xi)|_p^{-\alpha}, \quad n \equiv 0 \pmod 4, \quad p \neq 2$$
$$\text{или} \quad n \equiv 2 \pmod 4, \quad p \equiv 1 \pmod 4. \tag{16.38}$$

$$= (-1)^{\gamma((\xi,\xi))}\Gamma_p\left(\alpha-\frac{n}{2}+1\right)\widetilde{\Gamma}_p(\alpha)|(\xi,\xi)|_p^{-\alpha},$$
$$\alpha \neq \left\{\alpha_k - \frac{\pi i}{\ln p},\ \alpha_k+\frac{n}{2}-1,\ k\in Z\right\},$$
$$n\equiv 2 \pmod 4, \quad p\equiv 3 \pmod 4 \quad \text{(ср. (15.13))}. \tag{16.39}$$

$$= \Gamma_p^2(\alpha)|(\xi,\xi)|_p^{-\alpha}, \qquad n=2, \quad p\equiv 1 \pmod 4. \tag{16.40}$$

$$= \Gamma_p(\alpha)\widetilde{\Gamma}_p(\alpha)|(\xi,\xi)|_p^{-\alpha},$$
$$n=2, \quad p\equiv 3 \pmod 4 \quad \text{(см. (14.9))}. \tag{16.41}$$

$$G\int |(x,x)|_p^{\alpha-n/2}\chi_p((\xi,x))\,d_p^n x, \qquad (\xi,\xi)\neq 0,$$

$$= \Gamma_p\left(\alpha-\frac{n}{2}+1\right)\Gamma_p(\alpha)|(\xi,\xi)|_p^{-\alpha}, \quad n\equiv 0 \pmod 4, \quad p\neq 2$$
$$\text{или}\ \ n\equiv 2 \pmod 4, \quad p\equiv 1 \pmod 4. \tag{16.42}$$

$$= (-1)^{\gamma((\xi,\xi))}\Gamma_p\left(\alpha-\frac{n}{2}+1\right)\widetilde{\Gamma}_p(\alpha)|(\xi,\xi)|_p^{-\alpha},$$
$$n\equiv 2 \pmod 4, \quad p\equiv 3 \pmod 4 \quad \text{(см. (15.15))}. \tag{16.43}$$

$$= \Gamma_p^2(\alpha)|(\xi,\xi)|_p^{-\alpha},$$
$$n=2, \quad p\equiv 1 \pmod 4 \quad \text{(ср. (14.10))}. \tag{16.44}$$

$$= \Gamma_p(\alpha)\widetilde{\Gamma}_p(\alpha)|(\xi,\xi)|_p^{-\alpha},$$
$$n=2, \quad p\equiv 3 \pmod 4 \quad \text{(ср. (14.11))}. \tag{16.45}$$

$$G\int_{B_\gamma^n} |x|_p^{\alpha-n}\chi_p(x_1)\,d_p^n x = \Gamma_p^{(n)}(\alpha), \quad \gamma\in Z_+. \tag{16.46}$$

$$G\int |x|_p^{\alpha-n}\chi_p(x_1)\,d_p^n x = \Gamma_p^{(n)}(\alpha). \tag{16.47}$$

$$G\int |x|_p^{\alpha-n}\chi_p\big((\xi,x)\big)\,d_p^n x = \Gamma_p^{(n)}(\alpha)|\xi|_p^{-\alpha}, \qquad \xi\neq 0 \quad \text{(ср. (15.18))}. \tag{16.48}$$

$$|x|_p^{\alpha-n} * |x|_p^{\beta-n} = B_p^{(n)}(\alpha,\beta)|x|_p^{\alpha+\beta-n}. \tag{16.49}$$

$$G\int |x,m|_p^{\alpha-n}\chi_p\big((\xi,x)\big)\,d_p^n x = \Gamma_p^{(n)}(\alpha)\big(|\xi|_p^{-\alpha}-|pm|_p^{\alpha}\big)\Omega(|m\xi|_p),$$
$$m\neq 0, \quad \alpha\in\mathbb{C} \quad \text{(ср. (15.19))}. \tag{16.50}$$

$$G\int |x,1|_p^{-\alpha}\chi_p\big((\xi,x)\big)\,d_p^n x$$

$$= \Gamma_p^{(n)}(n-\alpha)\big(|\xi|_p^{\alpha-n} - p^{\alpha-n}\big)\Omega(|\xi|_p), \qquad \alpha\in\mathbb{C}. \tag{16.51}$$

$$|x,m|_p^{\alpha-n} * |x,m|_p^{\beta-n} = B_p^{(n)}(\alpha,\beta)|x,m|_p^{\alpha+\beta-n}$$

$$= -\,\Gamma_p^{(n)}(\alpha)|pm|_p^{\alpha}\,|x,m|_p^{\beta-n} - \Gamma_p^{(n)}(\beta)|pm|_p^{\beta}\,|x,m|_p^{\alpha-n},$$

$$m\neq 0 \quad \text{(ср. (15.25))}. \tag{16.52}$$

$$(D^\alpha\varphi)(x) = (f_{-\alpha}*\varphi)(x), \qquad \varphi\in\mathscr{S},$$

$$= \Gamma_p^{-1}(-\alpha)\int \frac{\varphi(y)-\varphi(x)}{|x-y|_p^{\alpha+1}}\,d_p y, \qquad \operatorname{Re}\alpha>0. \tag{16.53}$$

$$= (1-p^{-\alpha-1})^{-1}\int [\varphi(x+y)-\varphi(x+y/p)]|y|_p^{-\alpha-1}\,d_p y. \tag{16.54}$$

$$= -\frac{p-1}{p\ln p}\int \varphi(y)\ln|x-y|_p\,d_p y, \qquad \int f(y)\,d_p y = 0,$$

$$\alpha=\alpha_k-1, \quad k\in Z. \tag{16.55}$$

$$= \varphi(x), \qquad \alpha=\alpha_k, \quad k\in Z. \tag{16.56}$$

$$= \int |\xi|_p^{\alpha}\widetilde{\varphi}(\xi)\chi_p(-\xi x)\,d_p\xi, \qquad \operatorname{Re}\alpha>-1. \tag{16.57}$$

$$= \int |\xi|_p^{\alpha}[\widetilde{\varphi}(\xi)\chi_p(-\xi x)-\widetilde{\varphi}(0)]\,d_p\xi, \qquad \operatorname{Re}\alpha<-1. \tag{16.58}$$

$$= \int_{Z_p} |\xi|_p^{-1}[\widetilde{\varphi}(\xi)\chi_p(-\xi x)-\widetilde{\varphi}(0)]\,d_p\xi + \frac{1}{p}\,\widetilde{\varphi}(0)$$

$$+ \int_{\mathbb{Q}_p\setminus Z_p} |\xi|_p^{-1}\widetilde{\varphi}(\xi)\chi_p(-\xi x)\,d_p\xi, \quad \alpha=\alpha_k-1,\ k\in Z. \tag{16.59}$$

$$D^\alpha\chi_p(ax) = |a|_p^{\alpha}\chi_p(ax), \qquad \alpha\in\mathbb{C}, \quad a\neq 0. \tag{16.60}$$

$$D^\alpha\Phi(x) = p^{\gamma\alpha}\Phi(x), \qquad \alpha\in\mathbb{R}\ [1], \tag{16.61}$$

$$\text{если } \Phi(x) = F\big[\delta\big(|\xi|_p-p^\gamma\big)f(\xi)\big], \qquad f\in\mathscr{S}.$$

$$D^\alpha\big[\delta\big(|x|_p-p^\gamma\big)\chi_p(ax^2)\big] = p^{\gamma\alpha}|2a|_p^{\alpha}\delta\big(|x|_p-p^\gamma\big)\,\chi_p(ax^2),$$

$$\alpha\in\mathbb{R}, \quad |2a|_p\leqslant p^{2-2\gamma}\ [1]. \tag{16.62}$$

$$D^\alpha\big[\eta(x_0)\delta\big(|x|_p-p^\gamma\big)\big] = p^{\alpha(1-\gamma)}\eta(x_0)\delta\big(|x|_p-p^\gamma\big),$$

$$\alpha\in\mathbb{R}, \quad p\neq 2, \quad \sum_{k=1}^{p-1}\eta(k)=0\ [4]. \tag{16.63}$$

$$(D^\alpha f)(x), \qquad f \in \mathscr{S}', \quad \operatorname{spt} f \in B_N, \quad |x|_p > p^N,$$
$$= \Gamma_p^{-1}(\alpha)|x|_p^{\alpha-1}(f, \Omega_N), \qquad \alpha \neq -1 \text{ [3]}. \tag{16.64}$$
$$= -\frac{p-1}{p \ln p} \ln |x|_p (f, \Omega_N), \qquad \alpha = -1 \text{ [3]}. \tag{16.65}$$

$$D^\alpha 1 = 0, \qquad \alpha > 0. \tag{16.66}$$

$$D^\alpha \delta(x-a) = f_{-\alpha}(x-a), \qquad \alpha \in \mathbb{C}, \quad a \in \mathbb{Q}_p. \tag{16.67}$$

$$D^\alpha \big[\delta\big(|x|_p - p^{\ell-N}\big)\, \delta(x_0 - j)\, \chi_p\big(\epsilon_\ell p^{\ell-2N} x^2\big)\big]$$
$$= p^{\alpha N} \delta\big(|x|_p - p^{\ell-N}\big)\, \delta(x_0 - j)\, \chi_p\big(\epsilon_\ell p^{\ell-2N} x^2\big), \qquad N \in Z,$$
$$p \neq 2, \quad \alpha > 0, \quad \ell = 2, 3, \ldots, \quad j = 1, 2, \ldots, p-1,$$
$$\epsilon_\ell = \varepsilon_0 + \varepsilon_1 p + \cdots + \varepsilon_{\ell-2},$$
$$\varepsilon_s = 0, 1, \ldots, p-1, \quad \varepsilon_0 \neq 0, \quad s = 0, 1, \ldots, \ell - 2 \text{ [4]}. \tag{16.68}$$

$$D^\alpha \big[\Omega\big(p^{N-1}|x|_p\big)\, \chi_p(j p^{-N} x)\big] = p^{\alpha N} \Omega\big(p^{N-1}|x|_p\big)\, \chi_p\big(j p^{-N} x\big),$$
$$N \in Z, \quad p \neq 2, \quad \alpha > 0, \quad j = 1, 2, \ldots, p-1 \text{ [4]}. \tag{16.69}$$

$$D^\alpha \big[\delta\big(|x|_2 - 2^{\ell+1-N}\big)\, \chi_2\big(\epsilon_\ell 2^{\ell-2N} x^2 + 2^{\ell-N-j} x\big)\big]$$
$$= 2^{\alpha N} \delta\big(|x|_2 - 2^{\ell+1-N}\big)\, \chi_2\big(\epsilon_\ell 2^{\ell-2N} x^2 + 2^{\ell-N-j} x\big),$$
$$N \in Z, \quad p = 2, \quad \alpha > 0, \quad \ell = 2, 3, \ldots, \quad j = 0, 1,$$
$$\epsilon_\ell = 1 + \varepsilon_1 2 + \cdots + \varepsilon_{\ell-2} 2^{\ell-2},$$
$$\varepsilon_s = 0, 1, s = 1, 2, \ldots, \ell - 2 \text{ [4]}. \tag{16.70}$$

$$D^\alpha \big[\Omega\big(2^N |x - j 2^{N-2}|_2\big) - \delta\big(|x - j 2^{N-2}|_2 - 2^{1-N}\big)\big]$$
$$= 2^{\alpha N} \big[\Omega\big(2^N |x - j 2^{N-2}|_2\big) - \delta\big(|x - j 2^{N-2}|_2 - 2^{1-N}\big)\big],$$
$$N \in Z, \quad p = 2, \quad \alpha > 0, \quad j = 0, 1 \text{ [4]}. \tag{16.71}$$

$$D^\alpha \Omega\big(p^{-\gamma}|x|_p\big) = \frac{p-1}{p^{\alpha+1}-1}\, p^{\alpha(1-\gamma)}, \qquad x \in B_\gamma, \quad \alpha > 0 \text{ [5]}. \tag{16.72}$$

$$D^\alpha \delta\big(|x|_p - p^\gamma\big) = \frac{p^\alpha + p - 2}{p^{\alpha+1}-1}\, p^{\alpha(1-\gamma)}, \quad x \in S_\gamma, \quad \alpha > 0 \text{ [5]}. \tag{16.73}$$

Пусть $\mathscr{K}(t, \tau)$ – вещественное симметричное ядро

$$\mathscr{K}(t,t) = 0, \qquad \mathscr{K}(t,\tau) = \rho\left(1 - \frac{1}{p}\right)^{-1} t^{-\alpha-1}, \qquad \tau < t,$$

$$\sigma = \frac{p^\alpha + p - 2}{p^{\alpha+1}-1}\, p^\alpha, \qquad \rho = -\Gamma_p^{-1}(-\alpha)\left(1 - \frac{1}{p}\right), \qquad \sigma + \rho = p^\alpha,$$

и функция $f \in \mathscr{L}^1_{\mathrm{loc}}$ такова, что

$$\int_{|x|_p>1} |f(x)||x|_p^{-\alpha-1}\,d_px < \infty.$$

Тогда

$$(D^\alpha f)(x) = -\int \mathscr{K}(|x|_p,|y|_p)f(y)\,d_py + \sigma|x|_p^{-\alpha}f(x),\quad \alpha>0\ [5]. \tag{16.74}$$

В нижеследующих формулах § 16 все интегралы

$$G\!\!\int f(z,\bar z)\,d_pz$$

понимаются по нормированной мере $d_pz = \delta^{-1}\,d_px\,d_py$, $z = x+\sqrt{d}\,y$, $\bar z = x-\sqrt{d}\,y$, поля $\mathbb{Q}_p(\sqrt{d})$, $d \notin \mathbb{Q}_p^{\times 2}$ (см. (9.2)). В частности,

$$B_\gamma^2 = [z \in \mathbb{Q}_p(\sqrt{d}\,) : |z\bar z|_p \leqslant q^\gamma].$$

$$G\!\!\int_{B_0^2} d_pz = 1. \tag{16.75}$$

$$G\!\!\int_{B_0^2} |z\bar z|_p^{\alpha-1}\,d_pz = \frac{1-q^{-1}}{1-q^{-\alpha}}\,. \tag{16.76}$$

$$G\!\!\int |z\bar z|_p^{\alpha-1}\,d_pz = 0. \tag{16.77}$$

$$G\!\!\int |z\bar z|_p^{\alpha-1}\chi_p(z+\bar z)\,d_pz = \frac{\Gamma_{p,d}(\alpha)}{\delta\sqrt{|4d|_p}}\,. \tag{16.78}$$

$$G\!\!\int_{B_1^2} |z\bar z|_p^{\alpha-1}\chi_p(z+\bar z)\,d_pz = \frac{\Gamma_{p,d}(\alpha)}{\delta\sqrt{|4d|_p}}\,, \tag{16.79}$$

$$|z\bar z|_p^{\alpha-1} * |z\bar z|_p^{\beta-1} = B_q(\alpha,\beta)|z\bar z|_p^{\alpha+\beta-1}. \tag{16.80}$$

$$G\!\!\int |z\bar z|_p^{\alpha-1}|(1-z)(1-\bar z)|_p^{\beta-1}\,d_pz = B_q(\alpha,\beta). \tag{16.81}$$

$$G\!\!\int \chi_p(\xi z\bar z)\,d_pz = \frac{\operatorname{sgn}_{p,d}\,\xi}{|\xi|_p} + \frac{1+p}{2p}\,\delta(\xi),$$
$$p\neq 2,\quad |d|_p = 1,\quad d\notin\mathbb{Q}_p^{\times 2}\ [11]. \tag{16.82}$$

$$G\int \chi_p(\xi z\bar{z})\,d_p z = \pm\sqrt{p\,\mathrm{sgn}_{p,d}\,(-1)}\,\frac{\mathrm{sgn}_{p,d}\,\xi}{|\xi|_p} + \delta(\xi),$$
$$p \neq 2, \quad |d|_p = \frac{1}{p}\ [11]. \tag{16.83}$$

§ 17. Таблица преобразований Фурье

Для взаимно однозначного соответствия между *прообразом* $f \in \mathscr{S}$ и его *образом* $\widetilde{f} \in \mathscr{S}$ – преобразованием Фурье f – будем использовать обозначение (см. § 7)

$$f(x) \Longleftrightarrow \widetilde{f}(\xi).$$

$$\omega_\gamma(x) \Longleftrightarrow \delta_\gamma(\xi). \tag{17.1}$$

$$\delta(x) \Longleftrightarrow 1(\xi). \tag{17.2}$$

$$f(Ax+b) \Longleftrightarrow |\det A|_p^{-1}\chi_p\big(-(A^{-1}b,\xi)\big)\widetilde{f}(\bar{A}'\xi),$$
$$\det A \neq 0, \quad b \in \mathbb{Q}_p^n. \tag{17.3}$$

$$f(x-b) \Longleftrightarrow \chi_p((b,\xi))\widetilde{f}(\xi), \qquad b \in \mathbb{Q}_p^n. \tag{17.4}$$

$$\breve{f}(x) \Longleftrightarrow \breve{\widetilde{f}}(\xi). \tag{17.5}$$

$$f(x) \Longleftrightarrow \int f(x)\chi_p((\xi,x))\,d_p^n x, \qquad f \in \mathscr{L}^1. \tag{17.6}$$

$$f(x) \Longleftrightarrow \lim_{k\to\infty}\int_{B_k^n} f(x)\chi_p((\xi,x))\,d_p^n x \ \text{ в } \ \mathscr{S}, \qquad f \in \mathscr{L}^1_{\mathrm{loc}}. \tag{17.7}$$

$$f(x) \Longleftrightarrow \lim_{k\to\infty}\int_{B_k^n} f(x)\chi_p((\xi,x))\,d_p^n x \ \text{ в } \ \mathscr{L}^2, \qquad f \in \mathscr{L}^2. \tag{17.8}$$

$$f(x) \Longleftrightarrow \big(f(x), \Omega_N(x)\chi_p((\xi,x))\big), \qquad \mathrm{spt}\, f \in B_N. \tag{17.9}$$

$$f * g \Longleftrightarrow \widetilde{f}\cdot\widetilde{g}. \tag{17.10}$$

$$f \cdot g \Longleftrightarrow \widetilde{f} * \widetilde{g}. \tag{17.11}$$

$$\delta\big(|x|_p - p^\gamma\big) \Longleftrightarrow \left(1-\frac{1}{p}\right)p^\gamma\Omega\big(p^\gamma|\xi|_p\big) - p^{\gamma-1}\delta\big(|\xi|_p - p^{1-\gamma}\big). \tag{17.12}$$

$$f\big(|x|_p\big)\Omega_\gamma\big(|x|_p\big) \Longleftrightarrow \left(1-\frac{1}{p}\right)\sum_{k=-\infty}^{\gamma} p^k f(p^k)\Omega\big(p^\gamma|\xi|_p\big)$$
$$+|\xi|_p^{-1}\left[\left(1-\frac{1}{p}\right)\sum_{k=0}^{\infty} p^{-\gamma} f\big(p^{-\gamma}|\xi|_p^{-1}\big) - f\big(p|\xi|_p^{-1}\big)\right]$$
$$\times\,\big[1-\Omega\big(p^\gamma|\xi|_p\big)\big]. \tag{17.13}$$

$$f(|x|_p) \Longleftrightarrow |\xi|_p^{-1}\left[\left(1-\frac{1}{p}\right)\sum_{k=0}^{\infty} p^{-\gamma} f\big(p^{-\gamma}|\xi|_p^{-1}\big) - f\big(p|\xi|_p^{-1}\big)\right]. \tag{17.14}$$

$$|x|_p^{\alpha-1} \Longleftrightarrow \Gamma_p(\alpha)|\xi|_p^{-\alpha}. \tag{17.15}$$

$$\ln|x|_p \Longleftrightarrow -\left(1-\frac{1}{p}\right)^{-1}\ln p\left(\operatorname{reg}|\xi|_p^{-1}+\frac{1}{p}\,\delta(\xi)\right). \tag{17.16}$$

$$\frac{1}{|x|_p^2+m^2} \Longleftrightarrow \left(1-\frac{1}{p}\right)\frac{|\xi|_p}{p^2+m^2|\xi|_p^2}$$
$$\times\sum_{\gamma=0}^{\infty} p^{-\gamma}\,\frac{p^2-p^{-2\gamma}}{p^{-2\gamma}+m^2|\xi|_p^2}\,, \qquad m\neq 0. \tag{17.17}$$

$$|x|_p^{\alpha-1}|1-x|_p^{\beta-1} \Longleftrightarrow \big[\Gamma_p(\alpha+\beta-1)|\xi|_p^{1-\alpha-\beta}+B_p(\alpha,\beta)\big]\Omega(|\xi|_p)$$
$$+\,\big[\Gamma_p(\alpha)|\xi|_p^{-\alpha}+\Gamma_p(\beta)|\xi|_p^{-\beta}\chi_p(\xi)\big][1-\Omega(|\xi|_p)]. \tag{17.18}$$

$$\delta(|x|_p-1)|1-x|_p^{\alpha-1} \Longleftrightarrow \Gamma_p(\alpha)\chi_p(\xi)|\xi|_p^{-\alpha}, \qquad \gamma(\xi)\geqslant 2. \tag{17.19}$$

$$\eta_{x_0}\delta\big(|x|_p-p^\gamma\big) \Longleftrightarrow p^{\gamma-1}\eta'_{\xi_0}\delta\big(|\xi|_p-p^{1-\gamma}\big), \qquad p\neq 2, \tag{17.20}$$
$$\text{где}\quad \sum_{k=1}^{p-1}\eta_k=0, \qquad \eta'_j=\sum_{k=1}^{p-1}\eta_k\exp\left(2\pi i\frac{kj}{p}\right).$$

$$|x|_p^{\alpha-1}\Omega\big(p^{-\gamma}|x|_p\big) \Longleftrightarrow \frac{1-p^{-1}}{1-p^{-\alpha}}p^{\alpha\gamma}\,\Omega\big(p^\gamma|\xi|_p\big)$$
$$+\,\Gamma_p(\alpha)|\xi|_p^{-\alpha}\big[1-\Omega\big(p^\gamma|\xi|_p\big)\big]. \tag{17.21}$$

$$\delta(|x|_p-1)\delta(x_0-p+1) \Longleftrightarrow p^{-1}\chi_p(-\xi)\Omega(|p\xi|_p). \tag{17.22}$$

$$\chi_p(x)\Omega(|px|_p) \Longleftrightarrow p\delta(|\xi|_p-1)\delta(\xi_0-p+1). \tag{17.23}$$

$$|x,m|_p^{\alpha-1} \Longleftrightarrow \Gamma_p(\alpha)\big(|\xi|_p^{-\alpha} - |pm|_p^{\alpha}\big)\Omega(|m\xi|_p),$$
$$m \neq 0, \quad \alpha \in \mathbb{C}. \tag{17.24}$$

$$f((x,x)) \Longleftrightarrow |(\xi,\xi)|_p^{-1}\Big[(1-p^{-2})\sum_{\gamma=0}^{\infty} p^{-2\gamma} f\big(p^{-2\gamma}|(\xi,\xi)|_p^{-1}\big)$$
$$- f\big(p^2|(\xi,\xi)|_p^{-1}\big)\Big], \qquad n=2, \quad p \equiv 3 \pmod 4. \tag{17.25}$$

$$f((x,x)) \Longleftrightarrow |(\xi,\xi)|_p^{-1}\Bigg[\left(1-\frac{1}{p}\right)^2 \sum_{\gamma=0}^{\infty}\left(\gamma + \frac{p-3}{p-1}\right)$$
$$\times\, p^{-\gamma} f\big(p^{-\gamma}|(\xi,\xi)|_p^{-1}\big) - 2\left(1-\frac{1}{p}\right) f\big(p|(\xi,\xi)|_p^{-1}\big)$$
$$+ f\big(p^2|(\xi,\xi)|_p^{-1}\big)\Bigg], \qquad n=2, \quad p \equiv 1 \pmod 4. \tag{17.26}$$

$$|(x,x)|_p^{\alpha-1} \Longleftrightarrow \Gamma_p^2(\alpha)|(\xi,\xi)|_p^{-\alpha}, \qquad n=2, \quad p \equiv 1 \pmod 4. \tag{17.27}$$

$$|(x,x)|_p^{\alpha-1} \Longleftrightarrow \Gamma_p(\alpha)\widetilde{\Gamma}_p(\alpha)|(\xi,\xi)|_p^{-\alpha},$$
$$n=2, \quad p \equiv 3 \pmod 4. \tag{17.28}$$

$$\frac{1}{|(x,x)|_p + m^2} \Longleftrightarrow \frac{1-p^{-2}}{p^2 + m^2|(\xi,\xi)|_p} \sum_{\gamma=0}^{\infty} \frac{p^2 - p^{-2\gamma}}{1 + p^{\gamma} m^2 |(\xi,\xi)|_p},$$
$$n=2, \quad m \neq 0, \quad p \equiv 3 \pmod 4. \tag{17.29}$$

$$\frac{1}{|(x,x)|_p + m^2} \Longleftrightarrow \left(1-\frac{1}{p}\right)^2 \sum_{\gamma=0}^{\infty}\left(\gamma + \frac{p-3}{p-1}\right)\frac{1}{1 + p^{\gamma} m^2 |(\xi,\xi)|_p}$$
$$- 2\frac{1-1/p}{p + m^2|(\xi,\xi)|_p} + \frac{1}{p^2 + m^2|(\xi,\xi)|_p},$$
$$n=2, \quad m \neq 0, \quad p \equiv 1 \pmod 4. \tag{17.30}$$

$$|(x,x)|_p^{\alpha-n/2} \Longleftrightarrow \Gamma_p\left(\alpha - \frac{n}{2} + 1\right)\Gamma_p(\alpha)|(\xi,\xi)|_p^{-\alpha},$$
$$\alpha \neq \left\{\alpha_k,\ a_k + \frac{n}{2} - 1,\ k \in Z\right\}, \quad n \equiv 0 \pmod 4, \quad p \neq 2$$
$$\text{или } n \equiv 2 \pmod 4, \quad p \equiv 1 \pmod 4. \tag{17.31}$$

$$|(x,x)|_p^{\alpha-n/2} \Longleftrightarrow (-1)^{\gamma((\xi,\xi))}\Gamma_p\left(\alpha - \frac{n}{2} + 1\right)\widetilde{\Gamma}_p(\alpha)|(\xi,\xi)|_p^{-\alpha},$$
$$n \equiv 2 \pmod 4, \quad n \geqslant 6, \quad p \equiv 3 \pmod 4. \tag{17.32}$$

$$|x|_p^{\alpha-n} \Longleftrightarrow \Gamma_p^{(n)}(\alpha)|\xi|_p^{-\alpha}. \tag{17.33}$$

$$|x,m|_p^{\alpha-n} \Longleftrightarrow \Gamma_p^{(n)}(\alpha)\big(|\xi|_p^{-\alpha} - |pm|_p^{\alpha}\big)\Omega(|m\xi|_p), \quad m \neq 0, \quad \alpha \in \mathbb{C}. \tag{17.34}$$

$$\sqrt{|2a|_p}\,\chi_p(ax^2)\delta(|x|_p - p^{\gamma}) \Longleftrightarrow \lambda_p(a)\chi_p\left(-\frac{\xi^2}{4a}\right) \times\delta\big(|\xi|_p - |2a|_p p^{\gamma}\big), \qquad |4a|_p \geqslant p^{2-2\gamma}. \tag{17.35}$$

$$\sqrt{|2a|_p}\,\chi_p(ax^2)\delta(|x|_p - p^{\gamma}) \Longleftrightarrow \left[\lambda_p(a)\chi_p\left(-\frac{\xi^2}{4a}\right) - \frac{1}{\sqrt{p}}\right] \times\Omega\big(p^{1-\gamma}|\xi|_p\big), \qquad p \neq 2, \quad |a|_p = p^{1-2\gamma}. \tag{17.36}$$

$$\chi_p(ax^2)\Omega\big(p^{-\gamma}|x|_p\big) \Longleftrightarrow p^{\gamma}\Omega\big(p^{\gamma}|\xi|_p\big), \qquad |a|_p p^{2\gamma} \leqslant 1. \tag{17.37}$$

$$\sqrt{|2a|_p}\,\chi_p(ax^2)\Omega\big(p^{-\gamma}|x|_p\big) \Longleftrightarrow \lambda_p(a)\chi_p\left(-\frac{\xi^2}{4a}\right) \times\Omega\big(p^{-\gamma}|2a|_p^{-1}|\xi|_p\big), \qquad |4a|_p p^{2\gamma} \geqslant p. \tag{17.38}$$

$$\sqrt{|2a|_2}\,\chi_2(ax^2)\Omega\big(2^{-\gamma}|x|_2\big) \Longleftrightarrow \lambda_2(a)\chi_2\left(-\frac{\xi^2}{4a}\right) \times\delta(|\xi|_2 - 2^{1-\gamma}), \qquad p = 2, \quad |a|_2 2^{2\gamma} = 2. \tag{17.39}$$

$$\sqrt{|2a|_2}\chi_2(ax^2)\Omega(2^{-\gamma}|x|_2) \Longleftrightarrow \lambda_2(a)\chi_2\big(-\xi^2/4a\big)\Omega(2^{\gamma}|\xi|_2), \quad p = 2, \quad |a|_2 2^{2\gamma} = 4. \tag{17.40}$$

$$\chi_p(ax^2) \Longleftrightarrow \lambda_p(a)|2a|_p^{-1/2}\chi_p\left(-\frac{\xi^2}{4a}\right), \qquad a \neq 0. \tag{17.41}$$

$$\chi_p\left(\frac{x^2}{2}\right) \Longleftrightarrow \chi_p\left(-\frac{\xi^2}{2}\right), \qquad p \neq 2. \tag{17.42}$$

$$\chi_2\left(\frac{x^2}{2}\right) \Longleftrightarrow \exp\left(i\frac{\pi}{4}\right)\chi_2\left(-\frac{\xi^2}{2}\right), \qquad p = 2. \tag{17.43}$$

$$\sqrt{|a|_p}\,\exp\big(-|x|_p^2\big)\,\chi_p(ax^2) \Longleftrightarrow S\left(|a|_p^{-1},\frac{1}{p}\right)\chi_p\left(-\frac{\xi^2}{4a}\right)\Omega\big(|a|_p^{-1/2}|\xi|_p\big) + \left\{\lambda_p(a)\exp\left(-\left|\frac{\xi}{a}\right|_p^2\right)\chi_p\left(-\frac{\xi^2}{4a}\right) + |a|_p^{1/2}|\xi|_p^{-1}\left[S\left(|\xi|_p^{-2},\frac{1}{p}\right)\right.\right.$$

$$- \exp\bigl(-|p\xi|_p^{-2}\bigr)\Bigr]\Bigr\}\bigl[1-\Omega\bigl(|a|_p^{-1/2}|\xi|_p\bigr)\bigr],$$
$$p\neq 2,\quad \gamma(a)=2k. \tag{17.44}$$

$$\sqrt{|a|_p}\,\exp\bigl(-|x|_p^2\bigr)\chi_p(ax^2)\Longleftrightarrow\Bigl\{\frac{1}{\sqrt{p}}\,S\Bigl(p^{-1}|a|_p^{-1},\frac{1}{p}\Bigr)+\Bigl[\lambda_p(a)-\frac{1}{\sqrt{p}}\Bigr]$$
$$\times\exp\bigl(-|pa|_p^{-1}\bigr)\Bigr\}\chi_p\Bigl(-\frac{\xi^2}{4a}\Bigr)\Omega\bigl(\sqrt{p}\,|a|_p^{-1/2}|\xi|_p\bigr)$$
$$+\Bigl\{\lambda_p(a)\exp\Bigl(-\Bigl|\frac{\xi}{a}\Bigr|_p^2\Bigr)\chi_p\Bigl(-\frac{\xi^2}{4a}\Bigr)+|a|_p^{1/2}|\xi|_p^{-1}\Bigl[S\Bigl(|\xi|_p^{-2},\frac{1}{p}\Bigr)$$
$$-\exp\bigl(-|p\xi|_p^{-2}\bigr)\Bigr]\Bigr\}\bigl[1-\Omega\bigl(\sqrt{p}\,|a|_p^{-1/2}|\xi|_p\bigr)\bigr],$$
$$p\neq 2,\quad \gamma(a)=2k+1. \tag{17.45}$$

$$\sqrt{|a|_2}\,\exp\bigl(-|x|_2^2\bigr)\chi_2(ax^2)\Longleftrightarrow\Bigl\{\bigl[\sqrt{2}\,\lambda_2(a)-1\bigr]\exp\bigl(-|4a|_2^{-1}\bigr)$$
$$+S\Bigl(|a|_2^{-1},\frac{1}{2}\Bigr)\Bigr\}\chi_2\Bigl(-\frac{\xi^2}{4a}\Bigr)\Omega\bigl(|4a|_2^{-1/2}|\xi|_2\bigr)+\Bigl\{\exp\bigl(-|4a|_p^{-1}\bigr)$$
$$+\bigl[\sqrt{2}\,\lambda_2(a)-1\bigr]S\Bigl(|a|_2^{-1},\frac{1}{2}\Bigr)\Bigr\}\delta\bigl(|\xi|_2-|a|_2^{1/2}\bigr)\chi_2\Bigl(-\frac{\xi^2}{4a}\Bigr)$$
$$+\Bigl\{\sqrt{2}\,\lambda_2(a)\exp\bigl(-|2a|_2^{-2}|\xi|_2^2\bigr)\chi_2\Bigl(-\frac{\xi^2}{4a}\Bigr)$$
$$+|a|_2^{1/2}|\xi|_2^{-1}\Bigl[S\Bigl(|\xi|_2^{-2},1/2\Bigr)-2\exp\bigl(-|2\xi|_2^{-2}\bigr)\Bigr]\Bigr\}$$
$$\times\bigl[1-\Omega\bigl(|a|_2^{-1/2}|\xi|_2\bigr)\bigr],\qquad p=2,\quad \gamma(a)=2k. \tag{17.46}$$

$$\sqrt{|a|_2}\exp\bigl(-|x|_2^2\bigr)\chi_2(ax^2)\Longleftrightarrow\frac{1}{\sqrt{2}}\Bigl[S\Bigl(\Bigl|\frac{a}{2}\Bigr|_2^{-1},\frac{1}{2}\Bigr)-\exp\bigl(-|2a|_2^{-1}\bigr)$$
$$+2\lambda_2(a)\exp\bigl(-|8a|_2^{-1}\bigr)\Bigr]\chi_2\Bigl(-\frac{\xi^2}{4a}\Bigr)\Omega\bigl(|8a|_2^{-1/2}|\xi|_2\bigr)$$
$$+\sqrt{2}\,\Bigl[S\Bigl(|2a|_2^{-1},\frac{1}{2}\Bigr)+\lambda_2(a)\exp\bigl(-|8a|_2^{-1}\bigr)\Bigr]$$
$$\times\chi_2\Bigl(-\frac{\xi^2}{4a}\Bigr)\delta\bigl(|\xi|_2-\sqrt{2|a|_2}\,\bigr)$$
$$+\sqrt{2}\,\lambda_2(a)S\Bigl(|2a|_2^{-1},\frac{1}{2}\Bigr)\chi_2\Bigl(-\frac{\xi^2}{4a}\Bigr)\delta\bigl(|\xi|_2-\sqrt{2|a|_2}\,\bigr)$$

$$+\left\{|a|_2^{1/2}|\xi|_2^{-1}\left[S\left(|\xi|_2^{-2},\frac{1}{2}\right)-2\exp\bigl(-|2\xi|_2^{-2}\bigr)\right]\right.$$
$$\left.+\sqrt{2}\,\lambda_2(a)\exp\bigl(-|2a|_2^{-2}|\xi|_2^2\bigr)\chi_2\left(-\frac{\xi^2}{4a}\right)\right\}$$
$$\times\bigl[1-\Omega\bigl(2^{-1/2}|a|_2^{-1/2}|\xi|_2\bigr)\bigr],$$
$$p=2,\quad \gamma(a)=2k+1. \tag{17.47}$$

$$|x|_p^{\alpha-1}\theta(x)\Longleftrightarrow\Gamma_p(\pi_{\alpha,\theta})|\xi|_p^{-\alpha}\theta^{-1}(\xi),\qquad \theta\not\equiv 1,\quad \alpha\in\mathbb{C}. \tag{17.48}$$

$$\theta(p^k x)\delta\bigl(|x|_p-p^k\bigr)\Longleftrightarrow p^k a_{p,k}(\theta)\theta^{-1}(\xi)\delta\bigl(|\xi|_p-1\bigr),$$
$$k=\rho(\theta),\qquad \text{величина } a_{p,k} \text{ определена в (8.17).} \tag{17.49}$$

$$|z\bar z|_p^{\alpha-1}\Longleftrightarrow\Gamma_{p,d}(\alpha)|\zeta\bar\zeta|_p^{-\alpha},\qquad d\notin\mathbb{Q}_p^{\times 2}\quad\text{(см. (9.7))}. \tag{17.50}$$

$$|x|_p^{\alpha-1}\mathrm{sgn}_{p,d}\,x\Longleftrightarrow\widetilde\Gamma_p(\alpha)|\xi|_p^{-\alpha}\mathrm{sgn}_{p,d}\,\xi,$$
$$p\neq 2,\quad |d|_p=1,\quad d\notin\mathbb{Q}_p^{\times 2}\quad\text{(см. (8.8))}. \tag{17.51}$$

$$|x|_p^{\alpha-1}\mathrm{sgn}_{p,d}\,x\Longleftrightarrow\pm p^{\alpha-1/2}\sqrt{\mathrm{sgn}_{p,d}\,(-1)}\,|\xi|_p^{-\alpha}\mathrm{sgn}_{p,d}\,\xi,$$
$$p\neq 2,\quad |d|_p=\frac{1}{p}\quad\text{(см. (8.24))}. \tag{17.52}$$

Литература

[1] Владимиров В. С., Волович И. В., Зеленов Е. И., *p-Адический анализ и математическая физика.* – М.: Наука, 1994. То же на англ. яз. Vladimirov V. S., Volovich I. V., Zelenov E I., *p*-Adic Analysis and Mathematical Physics. – Singapore: World Scientific, 1994, XVIII

[2] Владимиров В. С., Волович И. В., Зеленов Е. И., "Спектральная теория в *p*-адической квантовой механике и теория представлений" // *Изв. АН СССР. Сер. матем.*, 1990. **54**(2), 275–302.

[3] Владимиров В. С., "Обобщенные функции над полем *p*-адических чисел" // *УМН*, 1988. **43**(5), 17–53.

[4] Владимиров В. С., "О спектре некоторых псевдо-дифференциальных операторов над полем *p*-адических чисел" // *Алгебра и анализ*, 1990. **2**(6), 107–124.

[5] Владимиров В. С., "О спектральных свойствах p-адических псевдо-дифференциальных операторов типа Шредингера" // *Изв. РАН. Сер. матем.*, 1992. **56**(4), 770–789.

[6] Владимиров В. С., "Адельные формулы Фрейнда–Виттена для амплитуд Венециано и Вирасоро–Шапиро" // *УМН*, 1993. **48**(6), 3–38.

[7] Vladimirov V. S., "On the Freund–Witten adelic formulafor Veneziano amplitudes" // *Lett. Math. Phys.*, 1993. **27**, 123–131.

[8] Vladimirov V. S., "Adelic formulas for gamma- and beta-functions in algebraic number fields" // *p-Adic Functional Analysis. Lect. Notes Pure and Appl. Math.* – New York: M. Dekker, 1997. **192**, 383–395.

[9] Бикулов А. Х., "Исследование p-адической функции Грина" // *ТМФ*, 1991. **87**(3), 376–390.

[10] Бикулов А. Х., *Частное сообщение.*

[11] Гельфанд И. М., Граев М. И., Пятецкий-Шапиро И. И., *Теория представлений и автоморфные функции.* – М.: Наука, 1966.

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

[13] Ruelle Ph., Thiran E., Verstegen D., Weyers J., "Quantum mechanics on p-adic fields" // *J. Math. Phys.*, 1989. **30**(12), 2854–2874.

[14] Ruelle Ph., Thiran E., Verstegen D., Weyers J., "Adelic string and superstring amplitudes" // *Mod. Phys. Lett. A*, 1989. **4**(18), 1745–1752.

[15] Vladimirov V. S., Volovich I. V., "p-Adic quantum mechanics" // *Commun. Mathem. Phys.*, 1989. **123**, 659–676.

[16] Meurice Y., "Quantum mechanics with p-adic numbers" // *Int. J. Modern Phys. A*, 1989. **4**(19), 5133–5147.

[17] Smirnov V. A., "Renormalization in p-adic quantum mechanics" // *Modern Phys. Lett. A.*, 1991. **6**(15), 1421–1427.

[18] Smirnov V. A., "Calculation of general p-adic Feynmann amplitude" // *Commun. Math Phys.*, 1992. **149**, 623–636.

[19] Zelenov E. I., "p-adic path integrals" // *J. Math. Phys.*, 1991. **32**, 147–152.

[20] Зеленов Е. И., "p-Адическая квантовая механика при $p = 2$" // *ТМФ*, 1989. **80**(2), 253–264.

[21] Kochubei A. N., "Additive and multiplicative fractional differentiations over the field of p-adic numbers" // *p-Adic Functional Analysis, Lect. Notes Pure and Appl. Math.* – New York: M.Dekker, 1997. **192**, 275–280.

[22] Kochubei A. N., "A Schrödinger-type equation over the field of p-adic numbers" // *J. Math. Phys.*, 1993. **34**(8), 3420–3428.

[23] Кочубей А. Н., "Параболические уравнения над полем p-адических чисел" // *Изв. РАН. Сер. матем.*, 1991. **55**(6), 1312–1330.

[24] Кочубей А. Н., "Гауссовы интегралы и спектральная теория над локальным полем" // *Изв. РАН. Сер. матем.*, 1994. **58**(6), 69–78.

[25] Кочубей А. Н., "Об асимптотике p-адических функций Грина" // *Труды Матем. ин-та им. В. А. Стеклова.* 1994. **203**, 116–125.

[26] Missarov M. D., "Renormalization group and renormalization theory in p-adic and adelic scalar models" // *Adv. Soviet Math.*, 1991. **3**, 143–164.

[27] Frampton P. H., "Retrospective on p-adic string theory" // *Труды Матем. ин-та им. В. А. Стеклова.* 1994. **203**, 287–291.

[28] Бикулов А. Х., Волович И. В., "p-Адическое броуновское движение" // *Изв. РАН. Сер. матем.*, 1997. **61**(3), 75–90.

[29] Dragović B. G., *Частное сообщение.*

[30] Taibleson M. H., *Fourier Analysis on Local Fields.* – Princeton: Princeton Univ. Press and Univ. of Tokio Press, 1975.

[31] Lerner E. Yu., Missarov M. D., "p-Adic Feynman and string amplitudes" // *Commun. Math. Phys.*, 1989. **121**, 35–48.

[32] Brekke L., Freund P. G. O., "p-Adic numbers in physics" // *Physics Reports* (*Rev. Sect. of Phys. Lett.*), 1993. **233**(1), 1–66.

[33] Козырев С. В., Теория всплесков как p-адический спектральный анализ // *Изв. РАН. Сер. матем.*, 2002. **66**(2), 149–158.

[34] Хренников А. Ю., *Неархимедов анализ и его приложения.* – М.: Физматлит, 2003.

Оглавление

Научное издание

СОВРЕМЕННЫЕ ПРОБЛЕМЫ МАТЕМАТИКИ

Выпуск 2

Василий Сергеевич Владимиров

Таблицы интегралов комплекснозначных функций p-адических аргументов

Ответственный за выпуск *А. Д. Изаак*
Компьютерная верстка *Е. И. Иванникова*

Сдано в набор 15.07.2003. Подписано в печать 08.09.2003.
Формат 60×90/16. Усл. печ. л. 5,63. Уч.-изд. л. 5,6. Тираж 100 экз.

Отпечатано в Математическом институте им. В. А. Стеклова РАН
Москва, 119991, ул. Губкина, 8.
http://www.mi.ras.ru/spm/ e-mail: spm@mi.ras.ru

Graduate Texts in Mathematics

58

NEAL KOBLITZ

p-ADIC NUMBERS, p-ADIC ANALYSIS, AND ZETA-FUNCTIONS

Springer-Verlag
New York Heidelberg Berlin
1977

«Современная математика»
Вводные курсы

Н. КОБЛИЦ

p-АДИЧЕСКИЕ ЧИСЛА, p-АДИЧЕСКИЙ АНАЛИЗ И ДЗЕТА-ФУНКЦИИ

Перевод с английского
В. В. Шокурова

под редакцией
Ю. И. Манина

Издательство «Мир»
Москва 1982

ОГЛАВЛЕНИЕ

Н. Коблиц

p-АДИЧЕСКИЕ ЧИСЛА
p-АДИЧЕСКИЙ АНАЛИЗ
И ДЗЕТА-ФУНКЦИИ

Ст. научный редактор Н. И. Плужникова
Мл. научный редактор Л. А. Королева
Художник А. В. Шипов
Художественный редактор В. И. Шаповалов
Технические редакторы Н. Д. Толстякова, Н. И. Борисова
Корректор Е. К. Монякова

ИБ № 2217

Сдано в набор 18.05.81. Подписано к печати 07.01.82. Формат 84×108¹/₃₂. Бумага типографская № 1. Объем 3,00 бум. л. Усл. печ. л. 10,08. Усл. кр.-отт. 10,28. Уч.-изд. л. 8,43. Изд. № 1/0787. Тираж 7900 экз. Заказ 1153. Цена 65 коп.

Издательство «Мир»
129820, Москва, И-110, ГСП 1-й Рижский пер., 2.

Набрано и сматрицировано в ордена Октябрьской Революции, ордена Трудового Красного Знамени Ленинградском производственно-техническом объединении «Печатный Двор» имени А. М. Горького Союзполиграфпрома при Государственном комитете СССР по делам издательств, полиграфии и книжной торговли. 197136, Ленинград, П-136, Чкаловский пр., 15. Отпечатано в Ленинградской типографии № 2 головном предприятии ордена Трудового Красного Знамени Ленинградского объединения «Техническая книга» им. Евгения Соколовой Союзполиграфпрома при Государственном комитете СССР по делам издательств, полиграфии и книжной торговли, 198052, г. Ленинград, Л-52, Измайловский проспект, 29.

ББК 22.132
К 55
УДК 517.1

Коблиц Н.

К 55 *p*-адические числа, *p*-адический анализ и дзета-функции. Пер. с англ. В. В. Шокурова / Под ред. и с предисловием Ю. И. Манина. — М.: Мир, 1981, 192 с., ил.

Вводный курс по *p*-адическому анализу — объекту многочисленных исследований в теории чисел, теории представлений групп, алгебраической геометрии, который служит связующим звеном между непрерывной и дискретной математикой, написаиный с большим педагогическим мастерством молодым американским математиком.

Для студентов-математиков младших курсов университетов и пединститутов.

К $\frac{20203-012}{041(01)-81}$ 12—81, ч. 1 1702030000 ББК 22.132
517.1

Редакция литературы по математическим наукам

ОТ РЕДАКТОРА ПЕРЕВОДА

Вещественные числа — это пополнение поля рациональных чисел в обычной топологии. Давно известно, что у поля рациональных чисел есть еще много топологий, согласованных с операциями. Эти топологии нумеруются простыми числами; пополнения по ним суть поля *p*-адических чисел. *p*-адический анализ создавался медленно. Перенос обычных определений в неархимедову ситуацию кажется обманчиво простым делом, но глубокие теоремы требуют деликатных изменений в структуре основных понятий.

Книга молодого американского математика Нила Коблица — одно из немногих в мировой литературе введений в этот быстро развивающийся предмет. В ней живо, с вниманием к читателю и на содержательном материале представлены первые идеи, проблемы и методы *p*-адического анализа. Очевидно, что некоторые основные задачи ставит теория чисел. Два круга вопросов, относящихся к дзета-функциям алгебраических многообразий над конечными полями и к классической дзета-функции Римана, изложены в книге подробно. Ознакомившись с этим материалом, читатель сможет работать с обширной журнальной литературой последних лет, посвященной увлекательным свойствам *p*-адических дзета-функций.

Рисунок д-ра физ.-мат. наук А. Т. Фоменко на следующей странице (деталь — на обложке) символизирует 2-адический соленоид. Как и все графические листы Фоменко, он отличается скрупулезной деталировкой, и стоящий за ним математический образ поддается точному анализу. Читателю, который склонен к целостному восприятию, глубокая работа Фоменко напомнит о почти всегда скрытой визионерской компоненте математического творчества.

Ю. Манин

Профессору Марку Кацу

ПРЕДИСЛОВИЕ

Эти записи лекций задуманы как элементарный вводный курс p-адического анализа. По этой причине требования к подготовке читателя минимальны. Помимо трехсеместрового курса математического анализа предполагается знакомство с некоторыми более абстрактными математическими понятиями — в такой степени, чтобы читателя не испугали матрицы с элементами не обязательно из вещественного поля, расширения поля рациональных чисел или непрерывные отображения топологических пространств.

Книга преследует двоякую цель: изложить некоторые основные понятия p-адического анализа и продемонстрировать два его замечательных применения. Исторически они серьезно стимулировали интерес к предмету; я надеюсь, что они могут быть столь же эффективны с педагогической точки зрения. Первый из этих результатов использует лишь самые элементарные свойства поля $\mathbb{Q}_p$ и поэтому помещен в гл. II. Это — предложенная Мазуром конструкция (с помощью p-адического интегрирования) p-адической дзета-функции Куботы — Леопольдта, которая «p-адически интерполирует» значения дзета-функции Римана в нечетных отрицательных целых числах. При изложении я пользовался (неопубликованными) записями Мазура, сделанными для Бурбаки. Затем я возвращаюсь к основаниям: устанавливается возможность продолжения p-адической нормы на алгебраические расширения поля $\mathbb{Q}_p$, строится p-адический аналог поля комплексных чисел и развивается теория p-адических степенных рядов. При этом специально подчеркнуты аналогии и различия с привычными понятиями и примерами из математического анализа. В гл. V содержится второй основной результат: данное Дворком доказательство части знаменитых гипотез А. Вейля о рациональности дзета-функции системы уравнений над конечным полем. В этой главе я следовал изложению Серра, помещенному в одном из выпусков Séminaire Bourbaki.

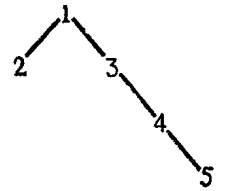
Эта книга не претендует на полноту. В ней не отражены такие темы, как теорема Хассе — Минковского (которую можно найти в гл. I книги З. И. Боревича и И. Р. Шафаревича [(b) 1]) и результаты диссертации Тэйта (которая воспроизведена также в учебнике Ленга [(b)2]). Кроме того, автор не пытался представить результаты в самой общей форме. Например, p-адические L-функции, соответствующие характерам Дирихле, лишь мимоходом упомянуты в гл. II. Целью автора был отбор материала для полугодового курса по p-адическому анализу, доступного второкурсникам.

Упражнения по большей части легкие, но они важны для активного овладения материалом. Кроме того, обилие упражнений позволит многим изучающим книгу овладеть предметом самостоятельно или при минимальном руководстве, проверяя и закрепляя свое понимание материала проработкой задач.

Интерес к p-адическому анализу объясняется несколькими причинами. Прежде всего p-адической технике отводится важное место во многих областях математических исследований — например, в теории чисел и теории представлений. Но немаловажно и то, что студенту, недавно познакомившемуся с рядами и интегралами, «прекрасный новый мир» неархимедова анализа представит классический анализ в неожиданном свете. Уходя корнями в классический анализ и в то же время в алгебру и теорию чисел, p-адический анализ открывает важные перспективы читателю, интересующемуся любой из этих областей.

Я хотел бы поблагодарить профессоров Марка Каца и Ю. И. Манина за их многолетнюю помощь и поддержку, а также за образцы педагогической проницательности в преподавании и изложении, образцы, которым их ученики могут ревностно подражать.

Схема зависимости глав



Глава I

p-АДИЧЕСКИЕ ЧИСЛА

§ 1. ОСНОВНЫЕ ПОНЯТИЯ

Пусть X — непустое множество. Функция d, определенная на множестве всех упорядоченных пар (x, y) элементов X и принимающая неотрицательные вещественные значения $d(x, y)$, называется расстоянием или *метрикой* в X, если она обладает следующими свойствами:

(1) $d(x, y) = 0$ тогда и только тогда, когда $x = y$;
(2) $d(x, y) = d(y, x)$;
(3) $d(x, y) \leqslant d(x, z) + d(z, y)$ для всех $z \in X$.

Множество X вместе с заданной в нем метрикой d называется *метрическим пространством*. Как мы вскоре увидим, одно и то же множество X может допускать много различных структур метрического пространства (X, d).

Чаще всего в качестве множеств X мы будем рассматривать поля. Напомним, что поле F есть множество с двумя бинарными операциями $+$ и $\cdot$, такими, что F является коммутативной группой относительно операции $+$, а $F - \{0\}$ относительно операции $\cdot$, и выполнен закон дистрибутивности. Примеры полей, которые следует пока иметь в виду, — это поле рациональных чисел $\mathbb{Q}$ и поле вещественных чисел $\mathbb{R}$.

Мы будем иметь дело с метриками d, соответствующими *нормам* на поле F. Нормой называется отображение, обозначаемое через $\| \ \|$, поля F в множество неотрицательных вещественных чисел, такое, что:

(1) $\|x\| = 0$ тогда и только тогда, когда $x = 0$;
(2) $\|x \cdot y\| = \|x\| \cdot \|y\|$;
(3) $\|x + y\| \leqslant \|x\| + \|y\|$.

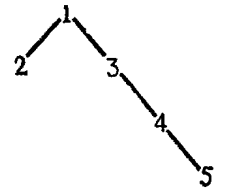
Эта книга не претендует на полноту. В ней не отражены такие темы, как теорема Хассе — Минковского (которую можно найти в гл. I книги З. И. Боревича и И. Р. Шафаревича [(b) 1]) и результаты диссертации Тэйта (которая воспроизведена также в учебнике Ленга [(b)2]). Кроме того, автор не пытался представить результаты в самой общей форме. Например, p-адические L-функции, соответствующие характерам Дирихле, лишь мимоходом упомянуты в гл. II. Целью автора был отбор материала для полугодового курса по p-адическому анализу, доступного второкурсникам.

Упражнения по большей части легкие, но они важны для активного овладения материалом. Кроме того, обилие упражнений позволит многим изучающим книгу овладеть предметом самостоятельно или при минимальном руководстве, проверяя и закрепляя свое понимание материала проработкой задач.

Интерес к p-адическому анализу объясняется несколькими причинами. Прежде всего p-адической технике отводится важное место во многих областях математических исследований — например, в теории чисел и теории представлений. Но немаловажно и то, что студенту, недавно познакомившемуся с рядами и интегралами, «прекрасный новый мир» неархимедова анализа представит классический анализ в неожиданном свете. Уходя корнями в классический анализ и в то же время в алгебру и теорию чисел, p-адический анализ открывает важные перспективы читателю, интересующемуся любой из этих областей.

Я хотел бы поблагодарить профессоров Марка Каца и Ю. И. Манина за их многолетнюю помощь и поддержку, а также за образцы педагогической проницательности в преподавании и изложении, образцы, которым их ученики могут ревностно подражать.

Схема зависимости глав



Глава I

p-АДИЧЕСКИЕ ЧИСЛА

§ 1. ОСНОВНЫЕ ПОНЯТИЯ

Пусть X — непустое множество. Функция d, определенная на множестве всех упорядоченных пар (x, y) элементов X и принимающая неотрицательные вещественные значения $d(x, y)$, называется расстоянием или *метрикой* в X, если она обладает следующими свойствами:

(1) $d(x, y)=0$ тогда и только тогда, когда $x=y$;
(2) $d(x, y)=d(y, x)$;
(3) $d(x, y)\leqslant d(x, z)+d(z, y)$ для всех $z\in X$.

Множество X вместе с заданной в нем метрикой d называется *метрическим пространством*. Как мы вскоре увидим, одно и то же множество X может допускать много различных структур метрического пространства (X, d).

Чаще всего в качестве множеств X мы будем рассматривать поля. Напомним, что поле F есть множество с двумя бинарными операциями $+$ и $\cdot$, такими, что F является коммутативной группой относительно операции $+$, а $F-\{0\}$ относительно операции $\cdot$, и выполнен закон дистрибутивности. Примеры полей, которые следует пока иметь в виду, — это поле рациональных чисел $\mathbb{Q}$ и поле вещественных чисел $\mathbb{R}$.

Мы будем иметь дело с метриками d, соответствующими *нормам* на поле F. Нормой называется отображение, обозначаемое через $\|\ \|$, поля F в множество неотрицательных вещественных чисел, такое, что:

(1) $\|x\|=0$ тогда и только тогда, когда $x=0$;
(2) $\|x\cdot y\|=\|x\|\cdot\|y\|$;
(3) $\|x+y\|\leqslant\|x\|+\|y\|$.

Когда мы говорим, что метрика d «соответствует» норме (или «индуцирована» нормой) $\|\ \|$, то под этим мы понимаем, что метрика d определяется соотношением $d(x, y) = \|x-y\|$. Легко проверить, что функция d, заданная таким образом по произвольной норме $\|\ \|$, будет действительно метрикой.

Основной пример нормы на поле рациональных чисел $\mathbb{Q}$ дает абсолютная величина $|x|$. Индуцированная ею метрика $d(x, y) = |x-y|$ совпадает с обычным расстоянием на числовой прямой.

Я начал с абстрактного определения расстояния потому, что отправным понятием для всего дальнейшего будет метрика нового типа. Она удовлетворяет условиям (1) — (3), но ее свойства существенно отличаются от привычных интуитивных представлений. Кроме того, я напомнил абстрактное определение поля, так как вскоре нам придется работать не только с полем $\mathbb{Q}$, но и с его различными расширениями.

§ 2. МЕТРИКИ ПОЛЯ РАЦИОНАЛЬНЫХ ЧИСЕЛ

Одну метрику с поля $\mathbb{Q}$ мы знаем: она индуцирована обычной абсолютной величиной. Есть ли еще какие-нибудь метрики? Следующее определение является основой для всего дальнейшего.

Определение. Пусть $p \in \{2, 3, 5, 7, 11, 13, \ldots\}$ — некоторое простое число. Для произвольного ненулевого целого числа a положим $\operatorname{ord}_p a$ равным кратности вхождения p в разложение a на простые сомножители, т. е. наибольшему целому неотрицательному числу m, для которого $a \equiv 0 \pmod{p^m}$. (Запись $a \equiv b \pmod{c}$ означает, что c делит $a-b$.) Например: $\operatorname{ord}_5 35 = 1, \operatorname{ord}_5 250 = 3$, $\operatorname{ord}_2 96 = 5$, $\operatorname{ord}_2 97 = 0$. (Если $a = 0$, то условимся писать $\operatorname{ord}_p 0 = \infty$.) Отметим, что функция ord_p немножко похожа на логарифм: $\operatorname{ord}_p(a_1 a_2) = \operatorname{ord}_p(a_1) + \operatorname{ord}_p(a_2)$.

Теперь для произвольного рационального числа $x = a/b$ положим $\operatorname{ord}_p x$ равным $\operatorname{ord}_p a - \operatorname{ord}_p b$. Так определенная величина зависит только от x, т. е. из представления $x = ac/bc$ мы получим то же самое значение для $\operatorname{ord}_p x = \operatorname{ord}_p ac - \operatorname{ord}_p bc$.

Кроме того, определим на $\mathbb{Q}$ следующее отображение $|\ |_p$:

$$|x|_p = \begin{cases} \dfrac{1}{p^{\operatorname{ord}_p x}}, & \text{если } x \neq 0; \\ 0, & \text{если } x = 0. \end{cases}$$

Предложение. *Функция* $|\ |_p$ *является нормой на поле* $\mathbb{Q}$.

Доказательство. Проверку свойств (1) и (2) оставим читателю в качестве легкого упражнения. Установим (3).

Если $x = 0$ или $y = 0$, или если $x + y = 0$, то свойство (3) очевидно. Поэтому предположим, что числа x, y, $x+y$ отличны от нуля. Пусть $x = a/b$ и $y = c/d$ — несократимые представления. Тогда $x + y = (ad+bc)/bd$ и $\operatorname{ord}_p(x+y) = \operatorname{ord}_p(ad+bc) - \operatorname{ord}_p b - \operatorname{ord}_p d$. Заметим теперь, что наибольшая степень p, делящая сумму двух целых чисел, *не меньше* любой степени p, которая делит одновременно каждое слагаемое. Поэтому

$$\begin{aligned} \operatorname{ord}_p(x+y) &\geqslant \min(\operatorname{ord}_p ad,\ \operatorname{ord}_p bc) - \operatorname{ord}_p b - \operatorname{ord}_p d = \\ &= \min(\operatorname{ord}_p a + \operatorname{ord}_p d,\ \operatorname{ord}_p b + \operatorname{ord}_p c) - \\ &\qquad - \operatorname{ord}_p b - \operatorname{ord}_p d = \\ &= \min(\operatorname{ord}_p a - \operatorname{ord}_p b,\ \operatorname{ord}_p c - \operatorname{ord}_p d) = \\ &= \min(\operatorname{ord}_p x,\ \operatorname{ord}_p y). \end{aligned}$$

Следовательно, $|x+y|_p = p^{-\operatorname{ord}_p(x+y)} \leqslant \max(p^{-\operatorname{ord}_p x}, p^{-\operatorname{ord}_p y}) = \max(|x|_p, |y|_p)$, а последнее $\leqslant |x|_p + |y|_p$. □

В действительности мы установили более сильное неравенство, чем требуется в условии (3), и именно это усиленное неравенство приводит нас к одному из основных понятий p-адического анализа.

Определение. Норма называется *неархимедовой*, если всегда выполнено неравенство $\|x+y\| \leqslant \max(\|x\|, \|y\|)$. Соответственно метрика называется *неархимедовой*, если $d(x, y) \leqslant \max(d(x, z), d(z, y))$; в частности, метрика, индуцированная неархимедовой нормой, неархимедова, так как в этом случае $d(x, y) = \|x-y\| = \|(x-z) + (z-y)\| \leqslant \max(\|x-z\|, \|z-y\|) = \max(d(x, z), d(z, y))$.

Таким образом, $|\ |_p$ является неархимедовой нормой на поле $\mathbb{Q}$.

Норму (или метрику), не являющуюся неархимедовой, называют *архимедовой*. Обычная абсолютная величина на поле $\mathbb{Q}$ дает пример архимедовой нормы.

Для каждого метрического пространства X определено понятие *последовательности Коши*. Последовательность $\{a_1, a_2, a_3, \ldots\}$ элементов X называется последовательностью Коши, если для всякого положительного числа ε найдется такой номер N, что $d(a_m, a_n) < \varepsilon$ при любых $m > N$ и $n > N$.

По определению, две метрики d_1 и d_2 на множестве X *эквивалентны*, если отвечающие им классы последовательностей Коши совпадают. Соответственно две нормы *эквивалентны*, если они индуцируют эквивалентные метрики.

Фиксируем вещественное число $\rho \in (0, 1)$, а затем в определении $|\ |_p$ подставим $\rho^{\operatorname{ord}_p x}$ вместо $(1/p)^{\operatorname{ord}_p x}$. Тогда мы получим неархимедову норму, эквивалентную $|\ |_p$ (см. упр. 4 и 5). Причину, по которой удобно выбирать $\rho = 1/p$, объясняет упр. 17 в конце параграфа.

Обычной абсолютной величине $|\ |$ также соответствует семейство эквивалентных ей архимедовых норм, а именно $|\ |^\alpha$, где $0 < \alpha \leqslant 1$ (см. упр. 7).

Обычную абсолютную величину мы иногда будем обозначать через $|\ |_\infty$. При этом никакой прямой связи между $|\ |_\infty$ и $|\ |_p$ не подразумевается, это всего лишь удобное обозначение.

Под «тривиальной» нормой понимается такая норма $\|\ \|$, что $\|0\| = 0$ и $\|x\| = 1$ для всех $x \neq 0$.

Теорема 1 (Островский). *Каждая нетривиальная норма $\|\ \|$ на поле $\mathbb{Q}$ эквивалентна $|\ |_p$ для некоторого простого p или $p = \infty$.*

Доказательство. Случай (i). Предположим, что существует натуральное число n, для которого $\|n\| > 1$. Пусть n_0 — наименьшее среди таких n. Так как $\|n_0\| > 1$, то $\|n_0\| = n_0^\alpha$ для некоторого положительного вещественного α. Запишем теперь произвольное целое положительное n в n_0-ичной системе:

$$n = a_0 + a_1 n_0 + a_2 n_0^2 + \ldots + a_s n_0^s,$$

где $0 \leqslant a_i < n_0$ и $a_s \neq 0$. Тогда

$$\|n\| \leqslant \|a_0\| + \|a_1 n_0\| + \|a_2 n_0^2\| + \ldots + \|a_s n_0^s\| =$$
$$= \|a_0\| + \|a_1\| \cdot n_0^\alpha + \|a_2\| \cdot n_0^{2\alpha} + \ldots + \|a_s\| \cdot n_0^{s\alpha}.$$

Так как $a_i < n_0$, то $\|a_i\| \leqslant 1$ по выбору n_0. Следовательно,

$$\|n\| \leqslant 1 + n_0^\alpha + n_0^{2\alpha} + \ldots + n_0^{s\alpha} =$$
$$= n_0^{s\alpha}(1 + n_0^{-\alpha} + \ldots + n_0^{-s\alpha}) \leqslant$$
$$\leqslant n^\alpha \left[\sum_{i=0}^{\infty} (1/n_0^\alpha)^i\right],$$

потому что $n \geqslant n_0^s$. Выражение в квадратных скобках является константой, которую мы обозначим через C. Таким образом,

$$\|n\| \leqslant C n^\alpha \quad \text{для всех} \quad n = 1, 2, 3, \ldots.$$

Рассмотрим теперь достаточно большое натуральное N. Затем подставим n^N вместо n в полученное неравенство и извлечем корень степени N из обеих частей. Получим

$$\|n\| \leqslant \sqrt[N]{C}\, n^\alpha.$$

Переход к пределу при $N \to \infty$ и фиксированном n дает неравенство $\|n\| \leqslant n^\alpha$.

Обратное неравенство можно доказать следующим образом. Как и выше, представим n в n_0-ичной записи. Тогда $n_0^{s+1} > n \geqslant n_0^s$. Кроме того, поскольку $\|n_0^{s+1}\| = \|n + n_0^{s+1} - n\| \leqslant \|n\| + \|n_0^{s+1} - n\|$, то

$$\|n\| \geqslant \|n_0^{s+1}\| - \|n_0^{s+1} - n\| \geqslant n_0^{(s+1)\alpha} - (n_0^{s+1} - n)^\alpha,$$

что следует из соотношения $\|n_0^{s+1}\| = \|n_0\|^{s+1}$ и уже установленного неравенства (т. е. $\|n\| \leqslant n^\alpha$) для вычитаемого члена. Значит,

$$\|n\| \geqslant n_0^{(s+1)\alpha} - (n_0^{s+1} - n_0^s)^\alpha = \quad \text{(так как } n \geqslant n_0^s\text{)}$$
$$= n_0^{(s+1)\alpha}\left[1 - \left(1 - \frac{1}{n_0}\right)^\alpha\right] \geqslant C' n^\alpha$$

для некоторой константы C', зависящей только от n_0 и α, но не от n. Затем, как и выше, подставим в

последнее неравенство n^N, извлечем корень степени N и перейдем к пределу при $N \to \infty$. В результате получаем $\|n\| \geqslant n^\alpha$.

Таким образом, $\|n\| = n^\alpha$. Далее, из свойства нормы (2) легко вывести, что $\|x\| = |x|^\alpha$ для всякого $x \in \mathbb{Q}$. Тогда из упр. 7 следует эквивалентность норм $\| \|$ и $| |$, что и заканчивает доказательство теоремы в случае (i).

Случай (ii). Предположим теперь, что $\|n\| \leqslant 1$ для всех натуральных чисел n. Пусть n_0 — наименьшее натуральное n, для которого $\|n\| < 1$. Такое n_0 существует, потому что рассматриваемая норма $\| \|$ нетривиальна.

Число n_0 должно быть простым. Действительно, если $n_0 = n_1 \cdot n_2$ и $n_1, n_2 < n_0$, то $\|n_1\| = \|n_2\| = 1$, а поэтому $\|n_0\| = \|n_1\| \|n_2\| = 1$. Обозначим простое число n_0 через p.

Покажем теперь, что $\|q\| = 1$ для каждого простого q, отличного от p. Предположим противное. Тогда $\|q\| < 1$ и для достаточно большого натурального N имеем $\|q^N\| = \|q\|^N < 1/2$. Аналогично, $\|p^M\| < 1/2$ для достаточно большого M. Числа p^M и q^N взаимно просты, т. е. не имеют общих делителей, отличных от 1. Поэтому можно найти (см. упр. 9) два целых числа n и m, таких, что $mp^M + nq^N = 1$. Тогда, согласно свойствам нормы (2) и (3),

$$1 = \|1\| = \|mp^M + nq^N\| \leqslant \|mp^M\| + \|nq^N\| = \\ = \|m\| \|p^M\| + \|n\| \|q^N\|.$$

Так как $\|m\|, \|n\| \leqslant 1$, то

$$1 \leqslant \|p^M\| + \|q^N\| < \frac{1}{2} + \frac{1}{2} = 1,$$

и мы пришли к противоречию. Следовательно, $\|q\| = 1$.

Теорема практически доказана, поскольку каждое положительное целое число a можно разложить на простые сомножители. Пусть $a = p_1^{b_1} p_2^{b_2} \ldots p_r^{b_r}$. Тогда $\|a\| = \|p_1\|^{b_1} \cdot \|p_2\|^{b_2} \ldots \|p_r\|^{b_r}$. В последнем произведении отличен от 1 лишь тот сомножитель $\|p_i\|$, для которого $p_i = p$ (если такой найдется), причем соответствующее b_i

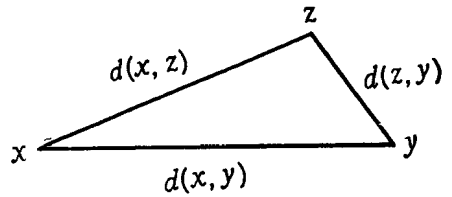
совпадает с $\operatorname{ord}_p a$. Поэтому

$$\|a\| = \rho^{\operatorname{ord}_p a},$$

где $\rho = \|p\| < 1$. На основании свойства нормы (2) легко установить, что последняя формула выполняется не только для натуральных a, но также для любого отличного от нуля рационального числа x. Из упр. 4 ниже следует эквивалентность такой нормы и нормы $| |_p$. Это заканчивает доказательство теоремы Островского. □

Конечно, наши интуитивные представления о расстоянии основаны на примере архимедовой метрики $| |_\infty$. Некоторые свойства неархимедовых метрик $| |_p$ поначалу кажутся довольно странными, и к ним нужно привыкать. Рассмотрим следующие два примера.

Свойство метрики (3): $d(x, y) \leqslant d(x, z) + d(z, y)$ — известно как «неравенство треугольника», поскольку в случае поля комплексных чисел $\mathbb{C}$ (с метрикой $d(a + bi, c + di) = \sqrt{(a-c)^2 + (b-d)^2}$) оно означает, что сумма длин двух сторон треугольника на комплексной плоскости больше длины третьей стороны.



Посмотрим, что происходит в случае поля F с неархимедовой нормой. Для простоты положим $z = 0$. Тогда неархимедово неравенство треугольника утверждает, что $\|x - y\| \leqslant \max(\|x\|, \|y\|)$. Предположим сначала, что «стороны» x и y имеют разную «длину», например $\|x\| < \|y\|$. Третья сторона $x - y$ имеет длину $\|x - y\| \leqslant \|y\|$. Но

$$\|y\| = \|x - (x - y)\| \leqslant \max(\|x\|, \|x - y\|),$$

и, значит, $\|y\| \leqslant \|x - y\|$, так как неравенство $\|y\| \leqslant \|x\|$ не выполнено. Поэтому $\|y\| = \|x - y\|$. Итак, если две

«стороны» x и y не равны, то наибольшая из них должна совпадать по длине с третьей стороной. Все «треугольники» равнобедренные!

Это не слишком удивительно, если понять, что означает подобное свойство для поля $\mathbb{Q}$ с нормой $|\ |_p$. Оно просто утверждает, что кратность вхождения p в разность двух рациональных чисел с неодинаковыми кратностями вхождения p совпадает с *наименьшей* из этих кратностей (это и значит равняться *наибольшей* из двух «сторон»).

Итак, для неархимедова поля $\|x \pm y\| \leqslant \max(\|x\|, \|y\|)$ и при $\|x\| \neq \|y\|$ достигается равенство. Это важное свойство впредь мы будем называть «принципом равнобедренного треугольника».

В качестве второго примера рассмотрим (открытый) диск радиуса r (r — положительное вещественное число) с центром в a (a — некоторый элемент поля F):

$$D(a, r^-) = \{x \in F \mid \|x-a\| < r\}.$$

Предположим, что норма $\|\ \|$ неархимедова. Пусть b — *произвольный* элемент $D(a, r^-)$. Тогда

$$D(a, r^-) = D(b, r^-),$$

т. е. каждая точка диска является его центром! Действительно,

$$\begin{aligned} x \in D(a, r^-) &\Rightarrow \|x-a\| < r \Rightarrow \\ &\Rightarrow \|x-b\| = \|(x-a)+(a-b)\| \leqslant \\ &\qquad \leqslant \max(\|x-a\|, \|a-b\|) < r \Rightarrow \\ &\Rightarrow x \in D(b, r^-), \end{aligned}$$

и точно так же доказывается обратная импликация.

Определим замкнутый диск радиуса r с центром в a как

$$D(a, r) = \{x \in F \mid \|x-a\| \leqslant r\};$$

тогда, как и выше, можно установить, что в случае неархимедовой нормы $\|\ \|$ каждая точка диска $D(a, r)$ является его центром.

Упражнения

1. Для произвольной нормы $\|\ \|$ на поле F докажите непрерывность операций сложения, умножения и нахождения обратного элемента относительно сложения и умножения, т. е. установите, что: (1) для любых $x, y \in F$ и любого $\varepsilon > 0$ существует такое $\delta > 0$, что $\|(x'+y')-(x+y)\| < \varepsilon$ при $\|x'-x\| < \delta$ и $\|y'-y\| < \delta$; (2) то же с заменой $\|(x'+y')-(x+y)\|$ на $\|x'y'-xy\|$; (3) для любого ненулевого $x \in F$ и любого $\varepsilon > 0$ существует такое $\delta > 0$, что $\|(1/x')-(1/x)\| < \varepsilon$ при $\|x'-x\| < \delta$; (4) для любого $x \in F$ и любого $\varepsilon > 0$ существует такое $\delta > 0$, что $\|(-x')-(-x)\| < \varepsilon$ при $\|x'-x\| < \delta$.

2. Докажите, что $\|-1\| = \|1\| = 1$ для произвольной нормы $\|\ \|$ на поле F. Докажите, что если $\|\ \|$ неархимедова, то $\|n\| \leqslant 1$ для любого целого n. (Здесь «n» обозначает $1+1+1+\ldots+1$ — результат n-кратного сложения $1 \in F$ при $n \geqslant 0$ и результат $(-n)$-кратного сложения $-1 \in F$ при $n < 0$.)

3. Докажите обратное: если норма $\|\ \|$ такова, что $\|n\| \leqslant 1$ для любого целого n, то эта норма неархимедова. (*Указание.* Рассмотрите тождество $\|x+y\|^N = \|(x+y)^N\|$. Затем, используя бином Ньютона и свойство нормы (3), оцените $\|x+y\|^N$ сверху через $\max(\|x\|, \|y\|)$. При этом нужно помнить, что N можно выбрать сколь угодно большим.)

4. Пусть $\|\ \|_1$ и $\|\ \|_2$ — две нормы на поле F. Докажите, что $\|\ \|_1 \sim \|\ \|_2$ тогда и только тогда, когда существует такое положительное вещественное число α, что $\|x\|_1 = \|x\|_2^\alpha$ для всех $x \in F$.

5. Докажите, что если $0 < \rho < 1$, то функция, определенная для $x \in \mathbb{Q}$ как $\rho^{\operatorname{ord}_p x}$ при $x \neq 0$ и 0 при $x = 0$, является неархимедовой нормой. Отметим, что по предыдущему упражнению эта норма эквивалентна $|\ |_p$. Что произойдет при $\rho = 1$? А при $\rho > 1$?

6. Докажите неэквивалентность норм $|\ |_{p_1}$ и $|\ |_{p_2}$ для различных простых чисел p_1 и p_2.

7. Для фиксированного вещественного $\alpha > 0$ и $x \in \mathbb{Q}$ положим $\|x\| = |x|^\alpha$, где $|\ |$ — обычная абсолютная величина. Докажите, что $\|\ \|$ является нормой тогда и только тогда, когда $\alpha \leqslant 1$, и что в этом случае она эквивалентна норме $|\ |$.

8. Докажите, что две эквивалентные нормы на поле F либо обе архимедовы, либо обе неархимедовы.

9. Пусть N и M — два взаимно простых целых числа. Докажите, что существуют целые n и m, для которых $nN+mM=1$. (*Указание.* Покажите, что наименьшее положительное число вида $nN+mM$ должно быть общим делителем N и M.)

10. Вычислите:

(i) $\mathrm{ord}_3 54$, (ii) $\mathrm{ord}_2 128$, (iii) $\mathrm{ord}_3 57$,
(iv) $\mathrm{ord}_7 (-700/197)$, (v) $\mathrm{ord}_2 (128/7)$, (vi) $\mathrm{ord}_3 (7/9)$,
(vii) $\mathrm{ord}_5 (0{,}0625)$, (viii) $\mathrm{ord}_3 (10^9)$, (ix) $\mathrm{ord}_3 (-13{,}23)$,
(x) $\mathrm{ord}_7 (-13{,}23)$, (xi) $\mathrm{ord}_5 (-13{,}23)$, (xii) $\mathrm{ord}_{11}(-13{,}23)$,
(xiii) $\mathrm{ord}_{13} (-26/169)$, (xiv) $\mathrm{ord}_{103} (-1/309)$, (xv) $\mathrm{ord}_3 (9!)$.

11. Докажите, что $\mathrm{ord}_p ((p^N)!) = 1+p+p^2+\ldots+p^{N-1}$.

12. Пусть $0 \leqslant a \leqslant p-1$. Докажите, что $\mathrm{ord}_p ((ap^N)!) = a(1+p+p^2+\ldots+p^{N-1})$.

13. Пусть $n = a_0 + a_1 p + a_2 p^2 + \ldots + a_s p^s$ есть p-ичное разложение натурального числа n, где $0 \leqslant a_i \leqslant p-1$. Положим $S_n = \sum a_i$ (сумма коэффициентов p-ичного разложения). Докажите, что

$$\mathrm{ord}_p (n!) = \frac{n - S_n}{p-1}.$$

14. Вычислите $|a-b|$, т. е. p-адическое расстояние от a до b, где:

(i) $a=1$, $b=26$, $p=5$; (ii) $a=1$, $b=26$, $p=\infty$;
(iii) $a=1$, $b=26$, $p=3$; (iv) $a=1/9$, $b=-1/16$, $p=5$;
(v) $a=1$, $b=244$, $p=3$; (vi) $a=1$, $b=1/244$, $p=3$;
(vii) $a=1$, $b=1/243$, $p=3$; (viii) $a=1$, $b=183$, $p=13$;
(ix) $a=1$, $b=183$, $p=7$; (x) $a=1$, $b=183$, $p=2$;
(xi) $a=1$, $b=183$, $p=\infty$; (xii) $a=9!$, $b=0$, $p=3$;
(xiii) $a=(9!)^2/3^9$, $b=0$, $p=3$; (xiv) $a=2^{2^N}/2^N$, $b=0$, $p=2$;
(xv) $a=2^{2^N}/(2^N)!$, $b=0$, $p=2$.

15. Объясните словами, в чем смысл неравенства $|x|_p \leqslant 1$ для рационального числа x?

16. Пусть $x \in \mathbb{Q}$. Докажите, что $\lim\limits_{i\to\infty} |x^i/i!|_p = 0$ тогда и только тогда, когда $\mathrm{ord}_p x \geqslant 1$ для $p \neq 2$ и $\mathrm{ord}_2 x \geqslant 2$.

17. Пусть x — ненулевое рациональное число. Докажите, что произведение чисел $|x|_p$ по *всем* простым p и $p=\infty$ равно 1: $\prod\limits_p |x|_p = 1$. (Отметим, что у этого «бесконечного произведения» в действительности лишь конечное число сомножителей, отличных от 1.)

18. Пусть p — простое число. Докажите, что каждая последовательность целых чисел содержит подпоследовательность Коши относительно нормы $|\ |_p$.

19. Пусть $x \in \mathbb{Q}$ и $|x|_p \leqslant 1$ для всех простых p. Докажите, что $x \in \mathbb{Z}$.

§ 3. КАК СТРОИТСЯ ПОЛЕ КОМПЛЕКСНЫХ ЧИСЕЛ

Теперь у нас есть новое понятие расстояния между рациональными числами: два рациональных числа в такой метрике тем ближе, чем на большую степень некоторого фиксированного простого p делится их разность. Чтобы работать с такими «p-адическими метриками», нам придется увеличить поле рациональных чисел $\mathbb{Q}$, подобно тому как в случае классической архимедовой метрики $|\ |$ оно пополняется до поля вещественных чисел $\mathbb{R}$ и затем расширяется до поля комплексных чисел $\mathbb{C}$. Поэтому прежде всего вспомним, как это делается.

Начнем с еще более ранней ступени, которая логически и исторически предшествовала определению поля $\mathbb{Q}$. Будем исходить из множества натуральных чисел $\mathbb{N} = \{1, 2, 3, \ldots\}$. Каждый шаг на пути от $\mathbb{N}$ к $\mathbb{C}$ можно мотивировать желанием делать без каких-либо ограничений следующие две операции:

(1) решать полиномиальные уравнения;
(2) находить пределы последовательностей Коши,

т. е. так «заполнить пробелы» в числовой системе, чтобы в новой числовой системе каждая последовательность Коши имела предел.

Прежде всего на этом пути можно ввести множество всех целых чисел $\mathbb{Z}$ (включающее 0, -1, -2, ...) как множество решений уравнений вида

$$a + x = b, \quad a,\ b \in \mathbb{N}.$$

После этого можно определить рациональные числа как решения уравнений вида

$$ax = b, \quad a,\ b \in \mathbb{Z}.$$

Пока что метрика не использовалась.

Один из возможных способов точного определения вещественных чисел заключается в рассмотрении множества S, состоящего из последовательностей Коши рациональных чисел. Назовем две последовательности $s_1 = \{a_j\} \in S$ и $s_2 = \{b_j\} \in S$ эквивалентными и будем писать $s_1 \sim s_2$, если $|a_j - b_j| \to 0$ при $j \to \infty$. Очевидно,

$\sim$ есть отношение эквивалентности, так как: (1) каждая последовательность s эквивалентна сама себе; (2) если $s_1 \sim s_2$, то $s_2 \sim s_1$; (3) если $s_1 \sim s_2$ и $s_2 \sim s_3$, то $s_1 \sim s_3$. Определим теперь $\mathbb{R}$ как множество *классов эквивалентности* последовательностей Коши рациональных чисел. На этом множестве нетрудно определить операции сложения, умножения и нахождения обратного относительно сложения и умножения, а затем показать, что $\mathbb{R}$ является полем. Хотя на первый взгляд это определение кажется громоздким и чересчур абстрактным, тем не менее оно приводит в точности к старинному образу вещественной числовой прямой, которая допускает простое наглядное представление.

Нечто подобное произойдет, когда мы станем работать с $|\ |_p$ вместо $|\ |$. Начав с абстрактного определения p-адического пополнения поля $\mathbb{Q}$, мы придем к числовой системе с очень прозрачной структурой, которую обозначим $\mathbb{Q}_p$.

Вернемся к нашему историческому экскурсу, где мы добрались до $\mathbb{R}$. Обратившись снова к первому методу расширения числовой системы — добавлению корней уравнений, математики сочли, что неплохо иметь в запасе числа, которые позволяли бы решать такие уравнения, как $x^2+1=0$. (Здесь мы излагаем логический ход событий; исторически введение комплексных чисел предшествовало строгому определению вещественных чисел в терминах последовательностей Коши.) Тут произошло нечто удивительное! Как только было введено число $i=\sqrt{-1}$ и определено поле комплексных чисел вида $a+bi$, $a, b \in \mathbb{R}$, оказалось, что:

(1) *все* полиномиальные уравнения с коэффициентами в $\mathbb{C}$ разрешимы в $\mathbb{C}$ — это знаменитая основная теорема алгебры (короче можно сказать так: поле $\mathbb{C}$ *алгебраически замкнуто*);

(2) поле $\mathbb{C}$ полно относительно (единственной) нормы $|\ |$ с $\mathbb{R}$ (эта норма задается формулой $|a+bi|=\sqrt{a^2+b^2}$), т. е. каждая последовательность Коши $\{a_j+b_ji\}$ имеет предел вида $a+bi$ (так как $\{a_j\}$ и $\{b_j\}$ — также последовательности Коши в $\mathbb{R}$, то в качестве a и b берутся их пределы).

Итак, в данном случае процесс оканчивается на $\mathbb{C}$, которое есть всего лишь «квадратичное расширение» поля $\mathbb{R}$ (т. е. оно получается присоединением корня квадратного уравнения $x^2+1=0$). *Поле $\mathbb{C}$ алгебраически замкнуто и полно относительно архимедовой метрики.*

Но увы! В случае нормы $|\ |_p$ все не так просто. Построив $\mathbb{Q}_p$, пополнение $\mathbb{Q}$ относительно $|\ |_p$, нам придется затем образовать бесконечную последовательность расширений, задаваемых присоединением корней уравнений старших степеней (не только квадратных). Хуже того, построенное в результате алгебраически замкнутое поле, которое обозначается через $\bar{\mathbb{Q}}_p$, *не полно*. Поэтому нужно будет «заткнуть дыры» в этом и так уже громадном поле, что приведет к еще большему полю Ω.

А что потом? Не придется ли еще увеличивать Ω, для того чтобы стали разрешимы все полиномиальные уравнения с коэффициентами в Ω? Не будет ли этот процесс продолжаться все дальше и дальше, как развертывающаяся спираль все более искусственных абстракций? К счастью, тут вмешивается ангел-хранитель p-адического анализа, и уже поле Ω оказывается алгебраически замкнутым и полным. На этом наш поиск неархимедова аналога поля $\mathbb{C}$ заканчивается.

Но это поле Ω, удобная числовая система, на которой можно было бы изучать p-адический вариант классического анализа, к сожалению, понято гораздо хуже, чем $\mathbb{C}$. Как заметил И. М. Гельфанд, даже некоторые из простейших вопросов, например описание всех $\mathbb{Q}_p$-линейных автоморфизмов поля Ω, остаются пока открытыми.

Итак, начнем наше путешествие к Ω.

§ 4. ПОЛЕ p-АДИЧЕСКИХ ЧИСЕЛ

До конца этой главы p обозначает фиксированное простое число.

Пусть S — множество таких последовательностей $\{a_i\}$ рациональных чисел, что при любом $\varepsilon>0$ существует такое N, что $|a_i-a_{i'}|_p<\varepsilon$ при $i, i'>N$. Две такие последовательности $\{a_i\}$ и $\{b_i\}$, называемые после-

довательностями Коши, считаются эквивалентными, если $|a_i - b_i|_p \to 0$ при $i \to \infty$. Множество $\mathbb{Q}_p$, по определению, есть множество классов эквивалентности этих последовательностей Коши.

Пусть $x \in \mathbb{Q}$. Обозначим через $\{x\}$ «постоянную» последовательность Коши, все члены которой равны x. Очевидно, $\{x\} \sim \{x'\}$ тогда и только тогда, когда $x = x'$. Класс $\{0\}$ обозначим просто через 0.

Определим норму $|\ |_p$ класса эквивалентности a как предел $\lim\limits_{i\to\infty} |a_i|_p$, где $\{a_i\}$ — некоторый представитель класса a. Этот предел существует, так как:

(1) если $a = 0$, то $\lim\limits_{i\to\infty} |a_i|_p = 0$ по определению;

(2) если $a \neq 0$, то для некоторого $\varepsilon > 0$ и любого N существует $i_N > N$ с $|a_{i_N}|_p > \varepsilon$.

Действительно, если N выбрано настолько большим, что $|a_i - a_{i'}|_p < \varepsilon$ при $i, i' > N$, то

$$|a_i - a_{i_N}|_p < \varepsilon \quad \text{для всех } i > N.$$

Так как $|a_{i_N}|_p > \varepsilon$, то $|a_i|_p = |a_{i_N}|_p$ по принципу равнобедренного треугольника. Поэтому $|a_i|_p$ имеет постоянное значение $|a_{i_N}|_p$ при всех $i > N$. А тогда предел $\lim\limits_{i\to\infty} |a_i|_p$ равен этому постоянному значению.

Следует отметить одно существенное отличие рассматриваемого сейчас процесса пополнения от пополнения $\mathbb{Q}$ до $\mathbb{R}$. Когда мы переходим от $\mathbb{Q}$ к $\mathbb{R}$, область возможных значений функции $|\ | = |\ |_\infty$ увеличивается до множества всех неотрицательных вещественных чисел. С другой стороны, при переходе от $\mathbb{Q}$ к $\mathbb{Q}_p$ множество возможных значений $|\ |_p$, а именно $\{p^n\}_{n\in\mathbb{Z}} \cup \{0\}$, остается одним и тем же.

Пусть a и b — два класса эквивалентности рассматриваемых последовательностей Коши, а $\{a_i\} \in a$ и $\{b_i\} \in b$ — их произвольные представители. Определим $a \cdot b$ как класс эквивалентности последовательности Коши $\{a_i b_i\}$. Если $\{a'_i\} \in a$, $\{b'_i\} \in b$ — другие представители, то

$$|a'_i b'_i - a_i b_i|_p = |a'_i (b'_i - b_i) + b_i (a'_i - a_i)|_p \leqslant$$
$$\leqslant \max\left(|a'_i (b'_i - b_i)|_p,\ |b_i (a'_i - a_i)|_p\right).$$

Первое выражение в последней строке при $i \to \infty$ стремится к $|a|_p \cdot \lim |b'_i - b_i|_p = 0$, а второе — к $|b|_p \times \lim |a'_i - a_i|_p = 0$. Следовательно, $\{a'_i b'_i\} \sim \{a_i b_i\}$.

Подобным же образом можно определить сумму двух классов эквивалентности последовательностей Коши, выбрав по последовательности в каждом из этих классов, сложив их почленно, а затем показав, что класс суммы зависит только от классов слагаемых. Аналогично определяется обратный класс относительно сложения.

Определяя обратный класс относительно умножения, нужно соблюдать осторожность, ибо в последовательности Коши могут встретиться нулевые члены. Однако легко увидеть, что каждая последовательность Коши эквивалентна некоторой последовательности Коши без нулевых членов (заменим, например, все $a_i = 0$ на $a'_i = p^i$). Рассмотрим после этого последовательность $\{1/a_i\}$. Она будет последовательностью Коши, за исключением случая $|a_i|_p \to 0$, т. е. $\{a_i\} \sim \{0\}$. Более того, если $\{a_i\} \sim \{a'_i\}$ и среди a_i, a'_i нет нулей, то, как легко доказать, $\{1/a_i\} \sim \{1/a'_i\}$.

После этого нетрудно установить, что множество $\mathbb{Q}_p$ классов эквивалентности последовательностей Коши вместе с введенными на нем операциями сложения, умножения и нахождения обратных элементов является полем. Проверим, например, дистрибутивность. Пусть $\{a_i\}$, $\{b_i\}$, $\{c_i\}$ — представители классов a, b, $c \in \mathbb{Q}_p$. Тогда $a(b+c)$ есть класс эквивалентности последовательности

$$\{a_i (b_i + c_i)\} = \{a_i b_i + a_i c_i\},$$

но $ab + ac$ также совпадает с классом эквивалентности этой последовательности.

Поле $\mathbb{Q}$ можно отождествить с *подполем* в $\mathbb{Q}_p$, которое состоит из классов, содержащих постоянные последовательности Коши.

И, наконец, легко доказать полноту поля $\mathbb{Q}_p$. Действительно, пусть $\{a_j\}_{j=1,2,\ldots}$ — последовательность классов эквивалентности, являющаяся последовательностью Коши в $\mathbb{Q}_p$. Выберем в каждом члене a_j этой последовательности по представителю, т. е. по последовательности Коши рациональных чисел $\{a_{ji}\}_{i=1,2,\ldots}$. Тогда,

как легко показать, предел последовательности a_j равен классу эквивалентности последовательности $\{a_{jj}\}_{j=1,2,\ldots}$. Проведение доказательства мы оставляем читателю.

Вероятно, в каждом курсе или семинаре полезно проделать один раз все хлопотные проверки такого рода, чтобы не забыть полностью об аксиоматическом основании, на котором покоится все остальное. В этом частном случае абстрактный подход позволяет, кроме того, сравнить p-адическую конструкцию с конструкцией вещественных чисел и убедиться в логическом совпадении этих процедур. Однако после доказательства следующей теоремы благоразумно как можно быстрее забыть все, что связано с классами эквивалентности последовательностей Коши, и начать мыслить более конкретными понятиями.

Теорема 2. *Каждый класс эквивалентности a из $\mathbb{Q}_p$ с $|a|_p \leqslant 1$ содержит ровно одну последовательность Коши целых чисел $\{a_i\}$, для которой:*

(1) $0 \leqslant a_i < p^i$ *при* $i = 1, 2, 3, \ldots$;

(2) $a_i \equiv a_{i+1} \pmod{p^i}$ *при* $i = 1, 2, 3, \ldots$.

Доказательство. Докажем прежде всего единственность. Если $\{a'_i\}$ — другая последовательность, удовлетворяющая (1) и (2), то $a_{i_0} \neq a'_{i_0}$ для некоторого i_0. Отсюда $a_{i_0} \not\equiv a'_{i_0} \pmod{p^{i_0}}$, так как оба эти числа расположены между 0 и p^{i_0}. Но тогда для каждого $i \geqslant i_0$ имеем $a_i \equiv a_{i_0} \not\equiv a'_{i_0} \equiv a'_i \pmod{p^{i_0}}$, т. е. $a_i \not\equiv a'_i \pmod{p^{i_0}}$. Следовательно,

$$|a_i - a'_i|_p > 1/p^{i_0}$$

для всех $i \geqslant i_0$ и $\{a_i\} \not\sim \{a'_i\}$.

Теперь предположим, что задана некоторая последовательность Коши $\{b_i\} \in a$ и мы хотим найти эквивалентную ей последовательность $\{a_i\}$, удовлетворяющую (1) и (2). Используем для этого одну простую лемму.

Лемма. *Пусть $x \in \mathbb{Q}$ и $|x|_p \leqslant 1$. Тогда для любого натурального i существует целое $\alpha \in \mathbb{Z}$, для которого $|\alpha - x|_p \leqslant p^{-i}$. Более того, такое α можно выбрать из множества $\{0, 1, 2, 3, \ldots, p^i - 1\}$.*

Доказательство леммы. Пусть $x = a/b$ — несократимая дробь. Тогда p не делит b, так как $|x|_p \leqslant 1$. Следовательно, b и p^i взаимно просты. Поэтому можно найти два целых числа m и n, для которых $mb + np^i = 1$. Положим $\alpha = am$. Идея дальнейшего вычисления заключается в том, что число mb отличается от 1 на p-адически малую величину и, значит, m хорошо приближает $1/b$, а потому am хорошо приближает $x = a/b$. Точнее, имеет место оценка

$$|\alpha - x|_p = |am - (a/b)|_p = |a/b|_p\,|mb - 1|_p \leqslant$$
$$\leqslant |mb - 1|_p = |np^i|_p = |n|_p/p^i \leqslant 1/p^i.$$

Наконец, для того чтобы число α принадлежало указанному в лемме интервалу целых чисел между 0 и p^i, достаточно добавить к нему подходящее кратное p^i; при этом неравенство $|\alpha - x|_p \leqslant p^{-i}$ сохранится. Лемма доказана. □

Вернемся к доказательству теоремы. Пусть $\{b_i\}$ — наша последовательность Коши. Сопоставим каждому $j = 1, 2, 3, \ldots$ такое натуральное число $N(j)$, что $|b_i - b_{i'}|_p \leqslant p^{-j}$ при любых i, $i' \geqslant N(j)$. (Мы можем считать, что последовательность чисел $N(j)$ строго возрастает с увеличением j; в частности, $N(j) \geqslant j$.) Тогда $|b_i|_p \leqslant 1$ при $i \geqslant N(1)$, потому что для любого $i' \geqslant N(1)$

$$|b_i|_p \leqslant \max(|b_{i'}|_p,\ |b_i - b_{i'}|_p) \leqslant \max(|b_{i'}|_p,\ 1/p),$$

а $|b_{i'}|_p \to |a|_p \leqslant 1$ при $i' \to \infty$.

По предыдущей лемме мы можем найти теперь последовательность целых чисел a_j, для которой $0 \leqslant a_j < p^j$ и

$$|a_j - b_{N(j)}|_p \leqslant 1/p^j.$$

Утверждается, что последовательность $\{a_j\}$ удовлетворяет всем необходимым требованиям. Очевидно, для этого достаточно проверить сравнения $a_{j+1} \equiv a_j \pmod{p^j}$ и эквивалентность $\{b_i\} \sim \{a_j\}$. Первое следует из неравенств

$$|a_{j+1} - a_j| = |a_{j+1} - b_{N(j+1)} + b_{N(j+1)} - b_{N(j)} - (a_j - b_{N(j)})|_p \leqslant$$
$$\leqslant \max(|a_{j+1} - b_{N(j+1)}|_p,\ |b_{N(j+1)} - b_{N(j)}|_p,\ |a_j - b_{N(j)}|_p) \leqslant$$
$$\leqslant \max(1/p^{j+1},\ 1/p^j,\ 1/p^j) = 1/p^j.$$

Для доказательства второго утверждения возьмем произвольное j. Тогда для любого $i \geqslant N(j)$

$$|a_i - b_i|_p = |a_i - a_j + a_j - b_{N(j)} - (b_i - b_{N(j)})|_p \leqslant$$
$$\leqslant \max(|a_i - a_j|_p, |a_j - b_{N(j)}|_p, |b_i - b_{N(j)}|_p) \leqslant$$
$$\leqslant \max(1/p^j, 1/p^j, 1/p^j) = 1/p^j.$$

Поэтому $|a_i - b_i|_p \to 0$ при $i \to \infty$, и теорема доказана. □

Что делать, если наше p-адическое число a не удовлетворяет неравенству $|a|_p \leqslant 1$? В этом случае умножим a на подходящую степень p^m числа p (например, на степень числа p, равную $|a|_p$) так, чтобы новое p-адическое число $a' = ap^m$ уже удовлетворяло неравенству $|a'|_p \leqslant 1$. Выберем затем в соответствии с теоремой 2 последовательность $\{a_i'\}$, представляющую a'. Тогда число $a = a'p^{-m}$ представляется последовательностью $\{a_i\}$ с $a_i = a_i' p^{-m}$.

Для удобства запишем теперь все числа a_i' последовательности, соответствующей a', в p-ичной системе счисления, т. е. положим

$$a_i' = b_0 + b_1 p + b_2 p^2 + \ldots + b_{i-1} p^{i-1},$$

где коэффициенты b_j обозначают «p-ичные знаки», т. е. целые числа из множества $\{0, 1, \ldots, p-1\}$. Сравнение $a_i' \equiv a_{i+1}' \pmod{p^i}$ из теоремы 2 эквивалентно тому, что все знаки числа

$$a_{i+1}' = b_0 + b_1 p + b_2 p^2 + \ldots + b_{i-1} p^{i-1} + b_i p^i,$$

от b_0 до b_{i-1} включительно, *совпадают* с соответствующими знаками числа a_i'. Поэтому a' можно представлять себе интуитивно как число, имеющее бесконечную вправо p-ичную запись: всякий раз, переходя от a_i' к a_{i+1}', мы добавляем в этой записи новый знак.

Теперь и наше исходное число a можно представлять себе как p-ичное число с конечным числом знаков «направо от запятой» (т. е. знаков, соответствующих отрицательным степеням p; в нашей записи они начинаются слева), но с бесконечным числом знаков при положительных степенях p:

$$a = \frac{b_0}{p^m} + \frac{b_1}{p^{m-1}} + \ldots + \frac{b_{m-1}}{p} + b_m + b_{m+1} p + b_{m+2} p^2 + \ldots.$$

Пока что правую часть этого равенства следует понимать как сокращенную запись последовательности $\{a_i\}$, где $a_i = b_0 p^{-m} + \ldots + b_{i-1} p^{i-1-m}$, т. е. как удобный способ изображения сразу всей последовательности $\{a_i\}$. Вскоре мы убедимся, что в некотором точном смысле это равенство есть «настоящее равенство». Оно называется «p-адическим разложением» числа a.

Пусть $\mathbb{Z}_p = \{a \in \mathbb{Q}_p \mid |a|_p \leqslant 1\}$. Это множество всех чисел из $\mathbb{Q}_p$, p-адическое разложение которых не содержит отрицательных степеней p. Элементы $\mathbb{Z}_p$ называются *целыми p-адическими числами*. (Чтобы избежать путаницы, начиная с этого места обычные целые из $\mathbb{Z}$ мы называем *целыми рациональными*.) Сумма, разность и произведение двух элементов из $\mathbb{Z}_p$ снова принадлежат $\mathbb{Z}_p$. Поэтому $\mathbb{Z}_p$ — *подкольцо* поля $\mathbb{Q}_p$.

Пусть $a, b \in \mathbb{Q}_p$. Мы пишем $a \equiv b \pmod{p^n}$, если $|a - b|_p \leqslant p^{-n}$, или, эквивалентно, $(a-b)/p^n \in \mathbb{Z}_p$, т. е. если первый отличный от нуля знак в p-адическом разложении числа $a - b$ встречается не ранее, чем на p^n-м месте. В случае когда a и b лежат не только в $\mathbb{Q}_p$, но также и в $\mathbb{Z}$ (т. е. они целые рациональные), это определение согласуется с данным выше определением сравнения $a \equiv b \pmod{c}$ для $c = p^n$.

В дальнейшем через $\mathbb{Z}_p^\times$ будем обозначать множество $\{x \in \mathbb{Z}_p \mid 1/x \in \mathbb{Z}_p\}$, или, эквивалентно, $\{x \in \mathbb{Z}_p \mid x \not\equiv 0 \pmod{p}\}$, или, эквивалентно, $\{x \in \mathbb{Z}_p \mid |x|_p = 1\}$. Целые p-адические числа из $\mathbb{Z}_p^\times$, т. е. числа, имеющие ненулевой первый знак, называют иногда p-адическими единицами.

Пусть теперь $\{b_i\}_{i=-m}^{\infty}$ — произвольная последовательность целых p-адических чисел. Рассмотрим частичные суммы

$$S_N = \frac{b_{-m}}{p^m} + \frac{b_{-m+1}}{p^{m-1}} + \ldots + b_0 + b_1 p + b_2 p^2 + \ldots + b_N p^N.$$

Последовательность, состоящая из этих сумм, является последовательностью Коши: если $M > N$, то $|S_N - S_M|_p < 1/p^N$. Следовательно, она сходится к некоторому элементу из $\mathbb{Q}_p$. Как и в случае бесконечных рядов вещест-

венных чисел, определим $\sum_{i=-m}^{\infty} b_i p^i$ как предел последовательности частичных сумм в $\mathbb{Q}_p$.

Более общо, если $\{c_i\}$ — *произвольная* последовательность p-адических чисел и $|c_i|_p \to 0$ при $i \to \infty$, то последовательность частичных сумм $S_N = c_1 + c_2 + \ldots + c_N$ сходится к пределу, который обозначается через $\sum_{i=1}^{\infty} c_i$. В самом деле, $|S_M - S_N|_p = |c_{N+1} + c_{N+2} + \ldots + c_M|_p \leqslant \max(|c_{N+1}|_p, |c_{N+2}|_p, \ldots, |c_M|_p)$, а потому $\to 0$ при $N \to \infty$. Отсюда видно, что проверять сходимость бесконечных p-адических рядов проще, чем бесконечных рядов вещественных чисел. *Ряд сходится в поле $\mathbb{Q}_p$ тогда и только тогда, когда последовательность его членов стремится к нулю.* В p-адическом случае нет ничего подобного гармоническому ряду $1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \ldots$ вещественных чисел, который расходится, несмотря на то, что его члены стремятся к 0. Напомним, почему это так: норма $|\ |_p$ суммы двух чисел не превосходит *максимума* (а не суммы) норм слагаемых, если $p \neq \infty$, т. е. если норма $|\ |_p$ неархимедова.

Вернемся к p-адическим разложениям. Бесконечный ряд

$$\frac{b_0}{p^m} + \frac{b_1}{p^{m-1}} + \ldots + \frac{b_{m-1}}{p} + b_m + b_{m+1}p + b_{m+2}p^2 + \ldots$$

(здесь $b_i \in \{0, 1, 2, \ldots, p-1\}$) в определении p-адического разложения сходится к a. Значит, это выражение можно истолковать содержательно как сумму бесконечного ряда.

Отметим, что утверждаемая в теореме 2 единственность не имеет места в архимедовом случае. Так, всякая конечная десятичная дробь может быть записана и в виде десятичной дроби с бесконечно повторяющейся цифрой 9 на конце, например $1 = 0{,}9999\ldots$. В противоположность этому два p-адических разложения, сходящихся к одному и тому же числу из $\mathbb{Q}_p$, совпадают, т. е. имеют все одинаковые знаки.

В заключение сделаем еще одно замечание. В качестве множества p-ичных знаков мы могли бы выбрать не только $\{0, 1, 2, \ldots, p-1\}$, но также и любое другое множество $S = \{\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_{p-1}\}$ целых p-адических чисел, для которых $\alpha_i \equiv i \pmod p$ при $i = 0, 1, 2, \ldots, p-1$. Тогда p-адическое разложение можно определить как сумму вида $\sum_{i=-m}^{\infty} = b_i p^i$, где теперь роль «знаков» b_i играют элементы множества S, а не множества $\{0, 1, \ldots, p-1\}$. Множество $\{0, 1, \ldots, p-1\}$ подходит для почти всех надобностей. Тем не менее существует другое множество S, в некоторых отношениях более естественное. Это множество так называемых представителей Тейхмюллера (см. ниже упр. 12).

§ 5. АРИФМЕТИКА В $\mathbb{Q}_p$

Техника выполнения операций сложения, вычитания, умножения и деления p-адических чисел во многом напоминает соответствующие операции с десятичными дробями, изучаемые в начальной школе. Единственное отличие в том, что «занимание», «перенос в другой разряд», «умножение столбиком» и т. д. делаются слева направо, а не справа налево. Вот несколько примеров вычислений в $\mathbb{Q}_7$:

$$\begin{array}{r} 3+6\times7+2\times7^2+\ldots \\ \times\ 4+5\times7+1\times7^2+\ldots \\ \hline 5+4\times7+4\times7^2+\ldots \\ 1\times7+4\times7^2+\ldots \\ 3\times7^2+\ldots \\ \hline 5+5\times7+4\times7^2+\ldots \end{array} \qquad \begin{array}{r} 2\times7^{-1}+0\times7^0+3\times7^1+\ldots \\ -\ 4\times7^{-1}+6\times7^0+5\times7^1+\ldots \\ \hline 5\times7^{-1}+0\times7^0+4\times7^1+\ldots \end{array}$$

$$\begin{array}{r} 1+2\times7+4\times7^2+\ldots \\ 1+6\times7+1\times7^2+\ldots \\ \hline 3\times7+2\times7^2+\ldots \\ 3\times7+5\times7^2+\ldots \\ \hline 4\times7^2+\ldots \\ 4\times7^2+\ldots \end{array} \qquad \begin{array}{|r} 3+5\times7+1\times7^2+\ldots \\ \hline 5+1\times7+6\times7^2+\ldots \end{array}$$

В качестве еще одного примера попробуем извлечь корень $\sqrt{6}$ в $\mathbb{Q}_5$. Мы хотим найти последовательность целых чисел a_0, a_1, a_2, ..., для которой $0 \leqslant a_i \leqslant 4$ и

$$(a_0 + a_1 \times 5 + a_2 \times 5^2 + \ldots)^2 = 1 + 1 \times 5.$$

Сравнивая коэффициенты при $1 = 5^0$ в обеих частях равенства, получаем $a_0^2 \equiv 1 \pmod 5$, откуда $a_0 = 1$ или 4. Возьмем $a_0 = 1$. Тогда, сравнивая коэффициенты при 5 в обеих частях, получаем $2a_1 \times 5 \equiv 1 \times 5^2 \pmod{5^2}$. Следовательно, $2a_1 \equiv 1 \pmod 5$ и $a_1 = 3$. На следующем шаге мы должны решить сравнение

$$1 + 1 \times 5 \equiv (1 + 3 \times 5 + a_2 \times 5^2)^2 \equiv$$
$$\equiv 1 + 1 \times 5 + 2a_2 \times 5^2 \pmod{5^3}.$$

Следовательно, $2a_2 \equiv 0 \pmod 5$ и $a_2 = 0$. Продолжая этот процесс далее, получаем ряд

$$a = 1 + 3 \times 5 + 0 \times 5^2 + 4 \times 5^3 + a_4 \times 5^4 + a_5 \times 5^5 + \ldots,$$

в котором каждый коэффициент a_i определяется однозначно после выбора a_0.

Напомним, однако, что при выборе a_0 мы имели две возможности, а именно 1 или 4. А если бы мы выбрали 4, а не 1? В этом случае мы получили бы

$$-a = 4 + 1 \times 5 + 4 \times 5^2 + 0 \times 5^3 +$$
$$+ (4 - a_4) \times 5^4 + (4 - a_5) \times 5^5 + \ldots.$$

Тот факт, что для a_0 имеется два возможных выбора и что, когда выбор сделан, последующие числа a_1, a_2, a_3, ... определены однозначно, просто отражает то обстоятельство, что в таких полях, как $\mathbb{Q}$, $\mathbb{R}$ или $\mathbb{Q}_p$, если у ненулевого элемента есть хоть один квадратный корень, то их ровно два.

Всякое ли число из $\mathbb{Q}_5$ имеет квадратный корень? Мы видели, что 6 имеет. А 7? Из равенства

$$(a_0 + a_1 \times 5 + \ldots)^2 = 2 + 1 \times 5$$

следовало бы сравнение $a_0^2 \equiv 2 \pmod 5$. Но оно неразрешимо — это легко установить перебором всех значений $a_0 = 0, 1, 2, 3, 4$. Поэтому 7 не имеет квадратного корня в $\mathbb{Q}_5$. Более систематическое представление о квадратных корнях в $\mathbb{Q}_p$ можно получить из упр. 5 — 11.

Как показывает следующая важная «лемма», изложенный выше метод решения уравнения $x^2 - 6 = 0$ в $\mathbb{Q}_5$ — решение сравнения $a_0^2 - 6 \equiv 0 \pmod 5$ и затем последовательное нахождение остальных a_i — является весьма общим.

Теорема 3 (лемма Гензеля). *Пусть* $F(x) = c_0 + c_1 x + \ldots + c_n x^n$ *— многочлен с целыми p-адическими коэффициентами, а* $F'(x) = c_1 + 2c_2 x + 3c_3 x^2 + \ldots + nc_n x^{n-1}$ *— его производная. Предположим, что* a_0 *— целое p-адическое число, для которого* $F(a_0) \equiv 0 \pmod p$, *а* $F'(a_0) \not\equiv 0 \pmod p$. *Тогда существует единственное целое p-адическое число a, такое, что*

$$F(a) = 0 \text{ и } a \equiv a_0 \pmod p.$$

(*Замечание.* В нашем примере $F(x) = x^2 - 6$, $F'(x) = 2x$, $a_0 = 1$.)

Доказательство леммы Гензеля. Прежде всего утверждается существование и единственность последовательности целых рациональных чисел a_1, a_2, a_3, ..., для которой при любом $n \geqslant 1$:

(1) $F(a_n) \equiv 0 \pmod{p^{n+1}}$;
(2) $a_n \equiv a_{n-1} \pmod{p^n}$;
(3) $0 \leqslant a_n < p^{n+1}$.

Докажем это индукцией по n.

Пусть $n = 1$. Обозначим через $\tilde{a}_0$ единственное целое число из множества $\{0, 1, \ldots, p-1\}$, сравнимое с a_0 по модулю p. Тогда всякое a_1, удовлетворяющее (2) и (3), можно представить в виде $\tilde{a}_0 + b_1 p$, где $0 \leqslant b_1 \leqslant p - 1$. Рассмотрим выражение $F(\tilde{a}_0 + b_1 p)$ и раскроем в нем скобки, помня, что нас интересует результат только по модулю p^2, так что все члены, делящиеся на p^2, можно опускать:

$$F(a_1) = F(\tilde{a}_0 + b_1 p) = \sum c_i (\tilde{a}_0 + b_1 p)^i =$$
$$= \sum (c_i \tilde{a}_0^i + i c_i \tilde{a}_0^{i-1} b_1 p + \text{члены, делящиеся на } p^2) \equiv$$
$$\equiv \sum c_i \tilde{a}_0^i + \left(\sum i c_i \tilde{a}_0^{i-1}\right) b_1 p \pmod{p^2} =$$
$$= F(\tilde{a}_0) + F'(\tilde{a}_0)\, b_1 p.$$

(Обратите внимание на сходство с формулой из анализа для приближения первого порядка функции рядом Тейлора: $F(x+h)=F(x)+F'(x)h+$ члены более высокого порядка.) По предположению, $F(a_0)\equiv 0 \pmod p$, откуда $F(\tilde a_0)\equiv \alpha p \pmod{p^2}$ для некоторого $\alpha\in\{0, 1, \ldots, p-1\}$. Поэтому сравнение $F(a_1)\equiv 0 \pmod{p^2}$ эквивалентно сравнению $\alpha p + F'(\tilde a_0) b_1 p \equiv 0 \pmod{p^2}$, или $\alpha + F'(\tilde a_0) b_1 \equiv 0 \pmod p$. Так как, по предположению, $F'(a_0)\not\equiv 0 \pmod p$, последнее сравнение разрешимо относительно неизвестного b_1. Действительно, пользуясь леммой из доказательства теоремы 2, выберем такое $b_1\in\{0, 1, \ldots, p-1\}$, что $b_1\equiv -\alpha/F'(\tilde a_0) \pmod p$. Очевидно, $b_1\in\{0, 1, \ldots, p-1\}$, удовлетворяющее данному условию, единственно.

Теперь, переходя к общему шагу индукции, предположим, что мы уже отыскали $a_1, a_2, \ldots, a_{n-1}$. Требуется найти a_n. По условиям (2) и (3) это число вида $a_n = a_{n-1} + b_n p^n$, где $b_n\in\{0, 1, \ldots, p-1\}$. Раскроем скобки и приведем выражение $F(a_{n-1}+b_n p^n)$ к подходящему виду, как и выше в случае $n=1$, только на этот раз не будем учитывать члены, делящиеся на p^{n+1}. Получим

$$F(a_n) = F(a_{n-1}+b_n p^n) \equiv F(a_{n-1}) + F'(a_{n-1}) b_n p^n \pmod{p^{n+1}}.$$

Так как по индуктивному предположению $F(a_{n-1})\equiv 0 \pmod{p^n}$, то $F(a_{n-1})\equiv \alpha' p^n \pmod{p^{n+1}}$. Нужное нам условие $F(a_n)\equiv 0 \pmod{p^{n+1}}$ принимает вид

$$\alpha' p^n + F'(a_{n-1}) b_n p^n \equiv 0 \pmod{p^{n+1}}, \quad \text{т. е.}$$
$$\alpha' + F'(a_{n-1}) b_n \equiv 0 \pmod p.$$

Из сравнения $a_{n-1}\equiv a_0 \pmod p$ легко вывести, что $F'(a_{n-1})\equiv F'(a_0)\not\equiv 0 \pmod p$. Тогда требуемое $b_n\in\{0, 1, \ldots, p-1\}$ находится точно так же, как и b_1 в рассмотренном выше случае, т. е. из сравнения $b_n\equiv -\alpha'/F'(a_{n-1}) \pmod p$. На этом индукция заканчивается, и наше утверждение доказано.

Теорема следует теперь непосредственно из этого утверждения. Действительно, возьмем $a=\tilde a_0 + b_1 p + b_2 p^2 + \ldots$. Тогда p-адическое число $F(a)$ равно 0, так как $F(a)\equiv F(a_n)\equiv 0 \pmod{p^{n+1}}$ для всех n. Обратно,

если a удовлетворяет требованиям теоремы и $a=\tilde a_0 + b_1 p + b_2 p^2 + \ldots$ — его p-адическое разложение, то последовательность $\{a_n\}$ удовлетворяет требованиям доказанного утверждения. Отсюда получаем единственность такой последовательности, а значит, и единственность искомого a. Лемма Гензеля доказана. □

Лемму Гензеля часто называют p-адической леммой Ньютона, потому что метод последовательного приближения, использованный в ее доказательстве, по существу

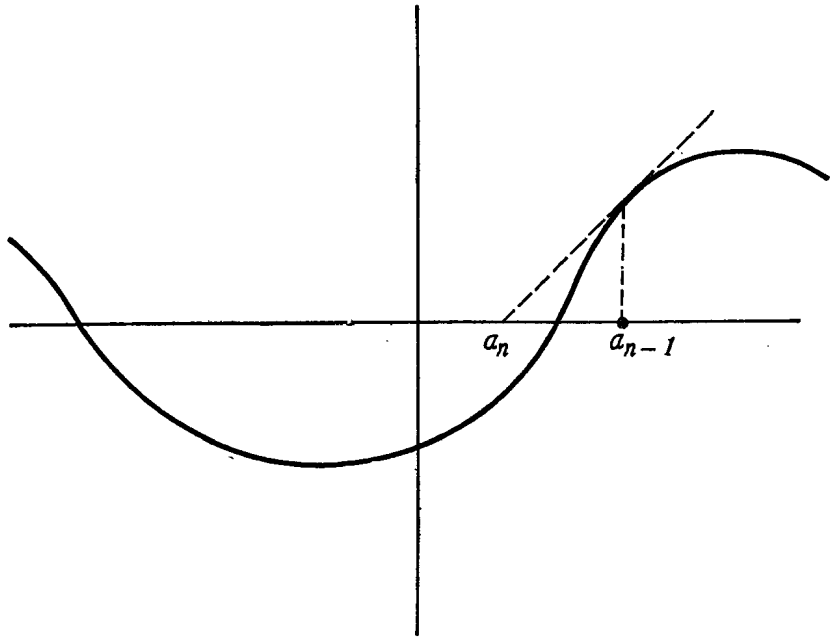


Рис. I.1. Метод Ньютона в вещественном случае.

совпадает с методом Ньютона нахождения *вещественного* корня вещественного многочлена. Если $f'(a_{n-1})\neq 0$, то в вещественном случае по методу Ньютона в качестве следующего приближения берется

$$a_n = a_{n-1} - \frac{f(a_{n-1})}{f'(a_{n-1})}$$

(см. рис. I.1). Поправочный член $-f(a_{n-1})/f'(a_{n-1})$ в этой формуле очень похож на «поправочный член» в дока-

зательстве леммы Гензеля:

$$b_n p^n \equiv -\frac{\alpha' p^n}{F'(a_{n-1})} \equiv -\frac{F(a_{n-1})}{F'(a_{n-1})} \pmod{p^{n+1}}.$$

Но в одном отношении p-адический метод Ньютона (лемма Гензеля) лучше, чем метод Ньютона в вещественном случае. В p-адическом варианте *гарантирована* сходимость к некоторому корню многочлена. В вещественном же случае метод Ньютона *обычно* сходится,

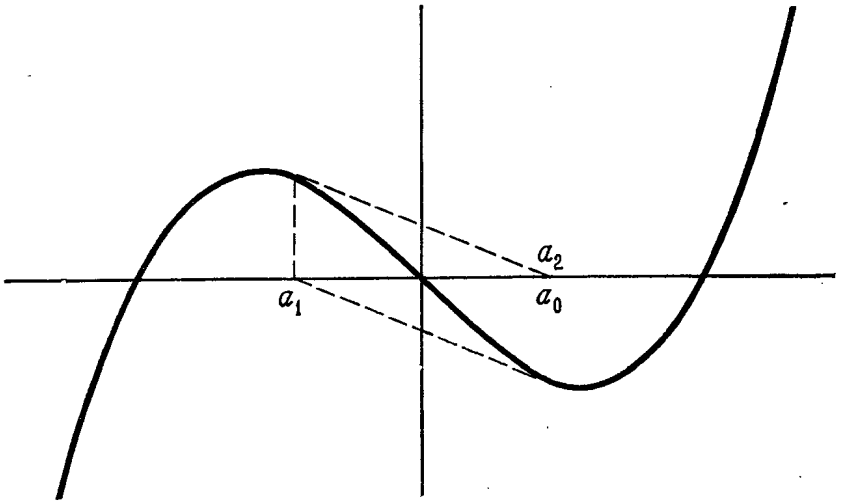


Рис. I.2. Неудачное применение метода Ньютона в вещественном случае.

но — не всегда. Например, если мы рассмотрим $f(x) = x^3 - x$ и сделаем неудачный выбор $a_0 = 1/\sqrt{5}$, то получим

$$a_1 = 1/\sqrt{5} - [1/5\sqrt{5} - 1/\sqrt{5}]/(3/5 - 1) = (1/\sqrt{5})[1 - (1/5 - 1)/(3/5 - 1)] = -1/\sqrt{5};$$

$$a_2 = 1/\sqrt{5}; \quad a_3 = -1/\sqrt{5}$$

и т. д. (см. рис. I.2). В $\mathbb{Q}_p$ такая несуразица невозможна.

Упражнения

1. Пусть $a \in \mathbb{Q}_p$ имеет p-адическое разложение $a_{-m}p^{-m} + a_{-m+1}p^{-m+1} + \ldots + a_0 + a_1 p \ldots$. Как выглядит p-адическое разложение $-a$?

2. Найдите p-адическое разложение для:

(i) $(6+4\times7+2\times7^2+1\times7^3+\ldots)(3+0\times7+0\times7^2+6\times7^3+\ldots)$ в $\mathbb{Q}_7$ с четырьмя знаками;
(ii) $1/(3+2\times5+3\times5^2+1\times5^3+\ldots)$ в $\mathbb{Q}_5$ с четырьмя знаками;
(iii) $9\times11^2-(3\times11^{-1}+2+1\times11^1+3\times11^2+\ldots)$ в $\mathbb{Q}_{11}$ с четырьмя знаками;
(iv) 2/3 в $\mathbb{Q}_2$; (v) $-1/6$ в $\mathbb{Q}_7$; (vi) 1/10 в $\mathbb{Q}_{11}$;
(vii) $-9/16$ в $\mathbb{Q}_{13}$; (viii) 1/1000 в $\mathbb{Q}_5$; (ix) 6! в $\mathbb{Q}_3$;
(x) 1/3! в $\mathbb{Q}_3$; (xi) 1/4! в $\mathbb{Q}_2$; (xii) 1/5! в $\mathbb{Q}_5$.

3. Докажите, что p-адическое разложение числа $a \in \mathbb{Q}_p$ обрывается (т. е. $a_i = 0$ для всех i, больших некоторого N) тогда и только тогда, когда a является *положительным* рациональным числом со знаменателем, равным степени p.

4. Докажите, что p-адическое разложение числа $a \in \mathbb{Q}_p$ начиная с некоторого места периодично (т. е. $a_{i+r} = a_i$ при некотором r и всех i, больших некоторого N) тогда и только тогда, когда $a \in \mathbb{Q}$.

5. Докажите следующее обобщение леммы Гензеля. Пусть $F(x)$ — многочлен с коэффициентами в $\mathbb{Z}_p$. Если для некоторого $a_0 \in \mathbb{Z}_p$ мы имеем $F(a_0) \equiv 0 \pmod{p^{2M+1}}$, $F'(a_0) \equiv 0 \pmod{p^M}$, но $F'(a_0) \not\equiv 0 \pmod{p^{M+1}}$, то существует и притом единственное $a \in \mathbb{Z}_p$, для которого $F(a) = 0$ и $a \equiv a_0 \pmod{p^{M+1}}$.

6. Воспользовавшись своим доказательством упр. 5, найдите квадратный корень из -7 в $\mathbb{Q}_2$ с пятью знаками.

7. Какие из следующих 11-адических чисел имеют квадратные корни в $\mathbb{Q}_{11}$?

(i) 5; (ii) 7; (iii) -7;
(iv) $5+3\times11+9\times11^2+1\times11^3$;
(v) $3\times11^{-2}+6\times11^{-1}+3+0\times11+7\times11^2$;
(vi) $3\times11^{-1}+6+3\times11+0\times11^2+7\times11^3$;
(vii) 1×11^7; (viii) $7-6\times11^2$; (ix) $5\times11^{-2}+\sum_{n=0}^{\infty} n\times11^n$.

8. Вычислите $\pm\sqrt{-1}$ в $\mathbb{Q}_{13}$ с четырьмя знаками.

9. Для каких $p = 2, 3, 5, 7, 11, 13, 17, 19$ можно извлечь квадратный корень из -1 в $\mathbb{Q}_p$?

10. Пусть p — произвольное нечетное простое число. Предположим, что $\alpha \in \mathbb{Q}_p$ и $|\alpha|_p = 1$. Опишите способ узнать, существует или нет квадратный корень из α в $\mathbb{Q}_p$. Как действовать, если $|\alpha|_p \neq 1$? Докажите существование такой четверки чисел α_1, α_2, α_3, $\alpha_4 \in \mathbb{Q}_p$, что для любого отличного от нуля $\alpha \in \mathbb{Q}_p$ среди чисел $\alpha_1\alpha$, $\alpha_2\alpha$, $\alpha_3\alpha$, $\alpha_4\alpha$ ровно одно имеет квадратный корень в $\mathbb{Q}_p$. (Если заменить p на ∞, а $\mathbb{Q}_p$ на $\mathbb{R}$, то существуют *два* числа, например ± 1, таких, что для любого ненулевого $\alpha \in \mathbb{R}$ ровно одно из чисел $1 \cdot \alpha$ и $-1 \cdot \alpha$ имеет квадратный корень в $\mathbb{R}$.)

11. Решите ту же задачу, что и в упр. 10, для $p=2$. В этом случае требуется найти *восемь* чисел $\alpha_1, \ldots, \alpha_8 \in \mathbb{Q}_2$, таких, что для любого ненулевого $\alpha \in \mathbb{Q}_2$ ровно одно из чисел $\alpha_1\alpha, \ldots, \alpha_8\alpha$ имеет квадратный корень в $\mathbb{Q}_2$. (Конечно, выбор такой восьмерки $\alpha_1, \ldots, \alpha_8$ *не однозначен*.)

12. Найдите первые четыре знака p-адических разложений всех четырех корней степени 4 из 1 в $\mathbb{Q}_5$. Докажите, что уравнение $x^p - x = 0$ всегда имеет p решений $a_0, a_1, \ldots a_{p-1}$ в $\mathbb{Q}_p$, для которых $a_i \equiv i \pmod p$. Эти p чисел называются представителями Тейхмюллера для $\{0, 1, 2, \ldots, p-1\}$ и используются иногда в качестве p-ичных знаков вместо $\{0, 1, 2, \ldots, p-1\}$.

13. Докажите следующий «признак неприводимости Эйзенштейна». Пусть $f(x) = a_0 + a_1x + \ldots + a_nx^n$ — многочлен с коэффициентами $a_i \in \mathbb{Z}_p$. Если $a_i \equiv 0 \pmod p$ при $i = 0, 1, 2, \ldots, n-1$, $a_n \not\equiv 0 \pmod p$ и $a_0 \not\equiv 0 \pmod{p^2}$, то $f(x)$ неприводим над $\mathbb{Q}_p$, т. е. не представим в виде произведения двух многочленов меньшей степени с коэффициентами в $\mathbb{Q}_p$.

14. Используя упр. 13, покажите, что 1 не имеет других корней степени p, кроме 1, в $\mathbb{Q}_p$ при $p > 2$. (*Указание*: подставьте $y = x - 1$ в $(x^p - 1)/(x - 1)$.) Докажите это также другим способом: представьте любой такой кореиь x в виде $1 + p^r x'$, где $|x'|_p = 1$, а $r > 0$ — некоторое целое (объясните, почему $x \equiv 1 \pmod p$), затем это выражение для x возведите в степень p, раскройте скобки и сравните коэффициенты при степенях p.

15. Докажите, что ряд $1 + p + p^2 + p^3 + \ldots$ сходится к $1/(1-p)$ в $\mathbb{Q}_p$. К чему сходятся $1 - p + p^2 - p^3 + p^4 - p^5 + \ldots$ и $1 + (p-1)p + p^2 + (p-1)p^3 + p^4 + (p-1)p^5 + \ldots$?

16. Предположим, что n — целое (положительное или отрицательное) число, не делящееся на p, и $\alpha \equiv 1 \pmod p$. Покажите, что α имеет корень степени n в $\mathbb{Q}_p$. Приведите пример, показывающий, что при $p = n$ это неверно. Покажите, что α имеет корень степени p, если $\alpha \equiv 1 \pmod{p^2}$ и $p \neq 2$.

17. Пусть $\alpha \in \mathbb{Z}_p$. Докажите сравнения $\alpha^{p^M} \equiv \alpha^{p^{M-1}} \pmod{p^M}$ для $M = 1, 2, 3, 4, \ldots$. Докажите, что последовательность $\{\alpha^{p^M}\}$ стремится к некоторому пределу в $\mathbb{Q}_p$ и что этот предел равен представителю Тейхмюллера, сравнимому с α по модулю p.

18. Докажите, что $\mathbb{Z}_p$ секвенциально компактно, т. е. что каждая последовательность целых p-адических чисел содержит сходящуюся подпоследовательность.

19. Рассмотрим матрицы с элементами в $\mathbb{Q}_p$. Суммы, произведения и определители этих матриц задаются точно так же, как и в вещественном случае. Пусть $M = \{r \times r$-матрицы с элементами в $\mathbb{Z}_p\}$, $M^\times = \{A \in M \mid A$ обратима в $M\}$ (легко видеть, что это равносильно условию $\det A \in \mathbb{Z}_p^\times$), и пусть $pM = \{A \in M \mid A = pB$, где $B \in M\}$. Докажите, что если $A \in M^\times$ и $B \in pM$, то существует единственная матрица $X \in M^\times$, для которой $X^2 - AX + B = 0$.

Глава II

p-АДИЧЕСКАЯ ИНТЕРПОЛЯЦИЯ ДЗЕТА-ФУНКЦИИ РИМАНА

Эта глава логически не связана с последующими и помещена здесь как плато (по уровню абстракции) на середине нашего восхождения к Ω. Все происходящее в этой главе еще не выходит за рамки полей $\mathbb{Q}$, $\mathbb{Q}_p$ и $\mathbb{R}$.

Дзета-функция Римана ζ определяется на множестве вещественных чисел > 1 формулой

$$\zeta(s) \underset{\text{def}}{=} \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Легко установить (сравнивая с интегралом $\int_1^\infty (dx/x^s) = 1/(s-1)$ при фиксированном $s > 1$) сходимость этой суммы при $s > 1$.

Пусть p — произвольное простое число. Цель этой главы заключается в доказательстве некоторой «p-адической непрерывности» последовательности чисел $\zeta(2k)$ для $k = 1, 2, 3, \ldots$. Точнее, пусть $2k$ пробегает все четные положительные целые числа из фиксированного класса вычетов по модулю $p-1$. Сопоставим каждому из них значение

$$f(2k) = (1 - p^{2k-1}) \frac{c_k}{\pi^{2k}} \zeta(2k),$$

где $c_k = (-1)^k (2k-1)!/2^{2k-1}$. Оказывается, число $f(2k)$ всегда рационально. Кроме того, если два числа вида $2k$ из рассматриваемого класса вычетов p-адически близки (т. е. их разность делится на большую степень p), то, как мы увидим в дальнейшем, соответствующие им

11. Решите ту же задачу, что и в упр. 10, для $p=2$. В этом случае требуется найти *восемь* чисел $\alpha_1, \ldots, \alpha_8 \in \mathbb{Q}_2$, таких, что для любого ненулевого $\alpha \in \mathbb{Q}_2$ ровно одно из чисел $\alpha_1\alpha, \ldots, \alpha_8\alpha$ имеет квадратный корень в $\mathbb{Q}_2$. (Конечно, выбор такой восьмерки $\alpha_1, \ldots, \alpha_8$ *не однозначен*.)

12. Найдите первые четыре знака p-адических разложений всех четырех корней степени 4 из 1 в $\mathbb{Q}_5$. Докажите, что уравнение $x^p - x = 0$ всегда имеет p решений $a_0, a_1, \ldots a_{p-1}$ в $\mathbb{Q}_p$, для которых $a_i \equiv i \pmod p$. Эти p чисел называются представителями Тейхмюллера для $\{0, 1, 2, \ldots, p-1\}$ и используются иногда в качестве p-ичных знаков вместо $\{0, 1, 2, \ldots, p-1\}$.

13. Докажите следующий «признак неприводимости Эйзенштейна». Пусть $f(x) = a_0 + a_1x + \ldots + a_nx^n$ — многочлен с коэффициентами $a_i \in \mathbb{Z}_p$. Если $a_i \equiv 0 \pmod p$ при $i = 0, 1, 2, \ldots, n-1$, $a_n \not\equiv 0 \pmod p$ и $a_0 \not\equiv 0 \pmod{p^2}$, то $f(x)$ неприводим над $\mathbb{Q}_p$, т. е. не представим в виде произведения двух многочленов меньшей степени с коэффициентами в $\mathbb{Q}_p$.

14. Используя упр. 13, покажите, что 1 не имеет других корней степени p, кроме 1, в $\mathbb{Q}_p$ при $p > 2$. (*Указание*: подставьте $y = x - 1$ в $(x^p - 1)/(x - 1)$.) Докажите это также другим способом: представьте любой такой корень x в виде $1 + p^r x'$, где $|x'|_p = 1$, а $r > 0$ — некоторое целое (объясните, почему $x \equiv 1 \pmod p$), затем это выражение для x возведите в степень p, раскройте скобки и сравните коэффициенты при степенях p.

15. Докажите, что ряд $1 + p + p^2 + p^3 + \ldots$ сходится к $1/(1-p)$ в $\mathbb{Q}_p$. К чему сходятся $1 - p + p^2 - p^3 + p^4 - p^5 + \ldots$ и $1 + (p-1)p + p^2 + (p-1)p^3 + p^4 + (p-1)p^5 + \ldots$?

16. Предположим, что n — целое (положительное или отрицательное) число, не делящееся на p, и $\alpha \equiv 1 \pmod p$. Покажите, что α имеет корень степени n в $\mathbb{Q}_p$. Приведите пример, показывающий, что при $p = n$ это неверно. Покажите, что α имеет корень степени p, если $\alpha \equiv 1 \pmod{p^2}$ и $p \neq 2$.

17. Пусть $\alpha \in \mathbb{Z}_p$. Докажите сравнения $\alpha^{p^M} \equiv \alpha^{p^{M-1}} \pmod{p^M}$ для $M = 1, 2, 3, 4, \ldots$. Докажите, что последовательность $\{\alpha^{p^M}\}$ стремится к некоторому пределу в $\mathbb{Q}_p$ и что этот предел равен представителю Тейхмюллера, сравнимому с α по модулю p.

18. Докажите, что $\mathbb{Z}_p$ секвенциально компактно, т. е. что каждая последовательность целых p-адических чисел содержит сходящуюся подпоследовательность.

19. Рассмотрим матрицы с элементами в $\mathbb{Q}_p$. Суммы, произведения и определители этих матриц задаются точно так же, как и в вещественном случае. Пусть $M = \{r \times r$-матрицы с элементами в $\mathbb{Z}_p\}$, $M^\times = \{A \in M \mid A$ обратима в $M\}$ (легко видеть, что это равносильно условию $\det A \in \mathbb{Z}_p^\times$), и пусть $pM = \{A \in M \mid A = pB$, где $B \in M\}$. Докажите, что если $A \in M^\times$ и $B \in pM$, то существует единственная матрица $X \in M^\times$, для которой $X^2 - AX + B = 0$.

Глава II

p-АДИЧЕСКАЯ ИНТЕРПОЛЯЦИЯ ДЗЕТА-ФУНКЦИИ РИМАНА

Эта глава логически не связана с последующими и помещена здесь как плато (по уровню абстракции) на середине нашего восхождения к Ω. Все происходящее в этой главе еще не выходит за рамки полей $\mathbb{Q}$, $\mathbb{Q}_p$ и $\mathbb{R}$.

Дзета-функция Римана ζ определяется на множестве вещественных чисел > 1 формулой

$$\zeta(s) \underset{\text{def}}{=} \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Легко установить (сравнивая с интегралом $\int_1^\infty (dx/x^s) = 1/(s-1)$ при фиксированном $s > 1$) сходимость этой суммы при $s > 1$.

Пусть p — произвольное простое число. Цель этой главы заключается в доказательстве некоторой «p-адической непрерывности» последовательности чисел $\zeta(2k)$ для $k = 1, 2, 3, \ldots$. Точнее, пусть $2k$ пробегает все четные положительные целые числа из фиксированного класса вычетов по модулю $p-1$. Сопоставим каждому из них значение

$$f(2k) = (1 - p^{2k-1}) \frac{c_k}{\pi^{2k}} \zeta(2k),$$

где $c_k = (-1)^k (2k-1)!/2^{2k-1}$. Оказывается, число $f(2k)$ всегда рационально. Кроме того, если два числа вида $2k$ из рассматриваемого класса вычетов p-адически близки (т. е. их разность делится на большую степень p), то, как мы увидим в дальнейшем, соответствующие им

значения $f(2k)$ также p-адически близки. (При этом нам понадобится еще одно предположение: $2k$ не делится на $p-1$.) По существу это означает, что функцию f можно однозначно продолжить до *непрерывной функции f, определенной на множестве целых p-адических чисел и принимающей значения в* $\mathbb{Q}_p$. (Непрерывность понимается здесь, как в классическом анализе: если $\{x_n\}$ p-адически сходится к x, то $\{f(x_n)\}$ p-адически сходится к $f(x)$.)

Эту процедуру мы называем *p-адической интерполяцией*. Она аналогична классическому методу, скажем, определения функции $f(x)=a^x$ (где a — фиксированное вещественное положительное число): сначала определяем значения $f(x)$ для рациональных x, затем доказываем близость значений a^x при близких рациональных x и в заключение определяем a^x для иррационального x как предел a^{x_n} по рациональным x_n, стремящимся к x.

Отметим, что любую функцию f на множестве S, например, четных положительных чисел можно продолжить до непрерывной функции на $\mathbb{Z}_p$ не более чем одним способом (при $p\neq 2$). Это следует из *плотности* подмножества S в $\mathbb{Z}_p$: любое $x\in\mathbb{Z}_p$ представимо в виде предела последовательности целых четных положительных чисел x_n. Действительно, если f — непрерывная функция, то $f(x)=\lim\limits_{n\to\infty} f(x_n)$. В вещественном же случае множество рациональных чисел плотно в $\mathbb{R}$, а S — нет. Поэтому условие непрерывности не определяет еще вещественную интерполяцию функции, заданной на множестве четных положительных чисел. Таких интерполяций всегда бесконечно много. (Однако при некоторых дополнительных требованиях на вещественную интерполирующую функцию, помимо непрерывности, она может оказаться единственной. Например, гамма-функция $\Gamma(x+1)$ интерполирует $k!$ для целых неотрицательных $x=k$. Кроме того, она удовлетворяет функциональному уравнению $\Gamma(x+1)=x\Gamma(x)$ при всех вещественных x, а ее логарифм является выпуклой функцией при $x>0$. Этими условиями гамма-функция характеризуется однозначно.)

§ 1. ФОРМУЛА ДЛЯ ЗНАЧЕНИЙ $\zeta(2k)$

Рассмотрим следующее разложение Тейлора:

$$\frac{t}{e^t-1}=\frac{1}{1+t/2!+t^2/3!+t^3/4!+\ldots+t^n/(n+1)!+\ldots}=$$
$$\overset{\text{def}}{=}\sum_{k=0}^{\infty} B_k t^k/k!.$$

Произведение k-го коэффициента этого степенного ряда на $k!$ называется k-м числом Бернулли и обозначается через B_k. Вот несколько первых B_k:

$$B_0=1,\quad B_1=-1/2,\quad B_2=1/6,\quad B_3=0,$$
$$B_4=-1/30,\quad B_5=0,\quad B_6=1/42,\ \ldots.$$

В этом параграфе мы установим формулу

$$\zeta(2k)=(-1)^k\pi^{2k}\frac{2^{2k-1}}{(2k-1)!}\left(-\frac{B_{2k}}{2k}\right)\quad\text{для } k=1,\ 2,\ 3,\ \ldots.$$

Напомним определение гиперболического синуса, обозначаемого через sh:

$$\operatorname{sh} x=\frac{e^x-e^{-x}}{2}.$$

Для него мы имеем следующее разложение Тейлора:

$$\operatorname{sh} x=x+\frac{x^3}{3!}+\frac{x^5}{5!}+\ldots+\frac{x^{2k+1}}{(2k+1)!}+\ldots,$$

которое получается усреднением соответствующих рядов для e^x и $-e^{-x}$. Отметим, что он отличается от ряда Тейлора для $\sin x$ отсутствием чередования знаков.

Предложение. *Бесконечное произведение*

$$\pi x\prod_{n=1}^{\infty}\left(1+\frac{x^2}{n^2}\right)$$

сходится при любом вещественном x и равно $\operatorname{sh}(\pi x)$.

Доказательство. Сходимость следует непосредственно из логарифмического признака:

$$\sum_{n=1}^{\infty}\left|\log\left(1+\frac{x^2}{n^2}\right)\right|\leqslant\sum_{n=1}^{\infty}\frac{x^2}{n^2}<\infty\quad\text{при любом } x.$$

Доказательству равенства мы предпошлем вывод разложения в бесконечное произведение для $\sin x$.

Лемма. *Пусть $n=2k+1$ — целое нечетное положительное число. Тогда существуют многочлены P_n и Q_{n-1} с целыми коэффициентами степени, не превосходящей n и $n-1$ соответственно, такие, что*

$$\sin(nx)=P_n(\sin x),\quad \cos(nx)=\cos x\,Q_{n-1}(\sin x).$$

Доказательство леммы. Воспользуемся индукцией по k. Для $k=0$ (т. е. $n=1$) лемма очевидна. Предположим, что она уже доказана для $k-1$. Тогда

$$\begin{aligned}\sin[(2k+1)x]&=\sin[(2k-1)x+2x]=\\&=\sin(2k-1)x\cos 2x+\cos(2k-1)x\sin 2x=\\&=P_{2k-1}(\sin x)(1-2\sin^2 x)+\\&\qquad+\cos x\,Q_{2k-2}(\sin x)\,2\sin x\cos x,\end{aligned}$$

откуда легко получить нужное представление вида $P_{2k+1}(\sin x)$. Проверка соответствующего утверждения для $\cos(2k+1)x$ аналогична, и мы оставляем ее читателю. □

Продолжим теперь доказательство предложения. Прежде всего, подставив $x=0$ в тождество $\sin nx=P_n(\sin x)$, мы устанавливаем, что постоянный член у P_n равен нулю. Затем, продифференцировав $\sin nx=P_n(\sin x)$ по x, получим

$$n\cos nx=P_n'(\sin x)\cos x.$$

Подставим в это тождество $x=0$; мы увидим, что $n=P_n'(0)$, т. е. первый коэффициент многочлена P_n равен n. Следовательно,

$$\begin{aligned}\frac{\sin nx}{n\sin x}&=\tilde P_{2k}(\sin x)=1+a_1\sin x+a_2\sin^2 x+\dots\\&\qquad\dots+a_{2k}\sin^{2k}x\quad(n=2k+1),\end{aligned}$$

где a_i — некоторые рациональные числа. Отметим теперь, что левая часть обращается в нуль при $x=\pm\pi/n,\dots,\pm k\pi/n$. Кроме того, все $2k$ значений $y=\pm\sin\pi/n,\pm\sin 2\pi/n,\dots,\sin k\pi/n$, в которых обращается в нуль многочлен $\tilde P_{2k}(y)$, различны; степень $\tilde P_{2k}$ равна $2k$,

а постоянный член равен 1. Поэтому

$$\begin{aligned}\tilde P_{2k}(y)&=\left(1-\frac{y}{\sin\pi/n}\right)\left(1-\frac{y}{-\sin\pi/n}\right)\left(1-\frac{y}{\sin 2\pi/n}\right)\times\\&\quad\times\left(1-\frac{y}{-\sin 2\pi/n}\right)\dots\left(1-\frac{y}{\sin k\pi/n}\right)\left(1-\frac{y}{-\sin k\pi/n}\right)=\\&=\prod_{r=1}^{k}\left(1-\frac{y^2}{\sin^2 r\pi/n}\right).\end{aligned}$$

Следовательно,

$$\frac{\sin nx}{n\sin x}=\tilde P_{2k}(\sin x)=\prod_{r=1}^{k}\left(1-\frac{\sin^2 x}{\sin^2 r\pi/n}\right).$$

Подставив $\pi x/n$ вместо x, получаем

$$\frac{\sin\pi x}{n\sin\pi x/n}=\prod_{r=1}^{k}\left(1-\frac{\sin^2\pi x/n}{\sin^2 r\pi/n}\right).$$

Перейдем теперь к пределу при $n=2k+1\to\infty$ в обеих частях последнего тождества. Левая часть стремится к $(\sin\pi x)/\pi x$. При r, достаточно малом по сравнению с n, r-й член произведения близок к $1-((\pi x/n)/(\pi r/n))^2=1-x^2/r^2$. Отсюда следует, что произведение сходится к $\prod_{r=1}^{\infty}(1-x^2/r^2)$. (Строгую проверку мы оставляем читателю в качестве одного из приведенных ниже упражнений.)

Таким образом,

$$\prod_{n=1}^{\infty}\left(1-\frac{x^2}{n^2}\right)=\frac{\sin\pi x}{\pi x}=1-\frac{\pi^2x^2}{3!}+\frac{\pi^4x^4}{5!}-\frac{\pi^6x^6}{7!}+\frac{\pi^8x^8}{9!}-\dots.$$

Правая часть — это разложение синуса в ряд Тейлора. С другой стороны,

$$\frac{\operatorname{sh}\pi x}{\pi x}=1+\frac{\pi^2x^2}{3!}+\frac{\pi^4x^4}{5!}+\frac{\pi^6x^6}{7!}+\frac{\pi^8x^8}{9!}+\dots.$$

Если мы раскроем скобки в бесконечном произведении для $\sin(\pi x)/\pi x$, то знак минус будет только у тех членов, которые содержат нечетное число сомножителей вида x^2/n^2, т. е. в точности у тех членов, которые подобны членам со знаком минус в ряде Тейлора для $\sin(\pi x)/\pi x$. Следовательно, изменение знака внутри сомножителей полученного разложения вызовет изменение в ряде справа всех минусов на плюсы, что и доказывает требуемое равенство. (Для «лучшего» понимания этого завершающего шага см. упр. 3.) □

Теперь мы готовы доказать обещанную выше формулу.

Теорема 4.

$$\zeta(2k) = (-1)^k \pi^{2k} \frac{2^{2k-1}}{(2k-1)!}\left(-\frac{B_{2k}}{2k}\right).$$

Доказательство. Прологарифмируем обе части тождества

$$\operatorname{sh} \pi x = \pi x \prod_{n=1}^{\infty}\left(1+\frac{x^2}{n^2}\right)$$

(при $x>0$). Слева мы получим

$$\log \operatorname{sh} \pi x = \log[(e^{\pi x}-e^{-\pi x})/2] = \log[(e^{\pi x}/2)(1-e^{-2\pi x})] = \log(1-e^{-2\pi x}) + \pi x - \log 2.$$

Справа, пользуясь разложением Тейлора функции $\log(1+x)$, получим

$$\log \pi + \log x + \sum_{n=1}^{\infty} \log(1+x^2/n^2) = \log \pi + \log x + \sum_{n=1}^{\infty}\sum_{k=1}^{\infty} (-1)^{k+1}\frac{x^{2k}}{kn^{2k}}.$$

Последний двойной ряд сходится абсолютно при $0<x<1$. Поэтому можно изменить в нем порядок суммирования и получить тождество

$$\log(1-e^{-2\pi x}) + \pi x - \log 2 = \log \pi + \log x + \sum_{k=1}^{\infty}\left[(-1)^{k+1}\frac{x^{2k}}{k}\sum_{n=1}^{\infty}\frac{1}{n^{2k}}\right] = \log \pi + \log x + \sum_{k=1}^{\infty}(-1)^{k+1}\frac{x^{2k}}{k}\zeta(2k).$$

Продифференцируем теперь обе части этого тождества по x. Ряд справа можно дифференцировать почленно, так как ряд из производных сходится равномерно на каждом интервале $0<x<1-\varepsilon$ при $\varepsilon>0$. Следовательно,

$$\frac{2\pi e^{-2\pi x}}{1-e^{-2\pi x}} + \pi = \frac{1}{x} + 2\sum_{k=1}^{\infty}(-1)^{k+1}x^{2k-1}\zeta(2k).$$

Умножив на x, а затем подставив $x/2$ вместо x, получим

$$\frac{\pi x}{e^{\pi x}-1} + \frac{\pi x}{2} = 1 + \sum_{k=1}^{\infty}\frac{(-1)^{k+1}\zeta(2k)}{2^{2k-1}}x^{2k}.$$

Левая часть разлагается в ряд $\pi x/2 + \sum_{k=0}^{\infty} B_k(\pi x)^k/k!$. Сравнивая коэффициенты при четных степенях x, получаем равенство $\pi^{2k}B_{2k}/(2k)! = ((-1)^{k+1}/2^{2k-1})\zeta(2k)$, что и завершает доказательство теоремы. □

Вот несколько примеров:

$$\zeta(2) = \frac{\pi^2}{6}, \quad \zeta(4) = \frac{\pi^4}{90}, \quad \zeta(6) = \frac{\pi^6}{945}.$$

Формула для $\zeta(2k)$ из теоремы 4 предусмотрительно записана в таком виде, в котором выделены «интересная» часть $-B_{2k}/2k$ и нежелательный множитель $(-1)^k\pi^{2k}\times 2^{2k-1}/(2k-1)!$. Именно эту интересную часть мы и будем p-адически интерполировать. Позднее (в § 7) мы представим некоторые мотивы для выделения $-B_{2k}/2k$

«из общего котла». Пока отметим лишь, что от π^{2k} обязательно следует избавиться при p-адической интерполяции значений дзета-функции, поскольку нет разумной p-адической интерпретации вещественных трансцендентных чисел. (Как определить, например, их p-адический порядок?)

§ 2. p-АДИЧЕСКАЯ ИНТЕРПОЛЯЦИЯ ФУНКЦИИ $f(s)=a^s$

Этот параграф сыграет свою роль в дальнейшем изложении. Сюда же он помещен в учебных целях: как на макете, мы ознакомимся с некоторыми чертами p-адической интерполяции, которые могли бы иначе вызвать недоумение.

Пусть a — некоторое фиксированное положительное вещественное число. Мы уже отмечали выше, что функцию $f(s)=a^s$ можно определить как непрерывную функцию вещественного аргумента, задав ее сначала на множестве рациональных чисел, а затем «интерполируя» или «продолжая по непрерывности» на все вещественные числа, каждое из которых представимо в виде предела последовательности рациональных чисел.

Предположим теперь, что $a=n$ — некоторое фиксированное целое положительное число. Будем рассматривать n как элемент $\mathbb{Q}_p$. Тогда для каждого целого неотрицательного s целое число n^s принадлежит $\mathbb{Z}_p$. Множество всех целых неотрицательных чисел плотно в $\mathbb{Z}_p$, как и множество $\mathbb{Q}$ в $\mathbb{R}$. Действительно, каждое целое p-адическое число представимо как предел последовательности целых неотрицательных чисел (например, последовательности частичных сумм его p-адического разложения). Поэтому функцию $f(s)=n^s$ можно попытаться продолжить по непрерывности с множества целых неотрицательных s на все целые p-адические s.

Для этого необходимо выяснить, близки ли два значения n^s и $n^{s'}$ для близких целых положительных s и s', например для $s'=s+p^N$ при достаточно большом N. Как показывают следующие два примера, это верно не всегда:

(1) $n=p$, $s=0$; тогда $|n^s-n^{s'}|_p=|1-p^{p^N}|_p=1$ независимо от N;

(2) $1<n<p$; тогда по малой теореме Ферма (см. первый абзац в доказательстве теоремы 9 из § III.1) $n\equiv n^p \pmod p$, поэтому $n\equiv n^p\equiv n^{p^2}\equiv n^{p^3}\equiv\ldots$ $\ldots\equiv n^{p^N} \pmod p$; отсюда $n^s-n^{s+p^N}=n^s(1-n^{p^N})\equiv n^s(1-n)\pmod p$, а значит, $|n^s-n^{s'}|_p=1$ независимо от N.

Но наше положение не столь безнадежно, как может показаться после двух таких примеров. Рассмотрим такое n, что $n\equiv 1 \pmod p$, т. е. $n=1+mp$. Пусть $|s'-s|_p\leqslant 1/p^N$, иными словами, $s'=s+s''p^N$ для некоторого $s''\in\mathbb{Z}$. Тогда (если, скажем, $s'>s$)

$$|n^s-n^{s'}|_p=|n^s|_p\,|1-n^{s'-s}|_p=|1-n^{s'-s}|_p=$$
$$=|1-(1+mp)^{s''p^N}|_p.$$

Но из разложения

$$(1+mp)^{s''p^N}=1+(s''p^N)\,mp+\frac{s''p^N\,(s''p^N-1)}{2}(mp)^2+\ldots$$
$$\ldots+(mp)^{s''p^N}$$

видно, что слагаемые в $1-(1+mp)^{s''p^N}$ делятся на p^{N+1}. Следовательно,

$$|n^s-n^{s'}|_p\leqslant|p^{N+1}|_p=\frac{1}{p^{N+1}}.$$

Иначе говоря, если $s'-s$ делится на p^N, то $n^s-n^{s'}$ делится на p^{N+1}.

Итак, если $n\equiv 1 \pmod p$, то мы можем определить значение функции $f(s)=n^s$ для *любого целого p-адического* s как целое p-адическое число, равное пределу значений n^{s_i} по любой последовательности целых неотрицательных чисел s_i, стремящейся к s (например, по последовательности частичных сумм p-адического разложения s). Тогда $f(s)$ — непрерывная функция на $\mathbb{Z}_p$ со значениями в $\mathbb{Z}_p$.

Можно добиться чуть большего и определить n^s для любого n, не делящегося на p. С этой целью потребуем, кроме сравнимости чисел s и s' по модулю большой степени p, их сравнимости по модулю $p-1$. Точнее, фиксируем некоторое $s_0\in\{0,\ 1,\ 2,\ 3,\ \ldots,\ p-2\}$ и вместо того, чтобы рассматривать значения n^s для всех

целых неотрицательных s, рассмотрим значения n^s только для s, сравнимых с фиксированным s_0 по модулю $p-1$. Пусть $s = s_0 + (p-1)s_1$, где s_1 — произвольное неотрицательное целое число. Тогда выделенные значения приводят к числам $n^{s_0+(p-1)s_1}$. После этого мы можем провести p-адическую интерполяцию, так как

$$n^s = n^{s_0}(n^{p-1})^{s_1}$$

и $n^{p-1} \equiv 1 \pmod p$ для любого n, не делящегося на p. Действительно, здесь n^{p-1} играет ту же роль, что и n в предыдущем абзаце, а s_1 — роль s (*постоянный множитель* n^{s_0} несуществен).

В результате мы получили интерполирующую функцию f, которую можно ввести еще так. Пусть S_{s_0} — множество целых неотрицательных чисел, сравнимых с s_0 по модулю $p-1$. Множество S_{s_0} плотно в $\mathbb{Z}_p$ (см. ниже упр. 7). Тогда функцию $f\colon S_{s_0} \to \mathbb{Z}_p$, заданную формулой $f(s) = n^s$, можно однозначно продолжить по непрерывности до функции $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$. Заметим, что так определенная функция f зависит от s_0, а не только от n.

В случае когда $n \equiv 0 \pmod p$, мы сталкиваемся с действительной трудностью. Это происходит потому, что $n^{s_i} \to 0$ p-адически для *любой* возрастающей последовательности целых неотрицательных чисел. В самом деле, любая последовательность целых неотрицательных чисел, стремящихся к числу $s \in \mathbb{Z}_p$, которое не является целым неотрицательным числом, содержит бесконечно возрастающую подпоследовательность. Поэтому единственным кандидатом на роль интерполирующей функции в этом случае будет нулевая функция, что нелепо.

В заключение отметим, что предыдущие рассуждения дословно переносятся на случай функции $1/n^s$ (см. ниже упр. 8).

Вернемся снова к дзета-функции Римана

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \quad (s > 1).$$

Можно попытаться наивно проинтерполировать каждый член ряда $\zeta(s)$ и затем сложить результаты. Но из

этого ничего не выйдет, потому что уже сумма одних только поддающихся интерполяции членов, для которых $p \nmid n$, расходится в $\mathbb{Z}_p$. Тем не менее давайте временно забудем про это и рассмотрим ряд почленно.

Прежде всего желательно избавиться от всех членов $1/n^s$, для которых n делится на p. Сделаем это следующим образом:

$$\zeta(s) = \sum_{n=1,\ p\nmid n}^{\infty} \frac{1}{n^s} + \sum_{n=1,\ p\mid n}^{\infty} \frac{1}{n^s} =$$

$$= \sum_{n=1,\ p\nmid n}^{\infty} \frac{1}{n^s} + \sum_{n=1}^{\infty} \frac{1}{p^s n^s} = \sum_{n=1,\ p\nmid n}^{\infty} \frac{1}{n^s} + \frac{1}{p^s}\zeta(s);$$

$$\zeta(s) = \frac{1}{1-1/p^s} \sum_{n=1,\ p\nmid n}^{\infty} \frac{1}{n^s}.$$

В дальнейшем мы будем работать именно с этой последней суммой

$$\zeta^*(s) \underset{\text{def}}{=} \sum_{n=1,\ p\nmid n}^{\infty} \frac{1}{n^s} = \left(1 - \frac{1}{p^s}\right)\zeta(s).$$

Эта процедура известна как *выделение эйлерова p-множителя*. Название связано со знаменитой формулой

$$\zeta(s) = \prod_{\text{простые } q} \frac{1}{1-1/q^s}$$

(см. ниже упр. 1). Множитель $1/(1-1/q^s)$ в этом произведении, соответствующий простому числу q, называется *эйлеровым q-множителем*. Таким образом, умножая $\zeta(s)$ на $(1-1/p^s)$, мы уничтожаем эйлеров p-множитель и получаем

$$\zeta^*(s) = \prod_{\text{простые } q\neq p} \frac{1}{1-1/q^s}.$$

Теперь мы намерены выбрать $s_0 \in \{0, 1, 2, \ldots, p-2\}$ и ограничить область изменения аргумента до множества всех $s \in S_{s_0} = \{s \mid s \equiv s_0 \pmod{p-1}\}$.

В дальнейшем окажется, что введенные в § 1 числа $-B_{2k}/2k$ после умножения на $1-p^{2k-1}$ могут быть проинтерполированы для $2k \in S_{2s_0}$ ($2s_0 \in \{0, 2, 4, \ldots, p-3\}$). Отметим здесь, что умножение происходит не на $[1-(1/p^{2k})]$, как можно было бы ожидать, а на эйлеров множитель с аргументом $1-2k$ вместо $2k$: $1-(1/p^{1-2k}) = 1-p^{2k-1}$. Причина довольно естественной замены $2k \leftrightarrow 1-2k$ будет объяснена в § 7. (Мы увидим, что «интересующий нас множитель» $-B_{2k}/2k$ в $\zeta(2k)$ равен в действительности $\zeta(1-2k)$; значения $\zeta(x)$ и $\zeta(1-x)$ связаны между собой некоторым «функциональным уравнением».)

Точнее, мы установим следующий факт: если $2k$, $2k' \in S_{2k_0}$ (где $2k_0 \in \{2, 4, \ldots, p-3\}$; в случае $k_0 = 0$ формулировка немного сложнее) и $k \equiv k' \pmod{p^N}$, то (см. § 6)

$$(1-p^{2k-1})(-B_{2k}/2k) \equiv (1-p^{2k'-1})(-B_{2k'}/2k') \pmod{p^{N+1}}.$$

Эти сравнения впервые были открыты Куммером около ста лет назад. Но их интерпретация в связи с p-адической интерполяцией ζ-функции Римана была получена только в 1964 г. Куботой и Леопольдтом.

Упражнения

1. Докажите, что для $s > 1$

$$\zeta(s) = \prod_{\text{простые } q} \frac{1}{1-q^{-s}}.$$

2. Докажите, что при $n = 2k+1 \to \infty$

$$\prod_{r=1}^{k} \frac{1-\sin^2(\pi x/n)/\sin^2(\pi r/n)}{1-x^2/r^2} \to 1.$$

3. Используя формулу $e^{ix} = \cos x + i \sin x$, покажите, что $\operatorname{sh} x = -i \sin ix$. Затем другим способом выведите бесконечное произведение для $\operatorname{sh} x$ из произведения для $\sin x$.

4. Докажите, что $B_k = 0$ для нечетных $k > 1$.

5. Используя формулу для $\zeta(2k)$ в сочетании с асимптотической формулой Стирлинга $n! \sim \sqrt{2\pi n}\, n^n e^{-n}$ (где знак $\sim$ означает, что отношение обеих частей стремится к 1 при $n \to \infty$), вычислите асимптотику обычной архимедовой абсолютной величины для B_{2k}.

6. Вычислите с четырьмя знаками p-адическую фуикцию из § 2 в следующих случаях:

(i) $11^{1/601}$ в $\mathbb{Q}_5$; (ii) $\sqrt{1/10}$ в $\mathbb{Q}_3$;

(iii) $(-6)^{2+4\cdot 7+3\cdot 7^2+7^3+\cdots}$ в $\mathbb{Q}_7$.

7. Пусть $s_0 \in \{0, 1, \ldots, p-2\}$. Докажите, что множество целых неотрицательных чисел, сравнимых с s_0 по модулю $p-1$, плотно в $\mathbb{Z}_p$, т. е. каждое число из $\mathbb{Z}_p$ приближается этими числами с любой степенью точности.

8. Что произойдет, если в рассуждениях § 2 целое положительное число n заменить на $n \in \mathbb{Z}_p$? А если вместо функции $f(s) = n^s$ рассмотреть $f(s) = 1/n^s$? Заметим, что последнее эквивалентно выбору в качестве плотного подмножества в $\mathbb{Z}_p$ множества *неположительных целых чисел* вместо *неотрицательных* при той же интерполируемой функции f.

9. Рассмотрим функцию χ, заданную на множестве целых положительных чисел следующим образом:

$$\chi(n) = \begin{cases} 1, & \text{если } n \equiv 1 \pmod 4; \\ -1, & \text{если } n \equiv 3 \pmod 4; \\ 0, & \text{если } 2 \mid n. \end{cases}$$

Положим $L_\chi(s) \overset{\text{def}}{=} \sum_{n=1}^{\infty} (\chi(n)/n^s) = 1-(1/3^s)+(1/5^s)-(1/7^s)+\ldots$. Докажите, что $L_\chi(s)$ сходится при $s > 0$, а при $s > 1$ сходится абсолютно. Найдите $L_\chi(1)$. Найдите также эйлеровы произведения для $L_\chi(s)$ и $L^*_\chi(s) \overset{\text{def}}{=} \sum_{n \geqslant 1,\ p \nmid n} (\chi(n)/n^s)$. (Оказывается, для значений $L_\chi(2k+1)$ (т. е. здесь для *нечетных* аргументов вместо четных) существует формула, аналогичная формуле теоремы 4: число

$$B_{\chi, n} \overset{\text{def}}{=} n! \cdot \left(\text{коэффициент при } t^n \text{ в } \frac{te^t}{e^{at}-1} - \frac{te^{3t}}{e^{4t}-1}\left(= \frac{-t}{e^t+e^{-t}}\right)\right)$$

заменяет B_n.)

Замечание. Упражнение 9 относится к частному случаю следующей ситуации. Пусть N — целое положительное число, а $(\mathbb{Z}/N\mathbb{Z})^\times$ — мультипликативная группа классов вычетов по модулю N целых чисел, взаимно простых с N. Пусть χ: $(\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ — гомоморфизм группы $(\mathbb{Z}/N\mathbb{Z})^\times$ в мультипликативную группу ненулевых элементов поля комплексных чисел. (Легко установить, что образу χ в $\mathbb{C}$ принадлежат только корни из 1.) Гомоморфизм χ называется *характером* группы $(\mathbb{Z}/N\mathbb{Z})^\times$. Предположим, что χ — *примитивный* характер, т. е. не существует целого M, делящего N, для которого $1 \leqslant M < N$ и значения χ на элементах из $(\mathbb{Z}/N\mathbb{Z})^\times$ зависят только от их класса по модулю M. Обозначим через χ также функцию на множестве всех целых чисел n, равную $\chi(n \bmod N)$ для n, взаимно простых с N, и 0 в остальных случаях. Такая функция χ называется *характером Дирихле с кондуктором* N.

Определим теперь

$$L_\chi(s) \overset{\text{def}}{=} \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

Для этой функции можно найти явную формулу, подобную формуле из теоремы 4: число

$$B_{\chi,n} \overset{\text{def}}{=} n! \cdot \left(\text{коэффициент при } t^n \text{ в } \sum_{a=1}^{N-1} \frac{\chi(a)\, te^{at}}{e^{Nt}-1} \right)$$

заменит B_n. Эта формула задает значения L_χ для четных целых, если $\chi(-1)=1$, и для нечетных, если $\chi(-1)=-1$. (См. книгу Ивасавы [(c) 1].)

Кроме того, имеет место явная формула

$$L_\chi(1) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n} =$$

$$= \begin{cases} -\dfrac{\tau(\chi)}{N} \displaystyle\sum_{a=1}^{N-1} \bar{\chi}(a) \log \sin \frac{a\pi}{N}, & \text{если} \quad \chi(-1)=1; \\ \dfrac{\pi i \tau(\chi)}{N^2} \displaystyle\sum_{a=1}^{N-1} \bar{\chi}(a) \cdot a, & \text{если} \quad \chi(-1)=-1, \end{cases}$$

где черта над χ обозначает комплексное сопряжение характера: $\bar{\chi}(a) \overset{\text{def}}{=} \overline{\chi(a)}$, а числа

$$\tau(\chi) \overset{\text{def}}{=} \sum_{a=1}^{N-1} \chi(a)\, e^{2\pi i a/N}$$

известны как гауссовы суммы. (Доказательство этого факта можно найти, например, в книге Боревича и Шафаревича [(b) 1], стр. 442—444.)

10. Используя предыдущую формулу для $L_\chi(1)$, проверьте полученное вами значение $L_\chi(1)$ в упр. 9. Докажите также, что:

(a) $\dfrac{1}{1} - \dfrac{1}{2} + \dfrac{1}{4} - \dfrac{1}{5} + \dfrac{1}{7} - \dfrac{1}{8} + \dfrac{1}{10} - \dfrac{1}{11} + \ldots + \dfrac{1}{3k+1} - \dfrac{1}{3k+2} + \ldots = \dfrac{\pi}{3\sqrt{3}}$;

(b) $\dfrac{1}{1} - \dfrac{1}{3} - \dfrac{1}{5} + \dfrac{1}{7} + \dfrac{1}{9} - \dfrac{1}{11} - \dfrac{1}{13} + \dfrac{1}{15} + \dfrac{1}{17} - \dfrac{1}{19} - \dfrac{1}{21} + \dfrac{1}{23} + \ldots = \dfrac{\log(1+\sqrt{2})}{\sqrt{2}}$.

§ 3. p-АДИЧЕСКИЕ РАСПРЕДЕЛЕНИЯ

В качестве «базиса открытых множеств» метрического пространства $\mathbb{Q}_p$ можно взять систему множеств $a + p^N\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x-a|_p \leqslant 1/p^N\}$, где $a \in \mathbb{Q}_p$, а $N \in \mathbb{Z}$. Это означает, что *любое* открытое подмножество в $\mathbb{Q}_p$ представимо в виде объединения открытых множеств такого вида. Множества $a + p^N\mathbb{Z}_p$ в этой главе называются *интервалами* (в других местах мы часто будем называть их *дисками*) и обозначаются также через $a + (p^N)$. Отметим, что все интервалы одновременно открыты и замкнуты. Они замкнуты, так как дополнение к $a + (p^N)$ равно объединению открытых множеств $a' + (p^N)$ по всем $a' \in \mathbb{Q}_p$, для которых $a' \notin a + (p^N)$.

Напомним, что пространство $\mathbb{Z}_p$ секвенциально компактно, т. е. каждая последовательность целых p-адических чисел содержит сходящуюся подпоследовательность (см. упр. 18 к § I.5). Очевидно, то же самое справедливо для любого интервала или их конечного объединения. Для любого метрического пространства X секвенциальная компактность некоторого подмножества $S \subset X$ эквивалентна следующему свойству, называемому просто *компактностью*: если S содержится в объединении открытых множеств, то оно содержится в некотором объединении конечного числа этих множеств (*каждое открытое покрытие обладает конечным подпокрытием*). (См. Симмонс [(a) 1], § 24; эта книга является хорошей сводкой понятий из общей топологии [1].) Отсюда следует, что открытое подмножество в $\mathbb{Q}_p$ компактно тогда и только тогда, когда оно есть объединение конечного числа интервалов (см. ниже упр. 1). Такие подмножества, называемые «компактно-открытыми», все время появляются в этом параграфе.

Определение. Пусть X и Y — два топологических пространства. Отображение $f\colon X \to Y$ называется *локально постоянным*, если каждая точка $x \in X$ обладает такой окрестностью U, что $f(U)$ — одноэлементное подмножество Y.

---

[1] См. также Куратовский [(a) 6], т. 1, § 41. — *Прим. перев.*

Очевидно, любая локально постоянная функция непрерывна.

В классическом анализе понятие локально постоянной функции малоупотребительно, потому что обычно все такие функции постоянны. Последнее верно для всякого связного X, например для $\mathbb{R}$ и $\mathbb{C}$.

Но у нас X будет компактно-открытым подмножеством в $\mathbb{Q}_p$ (как правило, $\mathbb{Z}_p$ или $\mathbb{Z}_p^\times = \{x \in \mathbb{Z}_p \mid |x|_p = 1\}$). На таких пространствах существует много нетривиальных локально постоянных функций. Точнее, $f\colon X \to \mathbb{Q}_p$ локально постоянна тогда и только тогда, когда f представима в виде конечной линейной комбинации характеристических функций компактно-открытых подмножеств (см. ниже упр. 4).

Локально постоянные функции играют для p-адических подпространств X ту же роль, что ступенчатые функции при определении интеграла Римана в случае $X = \mathbb{R}$.

Пусть теперь X — компактно-открытое подпространство в $\mathbb{Q}_p$, такое, как $\mathbb{Z}_p$ или $\mathbb{Z}_p^\times$.

Определение. Линейный над $\mathbb{Q}_p$ гомоморфизм μ $\mathbb{Q}_p$-векторного пространства локально постоянных функций на X в $\mathbb{Q}_p$ называется *p-адическим распределением на X*. Пусть $f\colon X \to \mathbb{Q}_p$ — некоторая локально постоянная функция. Вместо $\mu(f)$ мы обычно пишем $\int f\mu$.

Эквивалентное определение (см. ниже упр. 4). Аддитивное отображение μ множества компактно-открытых подмножеств в X со значениями в $\mathbb{Q}_p$ называется *p-адическим распределением на X*. Аддитивность означает, что для всякого разбиения множества $U \subset X$ на компактно-открытые подмножества $U_1, U_2, \ldots, U_n$

$$\mu(U) = \mu(U_1) + \mu(U_2) + \ldots + \mu(U_n).$$

Эквивалентность определений означает, что всякое μ во втором смысле однозначно «продолжается» до единственного μ в первом смысле, и наоборот, всякое μ в первом смысле «ограничивается» до некоторого μ во втором смысле. Точнее, пусть μ — распределение

в смысле первого определения. Тогда, положив

$$\mu(U) = \int (\text{характеристическая функция подмножества } U)\,\mu$$

для каждого компактно-открытого подмножества U, мы получим распределение (также обозначаемое через μ) в смысле второго определения. Обратно, если мы имеем распределение μ в смысле второго определения, то соответствующее распределение в первом смысле задается $\mathbb{Q}_p$-линейным продолжением с множества характеристических функций, для которых полагаем

$$\int (\text{характеристическая функция подмножества } U)\,\mu = \mu(U).$$

Итак, значение $\int f\mu$ для локально постоянной f легко вычислить, зная разложение f в линейную комбинацию характеристических функций.

Предложение. *Каждое отображение μ множества интервалов, содержащихся в X, в $\mathbb{Q}_p$, для которого*

$$\mu(a + (p^N)) = \sum_{b=0}^{p-1} \mu(a + bp^N + (p^{N+1}))$$

при любом $a + (p^N) \subset X$, однозначно продолжается до p-адического распределения на X.

Доказательство. Каждое компактно-открытое подмножество $U \subset X$ можно представить в виде конечного объединения непересекающихся интервалов: $U = \bigcup I_i$ (см. упр. 1). Положим тогда $\mu(U) \underset{\text{def}}{=} \sum \mu(I_i)$. (В силу аддитивности искомого μ, это значение $\mu(U)$ единственно возможное.) Проверим теперь независимость $\mu(U)$ от выбора разбиения множества U на интервалы. Для этого заметим прежде всего, что любые два разбиения $U = \bigcup I_i$ и $U = \bigcup I'_i$ на непересекающиеся интервалы имеют общее подразбиение (более мелкое, чем каждое из исходных) $I_i = \bigcup_j I_{ij}$, причем если $I_i = a + (p^N)$, то

I_{ij} пробегает все интервалы вида $a'+(p^{N'})$, где N' — некоторое фиксированное натуральное число $>N$, а $a' \equiv a \pmod{p^N}$. Тогда, применяя несколько раз формулу из условий предложения, мы получаем

$$\mu(I_i) = \mu(a+(p^N)) = \sum_{j=0}^{p^{N'-N}-1} \mu(a+jp^N+(p^{N'})) = \sum_j \mu(I_{ij}).$$

Следовательно, $\sum_i \mu(I_i) = \sum_{i,j} \mu(I_{ij})$. Отсюда $\sum_i \mu(I_i) = \sum_i \mu(I'_i)$, потому что обе части равны сумме по общему подразбиению. Теперь аддитивность μ очевидна. А именно, пусть U—объединение непересекающихся U_i. Разобьем каждое U_i в объединение непересекающихся интервалов I_{ij}. Тогда $U = \bigcup_{i,j} I_{ij}$ и

$$\mu(U) = \sum_{i,j} \mu(I_{ij}) = \sum_i \sum_j \mu(I_{ij}) = \sum_i \mu(U_i). \quad \square$$

Приведем теперь несколько простых примеров p-адических распределений.

(1) Распределение Хаара μ_{Haar}. Положим

$$\mu_{\text{Haar}}(a+(p^N)) \overset{\text{def}}{=} \frac{1}{p^N}.$$

По предыдущему предложению, эта функция продолжается до распределения на $\mathbb{Z}_p$, так как

$$\sum_{b=0}^{p-1} \mu_{\text{Haar}}(a+bp^N+(p^{N+1})) = \sum_{b=0}^{p-1} \frac{1}{p^{N+1}} = \frac{1}{p^N} = \mu_{\text{Haar}}(a+(p^N)).$$

Это единственное (с точностью до постоянного множителя) распределение, *инвариантное относительно сдвигов*, т. е. такое, что $\mu_{\text{Haar}}(a+U) = \mu_{\text{Haar}}(U)$ для всех $a \in \mathbb{Z}_p$, где $a+U \overset{\text{def}}{=} \{x \in \mathbb{Z}_p \mid x-a \in U\}$.

(2) Распределение Дирака μ_α, сосредоточенное в точке $\alpha \in \mathbb{Z}_p$ (α фиксировано). Положим

$$\mu_\alpha(U) \overset{\text{def}}{=} \begin{cases} 1, & \text{если } \alpha \in U, \\ 0 & \text{в противном случае.} \end{cases}$$

Аддитивность μ_α очевидна. Отметим, что $\int f \mu_\alpha = f(\alpha)$ для локально постоянных функций f.

(3) Распределение Мазура μ_{Mazur}. Прежде всего без ограничения общности запишем каждый интервал из $\mathbb{Z}_p$ в виде $a+(p^N)$, где a — целое рациональное число между 0 и p^N-1. Предполагая это, зададим

$$\mu_{\text{Mazur}}(a+(p^N)) \overset{\text{def}}{=} \frac{a}{p^N} - \frac{1}{2}.$$

Проверку аддитивности для μ_{Mazur} отложим до следующего параграфа, в котором она окажется частным случаем некоторого более общего утверждения.

В заключение укажем на одно существенное отличие распределений μ_{Haar} и μ_{Mazur} от классических мер. В этих двух примерах p-адических распределений мера «стягивающегося» интервала (т. е. при $N \to \infty$) *увеличивается* в p-адической метрике, а именно:

$$|\mu_{\text{Haar}}(a+(p^N))|_p = \left|\frac{1}{p^N}\right|_p = p^N$$

и для $p \nmid a$ (и $N>1$ в случае $p=2$)

$$|\mu_{\text{Mazur}}(a+(p^N))|_p = \left|\frac{a}{p^N} - \frac{1}{2}\right|_p = p^N.$$

С этой особенностью мы еще столкнемся ниже.

Упражнения

1. Дайте прямое доказательство компактности $\mathbb{Z}_p$ (т. е. существования конечного подпокрытия для каждого открытого покрытия $\mathbb{Z}_p$). Затем докажите, что открытое подмножество в $\mathbb{Z}_p$ компактно тогда и только тогда, когда оно представимо в виде конечного объединения непересекающихся интервалов. Заметим, что каждый интервал представим в виде конечного объединения

непересекающихся интервалов «равной длины»: $a+(p^n)=\bigcup_{b=0}^{p-1} a+bp^n+(p^{n+1})$. Докажите, что конечное повторное применение последней процедуры позволяет получить любое разбиение интервала в объединение непересекающихся подынтервалов.

2. Приведите пример открытого некомпактного подмножества в $\mathbb{Z}_p$.

3. Пусть U — открытое подмножество топологического пространства X, а $f\colon X\to\mathbb{Z}$ — его характеристическая функция, т. е.

$$f(x)=\begin{cases}1, & \text{если } x\in X,\\ 0 & \text{в противном случае.}\end{cases}$$

Покажите, что f локально постоянна для $X=\mathbb{Z}_p$ и любого компактно-открытого подмножества U, но не локально постоянна, если $X=\mathbb{R}$ и U — непустое открытое подмножество, отличное от $\mathbb{R}$.

4. Пусть X — компактно-открытое подмножество в $\mathbb{Q}_p$. Покажите, что функция $f\colon X\to\mathbb{Q}_p$ локально постоянна тогда и только тогда, когда она равна конечной линейной комбинации с коэффициентами в $\mathbb{Q}_p$ характеристических функций компактно-открытых подмножеств в X. Затем докажите эквивалентность двух определений распределения на X.

5. Пусть $\alpha\in\mathbb{Q}_p$ и $|\alpha|_p=1$. Покажите, что $\mu_{\text{Haar}}(\alpha U)=\mu_{\text{Haar}}(U)$ для каждого открытого компактного подмножества U, где αU обозначает множество $\{\alpha x \mid x\in U\}$.

6. Пусть $f\colon \mathbb{Z}_p\to\mathbb{Q}_p$ — локально постоянная функция, заданная следующим способом: $f(x)=$ первый знак p-адического разложения x. Найдите $\int f\mu$, когда: (1) $\mu=$ распределение Дирака μ_a; (2) $\mu=\mu_{\text{Haar}}$; (3) $\mu=\mu_{\text{Mazur}}$.

7. Пусть μ — функция на множестве интервалов $a+(p^N)$, заданная формулой

$$\mu(a+(p^N))=\begin{cases}p^{-[(N+1)/2]}, & \text{если первые } [N/2] \text{ знаков при нечетных степенях } p \text{ в } p\text{-адическом разложении } a \text{ равны 0,}\\ 0 & \text{в противном случае,}\end{cases}$$

где $[\ ]$ — целая часть. Докажите, что μ продолжается до распределения на $\mathbb{Z}_p$.

8. Обдумайте, как можно было бы построить примеры p-адических распределений с разной степенью роста $\max_{0\leqslant a<p^N}|\mu(a+(p^N))|_p$ при возрастании N.

§ 4. РАСПРЕДЕЛЕНИЯ БЕРНУЛЛИ

Прежде всего определим многочлены Бернулли $B_k(x)$. Рассмотрим следующую функцию от двух переменных t и x:

$$\frac{te^{xt}}{e^t-1}=\left(\sum_{k=0}^{\infty}B_k\frac{t^k}{k!}\right)\left(\sum_{k=0}^{\infty}\frac{(xt)^k}{k!}\right).$$

Собирая коэффициенты этого произведения при t^k, мы получим для каждого k многочлен от x. Произведение этого многочлена на $k!$ называется k-м многочленом Бернулли и обозначается через $B_k(x)$. Таким образом,

$$\frac{te^{xt}}{e^t-1}=\sum_{k=0}^{\infty}B_k(x)\frac{t^k}{k!}.$$

Вот несколько первых многочленов Бернулли:

$$B_0(x)=1,\quad B_1(x)=x-{}^1/_2,\quad B_2(x)=x^2-x+{}^1/_6,$$
$$B_3=x^3-{}^1/_2x^2+{}^3/_2x,\ \dots\ .$$

В этом параграфе, употребляя обозначение $a+(p^N)$, мы подразумеваем, что $0\leqslant a\leqslant p^N-1$. Фиксируем некоторое целое неотрицательное число k и определим отображение $\mu_{B,k}$ на множестве интервалов $a+(p^N)$ формулой

$$\mu_{B,k}(a+(p^N))=p^{N(k-1)}B_k(a/p^N).$$

Предложение. *Функция $\mu_{B,k}$ продолжается до распределения на $\mathbb{Z}_p$ (называемого k-м распределением Бернулли).*

Доказательство. По предложению из § 3 достаточно показать, что

$$\mu_{B,k}(a+(p^N))=\sum_{b=0}^{p-1}\mu_{B,k}(a+bp^N+(p^{N+1})).$$

Правая часть равна

$$p^{(N+1)(k-1)}\sum_{b=0}^{p-}B_k\left(\frac{a+bp^N}{p^{N+1}}\right).$$

Умножим доказываемое соотношение на $p^{-N(k-1)}$ и положим $\alpha = a/p^{N+1}$. Тогда мы увидим, что необходимо доказать соотношение

$$B_k(p\alpha) = p^{k-1}\sum_{b=0}^{p-1} B_k\left(\alpha + \frac{b}{p}\right).$$

Правая часть, деленная на $k!$, равна по определению многочленов $B_k(x)$ коэффициенту при t^k в разложении Тейлора функции

$$p^{k-1}\sum_{b=0}^{p-1}\frac{te^{(\alpha+b/p)t}}{e^t-1} = \frac{p^{k-1}te^{\alpha t}}{e^t-1}\sum_{b=0}^{p-1}e^{bt/p} = \frac{p^{k-1}te^{\alpha t}}{e^t-1}\cdot\frac{e^t-1}{e^{t/p}-1}.$$

Последний сомножитель получается суммированием геометрической прогрессии $\sum_{b=0}^{p-1} e^{bt/p}$. Далее находим

$$\frac{p^k(t/p)e^{(p\alpha)t/p}}{e^{t/p}-1} = p^k\sum_{j=0}^{\infty}B_j(p\alpha)\frac{(t/p)^j}{j!}$$

снова по определению $B_j(x)$. Следовательно, $k!$ раз взятый коэффициент этого ряда при t^k совпадает с

$$p^kB_k(p\alpha)\left(\frac{1}{p}\right)^k = B_k(p\alpha),$$

что и требовалось доказать. □

Несколько первых многочленов $B_k(x)$ дают следующие распределения:

$\mu_{B,0}(a+(p^N)) = p^{-N}$, т. е. $\mu_{B,0} = \mu_{\text{Haar}}$;

$\mu_{B,1}(a+(p^N)) = B_1\left(\frac{a}{p^N}\right) = \frac{a}{p^N} - \frac{1}{2}$, т. е. $\mu_{B,1} = \mu_{\text{Mazur}}$;

$\mu_{B,2}(a+(p^N)) = p^N\left(\frac{a^2}{p^{2N}} - \frac{a}{p^N} + \frac{1}{6}\right)$ и т. д.

Можно показать, что среди всех многочленов многочлены Бернулли единственные (с точностью до постоянного множителя), для которых можно задать распределения указанным выше способом. Этот факт нам не понадобится, поэтому мы его не доказываем. Однако

следует отметить важную и уникальную роль многочленов Бернулли $B_k(x)$ в p-адическом интегрировании. Это окажется связанным с появлением чисел Бернулли B_k (которые являются постоянными членами $B_k(x)$; см. ниже упр. 1) в доказанной выше формуле для $\zeta(2k)$.

§ 5. МЕРЫ И ИНТЕГРИРОВАНИЕ

Определение. *Мерой* называется p-адическое распределение μ на X, значения которого на открытых компактных подмножествах $U \subset X$ ограничены некоторой константой $B \in \mathbb{R}$, т. е.

$|\mu(U)|_p \leqslant B$ для всех компактно-открытых $U \subset X$.

Распределение Дирака μ_a для любого фиксированного $a \in \mathbb{Z}_p$ является мерой, но ни одно из распределений Бернулли не обладает этим свойством. Для превращения распределений Бернулли в меры существует стандартная процедура, называемая *регуляризацией*. Прежде всего введем некоторые обозначения. Для каждого $\alpha \in \mathbb{Z}_p$ обозначим через $\{\alpha\}_N$ целое рациональное число между 0 и p^N-1, сравнимое с $\alpha \pmod{p^N}$. Для $\alpha \in \mathbb{Q}_p$ и распределения μ обозначим через $\alpha\mu$ произведение этого распределения на α, т. е. $(\alpha\mu)(U) = \alpha\cdot(\mu(U))$ для каждого компактно-открытого подмножества U. И, наконец, если $U \subset \mathbb{Q}_p$ — компактно-открытое подмножество, $\alpha \in \mathbb{Q}_p$ и $\alpha \neq 0$, то положим $\alpha U \overset{\text{def}}{=} \{x \in \mathbb{Q}_p \mid x/\alpha \in U\}$. Легко проверить, что сумма двух распределений (или мер) является распределением (соответственно мерой), произведение $\alpha\mu$ распределения (или меры) μ на скаляр является распределением (соответственно мерой), а кроме того, если $\alpha \in \mathbb{Z}_p^\times$, а μ — распределение (или мера) на $\mathbb{Z}_p$, то функция μ': $\mu'(U) = \mu(\alpha U)$ задает распределение (соответственно меру) на $\mathbb{Z}_p$.

Рассмотрим целое рациональное α, отличное от 1 и не делящееся на p. *Регуляризованное* распределение Бернулли $\mu_{B,k,\alpha}$ на $\mathbb{Z}$, или, короче, $\mu_{k,\alpha}$, определяется формулой

$$\mu_{k,\alpha}(U) \overset{\text{def}}{=} \mu_{B,k}(U) - \alpha^{-k}\mu_{B,k}(\alpha U).$$

Вскоре мы установим, что $\mu_{k,a}$ — мера. Во всяком случае, как следует из замечаний в конце предыдущего абзаца, это заведомо распределение.

Его легко вычислить явно при $k=0$ или 1. Если $k=0$, то $\mu_{B,0}=\mu_{\text{Haar}}$ и, очевидно, $\mu_{0,a}(U)=0$ для любого U (см. упр. 5 к § 3). При $k=1$ получаем

$$\mu_{1,a}(a+(p^N)) = \frac{a}{p^N} - \frac{1}{2} - \frac{1}{\alpha}\left(\frac{\{\alpha a\}_N}{p^N} - \frac{1}{2}\right) =$$

$$= \frac{(1/\alpha)-1}{2} + \frac{a}{p^N} - \frac{1}{\alpha}\left(\frac{\alpha a}{p^N} - \left[\frac{\alpha a}{p^N}\right]\right) = \frac{1}{\alpha}\left[\frac{\alpha a}{p^N}\right] + \frac{(1/\alpha)-1}{2}$$

(где [ ] обозначает целую часть).

Предложение. *Для всех компактно-открытых $U \subset \mathbb{Z}_p$*

$$|\mu_{1,a}(U)|_p \leqslant 1.$$

Доказательство. Отметим, что $(\alpha^{-1}-1)/2 \in \mathbb{Z}_p$, так как $1/\alpha \in \mathbb{Z}_p$ и $1/2 \in \mathbb{Z}_p$, если $p \neq 2$. В случае $p=2$ верно то же самое, потому что $\alpha^{-1}-1 \equiv 0 \pmod 2$. Так как $[\alpha a/p^N] \in \mathbb{Z}$, то по предыдущей формуле $\mu_{1,a}(a+(p^N)) \in \mathbb{Z}_p$. С другой стороны, любое компактно-открытое множество U представимо в виде конечного объединения непересекающихся интервалов I_i. Поэтому $|\mu_{1,a}(U)|_p \leqslant \max |\mu_{1,a}(I_i)|_p \leqslant 1$. □

Итак, $\mu_{1,a}$ — мера. Это первый встретившийся нам интересный пример p-адической меры. Вскоре мы увидим, что мера $\mu_{1,a}$ играет почти такую же фундаментальную роль в p-адическом интегрировании, как «dx» в случае вещественного интегрирования.

Ниже мы докажем основное сравнение, связывающее распределения $\mu_{k,a}$ и $\mu_{1,a}$. Его доказательство на первый взгляд кажется просто непривлекательным вычислением, но оно становится понятнее, если рассмотреть аналогичную ситуацию из вещественного анализа. Предположим, что мы вычисляем интеграл вида $\int f\left(\sqrt[k]{x}\right) dx$ и хотим сделать замену переменных $x \longmapsto x^k$, т. е. перейти к вычислению интеграла $\int f(x)\, d(x^k)$. Далее используется простое правило: $d(x^k)/dx = kx^{k-1}$. На самом деле $d(x^k)$ можно рассматривать как «меру» μ_k

на вещественной прямой, для которой $\mu_k([a,b]) = b^k - a^k$. Тогда μ_1 является обычной длиной. Соотношение $d(x^k)/dx = kx^{k-1}$ в сущности означает, что

$$\lim_{b \to a} \mu_k([a,b])/\mu_1([a,b]) = ka^{k-1}.$$

Следовательно, заменяя $\mu_k(I_i)$ на $kx_i^{k-1}\mu_1(I_i)$ в интегральных суммах Римана $\sum f(x_i)\,\mu_k(I_i)$, мы получим при уменьшении длин всех I_i в пределе $\int f(x)\, kx^{k-1} dx$.

В доказательстве этого предельного соотношения используется биномиальное разложение для $(a+h)^k$ (где $h=b-a$). В действительности важны только первые два члена этого разложения: $a^k + kha^{k-1}$. Подобно этому в p-адическом случае при доказательстве асимптотической формулы $\mu_{k,a}(I) \sim ka^{k-1}\mu_{1,a}(I)$ для малых интервалов I, содержащих a, также используется биномиальное разложение. Таким образом, теорему 5 следует рассматривать как аналог теоремы из анализа, утверждающей, что $d(x^k)/dx = kx^{k-1}$. (При этом можно не обращать внимания на множители d_k в обеих частях сравнения из теоремы 5. Они означают лишь, что если разделить обе части на d_k, то p^N заменится на $p^{N-\operatorname{ord}_p d_k}$, где $\operatorname{ord}_p d_k$ — *константа*, не существенная при больших N.)

Теорема 5. *Пусть d_k — наименьшее общее кратное знаменателей всех коэффициентов многочлена $B_k(x)$: $d_1=2$, $d_2=6$, $d_3=2$ и т. д. Тогда*

$$d_k \mu_{k,a}(a+(p^N)) \equiv d_k\, ka^{k-1}\mu_{1,a}(a+(p^N)) \pmod{p^N}.$$

Доказательство. Из упр. 1 ниже следует, что многочлен $B_k(x)$ начинается с

$$B_0 x^k + kB_1 x^{k-1} + \ldots = x^k - \frac{k}{2}x^{k-1} + \ldots.$$

По определению,

$$d_k \mu_{k,a}(a+(p^N)) = d_k p^{N(k-1)}\left(B_k\left(\frac{a}{p^N}\right) - \alpha^{-k} B_k\left(\frac{\{\alpha a\}_N}{p^N}\right)\right).$$

Многочлен $d_k B_k(x)$ имеет целые коэффициенты и степень k. Поэтому в дальнейших рассмотрениях можно

учитывать только два его старших члена $d_k x^k$ — $-d_k(k/2)x^{k-1}$, ибо, так как x имеет знаменатель p^N, все остальные члены после умножения на $p^{N(k-1)}$ становятся целыми, делящимися на p^N. Кроме того, отметим, что $\alpha a \equiv \{\alpha a\}_N \pmod{p^N}$ и

$$\frac{\{\alpha a\}_N}{p^N} = \frac{\alpha a}{p^N} - \left[\frac{\alpha a}{p^N}\right] \quad ([\ ] - \text{целая часть}).$$

Следовательно,

$$d_k \mu_{k,\alpha}(a+(p^N)) \equiv d_k p^{N(k-1)} \left(\frac{a^k}{p^{Nk}} - \alpha^{-k}\left(\frac{\{\alpha a\}_N}{p^N}\right)^k - \right.$$

$$\left. - \frac{k}{2}\left(\frac{a^{k-1}}{p^{N(k-1)}} - \alpha^{-k}\left(\frac{\{\alpha a\}_N}{p^N}\right)^{k-1}\right)\right) \pmod{p^N} =$$

$$= d_k \left(\frac{a^k}{p^N} - \alpha^{-k} p^{N(k-1)}\left(\frac{\alpha a}{p^N} - \left[\frac{\alpha a}{p^N}\right]\right)^k - \right.$$

$$\left. - \frac{k}{2}\left(a^{k-1} - \alpha^{-k} p^{N(k-1)}\left(\frac{\alpha a}{p^N} - \left[\frac{\alpha a}{p^N}\right]\right)^{k-1}\right)\right) \equiv$$

$$\equiv d_k \left(\frac{a^k}{p^N} - \alpha^{-k}\left(\frac{\alpha^k a^k}{p^N} - k\alpha^{k-1}a^{k-1}\left[\frac{\alpha a}{p^N}\right]\right) - \right.$$

$$\left. - \frac{k}{2}\left(a^{k-1} - \alpha^{-k}\left(\alpha^{k-1}a^{k-1}\right)\right)\right) \pmod{p^N} =$$

$$= d_k k a^{k-1}\left(\frac{1}{\alpha}\left[\frac{\alpha a}{p^N}\right] + \frac{1/\alpha - 1}{2}\right) =$$

$$= d_k k a^{k-1} \mu_{1,\alpha}(a+(p^N)). \quad \square$$

Следствие. *Распределение $\mu_{k,\alpha}$ является мерой для любого $k = 1, 2, 3, \ldots$ и любого $\alpha \in \mathbb{Z}$, $\alpha \notin p\mathbb{Z}$, $\alpha \neq 1$.*

Доказательство. Мы должны установить ограниченность чисел $\mu_{k,\alpha}(a+(p^N))$. По теореме 5

$$|\mu_{k,\alpha}(a+(p^N))|_p \leqslant \max\left(\left|\frac{p^N}{d_k}\right|_p,\ |k a^{k-1}\mu_{1,\alpha}(a+(p^N))|_p\right) \leqslant$$

$$\leqslant \max\left(\left|\frac{1}{d_k}\right|_p,\ |\mu_{1,\alpha}(a+(p^N))|_p\right).$$

Но $|\mu_{1,\alpha}(a+(p^N))|_p \leqslant 1$, а d_k фиксировано. $\square$

Для чего же мы суетились и превратили (регуляризовали) распределения Бернулли в меры? Дело в том, что если μ — неограниченное распределение, то интеграл $\int f\mu$ определен лишь для локально постоянных функций f, и при попытках распространить интегрирование на непрерывные функции, рассматривая пределы римановых сумм, возникают трудности.

Возьмем, например, $\mu = \mu_{\text{Haar}}$ и простейшую функцию $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$, $f(x) = x$. Построим римановы суммы. Для заданной функции f и каждого N разобьем $\mathbb{Z}_p$ в объединение $\bigcup_{a=0}^{p^N-1}(a+(p^N))$, выберем в a-м интервале произвольную точку $x_{a,N}$ и определим N-ю риманову сумму функции f, соответствующую выбору точек $\{x_{a,N}\}$, как

$$S_{N,\{x_{a,N}\}}(f) \underset{\text{def}}{=} \sum_{a=0}^{p^N-1} f(x_{a,N})\mu(a+(p^N)).$$

В нашем примере эта сумма равна $\sum_{a=0}^{p^N-1} x_{a,N}\frac{1}{p^N}$. Например, при простейшем выборе $x_{a,N} = a$ получим

$$p^{-N}\sum_{a=0}^{p^N-1} a = p^{-N}\frac{(p^N-1)(p^N)}{2} = \frac{p^N-1}{2}.$$

При $N \to \infty$ эта сумма имеет предел в $\mathbb{Q}_p$, равный $-1/2$. Но если одно из выбранных значений $x_{a,N} = a \in a+(p^N)$ заменить на $a + a_0 p^N \in a+(p^N)$ для каждого N, где a_0 — некоторое фиксированное целое p-адическое число, то мы получим

$$p^{-N}\left(\sum_{a=0}^{p^N-1} a + a_0 p^N\right) = \frac{p^N-1}{2} + a_0,$$

что стремится к $a_0 - 1/2$. Следовательно, в этом случае римановы суммы не имеют предела, который бы не зависел от выбора точек в интервалах.

От «меры» μ мало толку, и она даже не заслуживает названия меры, если по ней нельзя проинтегрировать непрерывную функцию. (Здесь мы слегка преувеличиваем, см. ниже упр. 8—10.) Покажем теперь, что с этой точки зрения ограниченные распределения имеют право называться «мерами».

Напомним, что через X обозначается компактно-открытое подмножество в $\mathbb{Q}_p$, такое, например, как $\mathbb{Z}_p$ или $\mathbb{Z}_p^\times$. (Для простоты предположим, что $X \subset \mathbb{Z}_p$.)

Теорема 6. *Пусть μ — некоторая p-адическая мера на X, а $f\colon X \to \mathbb{Q}_p$ — непрерывная функция. Тогда существует предел при $N \to \infty$ римановых сумм*

$$S_{N,\{x_{a,N}\}} \underset{\text{def}}{=} \sum_{\substack{0 \leqslant n < p^N \\ n + (p^N) \subset X}} f(x_{a,N})\,\mu(a + (p^N))$$

(где суммирование ведется по всем a, для которых $a + (p^N) \subset X$, а $x_{a,N}$ — точки, выбранные в $a + (p^N)$), и этот предел не зависит от выбора $\{x_{a,N}\}$.

Доказательство. Предположим, что $|\mu(U)|_p \leqslant B$ для всех компактно-открытых подмножеств $U \subset X$. Оценим вначале $|S_{N,\{x_{a,N}\}} - S_{M,\{x_{a,M}\}}|_p$ при $M > N$. Выберем настолько большое натуральное N, что каждый интервал $a + (p^N)$ либо содержится в X, либо не пересекается с ним. Это возможно в силу представимости X в виде конечного объединения интервалов. Пользуясь аддитивностью μ, запишем $S_{N,\{x_{a,N}\}}$ следующим образом:

$$\sum_{\substack{0 \leqslant a < p^M \\ a + (p^M) \subset X}} f(x_{\bar{a},N})\,\mu(a + (p^M))$$

(где $\bar{a}$ обозначает приведенный вычет числа a по модулю p^N [1])). Кроме того, будем считать N настолько большим, что $|f(x) - f(y)|_p < \varepsilon$, когда $x \equiv y \pmod{p^N}$. (Отметим, что, поскольку X *компактно*, из непрерывности следует *равномерная* непрерывность; доказательство легко провести самостоятельно или можно обратиться к книге

[1]) То есть наименьшее целое неотрицательное число, сравнимое с a по модулю p^N. — *Прим. перев.*

Симмонса [(a) 1] [1]).) Тогда

$$|S_{N,\{x_{a,N}\}} - S_{M,\{x_{a,M}\}}|_p = \left| \sum_{\substack{0 \leqslant a < p^M \\ a + (p^M) \subset X}} (f(x_{\bar{a},N}) - f(x_{a,M}))\,\mu(a + (p^M)) \right|_p \leqslant$$
$$\leqslant \max\left(|f(x_{\bar{a},N}) - f(x_{a,M})|_p \cdot |\mu(a + (p^M))|_p\right) \leqslant \varepsilon B,$$

так как $x_{\bar{a},N} \equiv x_{a,M} \pmod{p^N}$. Поскольку B фиксировано, а ε произвольно, предел римановых сумм существует.

Независимость от выбора $\{x_{a,N}\}$ доказывается аналогично. А именно

$$|S_{N,\{x_{a,N}\}} - S_{N,\{x'_{a,N}\}}|_p = \left| \sum_{\substack{0 \leqslant a < p^N \\ a + (p^N) \subset X}} (f(x_{a,N}) - f(x'_{a,N}))\,\mu(a + (p^N)) \right|_p \leqslant$$
$$\leqslant \max_a \left(|f(x_{a,N}) - f(x'_{a,N})|_p \cdot |\mu(a + (p^N))|_p\right) \leqslant \varepsilon B. \quad \square$$

Определение. Пусть $f\colon X \to \mathbb{Q}_p$ — непрерывная функция, а μ — некоторая мера на X. Определим $\int f\mu$ как предел римановых сумм, существование которого было только что установлено. (Отметим, что так определенный интеграл совпадает с введенным ранее $\int f\mu$ для локально постоянных функций f.)

Следующие простые, но важные утверждения получаются непосредственно из этого определения.

Предложение. *Если $f\colon X \to \mathbb{Q}_p$ — такая непрерывная функция, что $|f(x)|_p \leqslant A$ для всех $x \in X$, а $|\mu(U)|_p \leqslant B$ для всех компактно-открытых подмножеств $U \subset X$, то*

$$\left|\int f\mu\right|_p \leqslant A \cdot B.$$

Следствие. *Если $f, g\colon X \to \mathbb{Q}_p$ — две такие непрерывные функции, что $|f(x) - g(x)|_p \leqslant \varepsilon$ для всех $x \in X$, а $|\mu(U)|_p \leqslant B$ для всех компактно-открытых подмножеств $U \subset X$, то*

$$\left|\int f\mu - \int g\mu\right|_p \leqslant \varepsilon B.$$

[1]) См. также [(a) 5]. — *Прим. перев.*

Упражнения

1. Покажите, что $B_k(x) = \sum_{i=0}^{k} \binom{k}{i} B_i x^{k-i}$ и, в частности, $B_k(0) = B_k$. Кроме того, покажите, что

$$\int_0^1 B_k(x)\,dx = \begin{cases} 1, & \text{если } k=0, \\ 0, & \text{если } k \neq 0, \end{cases} \quad \text{и} \quad \frac{d}{dx} B_k(x) = kB_{k-1}(x).$$

2. Докажите, что не существует распределения μ (кроме тождественно равного нулю), которое обладало бы следующим свойством:

$$\max_{0 \leqslant a < p^N} |\mu(a + (p^N))|_p \to 0 \quad \text{при} \quad N \to \infty.$$

3. Чему равно $\mu_{B,k}(\mathbb{Z}_p)$? $\mu_{B,k}(p\mathbb{Z}_p)$? $\mu_{B,k}(\mathbb{Z}_p^\times)$?

4. Докажите, что p-адическое распределение μ является мерой тогда и только тогда, когда при некотором $a \in \mathbb{Z}_p$ распределение $a \cdot \mu$ принимает значения в $\mathbb{Z}_p$. Докажите, что меры на X образуют векторное пространство над $\mathbb{Q}_p$.

5. Выразите $\mu_{k,\alpha}(\mathbb{Z}_p)$ и $\mu_{k,\alpha}(\mathbb{Z}_p^\times)$ через α и k. Вычислите $\int_{\mathbb{Z}_p^\times} f\mu_{1,\alpha}$ для $f(x) = \sum_{i=0}^{n} a_i x^i$.

6. Пусть p — нечетное простое число. Для $a = 0, 1, \ldots, p^n - 1$ обозначим через S_a сумму p-адических знаков числа a. Докажите, что функция $\mu(a + (p^n)) = (-1)^{S_a}$ определяет меру на $\mathbb{Z}_p$ и что $\int f\mu = 0$ для любой нечетной функции f (т. е. такой, что $f(-x) = -f(x)$).

7. Пусть $p > 2$, $f(x) = 1/x$ и $\alpha = 1 + p$. Докажите, что $\int_{\mathbb{Z}_p^\times} f\mu_{1,\alpha} \equiv -1 \pmod p$. (*Указание.* Воспользуйтесь следствием в конце § 5 с $g(x) = 1/(\text{первый знак } x)$, так что $(x) \equiv g(x) \pmod p$, а $g(x)$ локально постоянна.)

8. Распределение μ на X называется *распределением ограниченного роста*, если $\max_{0 \leqslant a < p^N} |p^N \mu(a + (p^N))|_p \to 0$ при $N \to \infty$, т. е. μ «возрастает строго медленнее, чем μ_{Haar}». Докажите справедливость теоремы 6 для таких μ и функций $f\colon X \to \mathbb{Q}_p$, удовлетворяющих условию Липшица: существует $A \in \mathbb{R}$ со свойством

$$|f(x) - f(y)|_p \leqslant A\,|x - y|_p \quad \text{при любых} \quad x, y \in X.$$

(Это понятие ввел Ю. И. Манин и применил его к p-адической интерполяции рядов Гекке.)

9. Пусть μ — распределение из упр. 7 к § 3. Проверьте, что μ имеет ограниченный рост. Пусть $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ — функция $f(x) = x$. Вычислите интеграл $\int f\mu$, который определен в силу предыдущего упражнения.

10. Пусть r — некоторое вещественное положительное число. Функцию $f\colon \mathbb{Z}_p \to \mathbb{Q}_p$ Мазур называет функцией «типа r», если существует такое $A \in \mathbb{R}$, что

$$|f(x) - f(x')|_p \leqslant A\,|x - x'|_p^r \quad \text{для всех} \quad x, x' \in \mathbb{Z}_p.$$

Отметим, что каждая такая функция непрерывна. Если $r \geqslant 1$, то f удовлетворяет условию Липшица (см. упр. 8). Рассмотрим p-адическое распределение μ на $\mathbb{Z}_p$, такое, что

$$p^{-Ns} \max_{0 \leqslant a < p^N} |\mu(a + (p^N))|_p \to 0 \quad \text{при} \quad N \to \infty$$

для некоторого положительного $s \in \mathbb{R}$. Докажите аналог теоремы 6 для такого μ и функций типа r, когда $r \geqslant s$.

§ 6. p-АДИЧЕСКАЯ ζ-ФУНКЦИЯ КАК ПРЕОБРАЗОВАНИЕ МЕЛЛИНА — МАЗУРА

Пусть X — компактно-открытое подмножество в $\mathbb{Z}_p$. Каждую заданную на $\mathbb{Z}_p$ меру μ можно ограничить на X. Это ограничение μ^* на X определяется как мера с $\mu^*(U) = \mu(U)$ для любого компактно-открытого подмножества $U \subset X$. В применении к интегрированию это означает, что

$$\int f\mu^* = \int f \cdot (\text{характеристическая функция } X)\,\mu.$$

Интеграл $\int f\mu^*$ будет обозначаться через $\int_X f\mu$.

Как уже было сказано, мы хотим проинтерполировать значения $-B_k/k$. Имеет место следующее простое соотношение:

$$\int 1 \cdot \mu_{B,k} = \mu_{B,k}(\mathbb{Z}_p) = B_k$$

(см. упр. 3 к § 5). Следовательно, нужно проинтерполировать числа $-\frac{1}{k}\int 1 \cdot \mu_{B,k}$.

Имеется ли непосредственная связь между распределениями $\mu_{B,k}$ при различных k? По-видимому, нет,

однако *регуляризованные* меры $\mu_{k,a}$ и $\mu_{1,a}$ связаны между собой по теореме 5. Точнее, из теорем 5 и 6 вытекает следующее

Предложение. *Пусть* $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ *— функция* $f(x) = x^{k-1}$ *(для фиксированного целого положительного* k*), а* X *— компактно-открытое подмножество в* $\mathbb{Z}_p$*. Тогда*

$$\int\limits_X 1 \cdot \mu_{k,a} = k \int\limits_X f\mu_{1,a}.$$

Доказательство. По теореме 5

$$\mu_{k,a}(a+(p^N)) \equiv ka^{k-1}\mu_{1,a}(a+(p^N)) \pmod{p^{N-\operatorname{ord}_p d_k}}.$$

Рассмотрим теперь настолько большое N, что X равно объединению интервалов вида $a+(p^N)$. Тогда

$$\int\limits_X 1 \cdot \mu_{k,a} = \sum_{\substack{0 \leqslant a < p^N \\ a+(p^N) \subset X}} \mu_{k,a}(a+(p^N)) \equiv$$

$$\equiv \sum_{\substack{0 \leqslant a < p^N \\ a+(p^N) \subset X}} ka^{k-1}\mu_{1,a}(a+(p^N)) \pmod{p^{N-\operatorname{ord}_p d_k}} =$$

$$= k \sum_{\substack{0 \leqslant a < p^N \\ a+(p^N) \subset X}} f(a)\,\mu_{1,a}(a+(p^N)).$$

Переходя к пределу при $N \to \infty$, мы получаем требуемое соотношение $\int\limits_X 1 \cdot \mu_{k,a} = k \int\limits_X f\mu_{1,a}$. □

Если мы заменим в наших обозначениях f на x^{k-1}, считая x «переменной интегрирования», то результат предложения примет вид

$$\int\limits_X 1 \cdot \mu_{k,a} = k \int\limits_X x^{k-1}\mu_{1,a}.$$

Выражение справа гораздо приятнее левого с точки зрения p-адической интерполяции, потому что вместо загадочного индекса переменная интерполирования k превратилась в показатель степени.

В § 2 мы уже выяснили, когда и как можно проинтерполировать функцию x^{k-1} при фиксированном x

(см. также упр. 8 к § 2). А именно, для интерполяции пригодны только $x \not\equiv 0 \pmod p$. Чтобы область интегрирования состояла только из таких чисел x, нужно взять $X = \mathbb{Z}_p^\times$.

Итак, утверждается, что значения $\int\limits_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,a}$ *можно* проинтерполировать. Чтобы добиться этого, скомбинируем результаты § 2 и следствия в конце § 5. Согласно следствию, если $|f(x) - x^{k-1}|_p \leqslant \varepsilon$ для всех $x \in \mathbb{Z}_p^\times$, то

$$\left| \int\limits_{\mathbb{Z}_p^\times} f\mu_{1,a} - \int\limits_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,a} \right|_p \leqslant \varepsilon$$

(напомним, что $|\mu_{1,a}(U)|_p \leqslant 1$ для каждого компактно-открытого подмножества U). Подставим вместо f функцию $x^{k'-1}$, для которой $k' \equiv k \pmod{p-1}$ и $k' \equiv k \pmod{p^N}$ (это равносильно выполнению одного сравнения $k' \equiv k \pmod{(p-1)p^N}$). Из рассуждений § 2 следует неравенство

$$|x^{k'-1} - x^{k-1}|_p \leqslant 1/p^{N+1}$$

для всех $x \in \mathbb{Z}_p^\times$. Поэтому

$$\left| \int\limits_{\mathbb{Z}_p^\times} x^{k'-1}\mu_{1,a} - \int\limits_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,a} \right|_p \leqslant \frac{1}{p^{N+1}}.$$

Итак, фиксируем $s_0 \in \{0, 1, 2, \ldots, p-2\}$. Пусть $S_{s_0} \overset{\text{def}}{=} \{$целые положительные числа, сравнимые с s_0 по модулю $p-1\}$ — область изменения переменной k. Тогда из предыдущего мы заключаем, что функция $\int\limits_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,a}$ от k продолжается до непрерывной функции $\int\limits_{\mathbb{Z}_p^\times} x^{s_0+s(p-1)-1}\mu_{1,a}$ от целого p-адического s.

Однако мы ушли немного в сторону от исходных чисел $\frac{1}{k}\int 1 \cdot \mu_{B,k}$. Выше было установлено, что значения

$$\int\limits_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,a} = \frac{1}{k} \int\limits_{\mathbb{Z}_p^\times} 1 \cdot \mu_{k,a}$$

можно проинтерполировать. Сравним эти числа с исходными:

$$\frac{1}{k}\int\limits_{\mathbb{Z}_p^\times} 1\cdot\mu_{k,\,a} = \frac{1}{k}\,\mu_{k,\,a}(\mathbb{Z}_p^\times) = \frac{1}{k}\,(1-\alpha^{-k})\,(1-p^{k-1})\,B_k =$$

(см. упр. 5 к § 5)

$$= (\alpha^{-k}-1)\,(1-p^{k-1})\left(-\frac{1}{k}\int\limits_{\mathbb{Z}_p} 1\cdot\mu_{B,\,k}\right).$$

Множитель $1-p^{k-1}$ появился в силу того, что интегрировать пришлось по $\mathbb{Z}_p^\times$, а не по $\mathbb{Z}_p$. Этот эффект уже был предсказан в конце § 2: перед интерполяцией ζ-функции следует убрать эйлеров p-множитель, так как функция n^s при $p\mid n$ не интерполируется. Поэтому ниже мы будем интерполировать числа $(1-p^{k-1})\times$ $\times\,(-B_k/k)$:

$$(1-p^{k-1})\left(-\frac{B_k}{k}\right) = \frac{1}{\alpha^{-k}-1}\int\limits_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\,\alpha}.$$

Как мы предупреждали в § 2, читателя не должен смущать вид эйлерова множителя $1-p^{k-1}$, хотя по эвристическим соображениям из § 2 следовало как будто ожидать множитель $1-p^{-k}$. Дело обстоит так, как если бы на самом деле интерполировались не значения $\zeta(k)$, а значения «$\zeta(1-k)$» (правда, мы их пока не определили при положительных k). Поэтому мы определим ниже p-адическую ζ-функцию так, чтобы она принимала значение $(1-p^{k-1})\,(-B_k/k)$ для целого числа $1-k$, а не для самого k.

Определение. Для целого положительного k пусть

$$\zeta_p(1-k) \overset{\text{def}}{=} (1-p^{k-1})\,(-B_k/k),$$

так что, по предыдущему,

$$\zeta_p(1-k) = \frac{1}{\alpha^{-k}-1}\int\limits_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\,\alpha}.$$

Заметим, что правая часть последнего выражения не зависит от α. Действительно, если $\beta\in\mathbb{Z}$, $p\nmid\beta$, $\beta\neq 1$, то $(\beta^{-k}-1)^{-1}\int\limits_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\,\beta} = (\alpha^{-k}-1)^{-1}\int\limits_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\,\alpha}$,

так как оба эти числа равны $(1-p^{k-1})\,(-B_k/k)$. Это равенство, т. е. независимость от α, также можно доказать непосредственно (см. упр. 1). Независимость от α будет использована ниже при определении $\zeta_p(s)$ для p-адических s.

Прежде всего выведем несколько классических теоретикочисловых результатов о числах Бернулли. Эти результаты всегда считались очень изящными, но загадочными, пока не была открыта их связь с дзета-функцией Куботы — Леопольдта ζ_p и мерой Мазура $\mu_{1,\,\alpha}$, которая показала, что они возникают естественным образом из «аналитических» соображений (а именно, из следствия в конце § 5, которое, грубо говоря, утверждает, что две функции, близкие на некотором интервале, имеют близкие интегралы).

Теорема 7 ((1) и (2) — Куммер, (3) — Клаузен и фон Штаудт).

(1) *Если* $(p-1)\nmid k$, *то* $|B_k/k|_p\leqslant 1$.

(2) *Если* $(p-1)\nmid k$ *и* $k\equiv k'\pmod{(p-1)\,p^N}$, *то*

$$(1-p^{k-1})\frac{B_k}{k}\equiv(1-p^{k'-1})\frac{B_{k'}}{k'}\pmod{p^{N+1}}.$$

(3) *Если* $(p-1)\mid k$ *и* k *четно* (*или* $k=1$, $p=2$), *то*

$$pB_k\equiv -1\pmod p.$$

Доказательство. Предположим, что $p>2$. Доказательство утверждения (3) при $p=2$ мы оставляем читателю в качестве упражнения (см. ниже упр. 6).

Сейчас нам понадобится один факт, доказательство которого будет дано ниже, в начале следующей главы (см. конец § III.1): существует такое $\alpha\in\{2,\ 3,\ \ldots\ \ldots,\ p-1\}$, что α^{p-1} есть степень числа α с наименьшим положительным показателем, сравнимая с 1 по модулю p. Иначе говоря, мультипликативная группа ненулевых классов вычетов кольца $\mathbb{Z}$ по модулю p является циклической группой порядка $p-1$, т. е. существует образующая $\alpha\in\{2,\ 3,\ \ldots,\ p-1\}$, для

которой наименьшие положительные вычеты элементов α, α^2, α^3, ..., α^{p-1} исчерпывают все множество $\{1, 2, 3, \ldots, p-1\}$.

При доказательстве утверждений (1) и (2) в качестве «регуляризатора меры» α берется такая образующая из $\{2, 3, \ldots, p-1\}$. Поэтому, так как $(p-1) \nmid (-k)$, то $\alpha^{-k} \not\equiv 1 \pmod p$ и $(\alpha^{-k}-1)^{-1} \in \mathbb{Z}_p^\times$.

Докажем теперь (1) (предполагая, что $k > 1$; если $k=1$ и $p>2$, то $|B_1/1|_p = |-1/2|_p = 1$). Имеем

$$|B_k/k|_p = \left|\frac{1}{\alpha^{-k}-1}\right|_p \left|\frac{1}{1-p^{k-1}}\right|_p \left|\int_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\alpha}\right|_p =$$

$$= \left|\int_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\alpha}\right|_p \leqslant 1,$$

по предложению в конце § 5 (с $A=B=1$), так как $|\mu_{1,\alpha}(U)|_p \leqslant 1$ для любого компактно-открытого подмножества $U \subset \mathbb{Z}_p^\times$ и $|x^{k-1}|_p \leqslant 1$ для всех $x \in \mathbb{Z}_p^\times$.

Чтобы доказать (2), запишем требуемое сравнение в виде

$$\frac{1}{\alpha^{-k}-1}\int_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\alpha} \equiv \frac{1}{\alpha^{-k'}-1}\int_{\mathbb{Z}_p^\times} x^{k'-1}\mu_{1,\alpha} \pmod{p^{N+1}}.$$

Заметим, что если для некоторых a, b, c, $d \in \mathbb{Z}_p$ выполнены сравнения $a \equiv c \pmod{p^n}$ и $b \equiv d \pmod{p^n}$, то $ab \equiv cb \equiv cd \pmod{p^n}$. Таким образом, поскольку $a = (\alpha^{-k}-1)^{-1}$, $b = \int_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\alpha}$, $c = (\alpha^{-k'}-1)^{-1}$, $d = \int_{\mathbb{Z}_p^\times} x^{k'-1}\mu_{1,\alpha}$ принадлежат $\mathbb{Z}_p$, достаточно установить сравнения $(\alpha^{-k}-1)^{-1} \equiv (\alpha^{-k'}-1)^{-1} \pmod{p^{N+1}}$ и $\int_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\alpha} \equiv \int_{\mathbb{Z}_p^\times} x^{k'-1}\mu_{1,\alpha} \pmod{p^{N+1}}$. Первое из них сводится к $\alpha^k \equiv \alpha^{k'} \pmod{p^{N+1}}$, а второе (согласно следствию в конце § 5 с $B=1$ и $\varepsilon = p^{-N-1}$) — к $x^{k-1} \equiv x^{k'-1} \pmod{p^{N+1}}$ для любых $x \in \mathbb{Z}_p^\times$. Оба эти факта нетрудно получить из рассуждений § 2.

В заключение докажем сравнение Клаузена — фон Штаудта. Для этого рассмотрим $\alpha = 1+p$. Напомним,

что мы ограничились случаем $p>2$. Итак,

$$pB_k = -kp(-B_k/k) = \frac{-kp}{\alpha^{-k}-1}\frac{1}{1-p^{k-1}}\int_{\mathbb{Z}_p^\times} x^{k-1}\mu_{\alpha,1}.$$

Вначале возьмем первый из трех сомножителей справа. Если $d = \operatorname{ord}_p k$, то $\alpha^{-k}-1 = (1+p)^{-k}-1 \equiv -kp \pmod{p^{d+2}}$, откуда

$$1 \equiv \frac{-kp}{\alpha^{-k}-1} \pmod p.$$

Далее, так как $k \geqslant 2$, имеем $(1-p^{k-1})^{-1} \equiv 1 \pmod p$. Следовательно,

$$pB_k \equiv \int_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\alpha} \pmod p.$$

Используя снова следствие в конце § 5, на этот раз для функций $f(x) = x^{k-1}$ и $g(x) = 1/x$, мы получаем

$$pB_k \equiv \int_{\mathbb{Z}_p^\times} x^{-1}\mu_{1,\alpha} \pmod p.$$

Последний интеграл сравним с -1 по модулю p в силу упр. 7 к § 5. □

Вернемся теперь к p-адической интерполяции.

Определение. Фиксируем некоторое $s_0 \in \{0, 1, 2, \ldots, p-2\}$. Для $s \in \mathbb{Z}_p$ ($s \neq 0$, если $s_0 = 0$) положим

$$\zeta_{p,s_0}(s) \underset{\text{def}}{=} \frac{1}{\alpha^{-(s_0+(p-1)s)}-1}\int_{\mathbb{Z}_p^\times} x^{s_0+(p-1)s-1}\mu_{1,\alpha}.$$

Смысл этого определения сейчас должен быть ясен: значения

$$\alpha^{-(s_0+(p-1)s)} = \alpha^{-s_0}(\alpha^{p-1})^{-s} \quad \text{и}$$

$$x^{s_0+(p-1)s-1} = x^{s_0-1}(x^{p-1})^s$$

для любого $x \in \mathbb{Z}_p^\times$ и целого p-адического s определяются как пределы соответствующих значений для последовательности целых положительных чисел $\{k_i\}$, p-адически стремящейся к s. Значение $\zeta_{p,s_0}(s)$ можно

также определить как предел

$$-\lim_{k_i \to s} \left(1 - p^{s_0 + (p-1)k_i - 1}\right) B_{s_0 + (p-1)k_i}/(s_0 + (p-1)k_i).$$

Теперь очевидно, что для каждого целого положительного k, сравнимого с s_0 по модулю $p-1$, т. е. $k = s_0 + (p-1)k_0$, мы имеем $\zeta_p(1-k) = \zeta_{p, s_0}(k_0)$. Поэтому функции ζ_{p, s_0} можно рассматривать как p-адические «ветви» функции ζ_p — одна ветвь для каждого класса вычетов по модулю $p-1$. (Отметим, что нечетным классам вычетов $s_0 = 1, 3, \ldots, p-2$ отвечает нулевая функция, так как $B_{s_0 + (p-1)k_i} = 0$ для таких s_0; по этой причине интересны только четные s_0.)

В определении ζ_{p, s_0} значение $s = 0$ при $s_0 = 0$ исключено. Причина этого в том, что при $s = 0$ было бы $\alpha^{-(s_0 + (p-1)s)} = 1$, так что знаменатель в определении функции обратился бы в нуль. Как видно из записи $\zeta_p(1-k) = \zeta_{p, s_0}(k_0)$, где $k = s_0 + (p-1)k_0$, исключенный случай соответствует значению $\zeta_p(1)$. Таким образом, p-адическая дзета-функция, подобно архимедовой дзета-функции Римана, обладает «полюсом» в 1.

Теорема 8. *Фиксируем простое p и некоторый вычет s_0. Тогда функция $\zeta_{p, s_0}(s)$ ($s \neq 0$ при $s_0 = 0$) является непрерывной функцией p-адического аргумента s и ее определение не зависит от выбора $\alpha \in \mathbb{Z}$, $p \nmid \alpha$, $\alpha \neq 1$.*

Доказательство. Непрерывность по s интеграла в определении функции получается непосредственно из рассуждений § 2 и следствия в конце § 5. Множитель $1/(\alpha^{-(s_0 + (p-1)s)} - 1)$ непрерывен, если при $s_0 = 0$ исключить значение $s = 0$, потому что непрерывна функция $\alpha^{-(s_0 + (p-1)s)}$ (согласно § 2). Поэтому $\zeta_{p, s_0}(s)$ также непрерывна.

Остается установить независимость $\zeta_{p, s_0}(s)$ от α. Пусть $\beta \in \mathbb{Z}$, $p \nmid \beta$, $\beta \neq 1$. Две функции

$$\frac{1}{\alpha^{-(s_0 + (p-1)s)} - 1} \int_{Z_p^\times} x^{s_0 + (p-1)s - 1} \mu_{1, \alpha},$$

$$\frac{1}{\beta^{-(s_0 + (p-1)s)} - 1} \int_{Z_p^\times} x^{s_0 + (p-1)s - 1} \mu_{1, \beta}$$

совпадают для любых целых $s_0 + (p-1)s = k$, бо́льших 0, т. е. для любых целых неотрицательных s ($s > 0$ при $s_0 = 0$), поскольку в этом случае обе данные функции принимают одно и то же значение $(1 - p^{k-1}) \times (-B_k/k)$. Но множество целых неотрицательных чисел плотно в $\mathbb{Z}_p$, поэтому любые две непрерывные функции, совпадающие на этом множестве, равны. Следовательно, замена α на β не влияет на определение ζ_{p, s_0}. □

Теорема 8 дает p-адическую интерполяцию «интересной части» $-B_{2k}/2k$ значений $\zeta(2k)$. Осталось только объяснить несколько вещей: (1) термин «преобразование Меллина — Мазура» в названии этого параграфа и (2) таинственную замену k на $1-k$. Кроме того, следует сказать кое-что о (3) более глубокой аналогии с классическими ζ-функциями и L-функциями, а также о (4) связи с модулярными формами. Так как эти четыре темы вывели бы нас далеко за рамки материала, отобранного для изложения с доказательствами в этой книге, то ниже мы лишь вкратце расскажем о самых основных фактах, сюда относящихся. Доказательства и дальнейшие сведения по темам (1) — (4) можно найти в следующих работах: (1) Манин [(c) 6], § 8; (2) Ивасава [(c) 1], § 1 и приложение; (3) Ивасава [(c) 1], особенно § 5, Боревич и Шафаревич [(b) 1], стр. 439—444; (4) Серр [(c) 5].

§ 7. КРАТКИЙ ОБЗОР (БЕЗ ДОКАЗАТЕЛЬСТВ)

(1) Функция $\zeta(s)$ при $s > 1$ представима в виде интеграла

$$\frac{1}{\Gamma(s)} \int_0^\infty x^{s-1} \frac{dx}{e^x - 1},$$

где $\Gamma(s)$ — гамма-функция, которая удовлетворяет функциональному уравнению $\Gamma(s+1) = s\Gamma(s)$, а $\Gamma(1) = 1$, откуда $\Gamma(k) = (k-1)!$ для всех целых положительных k. (Случай $s = k$ см. ниже в упр. 4.) Этот интеграл известен как преобразование Меллина. Вообще, если

$f(x)$ — некоторая функция, определенная на множестве положительных вещественных чисел, то функция

$$g(s)=\int_0^\infty x^{s-1}f(x)\,dx$$

всякий раз, когда она определена, называется преобразованием Меллина функции $f(x)$ (или дифференциальной формы $f(x)\,dx$). Таким образом, $\Gamma(s)\,\zeta(s)$ есть преобразование Меллина дифференциала $dx/(e^x-1)$, определенное при $s>1$ (см. ниже упр. 4).

В § 6 было показано, что функция, p-адически интерполирующая $(1-p^{k-1})(-B_k/k)$, совпадает по существу (с точностью до множителя $1/(\alpha^{-s}-1)$ и некоторого изменения аргумента в соответствии с выбором s_0) с интегралом

$$\int_{\mathbf{Z}_p^\times} x^{s-1}\mu_{1,\alpha},$$

где $\mu_{1,\alpha}$ — регуляризованная мера Мазура. Следовательно, подобно классической дзета-функции, p-адическую ζ-функцию можно рассматривать как «p-адическое преобразование Меллина — Мазура» регуляризованной меры Мазура $\mu_{1,\alpha}$.

(2) Рассмотрим ряд

$$\zeta(s)=\sum_{n=1}^\infty \frac{1}{n^s}$$

для комплексных значений s с вещественной частью >1. Этот ряд сходится и определяет в этой области значений s комплексно аналитическую функцию. Эта функция $\zeta(s)$ допускает *аналитическое продолжение* на всю комплексную плоскость, за исключением точки $s=1$ (в окрестности которой она ведет себя как $1/(s-1)$). Фундаментальное свойство $\zeta(s)$ заключается в том, что она удовлетворяет *функциональному уравнению*, связывающему ее значения в точках s и $1-s$, а именно:

$$\zeta(1-s)=\frac{2\cos(\pi s/2)\,\Gamma(s)}{(2\pi)^s}\,\zeta(s).$$

Пусть $s=2k$ — целое четное положительное число. Тогда

$$\zeta(1-2k)=\frac{2\cos\pi k\,(2k-1)!}{(2\pi)^{2k}}\,\zeta(2k)=$$

$$=\frac{2(-1)^k(2k-1)!}{(2\pi)^{2k}}\,\frac{(-1)^k\pi^{2k}2^{2k-1}}{(2k-1)!}\left(-\frac{B_{2k}}{2k}\right)=-\frac{B_{2k}}{2k}$$

(по теореме 4). С другой стороны, если s — *нечетное* целое число >1, то правая часть функционального уравнения обращается в нуль, так как $\cos(\pi s/2)=0$ (предположение $s>1$ необходимо для конечности $\zeta(s)$). Следовательно, $\zeta(1-s)$ равно нулю, что также согласуется с формулой $\zeta(1-k)=-B_k/k$. Иначе говоря, функциональное уравнение в этом случае утверждает, что $0=0$.

Вот несколько первых значений $\zeta(1-k)=-B_k/k$:

$1-k$	-1	-3	-5	-7	-9	-11	-13	-15	-17	-19	-21
$\zeta(1-k)$	$-\frac{1}{12}$	$\frac{1}{120}$	$-\frac{1}{252}$	$\frac{1}{240}$	$-\frac{1}{132}$	$-\frac{691}{32\,760}$	$-\frac{1}{12}$	$\frac{3617}{8160}$	$-\frac{43\,867}{14\,364}$	$\frac{174\,611}{6600}$	$-\frac{77\,683}{276}$

Поэтому «в действительности» мы интерполировали ζ-функцию Римана, заданную на множестве *целых отрицательных нечетных чисел*. Следующее соотношение устанавливает простую связь между ζ_p и ζ:

$$\zeta_p(1-k)=(1-p^{k-1})\,\zeta(1-k),\quad k=2,\ 3,\ 4,\ \ldots\ .$$

Пренебрегая всеми расходимостями, можно написать $\zeta(1-k)=\prod_{\text{простые } q} 1/(1-q^{k-1})$, откуда

$$\zeta^*(1-k)=\prod_{\text{простые } q,\ q\neq p} 1/(1-q^{k-1})=(1-p^{k-1})\,\zeta(1-k).$$

Появление множителя $1-p^{k-1}$ становится эвристически понятным с этой «беззаботной» точки зрения.

В том же стиле можно непосредственно вывести формулу $\zeta(1-k)=-B_k/k$:

$$\zeta(1-k)\overset{\text{def}}{=}\sum_{n=1}^\infty \frac{1}{n^{1-k}}=\sum_{n=1}^\infty n^{k-1}.$$

Так как $(d/dt)^{k-1}e^{nt}|_{t=0} = n^{k-1}$, то

$$\zeta(1-k) = \sum_{n=1}^{\infty}\left(\frac{d}{dt}\right)^{k-1} e^{nt}\Big|_{t=0} = \left(\frac{d}{dt}\right)^{k-1}\sum_{n=1}^{\infty} e^{nt}\Big|_{t=0} =$$

$$= \left(\frac{d}{dt}\right)^{k-1}\left(\frac{1}{1-e^t}-1\right)\Big|_{t=0} = \left(\frac{d}{dt}\right)^{k-1}\left(\frac{1}{1-e^t}\right)\Big|_{t=0} =$$

$$= \left(\frac{d}{dt}\right)^{k-1}\left(-\frac{1}{t}\sum_{n=1}^{\infty} B_n\frac{t^n}{n!}\right)\Big|_{t=0} =$$

$$= \left(\frac{d}{dt}\right)^{k-1}\sum\left(-\frac{B_n}{n}\right)\frac{t^{n-1}}{(n-1)!}\Big|_{t=0} = -\frac{B_k}{k}.$$

(3) Существуют и более глубокие связи между ζ_p и ζ. Один важный пример такой связи требует введения функций следующего вида:

$$L_\chi(s) \underset{\text{def}}{=} \sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}, \quad s>0,$$

обобщающих ζ-функцию; здесь χ — некоторый *характер Дирихле* (см. упр. 9—10 к § 2). Если характер χ *не тривиален* (т. е. отличен от 1 для некоторого n), то функция $L_\chi(s)$ сходится при $s=1$. Более того, имеет место явная формула

$$L_\chi(1) = -\frac{\tau(\chi)}{N}\sum_{a=1}^{N-1}\bar{\chi}(a)\log(1-e^{-2\pi ia/N}),$$

где N — кондуктор характера χ, а $\tau(\chi) = \sum_{a=1}^{N-1}\chi(a)e^{2\pi ia/N}$ (эта формула легко приводится к виду, указанному в упр. 9—10 к § 2).

Функция $L_\chi(1-k)$ допускает p-адическую интерполяцию; конструкция, аналогичная конструкции ζ_p, позволяет построить *p-адическую L-функцию* $L_{\chi,p}$. Неожиданно оказывается, что значение $L_{\chi,p}(1)$ равно следующему выражению:

$$-\left(1-\frac{\chi(p)}{p}\right)\frac{\tau(x)}{N}\sum_{a=1}^{N-1}\bar{\chi}(a)\log_p(1-e^{-2\pi ia/N}),$$

в котором $\log_p$ обозначает «*p-адический логарифм*», являющийся p-адической функцией от p-адического аргумента (см. § IV.1 и упр. 5 к § IV.2), и все встречающиеся в данном выражении корни из единицы, а именно $e^{2\pi ia/N}$ и значения характера χ, рассматриваются как элементы алгебраического расширения поля $\mathbb{Q}_p$ (см. § III. 2—3). Множитель $1-\chi(p)/p$ нужно представлять себе как p-множитель Эйлера (для обычной ζ-функции $\chi=1$ и множитель Эйлера для $\zeta(1)$, будь это значение конечным, был бы равен $1-1/p$; см. также часть упр. 9 к § 2, касающуюся эйлеровых произведений для L_χ). В остальном выражение для $L_{\chi,p}(1)$ совпадает с явной формулой для $L_\chi(1)$, за тем исключением, что в этой формуле классический log заменен его p-адическим аналогом $\log_p$.

(4) Важную роль при изучении эллиптических кривых и модулярных форм (см. Серр [(b) 3], гл. VII) играют ряды Эйзенштейна E_{2k}, $k\geqslant 2$, которые представляют собой функции, определенные для всех комплексных чисел z с положительной мнимой частью следующим образом:

$$E_{2k}(z) = -\frac{1}{2}\frac{B_{2k}}{2k} + \sum_{n=1}^{\infty}\sigma_{2k-1}(n)e^{2\pi inz},$$

где

$$\sigma_m(n) \underset{\text{def}}{=} \sum_{d\mid n} d^m.$$

Каждый такой ряд есть ряд Фурье, т. е. некоторый степенной ряд относительно $e^{2\pi iz}$, с постоянным членом $^1/_2\zeta(1-2k)$.

Оказывается, ряды Эйзенштейна допускают p-адическую интерполяцию. На это указывает, в частности, p-адическая интерполируемость n-го коэффициента, если только $p\nmid n$. Действительно, каждый такой коэффициент $\sigma_{2k-1}(n)$ равен конечной сумме значений функций d^{2k-1}, которые интерполируются согласно результатам § 2 при $p\nmid d$. Тогда интерполяцию $\zeta(1-2k)$ можно рассматривать как «вычисление нулевого коэффициента». Как бы туманно это ни выглядело, в действительности все результаты этой главы можно извлечь из теории

p-адических модулярных форм. Подробности см. в упомянутой выше статье Серра, а также в серии статей Н. Катца по p-адическим мерам Эйзенштейна и p-адической интерполяции рядов Эйзенштейна (см. литературу).

Упражнения

1. Используя соотношения между $\mu_{1,\alpha}$, $\mu_{k,\alpha}$ и $\mu_{B,k}$, докажите непосредственно (без упоминания чисел Бернулли) независимость от α выражения

$$\frac{1}{\alpha^{-k}-1}\int_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\alpha}.$$

2. Пользуясь таблицей значений $\zeta(1-k)$, проверьте сравнения Куммера для $p=5$, $k=2$, $k'=22$, $N=1$. Также по этой таблице проверьте, что эти сравнения неверны, если $(p-1)\nmid k$. Используя сравнения Куммера и несколько первых чисел B_k, вычислите следующие числа по модулю p^2:

(i) B_{102} в $\mathbb{Q}_5$; (ii) B_{296} в $\mathbb{Q}_7$; (iii) B_{592} в $\mathbb{Q}_7$.

3. Применяя теорему 7 и упр. 19 к § I.2, докажите следующий вариант теоремы Клаузена—фон Штаудта: $(B_k+\sum 1/p)\in\mathbb{Z}$, где суммирование производится по всем p, для которых $(p-1)\mid k$.

4. Установите существование интеграла $\int_0^\infty x^{s-1}\,dx/(e^x-1)$ при $s>1$. Записав $1/(e^x-1)=e^{-x}/(1-e^{-x})=\sum_{n=1}^{\infty} e^{-nx}$, покажите, что

$$\int_0^\infty \frac{x^{k-1}}{e^x-1}\,dx=(k-1)!\,\zeta(k),\qquad k=2,\ 3,\ 4,\ \ldots$$

(представьте обоснования ваших вычислений).

5. Докажите, что

$$\int_0^\infty \frac{x^{k-1}}{e^x+1}\,dx=(k-1)!\,(1-2^{1-k})\,\zeta(k)$$

для $k=2,\ 3,\ 4,\ \ldots$. Покажите, что функция

$$\frac{1}{\Gamma(s)(1-2^{1-s})}\int_0^\infty \frac{x^{s-1}}{e^x+1}\,dx,$$

которая, как вы только что доказали, совпадает с $\zeta(s)$ при $s=k=2,\ 3,\ 4,\ \ldots$, определена и непрерывна на множестве чисел $s>0$, $s\neq 1$.

6. Докажите теорему Клаузена—фон Штаудта для $p=2$. (*Указание.* Возьмите $\alpha=1+p^2=5$ и $g(x)=(a_0+2a_1)^{-1}$, где a_0, a_1 — два первых 2-адических знака x.) Скажите словами, что утверждает эта теорема о числителе и знаменателе числа B_k при четном k и $p=2$.

Глава III

КОНСТРУКЦИЯ ПОЛЯ Ω

§ 1. КОНЕЧНЫЕ ПОЛЯ

В дальнейшем нам придется предполагать, что читатель знаком с основными понятиями, касающимися алгебраических расширений полей. Повторение всех необходимых доказательств увело бы нас далеко в сторону. Достаточно полное и доступное изложение можно найти в книге Ленга [(а) 3] или Херстейна [(а) 2]. Нам понадобятся следующие понятия и факты.

(1) Абстрактное определение *поля* F; под *расширением* K поля F понимается произвольное поле K, содержащее F в качестве подполя; расширение K называется *алгебраическим,* если любой элемент $\alpha \in K$ является корнем некоторого многочлена с коэффициентами в F: $a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_n\alpha^n = 0$, где $a_i \in F$. Например, множество чисел вида $a + b\sqrt{2}$ с $a, b \in \mathbb{Q}$ представляет собой алгебраическое расширение поля $\mathbb{Q}$.

(2) Пусть F — некоторое поле. Наименьшее целое положительное число n, для которого 1, будучи сложена сама с собой n раз, дает в результате 0, называется *характеристикой* поля F и обозначается через $\mathrm{char}\,(F)$. Если $1+1+\ldots+1$ всегда $\neq 0$, то по определению $\mathrm{char}\,(F) = 0$. (Логичнее было бы полагать $\mathrm{char}\,(F) = \infty$, однако принято считать характеристику поля в этом случае равной 0.) Поля $\mathbb{Q}$, $\mathbb{Q}_p$, $\mathbb{R}$ и $\mathbb{C}$ имеют характеристику 0, тогда как множество классов вычетов кольца $\mathbb{Z}$ по простому модулю p является полем характеристики p. (Вскоре нам встретятся другие примеры полей характеристики p.)

(3) Определение *векторного пространства* V над полем F; понятие *базиса* V над F; свойство *конечномерности* векторного пространства V; если V конечномерно, то его *размерность* равна числу элементов любого базиса.

(4) Любое расширение K поля F можно рассматривать как векторное пространство над F; если это пространство конечномерно, то соответствующее расширение будет алгебраическим; размерность этого векторного пространства называется *степенью* расширения и обозначается $[K : F]$. Если $\alpha \in K$ обладает тем свойством, что каждый элемент поля K представим в виде рационального выражения от α над F, то говорят, что расширение K получено *присоединением* элемента α к полю F, и записывают это в виде $K = F(\alpha)$. Пусть K' — конечное расширение поля K. Тогда легко установить конечность K' как расширения поля F и соотношение $[K' : F] = [K' : K] \cdot [K : F]$.

(5) Пусть α — элемент алгебраического расширения K поля F. Тогда существует *единственный* неприводимый многочлен со старшим коэффициентом 1 (*неприводимость* означает, что его нельзя разложить в произведение многочленов меньшей степени с коэффициентами в F), такой, что

$$\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0, \quad a_i \in F.$$

Этот многочлен называется *минимальным многочленом* элемента α, а число n — *степенью* данного элемента α. Расширение $F(\alpha)$ имеет степень n над F (действительно, в качестве базиса векторного пространства $F(\alpha)$ над F можно взять набор элементов $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$).

(6) Если поле F имеет характеристику 0 (например, $\mathbb{Q}$ или $\mathbb{Q}_p$) или является конечным (подробное изложение теории конечных полей следует за данным обзором), то можно доказать, что каждое конечное расширение K поля F имеет вид $K = F(\alpha)$ для некоторого $\alpha \in K$. Такой элемент α называется *примитивным*. (На самом деле это верно, если поле F *совершенное*, т. е. либо $\mathrm{char}\,(F) = 0$, либо $\mathrm{char}\,(F) = p$ и каждый элемент поля F обладает корнем степени p в F.) Знание примитивного элемента α расширения K упрощает изучение этого K, так как в этом случае каждый эле-

мент из K представим в виде многочлена от α степени $<n$, т. е. $K=\left\{\sum_{i=0}^{n-1} a_i\alpha^i \mid a_i\in F\right\}$.

(7) Рассмотрим некоторый неприводимый многочлен f степени n с коэффициентами в F. Можно построить расширение $K\supset F$ степени n, в котором f имеет корень $\alpha\in K$. Последовательно присоединяя корни всех многочленов с коэффициентами в F, мы получаем *алгебраическое замыкание* (обозначаемое $F^{\text{alg cl}}$ или $\bar{F}$) поля F, т. е., по определению, наименьшее алгебраически замкнутое поле, содержащее F (напомним, что поле K называется *алгебраически замкнутым*, если всякий многочлен с коэффициентами в K имеет корень в K). Всякое алгебраическое расширение поля F содержится в некотором его алгебраическом замыкании (т. е. его можно расширить до алгебраического замыкания поля F). Любые два алгебраических замыкания поля F изоморфны. Поэтому мы обычно пишем «алгебраическое замыкание» вместо «любое алгебраическое замыкание». Как правило, алгебраическое замыкание поля F является объединением бесконечного множества конечных алгебраических расширений поля F. Так, например, алгебраическое замыкание поля $\mathbb{Q}$ состоит из всех комплексных чисел, являющихся корнями многочленов с рациональными коэффициентами. Однако алгебраическое замыкание поля вещественных чисел $\mathbb{R}$ равно $\mathbb{C}=\mathbb{R}(\sqrt{-1})$, т. е. это конечное расширение степени 2 поля $\mathbb{R}$. Но этот пример — скорее исключение, чем правило.

(8) Пусть $K=F(\alpha)$, K' — другое расширение поля F, а $\sigma: K\to K'$ — изоморфное вложение поля K в K' (где σ — некоторый F-гомоморфизм, т. е. это отображение сохраняет все операции поля и $\sigma(a)=a$ для любого $a\in F$). Тогда элемент α и его образ $\sigma(\alpha)$ в K' обладают одним и тем же минимальным многочленом. Обратно, пусть $K=F(\alpha)$, K' — другое расширение поля F и $\alpha'\in K'$ — корень минимального многочлена для α. Тогда существует единственный изоморфизм σ поля K на подполе $F(\alpha')\subset K'$, для которого $\sigma(a)=a$ при любом $a\in F$ и $\sigma(\alpha)=\alpha'$.

(9) Все корни минимального многочлена над F элемента $\alpha\in\bar{F}$, лежащие в поле $\bar{F}=F^{\text{alg cl}}$, называются элементами, *сопряженными* с α. Существует взаимно однозначное соответствие между изоморфными вложениями $F(\alpha)$ в $\bar{F}$ и элементами α', сопряженными с α (см. предыдущий пункт (8)). Если $\operatorname{char}(F)=0$ или F — конечное поле (или F — совершенное поле), то каждый неприводимый многочлен с коэффициентами в F не имеет кратных корней. В этом случае число элементов, сопряженных с α, равно $[F(\alpha):F]$.

(10) Расширение $K=F(\alpha)$ поля F называется *расширением Галуа*, если все элементы, сопряженные с α, лежат в K. В этом случае все сопряженные любого элемента $x=\sum_{i=0}^{n-1} a_i\alpha^i\in K$ также лежат в K, поскольку такие сопряженные имеют вид $\sum_{i=0}^{n-1} a_i\alpha'^i$, где α' — элемент, сопряженный с α. Приведем несколько примеров расширений Галуа поля $\mathbb{Q}$: $\mathbb{Q}(\sqrt{2})$ (так как $\alpha=\sqrt{2}$ обладает единственным сопряженным, равным другому корню $\alpha'=-\sqrt{2}$ уравнения $x^2-2=0$, и $-\sqrt{2}\in\mathbb{Q}(\sqrt{2})$); $\mathbb{Q}(i)$; $\mathbb{Q}(\sqrt{d})$ для любого $d\in\mathbb{Q}$; $\mathbb{Q}(\zeta_m)$, где $\zeta_m=e^{2\pi i/m}$ — примитивный корень из 1 степени m, лежащий в $\mathbb{C}$ (так как все сопряженные с ζ_m — это другие примитивные корни степени m, а они имеют вид $\zeta^i{}_m$, где i взаимно просто с m). Поле $\mathbb{Q}(\sqrt[4]{2})$ дает пример расширения поля $\mathbb{Q}$, которое не есть расширение Галуа. Действительно, сопряженные с $\sqrt[4]{2}$ — это 4 корня уравнения $x^4-2=0$, а именно: $\pm\sqrt[4]{2}$, $\pm i\sqrt[4]{2}$. Но $i\sqrt[4]{2}\notin\mathbb{Q}(\sqrt[4]{2})$ (так как $\mathbb{Q}(\sqrt[4]{2})$ содержится в поле вещественных чисел).

(11) Пусть K — некоторое расширение Галуа поля F. Тогда образ каждого изоморфизма из пункта (8) совпадает с K, т. е. все эти изоморфизмы являются F-изоморфизмами поля K в себя, или *F-автоморфизмами* поля K. Эти автоморфизмы образуют группу, которая называется *группой Галуа поля K над F*. Каждый автоморфизм σ из этой группы определяет множество

элементов $x \in K$, для которых $\sigma(x) = x$. Оно называется *полем σ-инвариантов* (легко проверить, что это действительно подполе в K, содержащее F). Рассмотрим следующий пример: поле $K = \mathbb{Q}(\sqrt{2}+\sqrt{3})$ — расширение Галуа поля $\mathbb{Q}$ степени 4; возьмем автоморфизм σ, переводящий $\sqrt{2}+\sqrt{3}$ в $\sqrt{2}-\sqrt{3}$; тогда поле σ-инвариантов совпадает с $\mathbb{Q}(\sqrt{2})$. Нетрудно установить, что если K — расширение Галуа поля F, а $K' \neq K$ — некоторое промежуточное поле между K и F: $F \subset K' \subset K$, то существует нетривиальный автоморфизм поля K, оставляющий неподвижными все элементы из K'. Более того, существует взаимно однозначное соответствие между подгруппами S группы Галуа поля K над F и промежуточными полями $F \subset K' \subset K$, такое, что

$$S \leftrightarrow K'_S = \{x \in K \mid \sigma x = x \text{ для любого } \sigma \in S\}.$$

Однако в дальнейшем теория Галуа не понадобится нам во всей своей силе; мы будем опираться лишь на некоторые частные случаи сформулированных здесь результатов.

Перейдем теперь к изучению конечных полей. Простейший пример такого поля есть поле *классов вычетов целых чисел по простому модулю p*. Элементами этого поля являются классы эквивалентности целых чисел по отношению эквивалентности $x \sim y$, определяемому как $x \equiv y \pmod p$. Существует ровно p таких классов эквивалентности, а именно классы элементов $0, 1, 2, 3, \ldots, p-2, p-1$. На множестве этих классов легко ввести операции сложения и умножения, а затем проверить, что при этом получится поле (в частности, каждый ненулевой класс эквивалентности обратим по умножению; иначе говоря, если x — целое, не делящееся на p, то существует целое y, для которого $xy \equiv 1 \pmod p$). Это поле обозначается $\mathbb{F}_p$, а иногда $\mathbb{Z}/p\mathbb{Z}$ (*факторкольцо кольца целых чисел по идеалу целых чисел, делящихся на p*). С таким же успехом можно построить это поле, исходя из множества целых p-адических чисел $\mathbb{Z}_p$ и отношения эквивалентности $x \sim y$ ($x, y \in \mathbb{Z}_p$), определяемого как $x \equiv y \pmod p$ (т. е. эквивалентные x и y

имеют один и тот же первый знак в p-адическом разложении). Поэтому поле $\mathbb{F}_p$ можно записывать также в виде $\mathbb{Z}_p/p\mathbb{Z}_p$ (*факторкольцо кольца целых p-адических чисел по идеалу p-адических целых, делящихся на p*.) Факторкольцо $\mathbb{Z}_p/p\mathbb{Z}_p$ называется *полем вычетов* кольца $\mathbb{Z}_p$. Причина нашего интереса к общим конечным полям заключается в том, что ниже, при исследовании алгебраических расширений поля $\mathbb{Q}_p$, мы столкнемся с их полями вычетов, которые строятся аналогично полю вычетов для $\mathbb{Z}_p \subset \mathbb{Q}_p$, однако оказываются уже совсем не такими простыми, как $\mathbb{F}_p$. Они представляют собой алгебраические расширения поля $\mathbb{F}_p$. Поэтому сейчас нам необходимо получить некоторое представление о том, как же выглядят конечные поля вообще.

Пусть F — конечное поле. Тогда характеристика $F \neq 0$, так как все элементы $0, 1, 1+1, 1+1+1, \ldots$ из F не могут быть различными. Пусть $n = \operatorname{char}(F)$. Заметим, что число n должно быть простым. Действительно, если $n = n_0 n_1$ для n_0 и $n_1 < n$, то $n_0 \neq 0$ и после умножения на n_0^{-1} мы получаем противоречие: $n_1 = n_0^{-1} n = 0$. Обозначим это простое число $\operatorname{char}(F)$ через p.

Очевидно, любое поле F характеристики p содержит в качестве подполя описанное выше поле из p элементов (оно состоит из элементов вида $1+1+\ldots+1$). Это подполе называется *простым подполем* в F.

Заметим теперь, что для каждого поля F характеристики p определено отображение $x \longmapsto x^p$, сохраняющее операции сложения и умножения:

$$xy \longmapsto (xy)^p = x^p y^p,$$

$$x+y \longmapsto (x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i} = x^p + y^p,$$

потому что целое число $\binom{p}{i} = p!/i!\,(p-i)!$ делится на p при $1 \leqslant i \leqslant p-1$, а поэтому соответствующий элемент в F равен 0.

Теорема 9. *Пусть F — конечное поле, состоящее из q элементов, а $f = [F : \mathbb{F}_p]$ (размерность F как векторного пространства над своим простым подполем $\mathbb{F}_p$). Обозначим через K некоторое алгебраическое замыкание поля $\mathbb{F}_p$, содержащее F. Тогда $q = p^f$; F — единственное под-*

поле в K, состоящее из q элементов; при этом F есть множество всех элементов из K, удовлетворяющих уравнению $x^q - x = 0$. Обратно, для каждой степени $q = p^f$ простого p корни уравнения $x^q - x = 0$ задают подполе из q элементов в K.

Доказательство. Так как F является f-мерным векторным пространством над $\mathbb{F}_p$, число элементов этого пространства равно числу всевозможных выборов значений для f компонент вектора (т. е. *координат* в некотором базисе, состоящем из f элементов) в $\mathbb{F}_p$, а поэтому равно p^f. Далее, каждое поле F из q элементов содержит $q-1$ ненулевых элементов. Эти ненулевые элементы из F образуют мультипликативную группу порядка $q-1$. Степени любого элемента $x \neq 0$ составляют подгруппу этой группы. Порядок ее равен показателю наименьшей степени x, равной 1 (этот показатель называется также *порядком* элемента x). Легко доказать, что порядок любой подгруппы конечной группы делит порядок всей группы. Следовательно, порядок x делит $q-1$, откуда $x^{q-1} = 1$ для любого ненулевого x из F. Поэтому $x^q - x = 0$ для любого x (включая 0) из F. Последнее справедливо для *каждого* подполя из q элементов в K. Кроме того, всякий многочлен степени q имеет в любом поле не более чем q различных корней. Из этого следует, что каждое поле из q элементов в K должно состоять из корней многочлена $x^q - x$, а такое множество единственно.

Обратно, пусть $q = p^f$. Тогда множество элементов поля K, для которых $x^q = x$, замкнуто относительно сложения и умножения (это доказывается так же, как и утверждение, предшествующее формулировке теоремы). Итак, это подполе поля K. Многочлен $x^q - x$ не имеет кратных корней. Действительно, в противном случае из упр. 10 ниже следовало бы, что кратный корень является также корнем формальной производной этого многочлена $qx^{q-1} - 1 = -1$ (так как $q = 0$ в K). Но многочлен -1 не имеет корней. □

Замечание. Поскольку любые два алгебраических замыкания поля $\mathbb{F}_p$ изоморфны, изоморфны также любые два поля, состоящие из $q = p^f$ элементов.

Обозначим через $\mathbb{F}_q$ единственное (с точностью до изоморфизма) поле из $q = p^f$ элементов.

Если F — некоторое поле, то через $F^\times$ обозначается группа его ненулевых элементов.

Предложение. *Группа $\mathbb{F}_q^\times$ является циклической группой порядка $q-1$.*

Доказательство. Пусть $o(x)$ обозначает порядок элемента x (наименьший показатель степени x, равной 1). Нам уже известно, что $o(x)$ делит $q-1$ при любом $x \in \mathbb{F}_q^\times$. Однако если d — делитель $q-1$, то уравнение $x^d = 1$ имеет не более чем d решений, потому что всякий полином степени d имеет в любом поле не более чем d корней. Следовательно, если $d = o(x)$, то d различных элементов $x, x^2, \ldots, x^{d-1}, x^d = 1$ удовлетворяют уравнению $x^d = 1$, и это все корни данного уравнения. Сколько из этих d элементов имеют порядок, равный *в точности* d? Ответ очевиден: число таких элементов равно количеству целых чисел из $\{1, 2, \ldots, d-1, d\}$, взаимно простых с d (т. е. не имеющих общих делителей с d, кроме 1). Это количество обозначается $\varphi(d)$. Итак, порядок d имеют не более чем $\varphi(d)$ элементов из $\mathbb{F}_q^\times$. Утверждается, что для любого d — делителя $q-1$ число элементов из $\mathbb{F}_q^\times$, имеющих порядок d, равно $\varphi(d)$. Этот факт будет выведен из следующей леммы.

Лемма. $\sum_{d \mid n} \varphi(d) = n$.

Доказательство леммы. Пусть $\mathbb{Z}/n\mathbb{Z}$ обозначает аддитивную группу $\{0, 1, \ldots, n-1\}$ целых чисел по модулю n. Каждому делителю d числа n соответствует ее подгруппа S_d, состоящая из элементов $\mathbb{Z}/n\mathbb{Z}$, кратных n/d. Очевидно, любая подгруппа в $\mathbb{Z}/n\mathbb{Z}$ получается таким способом.

Подгруппа S_d состоит из d элементов, $\varphi(d)$ из которых порождают ее (потому что множество элементов, кратных mn/d в $\mathbb{Z}/n\mathbb{Z}$, совпадает с множеством элементов, кратных n/d, тогда и только тогда, когда m и d взаимно просты). С другой стороны, каждое из чисел $0, 1, \ldots, n-1$ порождает одну из таких под-

групп S_d. Следовательно,

$$\{0, 1, \ldots, n-1\} = \bigcup_{d \mid n} \{\text{элементы, порождающие } S_d\}.$$

Множества этого объединения не пересекаются, поэтому $n = \sum_{d \mid n} \varphi(d)$. Лемма доказана.

Из нее немедленно вытекает предложение, ибо если число элементов порядка d для некоторого $d \mid n\,(=q-1)$ меньше $\varphi(d)$, то $n = \sum_{d \mid n}$ (число элементов порядка $d) < \sum_{d \mid n} \varphi(d) = n$. Следовательно, в частности, существует $\varphi(q-1)$ элементов порядка $q-1$. Так как $\varphi(q-1) \geqslant 1$ (например, 1 взаимно проста с $q-1$), то найдется элемент a порядка точно $q-1$. Тогда $\mathbb{F}_q^\times = \{a, a^2, \ldots, a^{q-1}\}$. □

Упражнения

1. Пусть F — поле, состоящее из $q = p^f$ элементов. Докажите, что F содержит (единственное) подполе из $q' = p^{f'}$ элементов тогда и только тогда, когда f' делит f.

2. Для $p = 2, 3, 5, 7, 11$ и 13 найдите некоторый элемент $a \in \{1, 2, \ldots, p-1\}$, порождающий $\mathbb{F}_p^\times$, т. е. такой, что $\mathbb{F}_p^\times = \{a, a^2, \ldots, a^{p-1}\}$. В каждом из этих случаев определите число всевозможных выборов таких a.

3. Пусть F — множество выражений вида $a+bj$, где $a, b \in \mathbb{F}_3 = \{0, 1, 2\}$. На этом множестве определим сложение покомпонентно, а умножение — по формуле $(a+bj)(c+dj) = (ac+2bd) + (ad+bc)j$. Покажите, что $F = \mathbb{F}_9$, а $1+j$ — образующая в $\mathbb{F}_9^\times$. Найдите все образующие для $\mathbb{F}_9^\times$.

4. Опишите явно $\mathbb{F}_4$ и $\mathbb{F}_8$ способом, аналогичным использованному в предыдущем упражнении для $\mathbb{F}_9$. Объясните, почему любой элемент из $\mathbb{F}_4^\times$ или $\mathbb{F}_8^\times$ является образующей.

5. Пусть $q = p^f$, а α — элемент, порождающий $\mathbb{F}_q^\times$. Обозначим через $P(X)$ минимальный многочлен элемента α над $\mathbb{F}_p$. Докажите, что $\deg P = f$.

6. Пусть $q = p^f$. Докажите, что все f автоморфизмов поля $\mathbb{F}_q$ над $\mathbb{F}_p$ исчерпываются автоморфизмами σ_i, $i = 0, 1, \ldots, f-1$, следующего вида: $\sigma_i(x) = x^{p^i}$ для $x \in \mathbb{F}_q$.

7. Пусть $\alpha \in \mathbb{F}_p^\times$, а $P(X) = X^p - X - \alpha$. Покажите, что если a — корень многочлена $P(X)$, то элементы $a+1$, $a+2$ и т. д. также являются его корнями. Кроме того, покажите, что поле, полученное присоединением a к $\mathbb{F}_p$, имеет степень p над $\mathbb{F}_p$, т. е. изоморфно $\mathbb{F}_{p^p}$.

8. Докажите, что $\mathbb{F}_q$ содержит квадратный корень из -1 тогда и только тогда, когда $q \not\equiv 3 \pmod 4$.

9. Пусть ξ — некоторое алгебраическое число степени n над $\mathbb{Q}_p$, т. е. ξ является корнем многочлена степени n с коэффициентами в $\mathbb{Q}_p$ и не является корнем никакого такого многочлена меньшей степени. Докажите существование целого числа N, для которого ξ не удовлетворяет ни одному из сравнений вида

$$a_{n-1}\xi^{n-1} + a_{n-2}\xi^{n-2} + \ldots + a_1\xi + a_0 \equiv 0 \pmod{p^N},$$

где a_i — целые рациональные числа, не все из которых делятся на p. (*Указание.* Предположите противное, а затем воспользуйтесь тем же подходом, что и в упр. 18 к § I.2 или в упр. 18 к § I.5.)

10. Пусть F — *произвольное* поле, а $f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$ — многочлен с коэффициентами в F, распадающийся на линейные множители над F, т. е. $f(X) = \prod_{i=1}^{n} (X - \alpha_i)$, где $\alpha_i \in F$. Покажите, что всякий кратный корень α_i этого многочлена является также корнем для $nX^{n-1} + a_{n-1}(n-1)X^{n-2} + a_{n-2} \times (n-2)X^{n-3} + \ldots + a_1$.

§ 2. ПРОДОЛЖЕНИЕ НОРМ

Метрическое пространство X называется (секвенциально) *компактным*, если каждая последовательность его элементов имеет сходящуюся подпоследовательность (см. начало § II.3). Например, $\mathbb{Z}_p$ — компактное метрическое пространство (см. упр. 18 к § I.5). Пространство X называется *локально компактным*, если каждая точка $x \in X$ обладает некоторой компактной окрестностью (т. е. компактным подмножеством в X, содержащим диск $\{y \mid d(x, y) < \varepsilon\}$ для некоторого $\varepsilon > 0$). Множество вещественных чисел $\mathbb{R}$ с обычной архимедовой метрикой, индуцированной абсолютной величиной, локально компактно, но не компактно. Другой пример

локально компактного метрического пространства дает поле $\mathbb{Q}_p$ с p-адической метрикой. В самом деле, для любой точки x окрестность $x+\mathbb{Z}_p \overline{\text{def}} \{y \mid |y-x|_p \leqslant 1\}$ компактна (ибо она изоморфна $\mathbb{Z}_p$ как метрическое пространство). Эти примеры можно включить в следующую более общую картину. Пусть X — метрическое пространство, обладающее структурой аддитивной группы, такой, что $d(x, y) = d(x-y, 0)$ для любых x, y (например, X — векторное пространство с метрикой, индуцированной нормой на X; определение см. ниже). Тогда X локально компактно всякий раз, когда 0 имеет компактную окрестность U. Действительно, для любой точки x окрестность $x+U \overline{\text{def}} \{y \mid y-x \in U\}$ (сдвиг U на x) компактна. Для $\mathbb{Q}_p$ в качестве компактной окрестности 0 можно взять $U=\mathbb{Z}_p$. Нетрудно установить (см. ниже упр. 6) полноту каждой такой локально компактной группы.

Пусть F — некоторое поле с неархимедовой нормой $\| \|$. До конца данного параграфа будем предполагать F локально компактным.

Пусть V — конечномерное векторное пространство над F. Норму на векторном пространстве V можно определить по аналогии с нормой в поле. А именно, отображение $\| \|_V$ из V в множество неотрицательных вещественных чисел называется *нормой* на V, если: (1) $\|x\|_V = 0$ тогда и только тогда, когда $x=0$; (2) $\|ax\|_V = \|a\| \|x\|_V$ для всех $x \in V$ и $a \in F$ (где $\|a\|$ есть норма в F); (3) $\|x+y\|_V \leqslant \|x\|_V + \|y\|_V$. Например, если K — конечное расширение поля F, то всякая норма на поле K, ограничение которой совпадает с $\| \|$ на F, есть норма на K, рассматриваемом как векторное пространство над F. Сразу же предупредим, что обратное, вообще говоря, не верно, так как свойство (2) нормы векторного пространства слабее соответствующего свойства нормы поля (см. ниже упр. 3 — 4).

Как и в случае полей, две нормы $\| \|_1$ и $\| \|_2$ на V считаются эквивалентными, если отвечающие им множества последовательностей Коши совпадают. Это свойство выполнено в том и только том случае, когда существуют две положительные константы c_1 и c_2, для которых $\|x\|_2 \leqslant c_1 \|x\|_1$ и $\|x\|_1 \leqslant c_2 \|x\|_2$ при любых $x \in V$ (см ниже упр. 1).

Теорема 10. *Пусть V — конечномерное векторное пространство над локально компактным полем F. Тогда все нормы на V эквивалентны.*

Доказательство. Пусть $\{v_1, \ldots, v_n\}$ — некоторый базис в V. Определим на V функцию $\| \|_{\sup}$ формулой

$$\|a_1 v_1 + \ldots + a_n v_n\|_{\sup} \overline{\text{def}} \max_{1 \leqslant i \leqslant n} (\|a_i\|).$$

Эта функция $\| \|_{\sup}$ является нормой (см. ниже упр. 2). Мы будем называть ее sup-нормой. Пусть теперь $\| \|_V$ — некоторая другая норма на V. Прежде всего для любого $x = a_1 v_1 + \ldots + a_n v_n$ выполнены неравенства

$$\|x\|_V \leqslant \|a_1\| \|v_1\|_V + \ldots + \|a_n\| \|v_n\|_V \leqslant$$
$$\leqslant n (\max \|a_i\|) \max \|v_i\|_V.$$

Поэтому $\| \|_V \leqslant c_1 \| \|_{\sup}$, где $c_1 = n \max\limits_{1 \leqslant i \leqslant n} (\|v_i\|_V)$. Таким образом, если мы найдем константу c_2, для которой будет выполнено братное неравенство, то тем самым установим эквивалентность любой нормы на V sup-норме. Пусть

$$U = \{x \in V \mid \|x\|_{\sup} = 1\}.$$

Тогда утверждается, что существует положительное ε, для которого $\|x\|_V \geqslant \varepsilon$ при любом $x \in U$. Предположим противное. В этом случае можно найти такую последовательность $\{x_i\}$ элементов U, что $\|x_i\|_V \to 0$. В силу компактности U относительно $\| \|_{\sup}$ (см. ниже упр. 2, 8) существует подпоследовательность $\{x_{i_j}\}$, сходящаяся относительно sup-нормы к некоторому $x \in U$. Но по доказанному выше неравенству

$$\|x\|_V \leqslant \|x - x_{i_j}\|_V + \|x_{i_j}\|_V \leqslant c_1 \|x - x_{i_j}\|_{\sup} + \|x_{i_j}\|_V$$

для любого j. Оба последних члена стремятся к 0 при $j \to \infty$, так как x_{i_j} стремится к x относительно $\| \|_{\sup}$, а $\|x_i\|_V \to 0$. Следовательно, $\|x\|_V = 0$, откуда $x = 0 \notin U$ — противоречие.

Используя это утверждение, теперь нетрудно доказать второе неравенство, а с ним и теорему. Идея рассуждения такова. Как было установлено, норма $\|\ \|_V$ на единичной сфере U относительно $\|\ \|_{\sup}$ принимает значения $\geqslant \varepsilon > 0$. Следовательно, $\|\ \|_{\sup} \leqslant c_2 \|\ \|_V$ на U, где $c_2 = 1/\varepsilon$ (левая часть по определению равна 1 на U). С другой стороны, все векторы из V можно получить, умножая векторы, лежащие в U, на элементы поля F. Поэтому такое же неравенство справедливо на всем V.

Точнее, пусть $x = a_1 v_1 + \ldots + a_n v_n$ — произвольный ненулевой элемент из V. Выберем такое j, что $\|a_j\| = \max \|a_i\| = \|x\|_{\sup}$. Тогда, очевидно, $(x/a_j) \in U$ и $\|x/a_j\|_V \geqslant \varepsilon = 1/c_2$. Поэтому

$$\|x\|_{\sup} = \|a_j\| \leqslant c_2 \|x\|_V. \quad \square$$

Следствие. *Пусть $V = K$ — некоторое поле. Тогда существует не более одного продолжения нормы $\|\ \|$, заданной на F, до нормы $\|\ \|_K$ на K (т. е. такой, что $\|a\|_K = \|a\|$ для $a \in F$).*

Доказательство следствия. Любые две такие нормы $\|\ \|_1$ и $\|\ \|_2$ эквивалентны по теореме 10. Следовательно, $\|\ \|_2 \leqslant c_1 \|\ \|_1$. Рассмотрим $x \in K$, для которого $\|x\|_1 \neq \|x\|_2$, скажем $\|x\|_1 < \|x\|_2$. Тогда при достаточно большом N получается противоречие: $c_1 \|x^N\|_1 < \|x^N\|_2$. $\square$

Это следствие, однако, оставляет открытым вопрос о существовании хотя бы одного продолжения $\|\ \|$ с F на K.

Напомним теперь одно из основных понятий, относящихся к расширениям полей: понятие «нормы» элемента. Новое словоупотребление не следует путать с прежним, относившимся к метрическим пространствам. «Норма» в новом смысле будет всегда в кавычках, и для нее мы введем специальное обозначение $\mathbb{N}$.

Пусть $K = F(\alpha)$ — конечное расширение поля F, порожденное некоторым элементом α с минимальным многочленом

$$x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n, \quad a_i \in F,$$

Тогда «норма элемента α из K в F», обозначаемая через $\mathbb{N}_{K/F}(\alpha)$, определяется одним из трех эквивалентных способов.

(1) Если K рассматривать как векторное пространство над F, то умножение на α задает F-линейное отображение с матрицей A_α в некотором базисе. Полагаем $\mathbb{N}_{K/F}(\alpha) \overset{\text{def}}{=} \det(A_\alpha)$.

(2) $\mathbb{N}_{K/F}(\alpha) \overset{\text{def}}{=} (-1)^n a_n$.

(3) $\mathbb{N}_{K/F}(\alpha) \overset{\text{def}}{=} \prod_{i=1}^{n} \alpha_i$, где через α_i обозначены все элементы, сопряженные с $\alpha = \alpha_1$ над F.

Эквивалентность (2) $\Leftrightarrow$ (3) следует из соотношения $x^n + a_1 x^{n-1} + \ldots + a_n = \prod_{i=1}^{n} (x - \alpha_i)$. Для доказательства эквивалентности (1) $\Leftrightarrow$ (2) возьмем в K над F базис $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$. Тогда матрица оператора умножения на α примет вид

$$\begin{pmatrix} 0 & 0 & & & -a_n \\ 1 & 0 & 0 & & -a_{n-1} \\ & 1 & 0 & & \vdots \\ & & & \ddots & \vdots \\ & & & 0 & -a_2 \\ & & & 1 & -a_1 \end{pmatrix}$$

(поскольку $\alpha^n = -a_1\alpha^{n-1} - \ldots - a_{n-1}\alpha - a_n$). Из разложения определителя этой матрицы по первой строке видно, что он равен $(-1)^n a_n$.

Пусть $\beta \in K = F(\alpha)$. Тогда $\mathbb{N}_{K/F}(\beta)$ определяется одним из двух способов: (1) как определитель матрицы линейного оператора умножения на β в K или (эквивалентно) (2) как $(\mathbb{N}_{F(\beta)/F}(\beta))^{[K:F(\beta)]}$. Для доказательства эквивалентности выберем базис в $F(\beta)$ как векторном пространстве над F, а также в K как векторном пространстве над $F(\beta)$. Тогда в качестве базиса K над F можно взять все попарные произведения элементов первого и второго базисов. В этом базисе

(при подходящем порядке элементов) матрица умножения на β «распадается на блоки»

$$\begin{pmatrix} A_\beta & 0 & & \\ 0 & A_\beta & & \\ & & \ddots & \\ & & & A_\beta \end{pmatrix},$$

где A_β — матрица умножения на β в $F(\beta)$. Определитель этой матрицы равен $[K:F(\beta)]$-й степени ($[K:F(\beta)]$ — это число блоков) $\det A_\beta$, т. е. $[K:F(\beta)]$-й степени элемента $N_{F(\beta)/F}(\beta)$. Итак, два определения действительно эквивалентны.

Из первого определения $N_{K/F}(\alpha)$ для *любого* $\alpha \in K$ как определителя оператора умножения на α в K следует *мультипликативность* отображения $N_{K/F}$ из K в F, т. е. $N_{K/F}(\alpha\beta) = N_{K/F}(\alpha) N_{K/F}(\beta)$. (В самом деле, матрица умножения на $\alpha\beta$ равна произведению матриц умножения на α и на β, а определитель произведения матриц равен произведению определителей сомножителей.)

Теперь можно догадаться, каким должно быть выражение для продолженной нормы $|\ |_p$ алгебраического числа $\alpha \in \mathbb{Q}_p^{\text{alg cl}}$, если такая норма существует. Предположим, что α имеет степень n, т. е. минимальный многочлен этого элемента над $\mathbb{Q}_p$ имеет степень n. Пусть K — конечное *расширение Галуа* поля $\mathbb{Q}_p$, содержащее α (см. пункт (10) в § 1). В качестве K можно взять, например, поле, полученное присоединением α и всех его сопряженных к $\mathbb{Q}_p$ (как легко проверить, это конечное расширение Галуа над $\mathbb{Q}_p$). Предположим, что найдено некоторое продолжение $\|\ \|$ нормы $|\ |_p$ на K. Эта норма $\|\ \|$ на K *единственна* в силу следствия из теоремы 10. Пусть теперь α' — элемент, сопряженный с α, а σ — некоторый автоморфизм поля K, переводящий α в α' (см. пункты (8), (9) и (11) в § 1). Очевидно, отображение $\|\ \|' \colon K \to \mathbb{R}$, заданное соотношением $\|x\|' = \|\sigma(x)\|$, является также продолжением нормы $|\ |_p$ на K. Следовательно, $\|\ \|' = \|\ \|$, откуда $\|\alpha\| = \|\alpha\|' = \|\sigma(\alpha)\| = \|\alpha'\|$. Значит, *норма элемента* α *равна норме каждого сопряженного с ним элемента*. С другой стороны, норма

элемента $N_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)$, лежащего в $\mathbb{Q}_p$, равна

$$|N_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)|_p = \|N_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)\| = \left\| \prod_{\text{сопряженные } \alpha' \text{ с } \alpha} \alpha' \right\| = \prod \|\alpha'\| = \|\alpha\|^n.$$

Поэтому

$$\|\alpha\| = |N_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)|_p^{1/n}.$$

Итак, для того чтобы найти p-адическую норму числа α, следует посмотреть на его минимальный многочлен. Если он имеет степень n и постоянный член a_n, то p-адическая норма α равна корню степени n из $|a_n|_p$. (Конечно, мы еще не доказали, что это правило определяет функцию, обладающую всеми необходимыми свойствами нормы; это будет доказано ниже в теореме 11.)

Отметим следующее эквивалентное определение $\|\alpha\|$:

$$|N_{K/\mathbb{Q}_p}(\alpha)|_p^{1/[K:\mathbb{Q}_p]},$$

где K — произвольное конечное расширение, содержащее α. Действительно,

$$N_{K/\mathbb{Q}_p}(\alpha) = (N_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p})^{[K:\mathbb{Q}_p(\alpha)]}$$

и $$n = [\mathbb{Q}_p(\alpha):\mathbb{Q}_p] = \frac{[K:\mathbb{Q}_p]}{[K:\mathbb{Q}_p(\alpha)]}.$$

Докажем теперь, что указанное правило вычисления $\|\ \|$ действительно задает норму. Ниже мы будем писать $|\ |_p$ вместо $\|\ \|$, указывая тем самым, что $\|\ \|$ продолжает $|\ |_p$. Это не должно приводить к путанице. Следует предупредить читателя, что теорему 11 доказать нелегко. Доказательство, изложенное ниже, которое я узнал от Д. Каждана, гораздо эффективнее других известных мне доказательств. Однако и его следует внимательно прочесть и перечесть, пока читатель не продумает рассуждения со всей основательностью.

Теорема 11. *Пусть K — конечное расширение поля $\mathbb{Q}_p$. Тогда на K существует некоторая норма, продолжающая норму $|\ |_p$ с $\mathbb{Q}_p$.*

Доказательство. Пусть $n=[K:\mathbb{Q}_p]$. Сначала мы определим $|\ |_p$ на K, а затем докажем, что эта функция в самом деле является нормой на K, продолжающей норму $|\ |_p$ с $\mathbb{Q}_p$. Для произвольного $\alpha\in K$ положим

$$|\alpha|_p \overset{\text{def}}{=} |\mathrm{N}_{K/\mathbb{Q}_p}(\alpha)|_p^{1/n},$$

где справа стоит определенная ранее норма на $\mathbb{Q}_p$. Легко проверить, что: (1) новое значение $|\alpha|_p$ совпадает с определенным ранее $|\alpha|_p$ для всех $\alpha\in\mathbb{Q}_p$; (2) $|\alpha|_p$ мультипликативна и (3) $|\alpha|_p=0\Leftrightarrow\alpha=0$. Трудная часть — доказательство свойства $|\alpha+\beta|_p\leqslant \leqslant\max(|\alpha|_p,\ |\beta|_p)$.

Предположим, что $|\beta|_p=\max(|\alpha|_p,\ |\beta|_p)$. Тогда, положив $\gamma=\alpha/\beta$, мы видим, что достаточно доказать неравенство

$$|1+\gamma|_p\leqslant 1 \quad \text{для всех } \gamma \text{ с } |\gamma|_p\leqslant 1.$$

Допустим сначала, что γ — «примитивный элемент» поля, т. е. $K=\mathbb{Q}_p(\gamma)$. Возьмем в качестве базиса векторного пространства K над $\mathbb{Q}_p$ набор $\{1,\gamma,\gamma^2,\ldots,\gamma^{n-1}\}$. Пусть A — матрица умножения на γ. Тогда A^i — матрица умножения на γ^i. Кроме того, $|\gamma|_p=|\det A|_p^{1/n}$, а $|1+\gamma|_p=|\det(1+A)|_p^{1/n}$. Пусть $\|\ \|$ обозначает sup-норму на n^2-мерном $\mathbb{Q}_p$-векторном пространстве $n\times n$-матриц с элементами в $\mathbb{Q}_p$. Утверждается, что последовательность значений $\{\|A^i\|\}$ ограничена.

Предположим противное. Тогда существует такая последовательность индексов i_j, что $\|A^{i_j}\|=b_j>j$. Пусть β_j — «максимальный» элемент матрицы A^{i_j}, т. е. $|\beta_j|_p=\max|\beta|_p=\|A^{i_j}\|$, где максимум берется по всем элементам β матрицы A^{i_j}. Рассмотрим последовательность матриц

$$B_j \overset{\text{def}}{=} A^{i_j}/\beta_j.$$

Очевидно, $\|B_j\|=1$. Единичная сфера в sup-норме компактна (см. ниже упр. 2 и 8), поэтому можно найти подпоследовательность $\{B_{j_k}\}$, сходящуюся в этой норме

к некоторой матрице B. Так как $\det B_j=\det A^{ij}/\beta_j^n$, то

$$|\det B_j|_p<|\det A^{ij}|_p/j^n=|\gamma|_p^{nij}/j^n\leqslant 1/j^n.$$

Но $B_{j_k}\to B$, т. е. максимум $|\ |_p$ от элементов матрицы $B_{j_k}-B$ стремится к 0, поэтому $\det B_{j_k}$ стремится к $\det B$. Следовательно, $\det B=0$.

Таким образом, существует ненулевой элемент $l\in K$, для которого $B(l)=0$. Покажем, что из этого следует тождественное обращение в нуль матрицы B, что противоречит равенству $\|B\|=1$.

Достаточно установить соотношение $B(\gamma^i l)=0$ для любого i, так как $\{\gamma^i l\}_{i=0}^{n-1}$ — базис в K. Но

$$B(\gamma^i l)=\lim_{k\to\infty} B_{j_k}(\gamma^i l)=\lim_{k\to\infty}\gamma^i B_{j_k}(l)$$

(потому что B_{j_k} — матрица умножения на степень γ, деленная на элемент β_{j_k} из $\mathbb{Q}_p$). Последний предел равен

$$\gamma^i\lim_{k\to\infty}B_{j_k}(l)=\gamma^i B(l)=0.$$

Следовательно, $\{\|A^i\|\}$ ограничена некоторой константой C.

Отметим, что для любой $n\times n$-матрицы $A=\{a_{ij}\}$ выполнено неравенство $|\det A|_p\leqslant(\max\limits_{i,\,j}|a_{ij}|_p)^n=\|A\|^n$. В этом легко убедиться, если разложить определитель и воспользоваться аддитивными и мультипликативными свойствами неархимедовой нормы.

Теперь возьмем достаточно большое N и рассмотрим разложение

$$(1+A)^N=1+\binom{N}{1}A+\ldots+\binom{N}{N-1}A^{N-1}+A^N.$$

Тогда

$$|1+\gamma|_p^N=|\det(1+A)^N|_p^{1/n}\leqslant\|(1+A)^N\|\leqslant$$
$$\leqslant\max_{0\leqslant i\leqslant N}\|\tbinom{N}{i}A^i\|\leqslant\max_{0\leqslant i\leqslant N}\|A^i\|\leqslant C.$$

Следовательно, $|1+\gamma|_p\leqslant\sqrt[N]{C}$. Переходя к пределу при $N\to\infty$, мы получаем требуемое неравенство $|1+\gamma|_p\leqslant 1$.

(Отметим сходство этого доказательства с доказательством теоремы Островского в § I.2.)

Если γ — не примитивный элемент, то, заменяя K на $\mathbb{Q}_p(\gamma)$, мы получим $1 \geqslant |N_{\mathbb{Q}_p(\gamma)/\mathbb{Q}_p}(1+\gamma)|_p^{1/[\mathbb{Q}_p(\gamma):\mathbb{Q}_p]} = |N_{K/\mathbb{Q}_p}(1+\gamma)|_p^{1/n} = |1+\gamma|_p$. Это неравенство завершает доказательство теоремы 11. □

Пусть R — (коммутативное) *кольцо*, т. е. множество с двумя операциями $+$ и $\cdot$, удовлетворяющими всем требованиям, предъявляемым к полю[1]), кроме, возможно, существования мультипликативно обратных элементов. Иначе говоря, это аддитивная группа относительно $+$; выполнены ассоциативность, коммутативность и существует единица относительно $\cdot$; кроме того, имеет место дистрибутивность. Кольцо R называется *областью целостности*, если из $xy=0$ всегда следует, что $x=0$ или $y=0$. Примеры областей целостности — кольца $\mathbb{Z}$ и $\mathbb{Z}_p$.

Собственное подмножество I кольца R называется *идеалом*, если оно является подгруппой в R относительно сложения и для всех $x \in R$ и $a \in I$ справедливо включение $xa \in I$. В кольце $\mathbb{Z}$ множество всех чисел, кратных некоторому фиксированному целому числу, задает идеал. В $\mathbb{Z}_p$ для любого $r \leqslant 1$ множество $\{x \in \mathbb{Z}_p \mid |x|_p < r\}$ есть идеал. Если, например, $r = p^{-n}$, то это множество всех целых p-адических чисел, первые $n+1$ знаков которых в p-адическом разложении равны нулю.

Пусть I_1 и I_2 — два идеала из R. Тогда легко проверить, что множество

$$\{x \in R \mid x \text{ представимо в виде } x = x_1x_1' + \ldots + x_mx_m' \text{ с } x_i \in I_1 \text{ и } x_i' \in I_2\}$$

также является идеалом. Этот идеал обозначается через I_1I_2 и называется произведением двух данных идеалов. Идеал I называется *простым*, если из включения $x_1x_2 \in I$ следует, что $x_1 \in I$ или $x_2 \in I$[2]).

[1]) В частности, $1 \neq 0$. — *Прим. перев.*

[2]) Заметим, что в этой книге все идеалы предполагаются собственными. — *Прим. перев.*

Легко проверить, что кольцо $\mathbb{Z}_p$ имеет единственный простой идеал ($\neq \{0\}$) (см. ниже упр. 5), а именно:

$$p\mathbb{Z}_p \overset{\text{def}}{=} \{x \in \mathbb{Z}_p \mid |x|_p < 1\}.$$

Кроме того, все идеалы ($\neq \{0\}$) кольца $\mathbb{Z}_p$ имеют вид

$$p^n\mathbb{Z}_p \overset{\text{def}}{=} \{x \in \mathbb{Z}_p \mid |x|_p \leqslant p^{-n}\}.$$

Пусть I — некоторый идеал кольца R. Тогда легко установить, что аддитивные классы смежности $x+I$ образуют кольцо. Это кольцо обозначается R/I и называется факторкольцом кольца R по идеалу I. (Другой способ описать это кольцо заключается в рассмотрении классов эквивалентности элементов из R по такому отношению: $x \sim y$, если $x-y \in I$.) Например, если $R=\mathbb{Z}$ (или $R=\mathbb{Z}_p$), то, как было установлено выше, кольцо R/pR совпадает с полем $\mathbb{F}_p$ из p элементов.

Идеал M из R называется *максимальным*, если не существует такого идеала I, что $M \subset I \subset R$ (оба включения строгие). Оставим в качестве легкого упражнения проверку следующих фактов.

(1) Идеал P прост тогда и только тогда, когда R/P — область целостности.

(2) Идеал M максимален тогда и только тогда, когда R/M — поле.

Предположим теперь, что K — некоторое конечное расширение поля $\mathbb{Q}_p$. (Или, более общо, пусть K — алгебраическое расширение поля частных F некоторой области целостности R, например: $F=\mathbb{Q}$ — поле частных для $R=\mathbb{Z}$, $F=\mathbb{Q}_p$ — поле частных для $R=\mathbb{Z}_p$ и т. д.) Пусть A — множество всех элементов $x \in K$, удовлетворяющих уравнению вида $x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n = 0$ с $a_i \in \mathbb{Z}_p$. (Конечно, каждый $x \in K$ удовлетворяет такому уравнению с коэффициентами a_i из $\mathbb{Q}_p$, но они не обязаны лежать в $\mathbb{Z}_p$.) Множество A называется *целым замыканием кольца $\mathbb{Z}_p$ в K*.

Нетрудно показать, что минимальный многочлен любого элемента $x \in A$ имеет указанный вид. Кроме того, целое замыкание всегда является кольцом. (Общее доказательство см. у Ленга [(a) 3], стр. 268 — 275.

Случай, который нам необходим в дальнейшем, — целое замыкание $\mathbb{Z}_p$ в K — рассмотрен в следующем предложении.)

Предложение. *Пусть K — конечное расширение степени n поля $\mathbb{Q}_p$ и*

$$A=\{x\in K \mid |x|_p\leqslant 1\},\quad M=\{x\in K \mid |x|_p<1\}.$$

Тогда A — кольцо, совпадающее с целым замыканием кольца $\mathbb{Z}_p$ в K, M — единственный максимальный идеал этого кольца, а A/M — конечное расширение поля $\mathbb{F}_p$ степени, не превосходящей n.

Доказательство. Используя мультипликативное и аддитивное свойства неархимедовой нормы, легко проверить, что A — кольцо, а M — его идеал. Пусть теперь $\alpha\in K$ — некоторый элемент степени m над $\mathbb{Q}_p$. Предположим, что α цел над $\mathbb{Z}_p$: $\alpha^m+a_1\alpha^{m-1}+\ldots+a_m=0$, $a_i\in\mathbb{Z}_p$. Предположив, что $|\alpha|_p>1$, мы придем к противоречию:

$$|\alpha|_p^m=|\alpha^m|_p=|a_1\alpha^{m-1}+\ldots+a_m|_p\leqslant \max_{1\leqslant i\leqslant m}|a_i\alpha^{m-i}|_p\leqslant$$
$$\leqslant \max_{1\leqslant i\leqslant m}|\alpha^{m-i}|_p=|\alpha|_p^{m-1}.$$

Обратно, пусть $|\alpha|_p\leqslant 1$. Тогда для всех сопряженных с $\alpha=\alpha_1$ над $\mathbb{Q}_p$ также $|\alpha_i|_p=\prod_{j=1}^{m}|\alpha_j|_p^{1/m}=|\alpha|_p\leqslant 1$. Так как все коэффициенты минимального многочлена для α равны суммам произведений α_i (*симметрическим многочленам* от α_i), для этих коэффициентов также $|\ |_p\leqslant 1$. Следовательно, они должны лежать в $\mathbb{Z}_p$, поскольку они лежат в $\mathbb{Q}_p$.

Докажем теперь, что M содержит каждый идеал из A. Предположим, что $\alpha\in A$ и $\alpha\notin M$. Тогда $|\alpha|_p=1$, откуда $|1/\alpha|_p=1$ и $1/\alpha\in A$. Поэтому любой идеал, содержащий α, должен содержать $(1/\alpha)\cdot\alpha=1$, что невозможно.

Отметим, что $M\cap\mathbb{Z}_p=p\mathbb{Z}_p$ по определению M.

Рассмотрим поле A/M. Напомним, что элементы этого поля суть классы смежности $a+M$. Заметим, что

если a и b окажутся в $\mathbb{Z}_p$, то класс $a+M$ совпадет с $b+M$ в том и только том случае, когда $a-b\in M\cap\mathbb{Z}_p=p\mathbb{Z}_p$. Отсюда получается естественное вложение $\mathbb{Z}_p/p\mathbb{Z}_p$ в A/M, задаваемое отображением (класс $a+p\mathbb{Z}_p)\longmapsto$ (класс $a+M$) для $a\in\mathbb{Z}_p$. Так как $\mathbb{Z}_p/p\mathbb{Z}_p$ есть поле $\mathbb{F}_p$, состоящее из p элементов, то A/M — расширение этого поля $\mathbb{F}_p$.

Утверждается, что A/M имеет конечную степень над $\mathbb{F}_p$. Точнее, установим неравенство $[A/M:\mathbb{F}_p]\leqslant[K:\mathbb{Q}_p]$. Для этого покажем, что любая система из $n+1$ элементов $\bar a_1,\bar a_2,\ldots,\bar a_{n+1}\in A/M$ линейно зависима над $\mathbb{F}_p$, где $n=[K:\mathbb{Q}_p]$. Для $i=1,2,\ldots,n+1$ выберем элемент a_i в A, который переходит в класс $\bar a_i$ при отображении $A\to A/M$ (т. е. a_i — некоторый элемент класса смежности $\bar a_i$, или, другими словами, $\bar a_i=a_i+M$). Так как $[K:\mathbb{Q}_p]=n$, то $a_1,a_2,\ldots,a_{n+1}$ линейно зависимы над $\mathbb{Q}_p$:

$$a_1b_1+a_2b_2+\ldots+a_{n+1}b_{n+1}=0,\quad b_i\in\mathbb{Q}_p.$$

После умножения на подходящую степень p можно предполагать, что все $b_i\in\mathbb{Z}_p$ и по крайней мере одно b_i не лежит в $p\mathbb{Z}_p$. После факторизации это выражение превращается в равенство

$$\bar a_1\bar b_1+\bar a_2\bar b_2+\ldots+\bar a_{n+1}\bar b_{n+1}=0$$

в A/M, где $\bar b_i$ — образ b_i в $\mathbb{Z}_p/p\mathbb{Z}_p$ (т. е. $\bar b_i$ определяется первым знаком p-адического разложения b_i). Поскольку по крайней мере одно b_i не принадлежит $p\mathbb{Z}_p$, то одно из $\bar b_i$ не равно 0. Поэтому, как и утверждалось, $\bar a_1,\bar a_2,\ldots,\bar a_{n+1}$ линейно зависимы. □

Поле A/M называется *полем вычетов* для K. Это расширение поля $\mathbb{F}_p$ некоторой конечной степени f. Кольцо A называется *кольцом нормирования*, соответствующим $|\ |_p$, в K.

Упражнения

1. Докажите, что две нормы $\|\ \|_1$ и $\|\ \|_2$ на конечномерном векторном пространстве эквивалентны в том и только том случае, когда существуют такие константы $c_1>0$ и $c_2>0$, что при всех $x\in V$

$$\|x\|_2\leqslant c_1\|x\|_1\quad\text{и}\quad\|x\|_1\leqslant c_2\|x\|_2.$$

2. Пусть F — поле с нормой $\| \|$, а V — конечномерное векторное пространство над F с базисом $\{v_1, \ldots, v_n\}$. Покажите, что функция $\|a_1v_1+\ldots+a_nv_n\|_{\sup} \underset{\text{def}}{=} \max_{1\leqslant i\leqslant n} (\|a_i\|)$ является нормой на V. Докажите, что из локальной компактности F следует локальная компактность V.

3. Пусть $V=\mathbb{Q}_p(\sqrt{p})$, $v_1=1$, $v_2=\sqrt{p}$. Докажите, что sup-норма не будет нормой на *поле* $\mathbb{Q}_p(\sqrt{p})$.

4. Пусть $V=K$ — некоторое поле. Может ли вообще sup-норма быть нормой на этом поле (хоть для какого-нибудь базиса $\{v_1, \ldots, v_n\}$) при $n=\dim K>1$? Для каких конечных расширений K поля $\mathbb{Q}_p$ sup-норма никогда не является нормой на этом поле?

5. Докажите, что $\mathbb{Z}_p$ имеет единственный максимальный идеал $p\mathbb{Z}_p$ и что все идеалы ($\neq\{0\}$) из $\mathbb{Z}_p$ имеют вид $p^n\mathbb{Z}_p$, $n\in\{1, 2, 3, \ldots\}$.

6. Докажите, что всякое локально компактное векторное пространство V с нормой $\| \|_p$ полно.

7. Докажите, что векторное пространство с нормой $\| \|_V$ локально компактно тогда и только тогда, когда компактен шар $\{x \mid \|x\|_V\leqslant 1\}$.

8. Докажите компактность сферы $\{x \mid \|x\|_V=1\}$ для локально компактного векторного пространства с нормой $\| \|_V$.

§ 3. АЛГЕБРАИЧЕСКОЕ ЗАМЫКАНИЕ ПОЛЯ $\mathbb{Q}_p$

Сопоставляя две теоремы из § 2, мы видим, что $|\ |_p$ имеет единственное продолжение (которое также обозначается через $|\ |_p$) на любое конечное расширение поля $\mathbb{Q}_p$. Поскольку алгебраическое замыкание $\overline{\mathbb{Q}}_p$ поля $\mathbb{Q}_p$ является объединением таких расширений, норма $|\ |_p$ однозначно продолжается на $\overline{\mathbb{Q}}_p$. Точнее, если $\alpha\in\overline{\mathbb{Q}}_p$ имеет минимальный многочлен $x^n+a_1x^{n-1}+\ldots+a_n$, то $|\alpha|_p=|a_n|_p^{1/n}$.

Пусть K — расширение степени n поля $\mathbb{Q}_p$. Для $\alpha\in K$ положим

$$\operatorname{ord}_p\alpha \underset{\text{def}}{=} -\log_p|\alpha|_p=-\log_p|\mathrm{N}_{K/\mathbb{Q}_p}(\alpha)|_p^{1/n}=$$
$$=-\frac{1}{n}\log_p|\mathrm{N}_{K/\mathbb{Q}_p}(\alpha)|_p.$$

При $\alpha\in\mathbb{Q}_p$ значение $\operatorname{ord}_p\alpha$ совпадает с определенным ранее. Кроме того, очевидно свойство $\operatorname{ord}_p\alpha\beta=\operatorname{ord}_p\alpha+\operatorname{ord}_p\beta$. Образ K при отображении ord_p попадает в множество $(1/n)\mathbb{Z}\underset{\text{def}}{=}\{x\in\mathbb{Q} \mid nx\in\mathbb{Z}\}$. Этот образ есть аддитивная подгруппа в $(1/n)\mathbb{Z}$. Поэтому он представим в виде $(1/e)\mathbb{Z}$ для некоторого целого положительного e, делящего n. Это целое число e называется *индексом ветвления* поля K над $\mathbb{Q}_p$. Если $e=1$, то говорят, что K — *неразветвленное* расширение поля $\mathbb{Q}_p$. Пусть $\pi\in K$ — элемент, для которого $\operatorname{ord}_p\pi=1/e$. Тогда, очевидно, любой $x\in K$ однозначно записывается в виде

$$\pi^m u, \quad \text{где } |u|_p=1, \quad \text{а } m\in\mathbb{Z} \quad (\text{при этом } m=e\cdot\operatorname{ord}_p x).$$

Можно доказать (см. ниже упр. 12), что $n=e\cdot f$, где $n=[K:\mathbb{Q}_p]$, e — индекс ветвления, а f — степень расширения поля вычетов A/M над $\mathbb{F}_p$. Во всяком случае, мы уже знаем, что $f\leqslant n$ и $e\leqslant n$. Если K — неразветвленное расширение, т. е. $e=1$, то в качестве π из предыдущего абзаца можно взять p, потому что $\operatorname{ord}_p p=1=1/e$. В другом крайнем случае, когда $e=n$, расширение K называется *вполне разветвленным*.

Предложение. *Пусть K — вполне разветвленное расширение, а $\pi\in K$ — такой элемент, что $\operatorname{ord}_p\pi=1/e$. Тогда π удовлетворяет некоторому уравнению Эйзенштейна (см. упр. 13 к § 1.5)*

$$x^e+a_{e-1}x^{e-1}+\ldots+a_0=0,$$

где $a_i\equiv 0 \pmod p$ при всех i, а $a_0\not\equiv 0 \pmod{p^2}$. Обратно, если α — корень некоторого такого уравнения Эйзенштейна над $\mathbb{Q}_p$, то $\mathbb{Q}_p(\alpha)$ — вполне разветвленное расширение степени e над $\mathbb{Q}_p$.

Доказательство. Прежде всего $|a_i|_p<1$, так как a_i — значения симметрических полиномов от элементов, сопряженных с π и имеющих норму $|\ |_p=p^{-1/e}$. Что касается a_0, то $|a_0|_p=|\pi|_p^e=1/p$.

Обратно, как видно из упр. 13 к § I.5, многочлен Эйзенштейна неприводим. Поэтому, присоединив его корень α, мы получим расширение степени e. Из равенства $\operatorname{ord}_p a_0=1$ следует, что $\operatorname{ord}_p\alpha=(1/e)\operatorname{ord}_p a_0=1/e$. Значит, $\mathbb{Q}_p(\alpha)$ вполне разветвлено над $\mathbb{Q}_p$. □

Более точное описание корней многочленов, присоединение которых задает вполне разветвленные расширения степени e, можно дать, если e не делится на p (в этом случае ветвление называется *ручным*; если $p \mid e$, ветвление называется *диким*). А именно, ручные вполне разветвленные расширения получаются присоединением решений уравнения $x^e - pu = 0$, где $u \in \mathbb{Z}_p^\times$, т. е. все такие расширения получаются добавлением корня степени e из произведения p на некоторую p-адическую единицу (см. ниже упр. 13 и 14).

Пусть теперь K — произвольное конечное расширение поля $\mathbb{Q}_p$. Следующее предложение утверждает, что если K не разветвлено, т. е. $e = 1$, то K имеет очень специальный вид: получается присоединением некоторого корня из 1. В случае же, когда K разветвлено, вначале следует построить его максимальное неразветвленное подполе, присоединяя некоторый подходящий корень из 1, а затем исходное расширение получается присоединением корня некоторого многочлена Эйзенштейна. *Предупреждение*: доказательство следующего предложения несколько утомительно, и читатель, который спешит перейти к менее сухим материям из следующей главы, может пропустить его (а также часть более трудных упражнений к § 4) при первом чтении.

Предложение. *Существует ровно одно неразветвленное расширение K_f^{unram} поля $\mathbb{Q}_p$ степени f, и оно может быть получено присоединением примитивного корня степени $p^f - 1$ из 1. Пусть K — некоторое расширение поля $\mathbb{Q}_p$ степени n с индексом ветвления e и степенью поля вычетов f (так что $n = ef$, как это будет доказано ниже в упр. 12). Тогда $K = K_f^{\mathrm{unram}}(\pi)$, где π — корень некоторого многочлена Эйзенштейна с коэффициентами в K_f^{unram}.*

Доказательство. Пусть $\bar{\alpha}$ — образующая мультипликативной группы $\mathbb{F}_{p^f}^\times$ (см. предложение в конце § 1), а $\bar{P}(x) = x^f + \bar{a}_1 x^{f-1} + \ldots + \bar{a}_f$ — ее минимальный многочлен над $\mathbb{F}_p$ (см. упр. 5 к § 1), где $\bar{a}_i \in \mathbb{F}_p$. Для каждого i выберем произвольный элемент $a_i \in \mathbb{Z}_p$ из класса $\bar{a}_i \pmod p$. Положим $P(x) = x^f + a_1 x^{f-1} + \ldots + a_f$. Очевидно, $P(x)$ неприводим над $\mathbb{Q}_p$, так как иначе его можно было бы записать в виде произведения двух многочленов с коэффициентами в $\mathbb{Z}_p$, что при редукции по модулю p дало бы разложение в произведение для $\bar{P}(x)$. Пусть $\alpha \in \mathbb{Q}_p^{\mathrm{alg\,cl}}$ — некоторый корень многочлена $P(x)$, $\tilde{K} = \mathbb{Q}_p(\alpha)$, $\tilde{A} = \{x \in K \mid |x|_p \leqslant 1\}$, $\tilde{M} = \{x \in K \mid |x|_p < 1\}$. Тогда $[\tilde{K} : \mathbb{Q}_p] = f$, в то время как класс смежности $\alpha + \tilde{M}$ является корнем неприводимого над $\mathbb{F}_p$ многочлена $\bar{P}(x)$ степени f. Следовательно, $[\tilde{A}/\tilde{M} : \mathbb{F}_p] = f$ и $\tilde{K}$ — неразветвленное расширение степени f. (Его единственность еще не доказана.)

Предположим теперь, что K — некоторое расширение из второй части данного предложения. Пусть $A = \{x \in K \mid |x|_p \leqslant 1\}$ — кольцо нормирования для $|\ |_p$ в K, а $M = \{x \in K \mid |x|_p < 1\}$ — максимальный идеал в A, так что $A/M = \mathbb{F}_{p^f}$. Рассмотрим $\bar{\alpha} \in \mathbb{F}_{p^f}$, образующую мультипликативной группы $\mathbb{F}_{p^f}^\times$. Пусть $\alpha_0 \in A$ — элемент, редуцирующийся в класс $\bar{\alpha} \pmod M$. И, наконец, пусть $\pi \in K$ — произвольный элемент с $\mathrm{ord}_p \pi = 1/e$. Таким образом, $M = \pi A$.

Утверждается, что существует элемент $\alpha \equiv \alpha_0 \pmod \pi$, для которого $\alpha^{p^f - 1} - 1 = 0$. Доказывается это аналогично лемме Гензеля. А именно, пусть $\alpha \equiv \alpha_0 + \alpha_1 \pi \pmod{\pi^2}$. Тогда выполнено сравнение $0 \equiv (\alpha_0 + \alpha_1 \pi)^{p^f - 1} - 1 \equiv \alpha_0^{p^f - 1} - 1 + (p^f - 1)\alpha_1 \pi \alpha_0^{p^f - 2} \equiv \alpha_0^{p^f - 1} - 1 - \alpha_1 \pi \alpha_0^{p^f - 2} \pmod{\pi^2}$. Но $\alpha_0^{p^f - 1} \equiv 1 \pmod \pi$, поэтому $\alpha_1 \equiv \left(\alpha_0^{p^f - 1} - 1\right)/\left(\pi \alpha_0^{p^f - 2}\right) \pmod \pi$ удовлетворяет нужному сравнению по модулю π^2. Продолжая этот процесс вычисления далее, как и в лемме Гензеля, мы находим $\alpha = \alpha_0 + \alpha_1 \pi + \alpha_2 \pi^2 + \ldots$, решение уравнения $\alpha^{p^f - 1} = 1$.

Отметим, что $\alpha, \alpha^2, \ldots, \alpha^{p^f - 1}$ — различные элементы, потому что различны их редукции $\bar{\alpha}, \bar{\alpha}^2, \ldots, \bar{\alpha}^{p^f - 1}$ по модулю M. Иначе говоря, α — примитивный корень степени $p^f - 1$ из 1. Кроме того, $[\mathbb{Q}_p(\alpha) : \mathbb{Q}_p] \geqslant f$, так как f — степень расширения поля вычетов. (Вскоре мы увидим, что $[\mathbb{Q}_p(\alpha) : \mathbb{Q}_p] = f$.)

Предыдущее рассуждение применимо, в частности, к полю $\tilde{K}$, построенному в первом абзаце доказательства. Следовательно, $\tilde{K} \supset \mathbb{Q}_p(\alpha)$, где α — примитивный корень степени $p^f - 1$ из 1. В силу неравенств $f = [\tilde{K} : \mathbb{Q}_p] \geqslant [\mathbb{Q}_p(\alpha) : \mathbb{Q}_p] \geqslant f$ получаем, что $\tilde{K} = \mathbb{Q}_p(\alpha)$. Значит, неразветвленное расширение степени f единственно. Обозначим его через K_f^{unram}.

Вернемся к нашему полю K степени $n = ef$ над $\mathbb{Q}_p$. Пусть $E(x)$ — минимальный многочлен элемента π над $\tilde{K} = K_f^{\mathrm{unram}}$. Обозначим через $\{\pi_i\}$ множество всех элементов, сопряженных с π над K_f^{unram}, так что $E(x) = \prod (x - \pi_i)$. Пусть d — степень, а c — постоянный член $E(x)$. Тогда $\mathrm{ord}_p c = d \,\mathrm{ord}_p \pi = d/e$. Но поскольку $ef = n = [K : \mathbb{Q}_p] = [K : K_f^{\mathrm{unram}}][K_f^{\mathrm{unram}} : \mathbb{Q}_p] = [K : K_f^{\mathrm{unram}}] \cdot f$, то $d \leqslant e$. С другой стороны, порядок $\mathrm{ord}_p c$ цел, так как $c \in K_f^{\mathrm{unram}}$. Отсюда мы заключаем, что $d = e$ и $\mathrm{ord}_p c = 1$. Таким образом, $E(x)$ — многочлен Эйзенштейна и $K = K_f^{\mathrm{unram}}(\pi)$. □

Следствие. *Пусть K — конечное расширение поля $\mathbb{Q}_p$ степени n с индексом ветвления e и полем вычетов степени f, а π — такой элемент, что $\mathrm{ord}_p \pi = 1/e$. Тогда каждый элемент $\alpha \in K$ однозначно представим в виде*

$$\sum_{i=m}^{\infty} a_i \pi^i,$$

где $m = e \,\mathrm{ord}_p \alpha$, а каждое a_i удовлетворяет уравнению $a_i^{p^f} = a_i$ (т. е. a_i — представители Тейхмюллера).

Доказательство этого следствия несложно, и мы оставляем его читателю.

Для всякого целого положительного m, не делящегося на p, можно найти степень p^f числа p, сравнимую с 1 по модулю m (действительно, пусть, например, f — порядок мультипликативной группы вычетов $(\mathbb{Z}/m\mathbb{Z})^\times$ по модулю m целых чисел, взаимно простых с m). Тогда $p^f - 1 = mm'$, и если к полю $\mathbb{Q}_p$ присоединить примитивный корень α из 1 степени $p^f - 1$, то в полученном поле элемент $\alpha^{m'}$ будет примитивным

корнем из 1 степени m. Из этого можно заключить, что *конечные неразветвленные расширения поля $\mathbb{Q}_p$ — это в точности все расширения, полученные присоединением корней из 1 степени, взаимно простой с p.*

Объединение всех конечных неразветвленных расширений поля $\mathbb{Q}_p$ обозначается $\mathbb{Q}_p^{\mathrm{unram}}$ и называется *максимальным неразветвленным расширением поля $\mathbb{Q}_p$*. Кольцо целых $\mathbb{Z}_p^{\mathrm{unram}}$ поля $\mathbb{Q}_p^{\mathrm{unram}}$ (также называемое *кольцом нормирования*) есть

$$\mathbb{Z}_p^{\mathrm{unram}} \underset{\text{def}}{=} \{x \in \mathbb{Q}_p^{\mathrm{unram}} \mid |x|_p \leqslant 1\}.$$

Оно имеет (единственный) максимальный идеал $M^{\mathrm{unram}} = p\mathbb{Z}_p^{\mathrm{unram}} = \{x \in \mathbb{Q}_p^{\mathrm{unram}} \mid |x|_p < 1\} = \{x \in \mathbb{Q}_p^{\mathrm{unram}} \mid |x|_p \leqslant 1/p\}$. Очевидно, поле вычетов $\mathbb{Z}_p^{\mathrm{unram}}/p\mathbb{Z}_p^{\mathrm{unram}}$ есть алгебраическое замыкание $\bar{\mathbb{F}}_p$ поля $\mathbb{F}_p$. Каждый $\bar{x} \in \bar{\mathbb{F}}_p$ обладает единственным *представителем Тейхмюллера* $x \in \mathbb{Z}_p^{\mathrm{unram}}$, который является корнем из 1 с образом $\bar{x}$ в $\mathbb{Z}_p^{\mathrm{unram}}/p\mathbb{Z}_p^{\mathrm{unram}}$. По этой причине $\mathbb{Z}_p^{\mathrm{unram}}$ часто называют «поднятием $\bar{\mathbb{F}}_p$ в характеристику нуль» (а также *кольцом векторов Витта поля $\bar{\mathbb{F}}_p$*).

Поле $\mathbb{Q}_p^{\mathrm{unram}}$, гораздо меньшее, чем $\mathbb{Q}_p^{\mathrm{algcl}}$, во многих ситуациях может использоваться вместо $\mathbb{Q}_p^{\mathrm{algcl}}$.

«Противоположный» к неразветвленным расширениям класс образуют вполне разветвленные расширения. Такое расширение можно построить, например, присоединением примитивного корня из 1 степени p^r; при этом получается вполне разветвленное расширение степени $n = e = p^{r-1}(p-1)$ (см. ниже упр. 7). Однако, к сожалению, далеко не все вполне разветвленные расширения задаются присоединением корня из 1. Например, присоединяя корень многочлена $x^m - p$, мы, очевидно, получаем вполне разветвленное расширение K степени m, и если бы K содержалось в поле, заданном присоединением примитивного корня из 1 степени p^r, то число m должно было бы делить $p^{r-1}(p-1)$, что невозможно, скажем, при $m > p$ и $p \nmid m$. Почти все, что мы можем сказать о вполне разветвленных расши-

рениях, содержится в первом предложении данного параграфа и в упр. 14 ниже.

Повторим: расширение K поля $\mathbb{Q}_p$ степени n с индексом ветвления e и степенью поля вычетов f задается присоединением примитивного корня из 1 степени p^f-1 и последующим присоединением к полученному полю K_f^{unram} корня некоторого многочлена Эйзенштейна с коэффициентами в K_f^{unram}.

Закончим этот параграф двумя полезными предложениями.

Предложение (лемма Краснера). *Пусть* $a,\ b\in\bar{\mathbb{Q}}_p\left(=\mathbb{Q}_p^{\mathrm{algcl}}\right)$. *Предположим, что элемент* b *расположен к* a *ближе, чем любой из сопряженных* $a_i\ (a_i\neq a)$ *для этого* a, *т. е.*

$$|b-a|_p<|a_i-a|_p.$$

Тогда $\mathbb{Q}_p(a)\subset\mathbb{Q}_p(b)$.

Доказательство. Пусть $K=\mathbb{Q}_p(b)$. Предположим, что $a\notin K$. Тогда имеется $[K(a):K]>1$ элементов, сопряженных с a над K. Следовательно, существует по крайней мере одно $a_i\notin K$, $a_i\neq a$, а также изоморфизм σ поля $\mathbb{Q}_p(a)$ в $\bar{\mathbb{Q}}_p(a_i)$, оставляющий на месте все элементы K и переводящий a в a_i. Мы уже знаем, что $|\sigma x|_p=|x|_p$ для любого $x\in K(a)$ в силу единственности продолжения нормы. В частности, $|b-a_i|_p=|\sigma b-\sigma a|_p=|b-a|_p$, откуда следует неравенство

$$|a_i-a|_p\leqslant\max(|a_i-b|_p,\ |b-a|_p)=|b-a|_p<|a_i-a|_p,$$

противоречащее предположению. □

Отметим, что точно таким же методом лемму Краснера можно доказать в более общей формулировке: если $a,\ b\in\bar{\mathbb{Q}}_p$, K — конечное расширение поля $\mathbb{Q}_p$ и $|b-a|_p<|a_i-a|_p$ для всех a_i, сопряженных с a над $K\ (a_i\neq a)$, то $K(a)\subset K(b)$.

Рассмотрим теперь произвольное поле K с нормой $\|\ \|$. Пусть $f,\ g\in K[X]$, т. е. $f=\sum a_iX^i$ и $g=\sum b_iX^i$ — два многочлена с коэффициентами в K. Определим расстояние $\|f-g\|$ от f до g как

$$\|f-g\|\overset{\mathrm{def}}{=}\max_i\|a_i-b_i\|.$$

Предложение. *Пусть* K — *конечное расширение поля* $\mathbb{Q}_p$, $f(X)\in K[X]$ — *многочлен степени* n,

$$f(X)=a_nX^n+a_{n-1}X^{n-1}+\ldots+a_1X+a_0.$$

Предположим, что все корни f *в* $\bar{\mathbb{Q}}_p$ *различны. Тогда для любого (достаточно малого)* $\varepsilon>0$ *существует такое* δ, *что если многочлен* $g=\sum_{i=0}^{n}b_iX^i\in K[X]$ *имеет степень* n *и* $|f-g|_p<\delta$, *то для каждого корня* α_i *многочлена* $f(X)$ *существует в точности один корень* β_i *многочлена* $g(X)$, *для которого* $|\alpha_i-\beta_i|_p<\varepsilon$.

Доказательство. Если β — корень $g(X)$, то

$$|f(\beta)|_p=|f(\beta)-g(\beta)|_p=\left|\sum_{i=0}^{n}(a_i-b_i)\beta^i\right|_p\leqslant$$

$$\leqslant\max_i\left(|a_i-b_i|_p|\beta|_p^i\right)\leqslant|f-g|_p\max\left(1,|\beta|_p^n\right)<\delta C_1^n$$

для некоторой константы C_1 (см. ниже упр. 3).

Пусть $C_2=\min_{1\leqslant i<j\leqslant n}|\alpha_i-\alpha_j|_p$. Очевидно, $C_2\neq0$, так как все α_i различны. Тогда неравенство $|\beta-\alpha_i|_p<C_2$ имеет место не более чем для одного α_i (так как если бы оно выполнялось для другого $\alpha_j\neq\alpha_i$, то мы имели бы $|\alpha_i-\alpha_j|_p\leqslant\max(|\alpha_i-\beta|_p,\ |\beta-\alpha_j|_p)<C_2$). Поскольку

$$C_1^n\delta>|f(\beta)|_p=\left|a_n\prod(\beta-\alpha_i)\right|_p=|a_n|_p\prod|\beta-\alpha_i|_p$$

$\left(\text{так как } f(X)=a_n\prod(X-\alpha_i)\right)$, то при достаточно малом δ такое α_i, для которого $|\beta-\alpha_i|_p<C_2$, существует. Более того, для этого α_i

$$|\beta-\alpha_i|_p<\frac{C_1^n\delta}{|a_n|_p\prod_{j\neq i}|\beta-\alpha_j|_p}\leqslant\frac{C_1^n\delta}{|a_n|_p\cdot C_2^{n-1}},$$

а последнюю величину можно сделать $<\varepsilon$ при подходящем выборе δ. □

§ 4. ПОЛЕ Ω

До сих пор мы имели дело исключительно с алгебраическими расширениями поля $\mathbb{Q}_p$. Но, как отмечалось выше, для конструкции p-адического аналога поля комплексных чисел этого недостаточно.

Теорема 12. *Поле $\overline{\mathbb{Q}}_p$ не полно.*

Доказательство. Нужно построить пример последовательности Коши $\{a_i\}$ в $\overline{\mathbb{Q}}_p$, которая не сходится ни к какому $a \in \overline{\mathbb{Q}}_p$.

Пусть b_i — примитивный корень из 1 степени $p^{2^i}-1$ в $\overline{\mathbb{Q}}_p$, т. е. $b_i^{p^{2^i}-1}=1$ и $b_i^m \neq 1$ для $0<m<p^{2^i}-1$. Заметим, что $b_i^{p^{2^{i'}}-1}=1$, если $i'>i$, так как $2^i \mid 2^{i'}$ влечет за собой $(p^{2^i}-1)\mid(p^{2^{i'}}-1)$. (На самом деле 2^i можно заменить любой возрастающей последовательностью натуральных чисел, i-й член которой делит $(i+1)$-й, например: 3^i, $i!$ и т. д.) Таким образом, b_i есть степень $b_{i'}$ при $i'>i$. Пусть

$$a_i=\sum_{j=0}^{i} b_j p^{N_j},$$

где $0=N_0<N_1<N_2<\ldots$ — возрастающая последовательность целых положительных чисел, которая будет выбрана позже. Отметим, что b_j при $j=0, 1, \ldots, i$ являются знаками p-адического разложения числа a_i в неразветвленном расширении $\mathbb{Q}_p(b_i)$, так как b_j — представители Тейхмюллера. Последовательность $\{a_i\}$, очевидно, будет последовательностью Коши.

Выберем теперь по индукции подходящие N_j для $j>0$. Предположим, что N_j уже определены для $j\leqslant i$; тогда определено также $a_i=\sum_{j=0}^{i} b_j p^{N_j}$. Пусть $K=\mathbb{Q}_p(b_i)$. В § 3 было доказано, что K есть неразветвленное расширение Галуа степени 2^i. Отметим прежде всего совпадение $\mathbb{Q}_p(a_i)$ с K. В противном случае существовал бы нетривиальный автоморфизм σ поля K, оставляющий a_i на месте (см. пункт (11) § 1). Но $\sigma(a_i)$ имеет

p-адическое разложение $\sum_{j=0}^{i} \sigma(b_j)\, p^{N_j}$ и $\sigma(b_i)\neq b_i$. Поэтому $\sigma(a_i)\neq a_i$, ибо различны их p-адические разложения.

Из упр. 9 к § 1 следует существование такого $N_{i+1}>N_i$, что при $n<2^i$ и $\alpha_j \in \mathbb{Z}_p$, не делящихся одновременно на p, a_i не удовлетворяет ни одному из сравнений

$$\alpha_n a_i^n+\alpha_{n-1}a_i^{n-1}+\ldots+\alpha_1 a_i+\alpha_0 \equiv 0 \pmod{p^{N_{i+1}}}.$$

Итак, мы построили требуемую последовательность $\{a_i\}$.

Действительно, предположим, что $a \in \overline{\mathbb{Q}}_p$ является пределом этой последовательности. Тогда a удовлетворяет уравнению

$$\alpha_n a^n+\alpha_{n-1}a^{n-1}+\ldots+\alpha_1 a+\alpha_0=0,$$

причем можно считать, что $\alpha_i \in \mathbb{Z}_p$ и не делятся одновременно на p. Выберем i, для которого $2^i>n$. Так как $a \equiv a_i \pmod{p^{N_{i+1}}}$, это приводит к противоречию:

$$\alpha_n a_i^n+\alpha_{n-1}a_i^{n-1}+\ldots+\alpha_1 a_i+\alpha_0 \equiv 0 \pmod{p^{N_{i+1}}}.$$

Теорема доказана. □

Заметим, что мы установили неполноту, используя последовательность из $\mathbb{Q}_p^{\mathrm{unram}}$, а не из всего замыкания $\overline{\mathbb{Q}}_p=\mathbb{Q}_p^{\mathrm{alg\,cl}}$.

Перейдем теперь к «залатыванию дыр» и определим новое поле Ω как *пополнение* поля $\overline{\mathbb{Q}}_p$. Строго говоря, следует рассмотреть классы эквивалентности последовательностей Коши в $\overline{\mathbb{Q}}_p$, а затем определить все необходимые структуры на полученном множестве, поступая при этом точно так же, как и при конструкции $\mathbb{Q}_p$ по $\mathbb{Q}$ (или $\mathbb{R}$ по $\mathbb{Q}$, или как при конструкции пополнения *произвольного* метрического пространства). Интуитивный смысл построения Ω заключается в добавлении всех тех чисел, которые должны быть пределами

сходящихся [1]) бесконечных сумм чисел из $\overline{\mathbb{Q}}_p$, например сумм вида, рассмотренного в доказательстве теоремы 12.

Точно так же, как и при переходе от $\mathbb{Q}$ к $\mathbb{Q}_p$, при переходе от $\overline{\mathbb{Q}}_p$ к Ω можно продолжить норму $|\ |_p$ с $\overline{\mathbb{Q}}_p$ до нормы на Ω, положив $|x|_p = \lim\limits_{i\to\infty} |x_i|_p$, где $\{x_i\}$ — некоторая последовательность Коши элементов из $\overline{\mathbb{Q}}_p$, лежащая в классе эквивалентности x (см. § I.4). Как и в случае перехода от $\mathbb{Q}$ к $\mathbb{Q}_p$, нетрудно показать, что на самом деле при $x\neq 0$ этот предел $|x|_p$ равен $|x_i|_p$ для достаточно больших i.

Продолжим также функцию ord_p на Ω:

$$\mathrm{ord}_p x = -\log_p |x|_p.$$

Следующая теорема утверждает, что на этом работа окончена: Ω может служить p-адическим аналогом поля комплексных чисел.

Теорема 13. *Поле Ω алгебраически замкнуто.*

Доказательство. Пусть $f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$, $a_i \in \Omega$. Мы должны установить существование корня у $f(X)$ в Ω. Для каждого $i = 0, 1, \ldots, n-1$ выберем последовательность $\{a_{ij}\}_j$ элементов поля $\overline{\mathbb{Q}}_p$, сходящуюся к a_i. Пусть $g_j(X) = X^n + a_{n-1,j}X^{n-1} + \ldots + a_{1,j}X + a_{0,j}$, а r_{ij} — корни многочлена $g_j(X)$ $(i = 1, 2, \ldots, n)$. Утверждается, что можно найти такую последовательность индексов i_j $(1 \leqslant i_j \leqslant n)$, $j = 1, 2, 3, \ldots$, для которой $\{r_{i_j,j}\}$ — последовательность Коши. Действительно, предположим, что мы уже имеем $r_{i_j,j}$ и хотим указать следующее $r_{i_{j+1},j+1}$. Пусть $\delta_j = |g_j - g_{j+1}|_p = \max\limits_i (|a_{i,j} - a_{i,j+1}|_p)$ (это число стремится к 0 при $j\to\infty$). Положим $A_j = \max(1, |r_{i_j,j}|_p^n)$. Очевидно, существует некоторая константа A, такая, что $A_j \leqslant A$ для всех j (см. ниже упр. 3). Тогда

$$\prod_i |r_{i_j,j} - r_{i,j+1}|_p = |g_{j+1}(r_{i_j,j})|_p = |g_{j+1}(r_{i_j,j}) - g_j(r_{i_j,j})|_p \leqslant \delta_j A.$$

[1]) В смысле Коши. — *Прим. перев.*

Следовательно, по крайней мере одно из чисел $|r_{i_j,j} - r_{i,j+1}|_p$ слева $\leqslant \sqrt[n]{\delta_j A}$. Пусть $r_{i_{j+1},j+1}$ — соответствующее $r_{i,j+1}$. Построенная последовательность $\{r_{i_j,j}\}$, очевидно, является последовательностью Коши.

Пусть теперь $r = \lim\limits_{j\to\infty} r_{i_j,j} \in \Omega$. Тогда

$$f(r) = \lim_{j\to\infty} f(r_{i_j,j}) = \lim_{j\to\infty} g_j(r_{i_j,j}) = 0. \ \square$$

Резюмируя результаты глав I и III, можно сказать, что мы построили наименьшее алгебраически замкнутое поле Ω, содержащее $\mathbb{Q}$ и полное относительно $|\ |_p$. (Строго говоря, это видно из следующего рассуждения: пусть Ω' — другое такое поле; так как Ω' полно, оно должно содержать поле, изоморфное p-адическому пополнению поля $\mathbb{Q}$, которое можно обозначить $\mathbb{Q}_p$; далее, поскольку Ω' содержит $\mathbb{Q}_p$ и алгебраически замкнуто, оно должно содержать поле, изоморфное алгебраическому замыканию поля $\mathbb{Q}_p$; это замыкание можно обозначить $\overline{\mathbb{Q}}_p$; и, наконец, так как Ω' содержит $\overline{\mathbb{Q}}_p$ и полно, оно должно содержать поле, изоморфное пополнению $\overline{\mathbb{Q}}_p$, которое можно обозначить Ω. Таким образом, любое поле, обладающее указанными выше свойствами, должно содержать поле, изоморфное Ω. Это объясняется тем, что и пополнение, и алгебраическое замыкание определены однозначно с точностью до изоморфизма.)

Поле Ω следовало бы обозначать через Ω_p, напоминая о простом числе p, от которого зависят все конструкции. Но для краткости индекс p мы опускаем.

Построенное поле Ω — это обширная и прекрасная область, место обитания p-адического анализа.

Упражнения

1. Докажите, что множество всевозможных значений $|\ |_p$ на $\overline{\mathbb{Q}}_p$ состоит из всех рациональных степеней p (лежащих в множестве положительных вещественных чисел). Каково это множество для Ω? Напомним, что функция ord_p продолжается на Ω следующим способом: $\mathrm{ord}_p x = -\log_p |x|_p$ (т. е. чтобы получить $|x|_p$, нужно возвести $1/p$ в эту степень). Каково множество всевозможных значений ord_p на Ω? Докажите, что $\overline{\mathbb{Q}}_p$ и Ω *не* яв-

ляются локально компактными. Это одно из существенных отличий Ω от ℂ, которое локально компактно в архимедовой метрике (обычное расстояние на комплексной плоскости).

2. Что получится, если на Ω определить «эллипс» как множество точек, сумма расстояний которых от двух заданных точек a, $b \in \Omega$ постоянна и равна некоторому фиксированному вещественному числу r? Покажите, что этот «эллипс» является либо объединением двух непересекающихся окружностей, либо пересечением двух окружностей, либо пустым множеством в зависимости от выбора a, b и r. Что будет, если определить «гиперболу» как $\{x \in \Omega \mid |x-a|_p - |x-b|_p = r\}$?

3. Пусть $g(X) = X^n + b_{n-1}X^{n-1} + \ldots + b_1 X + b_0$, $C_0 = |g|_p \overset{\text{def}}{=} \max_i |b_i|_p$. Докажите существование такой константы C_1, зависящей только от C_0, что любой корень β многочлена $g(X)$ удовлетворяет неравенству $|\beta|_p < C_1$.

4. Пусть α — корень многочлена $f(X) \in K[X]$ со старшим коэффициентом 1, где K — конечное расширение поля $\mathbb{Q}_p$. Докажите существование такого $\varepsilon > 0$, что всякий полином $g(X)$ такой же степени, как и f, удовлетворяющий неравенству $|f-g|_p < \varepsilon$, имеет корень β, для которого $K(\alpha) = K(\beta)$.

5. Докажите, что всякое конечное расширение K поля $\mathbb{Q}_p$ содержит конечное расширение F поля рациональных чисел $\mathbb{Q}$, для которого $[F:\mathbb{Q}] = [K:\mathbb{Q}_p]$ и F *плотно* в K, т. е. для каждого элемента $x \in K$ и любого $\varepsilon > 0$ существует $y \in F$ с $|x-y|_p < \varepsilon$.

6. Пусть p — такое простое число, что -1 не имеет квадратного корня в $\mathbb{Q}_p$ (см. упр. 8 к § 1). Используя лемму Краснера, найдите ε, для которого $\mathbb{Q}_p(\sqrt{-a}) = \mathbb{Q}_p(\sqrt{-1})$ при любом a с $|a-1|_p < \varepsilon$. Для какого ε из неравенства $|a-p|_p < \varepsilon$ следует совпадение $\mathbb{Q}_p(\sqrt{a})$ с $\mathbb{Q}_p(\sqrt{p})$? (Отдельно исследуйте случай $p=2$.)

7. Пусть a — примитивный корень из 1 степени p^n в $\overline{\mathbb{Q}}_p$, т. е. $a^{p^{n-1}} \neq 1$. Найдите $|a-1|_p$. (*Указание*: a имеет минимальный многочлен $(X^{p^n}-1)/(X^{p^{n-1}}-1)$; при $n=1$ см. упр. 14 к § I.5.) Пусть $n=1$. Докажите, что $\mathbb{Q}_p(a) = \mathbb{Q}_p((-p)^{1/(p-1)})$. Докажите, что если a — примитивный корень из 1 степени m и m не равно степени числа p, то $|a-1|_p = 1$.

8. Пусть K — конечное расширение поля $\mathbb{Q}_p$, m — некоторое целое положительное число, а $(K^\times)^m$ обозначает множество m-х степеней элементов из $K^\times$. Предположим, что: (1) $|m|_p = 1$ и (2) K не содержит корней степени m из 1, отличных от 1. (Например, для $K = \mathbb{Q}_p$ легко проверить, что эти два условия выполнены тогда и только тогда, когда m взаимно просто с p и $p-1$.) Докажите, что индекс мультипликативной подгруппы $(K^\times)^m$ в $K^\times$ (т. е. число различных классов смежности) равен m.

9. Опустим оба предположения предыдущего упражнения. Докажите, что индекс $(K^\times)^m$ в $K^\times$ равен $m\omega/|m|_p$, где ω — число корней из 1 степени m, содержащихся в поле K.

10. Пусть K — вполне разветвленное расширение поля $\mathbb{Q}_p$. Покажите, что каждый корень степени m из 1 в поле K лежит на самом деле в $\mathbb{Q}_p$, если p не делит m.

11. Определите мощность множеств $\mathbb{Q}_p$, $\overline{\mathbb{Q}}_p$ и Ω.

12. Докажите, что $ef = n$, где $n = [K:\mathbb{Q}_p]$, e — индекс ветвления, а f — степень поля вычетов. (*Указание*. Пусть $y_1, \ldots, y_f$ — элементы поля K, для которых $|y_i|_p = 1$, а их образы в поле вычетов составляют базис этого поля над $\mathbb{F}_p$. Покажите, что $y_i\pi^j$, $1 \leqslant i \leqslant f$, $0 \leqslant j \leqslant e-1$, составляют базис в K над $\mathbb{Q}_p$, где $\operatorname{ord}_p \pi = 1/e$.)

13. Пусть K — вполне разветвленное расширение степени e поля $\mathbb{Q}_p$. Установите существование такого $\beta \in K$, что $|\beta^e - \alpha|_p < 1/p$ для некоторого $\alpha \in \mathbb{Z}_p$ с $\operatorname{ord}_p \alpha = 1$

14. Предположим, что K — *ручное* вполне разветвленное расширение. Используя метод леммы Гензеля, покажите, что найденное выше β можно подправить так, чтобы для него было справедливо включение $\beta^e \in \mathbb{Q}_p$, т. е. β удовлетворяло уравнению $X^e - \alpha = 0$, где $\alpha \in \mathbb{Z}_p$ и $\operatorname{ord}_p \alpha = 1$. Заметим, что тогда $K = \mathbb{Q}_p(\beta)$ (объясните почему).

15. Докажите для любого натурального n конечность числа расширений поля $\mathbb{Q}_p$ степени, не превосходящей n.

16. Комплексных чисел гораздо больше, чем рациональных и даже алгебраических, потому что два последних множества счетны, а ℂ имеет мощность континуума. Поле Ω также много больше, чем $\mathbb{Q}_p^{\text{alg cl}}$, хотя и в другом смысле (см. выше упр. 11). Докажите, что Ω нельзя представить в виде алгебраического расширения поля, полученного присоединением счетного числа элементов поля Ω к $\overline{\mathbb{Q}}_p$ (т. е. поля, состоящего из всех рациональных выражений от этих элементов и элементов поля $\overline{\mathbb{Q}}_p$). Можно сказать, что Ω имеет *несчетную степень трансцендентности над* $\overline{\mathbb{Q}}_p$. (*Предупреждение*. Это упражнение и следующее — трудные!

17. Будет ли счетной степень трансцендентности Ω над p-адическим пополнением поля $\mathbb{Q}_p^{\text{unram}}$?

Глава IV

p-АДИЧЕСКИЕ СТЕПЕННЫЕ РЯДЫ

§ 1. ЭЛЕМЕНТАРНЫЕ ФУНКЦИИ

Напомним, что в метрическом пространстве, метрика которого индуцирована некоторой неархимедовой нормой $\| \ \|$, последовательность удовлетворяет условию Коши в том и только том случае, когда разность между ее соседними членами стремится к нулю. Более того, если это метрическое пространство полно, бесконечная сумма в нем сходится тогда и только тогда, когда ее общий член стремится к нулю. Поэтому выражения вида

$$f(X)=\sum_{n=0}^{\infty} a_n X^n, \quad a_n \in \Omega,$$

позволяют задать значение функции $f(x)$ как $\sum_{n=0}^{\infty} a_n x^n$ для всех тех значений $x \in \Omega$ переменной X, для которых $|a_n x^n|_p \to 0$.

Следуя архимедову случаю (степенных рядов над $\mathbb{R}$ или $\mathbb{C}$), определим *радиус сходимости* соотношением

$$r=\frac{1}{\limsup |a_n|_p^{1/n}},$$

где выражение $1/r=\limsup |a_n|_p^{1/n}$ обозначает *наименьшее* вещественное число $1/r$, для которого при *любом* $C>1/r$ существует лишь конечное число величин $|a_n|_p^{1/n}$, больших C. Иначе говоря, $1/r$ есть наибольшая *точка накопления*, т. е. наибольшее вещественное число, представимое в виде предела некоторой подпоследовательности из $\{|a_n|_p^{1/n}\}$. Так, например, $1/r$ равно $\lim\limits_{n\to\infty} |a_n|_p^{1/n}$, если последний предел существует.

Чтобы обосновать употребление термина «радиус сходимости», покажем, что соответствующий ряд сходится при $|x|_p<r$ и расходится при $|x|_p>r$. Пусть сначала $|x|_p<r$. Тогда, положив $|x|_p=(1-\varepsilon)r$, получим $|a_n x^n|_p=\left(r\,|a_n|_p^{1/n}\right)^n(1-\varepsilon)^n$. Так как $|a_n|_p^{1/n}>$ $>1/(r-{}^1/_2\varepsilon r)$ только для конечного числа значений n, то

$$\lim_{n\to\infty} |a_n x^n|_p \leqslant \lim_{n\to\infty}\left(\frac{(1-\varepsilon)\,r}{(1-{}^1/_2\varepsilon)\,r}\right)^n=\lim_{n\to\infty}\left(\frac{1-\varepsilon}{1-{}^1/_2\varepsilon}\right)^n=0.$$

Если $|x|_p>r$, то подобным же образом легко установить, что $a_n x^n$ не стремится к 0 при $n\to\infty$.

Что происходит при $|x|_p=r$? В архимедовом случае ряды могут вести себя довольно сложно на границе интервала или круга сходимости. Например, $\log(1+x)=$ $=\sum\limits_{n=1}^{\infty}(-1)^{n+1}x^n/n$ имеет радиус сходимости 1. При $|x|=1$ этот ряд расходится для $x=-1$ и сходится (*условно*, не абсолютно) для всех остальных значений x (т. е. для $x=1$ в вещественном случае и во всех точках единичной окружности, исключая $x=-1$, в комплексном).

В неархимедовом же случае ответ не зависит от точки границы $|x|_p=r$. Это происходит по той причине, что в данной ситуации ряд сходится тогда и только тогда, когда его члены стремятся к нулю, т. е. тогда и только тогда, когда $|a_n|_p|x|_p^n\to 0$. Но это условие зависит только от нормы $|x|_p$, а не от конкретного значения x с заданной нормой. Такого явления, как условная сходимость, здесь просто не существует (ряд $\sum \pm a_n$ сходится или расходится независимо от выбора знаков $\pm$).

Если мы рассмотрим тот же пример $\sum\limits_{n=1}^{\infty}(-1)^{n+1}\frac{X^n}{n}$, то найдем, что $|a_n|_p=p^{\operatorname{ord}_p n}$ и $\lim\limits_{n\to\infty}|a_n|_p^{1/n}=1$. Поэтому этот ряд сходится при $|x|_p<1$ и расходится при $|x|_p>1$. Когда $|x|_p=1$, $|a_n x^n|_p=p^{\operatorname{ord}_p n}\geqslant 1$ и ряд расходится для всех таких x.

Введем теперь некоторые обозначения. Пусть R — кольцо. Обозначим через $R[[X]]$ кольцо формальных степенных рядов от X с коэффициентами в R, т. е. множество выражений $\sum_{n=0}^{\infty} a_n X^n$, $a_n \in R$, которые складываются и умножаются по обычным правилам. Обычно в дальнейшем R будет одним из следующих колец: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}_p$, $\mathbb{Q}_p$ или Ω. Это обозначение часто используется для компактной записи других множеств, например:

$$1+XR[[X]] \overset{\text{def}}{=} \{f \in R[[X]] \mid \text{постоянный член } a_0 \text{ ряда } f \text{ равен } 1\}.$$

Множество

$$D_a(r) \overset{\text{def}}{=} \{x \in \Omega \mid |x-a|_p \leqslant r\}$$

называется *замкнутым диском радиуса* $r \in \mathbb{R}$ *с центром в точке* $a \in \Omega$, а

$$D_a(r^-) \overset{\text{def}}{=} \{x \in \Omega \mid |x-a|_p < r\}$$

— *открытым диском радиуса* r *с центром в* a. Кроме того, положим $D(r) \overset{\text{def}}{=} D_0(r)$ и $D(r^-) \overset{\text{def}}{=} D_0(r^-)$. (Замечание: сразу оговоримся, что ниже, говоря о замкнутом диске $D(r)$ из Ω, мы всегда подразумеваем, что r — одно из возможных значений $|\ |_p$, т. е. рациональная степень числа p; в противном случае, когда не существует $x \in \Omega$ с $|x|_p = r$, мы всегда пишем $D(r^-)$.)

(Предостережение. Термины «открытый» и «замкнутый» введены лишь по аналогии с архимедовым случаем. С топологической точки зрения такая терминология неудачна. А именно, множество $C_c = \{x \in \Omega \mid |x - a|_p = c\}$ открыто в топологическом смысле, так как каждая точка $x \in C_c$ обладает открытой окрестностью, например $D_x(c^-)$, все точки которой лежат в C_c. Поэтому любое объединение этих множеств C_c открыто. Оба диска $D_a(r)$ и $D_a(r^-)$, так же как и их дополнения, являются такими объединениями, например $D_a(r^-) = \bigcup_{c<a} C_c$. Следовательно, диски $D_a(r)$ и $D_a(r^-)$ одновременно *открыты и замкнуты*. Топологическое пространство, подобное Ω, с такими странными свойствами называется *вполне несвязным*.)

Чтобы привыкнуть к обозначениям, докажем следующую тривиальную лемму.

Лемма 1. *Каждый ряд* $f(X) \in \mathbb{Z}_p[[X]]$ *сходится на* $D(1^-)$.

Доказательство. Пусть $f(X) = \sum_{n=0}^{\infty} a_n X^n$, $a_n \in \mathbb{Z}_p$ и $x \in D(1^-)$. Тогда $|x|_p < 1$. Кроме того, $|a_n|_p \leqslant 1$ для всех n. Следовательно, $|a_n x^n|_p \leqslant |x|_p^n \to 0$ при $n \to \infty$. □

Установим еще один простой результат.

Лемма 2. *Каждый ряд* $f(X) = \sum_{n=0}^{\infty} a_n X^n \in \Omega[[X]]$, *сходящийся на некотором (открытом или замкнутом) диске* $D = D(r)$ *или* $D(r^-)$, *непрерывен на* D.

Доказательство. Пусть x — точка в D. Предположим, что $|x' - x|_p < \delta$, где $\delta < |x|_p$ будет выбрано позже. Тогда $|x'|_p = |x|_p$. (Ниже предполагаем, что $x \neq 0$; случай $x = 0$ очень легко проверить отдельно.) Имеем

$$|f(x) - f(x')|_p = \left| \sum_{n=0}^{\infty} (a_n x^n - a_n x'^n) \right|_p \leqslant$$

$$\leqslant \max_n (|a_n x^n - a_n x'^n|_p) = \max_n (|a_n|_p |(x-x')(x^{n-1} + x^{n-2}x' + \ldots + xx'^{n-2} + x'^{n-1}|_p).$$

Но $|x^{n-1} + x^{n-2}x' + \ldots + xx'^{n-2} + x'^{n-1}|_p) \leqslant \max_{1 \leqslant i \leqslant n} |x^{n-i}x'^{i-1}|_p = |x|_p^{n-1}$. Следовательно,

$$|f(x) - f(x')|_p \leqslant \max_n (|x - x'|_p |a_n|_p |x|_p^{n-1}) < \frac{\delta}{|x|_p} \max_n (|a_n|_p |x|_p^n).$$

Так как $|a_n|_p |x|_p^n$ ограничено при $n \to \infty$, то $|f(x) - f(x')|_p < \varepsilon$ для подходящего δ. □

Вернемся к ряду $\sum_{n=1}^{\infty}(-1)^{n+1}X^n/n$, который, как мы уже выяснили, имеет диск сходимости $D(1^-)$. Таким образом, этот ряд задает функцию на $D(1^-)$, принимающую значения в Ω. Обозначим эту функцию $\log_p(1+X)$, где индекс p напомнит нам о простом числе, определяющем норму на $\mathbb{Q}$, по которой строится Ω, а также не даст перепутать эту функцию с классическим логарифмом $\log(1+X)$, имеющим другую область определения (подмножество в $\mathbb{R}$ или $\mathbb{C}$) и область значений ($\mathbb{R}$ или $\mathbb{C}$). К сожалению, обозначение *p-адического логарифма* $\log_p$ совпадает с классическим обозначением для логарифма по основанию p. Начиная с этого места, под $\log_p$ всегда понимается p-адический логарифм

$$\log_p(1+X)\colon D(1^-)\to\Omega, \quad \log_p(1+x)=\sum_{n=1}^{\infty}(-1)^{n+1}x^n/n,$$

если противное не оговорено *явно*.

Ловушки, подстерегающие тех, кто путает архимедовы и p-адические функции, будут проиллюстрированы ниже, а также в упр. 8—10 к § 2.

Все когда-либо изучавшие дифференциальные уравнения (и многие не изучавшие) понимают, что функция $\exp(x)=e^x=\sum_{n=0}^{\infty}x^n/n!$ является, может быть, самой важной в классической математике. Поэтому взглянем на этот ряд $\sum_{n=0}^{\infty}X^n/n!$ p-адически. Классический экспоненциальный ряд сходится всюду благодаря стремительному росту величины $n!$ в знаменателе. Но если в классическом случае большой знаменатель способствует сходимости, в p-адической ситуации он может играть обратную роль. Действительно, нетрудно вычислить (см. упр. 13 к § I.2), что

$$\operatorname{ord}_p(n!)=\frac{n-S_n}{p-1}$$

(S_n = сумма знаков p-ичной записи числа n);

$$|1/n!|_p=p^{(n-S_n)/(p-1)}.$$

Из формулы $r=1/(\limsup|a_n|_p^{1/n})$ для радиуса сходимости получаем

$$\operatorname{ord}_p r=\liminf\left(\frac{1}{n}\operatorname{ord}_p a_n\right)$$

(где $\liminf$ некоторой последовательности обозначает наименьшую точку накопления). Тогда в случае $a_n=1/n!$ имеем

$$\operatorname{ord}_p r=\liminf\left(-\frac{n-S_n}{n(p-1)}\right),$$

но $\lim_{n\to\infty}(-(n-S_n)/(n(p-1)))=-1/(p-1)$. Следовательно, $\sum_{n=0}^{\infty}x^n/n!$ сходится при $|x|_p<p^{-1/(p-1)}$ и расходится при $|x|_p>p^{-1/(p-1)}$. Что происходит при $|x|_p=p^{-1/(p-1)}$, т. е. когда $\operatorname{ord}_p x=1/(p-1)$? В этом случае

$$\operatorname{ord}_p(a_nx^n)=-\frac{n-S_n}{p-1}+\frac{n}{p-1}=\frac{S_n}{p-1}.$$

Если, например, $n=p^m$ — степень p, то $S_n=1$. Поэтому $\operatorname{ord}_p\left(a_{p^m}x^{p^m}\right)=1/(p-1)$, $|a_{p^m}x^{p^m}|_p=p^{-1/(p-1)}$ и a_nx^n не стремится к 0 при $n\to\infty$. Итак, $\sum_{n=0}^{\infty}X^n/n!$ имеет диск сходимости $D(p^{-1/(p-1)-})$ (последний минус, как обычно, обозначает открытый диск). Положим $\exp_p(X)\overset{\text{def}}{=}\sum_{n=0}^{\infty}X^n/n!\in\mathbb{Q}_p[[X]]$. Отметим, что $D(p^{-1/(p-1)-})\subset D(1^-)$. Поэтому $\exp_p$ сходится в *меньшем* диске, чем $\log_p$!

Несмотря на важные различия между log (exp) и $\log_p$ ($\exp_p$), о которых никогда не следует забывать, некоторые из основных свойств log и exp переносятся на p-адический случай. Установим, например, основное свойство логарифма: логарифм произведения равен сумме логарифмов сомножителей. Прежде всего заме-

тим, что если $x \in D(1^-)$, $y \in D(1^-)$, то $(1+x)(1+y) = 1+(x+y+xy) \in 1+D(1^-)$. Таким образом,

$$\log_p[(1+x)(1+y)] = \sum_{n=1}^{\infty} (-1)^{n+1}(x+y+xy)^n/n.$$

Но в кольце формальных степенных рядов от *двух* переменных над $\mathbb{Q}$ (оно обозначается $\mathbb{Q}[[X, Y]]$) выполнено соотношение

$$\sum (-1)^{n+1}X^n/n + \sum (-1)^{n+1}Y^n/n = \sum (-1)^{n+1}(X+Y+XY)^n/n.$$

Оно вытекает из соотношения $\log(1+x)(1+y) = \log(1+x)+\log(1+y)$, верного для $\mathbb{R}$ и $\mathbb{C}$. Тогда разность между двумя частями доказываемого равенства, скажем $F(X, Y)$, обращается в нуль для всех вещественных значений X и Y из интервала $(-1, 1)$. Поэтому коэффициенты при X^mY^n в $F(X, Y)$ равны нулю для всех m и n.

Этот способ доказательства обращения в нуль формального степенного ряда $F(X, Y)$ типичен для многих последующих рассуждений. Предположим, что некоторое выражение, содержащее формальные степенные ряды от X и Y, например $\log(1+X)$, $\log(1+Y)$ или $\log(1+X+Y+XY)$, тождественно обращается в нуль после подстановки в него вместо переменных вещественных чисел из некоторого интервала. Тогда ряд, полученный приведением подобных членов по X^mY^n, будет иметь лишь нулевые коэффициенты. Мы опускаем детали, так как это общий факт, не связанный непосредственно с p-адическими числами. Если вы не уверены, что смогли бы доказать его самостоятельно, посмотрите упр. 25 к § 2, где даны разъяснения и указания.

Возвращаясь к p-адической ситуации, отметим, что члены любого ряда, сходящегося в Ω, можно поставить в любом порядке и полученный ряд будет сходиться к тому же пределу. (Это легко проверить: ведь условной сходимости в этом случае не бывает.) Итак,

$\log_p[(1+x)(1+y)] = \sum_{n=1}^{\infty} (-1)^{n+1}(x+y+xy)^n/n$ можно переписать как $\sum_{m,\,n=0}^{\infty} c_{m,n}x^ny^m$. Но по «формальному тождеству» в $\mathbb{Q}[[X, Y]]$ все рациональные числа $c_{m,n}$ равны 0, кроме чисел с $n=0$ или $m=0$, а для них $c_{0,n} = c_{n,0} = (-1)^{n+1}/n$ $(c_{0,0}=0)$. Отсюда можно заключить, что

$$\log_p[(1+x)(1+y)] = \sum_{n=1}^{\infty} (-1)^{n+1}x^n/n + \sum_{n=1}^{\infty} (-1)^{n+1}y^n/n = \log_p(1+x)+\log_p(1+y).$$

В качестве следствия этой формулы рассмотрим случай, когда $1+x$ есть корень степени p^m из 1. Тогда $|x|_p < 1$ (см. упр. 7 к § III.4) и $p^m\log_p(1+x) = \log_p(1+x)^{p^m} = \log_p 1 = 0$. Следовательно, $\log_p(1+x) = 0$.

Точно так же доказывается следующий p-адический вариант известного свойства экспоненты: если $x, y \in D(p^{-1/(p-1)-})$, то $x+y \in D(p^{-1/(p-1)-})$ и $\exp_p(x+y) = \exp_p(x)\cdot\exp_p(y)$.

Более того, как и в архимедовом случае, функции $\log_p$ и $\exp_p$ взаимно обратны. Точнее, предположим, что $x \in D(p^{-1/(p-1)-})$. Тогда $\exp_p x = 1 + \sum_{n=1}^{\infty} x^n/n!$ и $\operatorname{ord}_p(x^n/n!) > n/(p-1) - (n-S_n)/(p-1) = S_n/(p-1) > 0$. Отсюда $\exp_p x - 1 \in D(1^-)$. Рассмотрим

$$\log_p(1+\exp_p x - 1) = \sum_{n=1}^{\infty} (-1)^{n+1}(\exp_p x - 1)^n/n = \sum_{n=1}^{\infty} (-1)^{n+1}\left(\sum_{m=1}^{\infty} x^m/m!\right)^n \Big/ n.$$

Этот ряд приводится к виду $\sum_{n=1}^{\infty} c_n x^n$. Но по тем же соображениям, что и выше, в $\mathbb{Q}[[X]]$ имеет место

формальное тождество

$$\sum_{n=1}^{\infty}(-1)^{n+1}\Big(\sum_{m=1}^{\infty}X^m/m!\Big)^n\Big/n=X,$$

вытекающее из того, что $\log(\exp x)=x$ для поля $\mathbb{R}$ или $\mathbb{C}$. Следовательно, $c_1=1$ и $c_n=0$ при $n>1$, откуда

$$\log_p(1+\exp_p x-1)=x \quad \text{для всех } x\in D(p^{-1/(p-1)}-).$$

Вычисляя выражение $\exp_p(\log_p(1+x))$, нужно быть немного осторожнее. Дело в том, что даже если x принадлежит области сходимости $D(1^-)$ ряда $\log_p(1+X)$, то совсем *необязательно*, чтобы $\log_p(1+x)$ принадлежал области сходимости $D(p^{-1/(p-1)}-)$ ряда $\exp_p(X)$. Это *верно*, если $x\in D(p^{-1/(p-1)}-)$, ибо тогда при $n\geqslant 1$

$$(\operatorname{ord}_p x^n/n)-\frac{1}{p-1}>\frac{n}{p-1}-\operatorname{ord}_p n-\frac{1}{p-1}=\frac{n-1}{p-1}-\operatorname{ord}_p n,$$

а последнее выражение достигает минимума, равного нулю, при $n=1$ и $n=p$. Поэтому $\operatorname{ord}_p\log_p(1+x)\geqslant \min_n \operatorname{ord}_p x^n/n>1/(p-1)$. Затем, как и выше, получаем

$$\exp_p(\log_p(1+x))=1+x \quad \text{для всех} \quad x\in D(p^{-1/(p-1)}-).$$

Все установленные нами факты о $\log_p$ и $\exp_p$ можно кратко резюмировать в следующем утверждении.

Предложение. *Функции* $\log_p$ *и* $\exp_p$ *задают взаимно обратные изоморфизмы между мультипликативной группой точек открытого диска радиуса* $p^{-1/(p-1)}$ *с центром в* 1 *и аддитивной группой точек открытого диска радиуса* $p^{-1/(p-1)}$ *с центром в* 0.

(Это означает в точности следующее: $\log_p$ задает взаимно однозначное соответствие между двумя указанными множествами, при котором образ произведения двух чисел равен сумме образов сомножителей, а $\exp_p$ — обратное отображение.)

Этот изоморфизм подобен изоморфизму в вещественном случае между мультипликативной группой положительных вещественных чисел и аддитивной группой

вещественных чисел, который задается взаимно обратными функциями log и exp.

В частности, в силу этого предложения $\log_p$ инъективен на $D_1(p^{-1/(p-1)}-)$, т. е. в $D_1(p^{-1/(p-1)}-)$ не существует двух чисел с одним и тем же значением $\log_p$. Легко показать, что $D_1(p^{-1/(p-1)}-)$ — наибольший диск, для которого это справедливо. В самом деле, $|\zeta-1|_p=p^{-1/(p-1)}$ для примитивного корня ζ степени p из 1 (см. упр. 7 к § III.4), а $\log_p\zeta=0=\log_p 1$.

Аналогично определяются функции

$$\sin_p\colon D(p^{-1/(p-1)}-)\to\Omega,$$

$$\sin_p X=\sum_{n=0}^{\infty}(-1)^n X^{2n+1}/(2n+1)!;$$

$$\cos_p\colon D(p^{-1/(p-1)}-)\to\Omega,$$

$$\cos_p X=\sum_{n=0}^{\infty}(-1)^n X^{2n}/(2n)!.$$

Другой тип функций, важных для классической математики, представляют биномиальные разложения $B_a(x)=(1+x)^a=\sum_{n=0}^{\infty}\frac{a(a-1)\dots(a-n+1)}{n!}x^n$. Если $a\in\mathbb{R}$ или $\mathbb{C}$, этот ряд сходится в $\mathbb{R}$ или $\mathbb{C}$ при $|x|<1$ и расходится при $|x|>1$ (кроме случая, когда a — целое неотрицательное число); при $|x|=1$ этот ряд имеет достаточно сложное поведение, зависящее от конкретного значения a.

Определим теперь для каждого $a\in\Omega$ ряд

$$B_{a,p}(X)\underset{\text{def}}{=}\sum_{n=0}^{\infty}\frac{a(a-1)\dots(a-n+1)}{n!}X^n$$

и проанализируем его сходимость. Предположим вначале, что $|a|_p>1$. Тогда $|a-i|_p=|a|_p$ и норма $|\ |_p$ n-го члена этого ряда равна $|ax^n/n!|_p$. Поэтому при $|a|_p>1$ ряд $B_{a,p}(X)$ имеет область сходимости $D(p^{-1/(p-1)}/|a|_p)$.

Предположим теперь, что $|a|_p \leqslant 1$. В этом случае картина становится более сложной и зависит от a. Мы не будем приводить здесь ее полное описание. Во всяком случае, $|a-i|_p \leqslant 1$ для любого такого a, откуда $|a(a-1)\ldots(a-n+1)x^n/n!|_p \leqslant |x^n/n!|_p$. Поэтому $B_{a,p}(X)$ сходится по крайней мере на $D(p^{-1/(p-1)-})$.

Вскоре нам понадобится более точный результат о сходимости $B_{a,p}(X)$ для $a \in \mathbb{Z}_p$. Утверждается, что тогда $B_{a,p}(X) \in \mathbb{Z}_p[[X]]$ (и, в частности, этот ряд сходится на $D(1^-)$ по лемме 1). Итак, надо показать, что $a(a-1)\ldots(a-n+1)/n! \in \mathbb{Z}_p$. Пусть a_0 — целое положительное число, большее n, для которого $\operatorname{ord}_p(a-a_0) > N$ (подходящее N будет выбрано позже). Тогда $a_0(a_0-1)\ldots(a_0-n+1)/n! = \binom{a_0}{n} \in \mathbb{Z} \subset \mathbb{Z}_p$. Поэтому достаточно установить, что разность между $a_0(a_0-1)\ldots(a_0-n+1)/n!$ и $a(a-1)\ldots(a-n+1)/n!$ для некоторого N имеет $|\ |_p \leqslant 1$. А это следует прямо из непрерывности многочлена $X(X-1)\ldots(X-n+1)$. Таким образом,

$$B_{a,p}(X) \in \mathbb{Z}_p[[X]], \quad \text{если} \quad a \in \mathbb{Z}_p.$$

Возьмем, например, $a = 1/m$, где $m \in \mathbb{Z}$ и $p \nmid m$. Это один из важных случаев, когда $a \in \mathbb{Z}_p$. Пусть $x \in D(1^-)$. Тогда, используя те же соображения, что и при доказательстве тождества $\log_p(1+x)(1+y) = \log_p(1+x) + \log_p(1+y)$, получаем

$$[B_{1/m,p}(x)]^m = 1+x.$$

Таким образом, $B_{1/m,p}(x)$ есть корень степени m из $1+x$ в Ω. (При $p \mid m$ последнее также имеет место, но только для тех значений x, которые лежат в $D(|m|_p p^{-1/(p-1)-})$.) Поэтому для обычных рациональных чисел a можно пользоваться сокращенной записью $B_{a,p}(X) = (1+X)^a$.

Но при этом необходима осмотрительность! Как быть, например, со следующим «парадоксом»? Рассмотрим $^4/_3 = (1+{}^7/_9)^{1/2}$; $\operatorname{ord}_7 {}^7/_9 = 1$ в $\mathbb{Z}_7$. Поэтому для $x = {}^7/_9$ и $n \geqslant 1$

$$\left| \frac{{}^1/_2({}^1/_2-1)\ldots({}^1/_2-n+1)}{n!} x^n \right|_7 \leqslant \frac{7^{-n}}{|n!|_7} < 1.$$

Следовательно,

$$1 > |(1+{}^7/_9)^{1/2} - 1|_7 = |{}^4/_3 - 1|_7 = |{}^1/_3|_7 = 1.$$

Что стряслось?

Мы чересчур опрометчиво написали $^4/_3 = (1+{}^7/_9)^{1/2}$. Как известно, в $\mathbb{R}$ и в $\mathbb{Q}_7$ число $^{16}/_9$ имеет два квадратных корня $\pm {}^4/_3$. В $\mathbb{R}$ ряд для $(1+{}^7/_9)^{1/2}$ сходится к $^4/_3$, и мы отдаем предпочтение положительному корню. А в $\mathbb{Q}_7$ предпочтение отдается другому корню $-{}^4/_3 = 1 - {}^7/_3$, поскольку он сравним с 1 по модулю 7. Значит, *один и тот же ряд* рациональных чисел

$$\sum_{n=0}^{\infty} \frac{{}^1/_2({}^1/_2-1)\ldots({}^1/_2-n+1)}{n!} \left(\frac{7}{9}\right)^n$$

сходится к некоторому рациональному числу как в 7-адической, так и в архимедовой метрике; но те числа, к которым он сходится, различны! Это контрпример к следующей неверной «теореме».

Не-теорема 1. *Пусть* $\sum_{n=1}^{\infty} a_n$ *— сумма рациональных чисел, сходящаяся к некоторому рациональному числу относительно* $|\ |_p$, *а также к некоторому рациональному числу относительно* $|\ |_\infty$. *Тогда рациональные значения этой суммы для двух метрик совпадают.*

Другие «парадоксы» можно найти ниже в упр. 8—10.

§ 2. ЭКСПОНЕНТА АРТИНА—ХАССЕ

Введем теперь одну «элементарную функцию», которая несколько «лучше», чем $\exp_p$, так как имеет больший диск сходимости, и которая часто используется вместо exp, особенно в тех случаях, когда нужна лучшая сходимость, чем только на $D(p^{-1/(p-1)-})$. Для этого прежде всего разложим в бесконечное произведение обычную экспоненциальную функцию. Это разложение использует функцию Мёбиуса $\mu(n)$, часто встречающуюся в теории чисел. Для $n \in \{1, 2, 3, \ldots\}$

положим

$$\mu(n)=\begin{cases}0, & \text{если } n \text{ делится на полный квадрат натурального числа, большего 1;}\\ (-1)^k, & \text{если } n \text{ равно произведению } k \text{ различных простых чисел.}\end{cases}$$

Таким образом, $1=\mu(1)=\mu(6)=\mu(221)=\mu(1155)$, $0=\mu(9)=\mu(98)$, $-1=\mu(2)=\mu(97)=\mu(30)=\mu(105)$. Основное свойство функции μ заключается в том, что сумма ее значений по всем делителям некоторого целого положительного числа n равна 1, если $n=1$, и 0 в остальных случаях. Действительно, если $n=p_1^{a_1}\dots p_s^{a_s}$ — разложение на простые множители и $s\geqslant 1$, то

$$\sum_{d\mid n}\mu(d)=\sum_{\substack{\text{всевозможные}\\ \varepsilon_i=0 \text{ или } 1,\ i=1,\ \dots,\ s}}\mu\left(p_1^{\varepsilon_1}\dots p_s^{\varepsilon_s}\right)=$$

$$=\sum(-1)^{\sum\varepsilon_i}=(1-1)^s=0.$$

Теперь утверждается, что в $\mathbb{Q}[[X]]$ имеет место формальное тождество

$$\exp(X)=\prod_{n=1}^{\infty}(1-X^n)^{-\mu(n)/n}\underset{\text{def}}{=}\prod_{n=1}^{\infty}B_{-\mu(n)/n}(-X^n).$$

(Сразу отметим, что это бесконечное произведение бесконечных рядов корректно определено (формально), так как n-й ряд в этом произведении начинается с $1-\mu(n)/nX^n$, т. е. не имеет членов со степенью X, меньшей n, кроме постоянного члена 1; поэтому для того, чтобы найти коэффициент для каждой заданной степени X, достаточно перемножить лишь конечное число рядов.) Для доказательства прологарифмируем правую часть. После приведения подобных членов с одинаковой степенью X получим

$$\log\prod_{n=1}^{\infty}(1-X^n)^{-\mu(n)/n}=-\sum_{n=1}^{\infty}\frac{\mu(n)}{n}\log(1-X^n)=$$

$$=\sum_{n=1}^{\infty}\frac{\mu(n)}{n}\sum_{m=1}^{\infty}\frac{X^{nm}}{m}=\sum_{j=1}^{\infty}\left[\frac{X^j}{j}\sum_{n\mid j}\mu(n)\right]$$

(j — прежнее mn). По доказанному выше основному свойству μ последний ряд равен X. Взяв экспоненту от обеих частей, получаем требуемое формальное тождество.

(В этом доказательстве несколько раз неявно использовался принцип, упоминавшийся при обсуждении $\log_p$. Его подробное изложение дано ниже в упр. 25. Согласно этому принципу, манипуляции с формальными степенными рядами как с функциями вещественных переменных законны, если все получающиеся ряды сходятся в некотором интервале около нуля.)

В p-адическом случае, рассматривая произведение $\prod_{n=1}^{\infty}(1-X^n)^{-\mu(n)/n}$, можно выделить все «нежелательные» сомножители. Под «нежелательными» подразумеваются сомножители, сходящиеся только на $D(p^{-1/(p-1)-})$, а не на $D(1^-)$. А именно, пусть $p\mid n$ и n не содержит полного квадрата >1. В этом случае $(1-X^n)^{-\mu(n)/n}$ сходится только для тех значений x, для которых

$$|x^n|_p=|x|_p^n\in D(r),$$

где

$$r=p^{-1/(p-1)}\left(\left|-\frac{\mu(n)}{n}\right|_p\right)^{-1}=p^{-1/(p-1)}|n|_p.$$

Например, если $n=p$, сходимость имеет место в точности тогда, когда

$$|x|_p<\left(p^{-1/(p-1)}\frac{1}{p}\right)^{1/p}=p^{-1/(p-1)}.$$

До тех пор пока $p\nmid n$, все в порядке, т. е. $(1-X^n)^{-\mu(n)/n}\in\mathbb{Z}_p[[X]]$, так как $-\mu(n)/n\in\mathbb{Z}_p$. (Напомним, что здесь и ниже $(1-X^n)^a$ — всего лишь краткое обозначение для $B_{a,p}(-X^n)=\sum_{i=0}^{\infty}a(a-1)\dots(a-i+1)(-X^n)^i/i!$.)

Поэтому определим новую функцию E_p, которую называют *экспонентой Артина — Хассе*, опуская все «плохие» сомножители в рассматриваемом бесконечном произведении (это похоже на отбрасывание эйлерова

множителя при определении p-адической дзета-функции в гл. II):

$$E_p(X) \underset{\text{def}}{=} \prod_{\substack{n=1 \\ p \nmid n}}^{\infty} (1-X^n)^{-\mu(n)/n} \in \mathbb{Q}[[X]].$$

Так как каждый ряд $B_{-\mu(n)/n,\,p}(-X^n)$ принадлежит $1+X^n\mathbb{Z}_p[[X]]$, их бесконечное произведение определено (для того чтобы получить коэффициент при заданной степени X, необходимо перемножить лишь конечное число сомножителей) и лежит в $1+X\mathbb{Z}_p[[X]]$.

Легко найти более простое выражение для $E_p(X)$. Для этого воспользуемся следующим свойством функции μ:

$$\sum_{d \mid n,\ p \nmid d} \mu(d) = \begin{cases} 1, & \text{если } n \text{ равно степени } p, \\ 0 & \text{в противном случае.} \end{cases}$$

Это свойство выводится непосредственно из ранее доказанного свойства μ для $n/p^{\operatorname{ord}_p n}$ вместо n. Рассмотрим $E_p(X)$ над $\mathbb{R}$ (или над $\mathbb{C}$). Логарифмируя, мы получим, как и выше:

$$\log E_p(X) = -\sum_{\substack{n=1 \\ p \nmid n}}^{\infty} \frac{\mu(n)}{n} \sum_{m=1}^{\infty} \frac{X^{mn}}{m} =$$

$$= \sum_{j=1}^{\infty} \left[\frac{X^j}{j} \sum_{n \mid j,\ p \nmid n} \mu(n) \right] = \sum_{m=0}^{\infty} \frac{X^{p^m}}{p^m}.$$

Отсюда следует равенство формальных рядов в $\mathbb{Q}[[X]]$:

$$E_p(X) = \exp\left(X + \frac{X^p}{p} + \frac{X^{p^2}}{p^2} + \frac{X^{p^3}}{p^3} + \ldots\right).$$

Важнейшее отличие $E_p(X)$ от $\exp_p(X)$ состоит в том, что $E_p(X) \in \mathbb{Z}_p[[X]]$. Поэтому $E_p(X)$ сходится на

$D(1^-)$. Можно показать (см. упр. 11 к § IV.4), что это в точности диск сходимости, т. е. ряд не сходится на $D(1)$.

В заключение этого параграфа докажем одну полезную общую лемму, принадлежащую Дворку.

Лемма 3. *Пусть* $F(X) = \sum a_i X^i \in 1 + X\mathbb{Q}_p[[X]]$. *Тогда* $F(X) \in 1 + X\mathbb{Z}_p[[X]]$ *в том и только том случае, когда* $F(X^p)/(F(X))^p \in 1 + pX\mathbb{Z}_p[[X]]$.

Доказательство. Пусть $F(X) \in 1 + X\mathbb{Z}_p[[X]]$. Тогда из сравнений $(a+b)^p \equiv a^p + b^p \pmod p$ и $a^p \equiv a \pmod p$ для $a \in \mathbb{Z}_p$ следует, что $(F(X))^p = F(X^p) + pG(X)$ при некотором $G(X) \in X\mathbb{Z}_p[[X]]$. Поэтому

$$\frac{F(X^p)}{(F(X))^p} = 1 - \frac{pG(X)}{(F(X))^p} \in 1 + pX\mathbb{Z}_p[[X]],$$

так как $(F(X))^p \in 1 + X\mathbb{Z}_p[[X]]$, а значит, и обратный к нему ряд лежит в этом же множестве (см. упр. 3).

В другую сторону, пусть

$$F(X^p) = (F(X))^p G(X), \quad G(X) \in 1 + pX\mathbb{Z}_p[[X]],$$
$$G(X) = \sum b_i X^i, \qquad F(X) = \sum a_i X^i.$$

Докажем по индукции включение $a_i \in \mathbb{Z}_p$. По предположению $a_0 = 1$. Допустим, что $a_i \in \mathbb{Z}_p$ при $i < n$. Тогда, приравнивая коэффициенты при X^n в обеих частях равенства, получим соотношение

$$\left.\begin{matrix} a_{n/p}, & \text{если } p \text{ делит } n \\ 0 & \text{в противном случае} \end{matrix}\right\} =$$

$$= \text{коэффициент при } X^n \text{ в } \left(\sum_{i=0}^{n} a_i X^i\right)^p \left(1 + \sum_{i=1}^{n} b_i X^i\right).$$

Разложим произведение справа по степеням X, а затем вычтем из него $a_{n/p}X^n$, если $p \mid n$ (напомним, что $a_{n/p} \equiv a_{n/p}^p \pmod p$). У полученного многочлена коэффициент при X^n обращается в нуль. С другой стороны, он равен сумме, одно из слагаемых которой есть pa_n,

а остальные принадлежат $p\mathbb{Z}_p$. Отсюда можно заключить, что $pa_n \in p\mathbb{Z}_p$, т. е. $a_n \in \mathbb{Z}_p$. □

Леммой Дворка можно воспользоваться для прямого доказательства (не опирающегося на разложение в бесконечное произведение) того, что все коэффициенты формального степенного ряда $E_p(X) = e^{X+(X^p/p)+(X^{p^2}/p^2)+\dots}$ лежат в $\mathbb{Z}_p$ (см. ниже упр. 17).

Лемма Дворка, которая на первый взгляд кажется странноватой, в действительности представляет собой образец одного глубокого явления, свойственного p-адическому анализу. Она утверждает, что если известно нечто о $F(X^p)/(F(X))^p$, то известно нечто и о F. Отношение $F(X^p)/(F(X))^p$ измеряет разницу между возведением X в степень p с последующим применением F и между применением F с последующим возведением в степень p, т. е. измеряет, насколько F коммутирует с возведением в p-ю степень. Отображение возведения в степень p играет фундаментальную роль, как мы уже видели в другой p-адической ситуации (ср. с параграфом о конечных полях). Итак, лемма Дворка утверждает, что если F «коммутирует по модулю p» с возведением в степень p, т. е. $F(X^p)/(F(X))^p = 1 + p \cdot \Sigma(p\text{-адическое целое})X^i$, то F имеет целые p-адические коэффициенты.

Продемонстрируем одно приложение этой леммы к функции, которая нам встретится в доказательстве теоремы Дворка о рациональности дзета-функции. Отметим прежде всего следующее обобщение леммы 3. Пусть $F(X, Y) = \Sigma a_{m,n} X^n Y^m$ — формальный степенной ряд от *двух* переменных X и Y с постоянным членом 1, т. е.

$$F(X, Y) \in 1 + X\mathbb{Q}_p[[X, Y]] + Y\mathbb{Q}_p[[X, Y]].$$

Тогда все $a_{m,n}$ принадлежат $\mathbb{Z}_p$ в том и только том слчуае, когда

$$F(X^p, Y^p)/(F(X, Y))^p \in$$
$$\in 1 + pX\mathbb{Z}_p[[X, Y]] + pY\mathbb{Z}_p[[X, Y]].$$

Доказывается это в точности так же, как лемма 3.

Определим теперь ряд $F(X, Y)$ из $\mathbb{Q}[[X, Y]]$ следующим образом:

$$F(X, Y) = B_{X,p}(Y)B_{(X^p-X)/p,p}(Y^p)B_{(X^{p^2}-X^p)/p^2,p}(Y^{p^2})\dots$$
$$\dots B_{(X^{p^n}-X^{p^{n-1}})/p^n,p}(Y^{p^n})\dots =$$
$$= (1+Y)^X(1+Y^p)^{(X^p-X)/p}(1+Y^{p^2})^{(X^{p^2}-X^p)/p^2}\dots$$
$$\dots(1+Y^{p^n})^{(X^{p^n}-X^{p^{n-1}})/p^n}\dots =$$
$$= \sum_{i=0}^{\infty} \frac{X(X-1)\dots(X-i+1)}{i!}Y^i \times$$
$$\times \prod_{n=1}^{\infty}\left(\sum_{i=0}^{\infty}\frac{X^{p^n}-X^{p^{n-1}}}{p^n}\left(\frac{X^{p^n}-X^{p^{n-1}}}{p^n}-1\right)\dots\right.$$
$$\left.\dots\left(\frac{X^{p^n}-X^{p^{n-1}}}{p^n}-i+1\right)\frac{Y^{ip^n}}{i!}\right).$$

Этот ряд определен корректно, поскольку для того, чтобы найти его коэффициент при любом X^nY^m, достаточно перемножить лишь конечное число сомножителей. Кроме того, ряд $F(X, Y) = \Sigma a_{m,n}X^nY^m$ лежит в $1 + X\mathbb{Q}_p[[X, Y]] + Y\mathbb{Q}_p[[X, Y]]$. Используя отмеченное выше обобщение леммы 3, докажем, что $a_{m,n} \in \mathbb{Z}_p$. А именно,

$$\frac{F(X^p, Y^p)}{(F(X, Y))^p} =$$
$$= \frac{(1+Y^p)^{X^p}(1+Y^{p^2})^{(X^{p^2}-X^p)/p}(1+Y^{p^3})^{(X^{p^3}-X^{p^2})/p^2}\dots}{(1+Y)^{pX}(1+Y^p)^{X^p-X}(1+Y^{p^2})^{(X^{p^2}-X^p)/p}\dots} =$$
$$= \frac{(1+Y^p)^X}{(1+Y)^{pX}}.$$

Поэтому достаточно показать, что $(1+Y^p)^X/(1+Y)^{pX}$ содержится в $1 + pX\mathbb{Z}_p[[X, Y]] + pY\mathbb{Z}_p[[X, Y]]$. Применив лемму 3 в другом направлении к ряду $1 + Y \in 1 + Y\mathbb{Z}_p[[Y]]$, получим

$$(1+Y^p)/(1+Y)^p = 1 + pYG(Y), \quad G(Y) \in \mathbb{Z}_p[[Y]].$$

Отсюда

$$\frac{(1+Y^p)^X}{(1+Y)^{pX}} = (1+pYG(Y))^X = \sum_{i=0}^{\infty} \frac{X(X-1)\dots(X-i+1)}{i!} p^i (YG(Y))^i$$

и последний ряд, очевидно, лежит в $1+pX\mathbb{Z}_p[[X, Y]]+pY\mathbb{Z}_p[[X, Y]]$. Из этого мы заключаем, что $F(X, Y) \in \mathbb{Z}_p[[X, Y]]$.

Упражнения

1. Найдите точный диск сходимости (указывая при этом, замкнут он или открыт) для следующих рядов. (В пунктах (v) и (vi) $\log_p$ обозначает классический логарифм по основанию p; а ζ в (vii) — примитивный корень степени p из 1. Скобки [ ] означают взятие целой части.)

(i) $\sum n!\, X^n$; (iii) $\sum p^n X^n$; (v) $\sum p^{[\log_p n]} X^n$;

(ii) $\sum p^{n[\log n]} X^n$; (iv) $\sum p^n X^{p^n}$; (vi) $\sum p^{[\log_p n]} X^{n/n}$;

(vii) $\sum (\zeta-1)^n X^n/n!$.

2. Докажите, что если $\sum a_n$ и $\sum b_n$ сходятся соответственно к a и b (где a_i, b_i, a, $b \in \Omega$), то $\sum c_n$ сходится к ab, где $c_n = \sum_{i=0}^{n} a_i b_{n-i}$.

3. Докажите, что элементы множества $1+X\mathbb{Z}_p[[X]]$ образуют группу по умножению. Пусть D — некоторый открытый или замкнутый диск в Ω с центром в 0. Докажите, что множество $\{f \in 1+X\Omega[[X]] \mid f$ сходится на $D\}$ замкнуто относительно умножения, но не является группой. Покажите, что при фиксированном λ множество рядов $f(X) = 1 + \sum_{i=1}^{\infty} a_i X^i$, для которых $\operatorname{ord}_p a_i - \lambda i$ больше 0 при всех $i = 1, 2, \dots$ и стремится к ∞ при $i \to \infty$, есть мультипликативная группа. Далее, пусть $f_j \in 1+X\mathbb{Z}_p[[X]]$, $j = 1, 2, 3, \dots$, а $f(X) = \prod_{j=1}^{\infty} f_j(X^j)$. Проверьте включение $f(X) \in 1+X\mathbb{Z}_p[[X]]$. Предположим, что каждое f_j сходится на замкнутом единичном диске $D(1)$. Сходится ли тогда $f(X)$ на $D(1)$ (приведите доказательство или контрпример)? Если все непостоянные коэффициенты для всех f_j делятся на p, то меняется ли от этого ответ (дайте доказательство или контрпример)?

4. Пусть $\{a_n\} \subset \Omega$ — некоторая последовательность и $p^n \mid a_n \mid_p \to 0$. Докажите, что

$$\sum_{n=0}^{\infty} a_n \frac{n!}{x(x+1)(x+2)\dots(x+n)}$$

сходится при всех $x \in \Omega$, не лежащих в $\mathbb{Z}_p$. Что можно сказать о случае, когда $x \in \mathbb{Z}_p$?

5. Докажите существование, единственность и непрерывность функции f: $\Omega - \{0\} \to \Omega$, для которой

$$f(x) = \log_p x, \text{ если } |x-1|_p < 1; \quad f(p) = 0;$$
$$f(xy) = f(x) + f(y) \quad \text{для всех } x, y \in \Omega - \{0\}.$$

Эта функция называется *логарифмической функцией Ивасавы* и также обозначается через $\log_p$. Покажите, что f нельзя доопределить по непрерывности в 0. (Именно эта функция $\log_p$ уже встречалась нам ранее в формуле для $L_{\chi, p}(1)$ из § II.7.)

6. Пусть i — квадратный корень из -1 в $\overline{\mathbb{Q}}_p$ (на самом деле i лежит в $\mathbb{Q}_p$, если $p \not\equiv 3 \pmod 4$ и $p \neq 2$). Докажите, что $\exp_p(ix) = \cos_p x + i \sin_p x$ для $x \in D(p^{-1/(p-1)-})$.

7. Покажите, что 2-адический порядок рационального числа

$$2 + 2^2/2 + 2^3/3 + 2^4/4 + 2^5/5 + \dots + 2^n/n$$

стремится к бесконечности с ростом n. Постарайтесь дать хорошую оценку этому 2-адическому порядку в зависимости от n. Можете ли вы придумать полностью элементарное доказательство (без использования p-адического анализа) этого факта, который формулируется совершенно элементарно?

8. Найдите ошибку в следующем «доказательстве» иррациональности числа π, которое слишком прекрасно, чтобы быть верным. Пусть $\pi = a/b$, а $p \neq 2$ — простое число, не делящее a. Тогда

$$0 = \sin(pb\pi) = \sin(pa) = \sum_{n=0}^{\infty} (-1)^n (pa)^{2n+1}/(2n+1)! \equiv pa \pmod{p^2},$$

что невозможно.

9. Найдите ошибку в следующем «доказательстве» трансцендентности e. Предположим, что e алгебраично. Тогда $e-1$ также алгебраично. Возьмем простое число $p \neq 2$, не делящее ни числитель, ни знаменатель никакого коэффициента минимальных многочленов для e и $e-1$ над $\mathbb{Q}$. Тогда $|e|_p = |e-1|_p = 1$. Поэтому $1 = |e-1|_p^p = |(e-1)^p|_p = \left| e^p - 1 - \sum_{i=1}^{p-1} \binom{p}{i} (-e)^i \right|_p$. В последней сумме все биномиальные коэффициенты делятся на p, а $|-e|_p = 1$.

Следовательно, $1=|e^p-1|_p=\left|\sum_{n=1}^{\infty} p^n/n!\right|_p$, что невозможно, так как каждое слагаемое в данной сумме имеет $|\ |_p<1$.

10. (a) Покажите, что биномиальные ряды для $(1-p/(p+1))^{-n}$ (где n — целое положительное рациональное число) и для $(1+(p^2+2mp)/m^2)^{1/2}$ (где m — целое рациональное $>(\sqrt{2}+1)p$ и $p\nmid m$) сходятся к одному и тому же рациональному числу независимо от того, рассматриваем ли мы эту сумму как сумму вещественных или как сумму p-адических чисел.

(b) Пусть $p\geqslant 7$, а $n=(p-1)/2$. Покажите, что $(1+p/n^2)^{1/2}$ дает контрпример к не-теореме 1.

11. Докажите, что для любого целого неотрицательного k p-адическое число $\sum_{n=0}^{\infty} n^k p^n$ лежит в $\mathbb{Q}$.

12. Докажите следующее равенство в $\mathbb{Q}_3$:

$$\sum_{n=1}^{\infty}(-1)^n\frac{3^{2n}}{n4^{2n}}=2\cdot\sum_{n=1}^{\infty}\frac{3^{2n}}{n4^n}.$$

13. Покажите, что диск сходимости степенного ряда $f(X)=\sum a_nX^n$ содержится в диске сходимости формальной производной этого ряда $f'(X)=\sum na_nX^{n-1}$. Постройте пример, в котором эти области сходимости не совпадают.

14. Докажите, что $\exp_p X$, $\sin_p X/X$ и $\cos_p X$ не имеют нулей в своей области сходимости, а $E_p(X)$ не имеет нулей на $D(1^-)$.

15. Найдите коэффициенты ряда $E_p(X)$ при X^i для $i\leqslant 4$ и $p=2$, 3.

16. Найдите коэффициенты всех членов ряда $E_p(X)$ вплоть до X^{p-1}. Найдите также коэффициент при X^p. Какой теореме элементарной теории чисел соответствует тот факт, что коэффициент при X^p лежит в $\mathbb{Z}_p$?

17. Используя лемму Дворка, докажите другим способом, что все коэффициенты ряда $E_p(X)$ принадлежат $\mathbb{Z}_p$.

18. Пусть $f(X)=\exp_p\left(\sum_{i=0}^{\infty} b_iX^{p^i}\right)$, $b_i\in\mathbb{Q}_p$. Используя лемму Дворка, докажите, что $f(X)\in 1+X\mathbb{Z}_p[[X]]$ тогда и только тогда, когда $b_{i-1}-pb_i\in p\mathbb{Z}_p$ для всех $i=0$, 1, 2, ... (где $b_{-1}\overset{\text{def}}{=}0$).

19. (a) Приведите пример бесконечной суммы ненулевых рациональных чисел, которая сходится по норме $|\ |_p$ при *всех* простых p, а также как сумма вещественных чисел (т. е. по норме $|\ |_\infty=|\ |$).

(b) Может ли такая сумма сходиться к некоторому рациональному числу по какой-нибудь из норм $|\ |_p$ или $|\ |_\infty$?

20. Возьмем теперь вместо степенного ряда некоторую функцию $f\colon \Omega\to\Omega$. Копируя известное определение из классического анализа, скажем, что эта функция *дифференцируема* в точке $a\in\Omega$, если существует предел $(f(x)-f(a))/(x-a)$ при $|x-a|_p\to 0$. Пусть $f(X)=\sum_{n=0}^{\infty} a_nX^n$ — некоторый степенной ряд. Докажите прежде всего его дифференцируемость в каждой точке диска сходимости. Кроме того, покажите, что это дифференцирование можно производить почленно, т. е. его производная в каждой точке a диска сходимости равна $\sum_{n=1}^{\infty} na_na^{n-1}$. Иначе говоря, ряд, соответствующий производной, совпадает с формальной производной степенного ряда.

21. Используя определение дифференцируемости из предыдущего упражнения, постройте пример всюду дифференцируемой функции $f\colon \Omega\to\Omega$, производная которой тождественно равна 0, а сама эта функция не локально постоянна (подробности о локально постоянных функциях см. в начале § II.3). Более того, эту функцию можно выбрать так, чтобы она обращалась в нуль вместе со всеми производными при $x=0$, но не была постоянной ни в какой окрестности 0. Такая функция подобна замечательной функции e^{-1/x^2} из классического анализа, которая не равна своему ряду Тейлора (тождественно равному нулю) в окрестности начала координат.

22. Теорема о среднем значении из математического анализа в применении к функции $f\colon \mathbb{R}\to\mathbb{R}$, $f(x)=x^p-x$, на интервале $\{x\in\mathbb{R}\mid |x|\leqslant 1\}$ утверждает, что

$$f'(\alpha)=0 \text{ для некоторого } \alpha\in\mathbb{R},\ |\alpha|\leqslant 1,$$

так как $f(1)=f(-1)=0$. (На самом деле $\alpha=\pm(1/p)^{1/(p-1)}$ при $p\neq 2$ и $\alpha=1/2$ при $p=2$.) Останется ли это верным, если $\mathbb{R}$ заменить на Ω, а $|\ |$ на $|\ |_p$?

23. Определим функцию $f\colon \mathbb{Q}_p\to\mathbb{Q}_p$ сопоставлением $x=\sum a_np^n\longmapsto\sum g(a_n)p^n$, где $\sum a_np^n$ есть p-адическое разложение числа x, а $g\colon \{0, 1, \ldots, p-1\}\to\mathbb{Q}_p$ — произвольная функция. Докажите непрерывность f. Пусть теперь $g(a)=a^2$, а $p\neq 2$. Докажите, что f *не* дифференцируема.

24. Докажите включение

$$(1+X)^{p^N}-1\in p^j\mathbb{Z}[X]+X^{p^N-j+1}\mathbb{Z}[X]$$

для любого натурального N и любого $j=1, 2, \ldots, N$. Предположим, что a/b — некоторое рациональное число с $|a/b|_p\leqslant 1$ и мы хотим найти первые M коэффициентов (для достаточного большого M) степенного ряда $(1+X)^{a/b}$ с определенной p-адической точностью. Для решения этой задачи предложите какой-нибудь простой алгоритм (например, программу для ЭВМ). (Все операции

при этом должны выполняться в $\mathbb{Z}/p^n\mathbb{Z}$, а не в $\mathbb{Q}$, так как машинные вычисления обычно гораздо проще производить в первом случае.)

25. Пусть R — некоторое кольцо. Определим кольцо $R[[X_1, \ldots, X_n]]$ (или, короче, $R[[X]]$) формальных степенных рядов от n переменных как множество «последовательностей» $\{r_{i_1, \ldots, i_n}\}$ элементов кольца R, занумерованных наборами n целых неотрицательных чисел $i_1, \ldots, i_n$ (каждая такая последовательность интерпретируется как ряд $\sum r_{i_1, \ldots, i_n} X_1^{i_1} \ldots X_n^{i_n}$ (или, короче, $\sum r_i X^i$), с операциями сложения и умножения, заданными обычным способом. Точнее, $\{r_{i_1, \ldots, i_n}\} + \{s_{i_1, \ldots, i_n}\} = \{t_{i_1, \ldots, i_n}\}$, где $t_{i_1, \ldots, i_n} = r_{i_1, \ldots, i_n} + s_{i_1, \ldots, i_n}$, а $\{r_{i_1, \ldots, i_n}\} \cdot \{s_{i_1, \ldots, i_n}\} = \{t_{i_1, \ldots, i_n}\}$, где $t_{i_1, \ldots, i_n} = \sum r_{j_1, \ldots, j_n} s_{k_1, \ldots, k_n}$, причем суммирование производится по всем парам наборов $j_1, \ldots, j_n$ и $k_1, \ldots, k_n$ с $j_1 + k_1 = i_1$, $j_2 + k_2 = i_2$, $\ldots$, $j_n + k_n = i_n$.

Для каждого ненулевого степенного ряда f определена минимальная степень ненулевых членов $\deg f$: это наименьшее d, для которого существует не равное нулю $r_{i_1, \ldots, i_n}$ с $i_1 + i_2 + \ldots + i_n = d$. Фиксируя некоторое положительное вещественное $\rho < 1$, можно определить на $R[[X]]$ так называемую *X-адическую топологию*, индуцированную *X-адической нормой*

$$|f|_X \underset{\text{def}}{=} \rho^{\deg f} \quad (|0|_X = 0 \text{ по определению}).$$

(1) Покажите, что $|\ |_X$ превращает $R[[X]]$ в неархимедово метрическое пространство (см. самое первое определение в § I.1; под «неархимедовостью» здесь, конечно, понимается выполнение неравенства $d(x, y) \leqslant \max(d(x, z), d(z, y))$, соответствующего третьему свойству нормы). Что означает неравенство $|f|_X < 1$?

(2) Покажите, что $R[[X]]$ полно относительно $|\ |_X$.

(3) Установите, что бесконечное произведение рядов $f_j \in R[[X]]$ сходится тогда и только тогда, когда $|f_j - 1|_X \to 0$ (где 1 обозначает постоянный степенной ряд $\{r_{i_1, \ldots, i_n}\}$ с $r_{0, \ldots, 0} = 1$ и остальными $r_{i_1, \ldots, i_n} = 0$). Поэтому, например, имеет смысл тот ужасный степенной ряд, который определен в конце § 2.

(4) Пусть $f \in R[[X]]$. Обозначим через f_d ряд, полученный из f заменой всех коэффициентов $r_{i_1, \ldots, i_n}$ с $i_1 + \ldots + i_n > d$ на 0. Таким образом, f_d можно считать многочленом от n переменных. Пусть $g_1, \ldots, g_n \in R[[X]]$. Заметим, что $f_d(g_1(X), g_2(X), \ldots, g_n(X))$ определено при любом d, так как это всего лишь конечная сумма произведений степенных рядов. Докажите, что $\{f_d(g_1(X), \ldots, g_n(X))\}_{d=0, 1, 2 \ldots}$ является последовательностью Коши в $R[[X]]$, если $|g_j|_X < 1$ для $j = 1, \ldots, n$. Ее предел в этом случае обозначается через $f \circ g$.

(5) Рассмотрим теперь в качестве R поле вещественных чисел $\mathbb{R}$. Пусть f, f_d, $g_1, \ldots, g_n$ — такие же ряды, как и в (4), с $|g_j|_X < 1$. Кроме того, предположим, что f и все g_j сходятся абсолютно для всех значений $X_i = x_i$ из интервала $[-\varepsilon, \varepsilon] \subset \mathbb{R}$ при некотором $\varepsilon > 0$. Докажите, что тогда ряд $f \circ g$ сходится абсолютно для всех значений $X_i = x_i$ из (возможно, меньшего) иитервала $[-\varepsilon', \varepsilon']$ при некотором $\varepsilon' > 0$.

(6) В предположениях пункта (5) докажите, что $f \circ g$ — нулевой степенной ряд из $\mathbb{R}[[X]]$, если $f \circ g(x_1, \ldots, x_n) = 0$ при любых $x_1, \ldots, x_n \in [-\varepsilon', \varepsilon']$. (*Указание*: прежде всего покажите, что при данных предположениях о сходимости можно переставлять члены встречающихся рядов; затем сведите все к доказательству совпадения с нулевым степенным рядом всякого ряда из $\mathbb{R}[[X]]$, равного нулю при всех значеннях переменных из $[-\varepsilon', \varepsilon']$; последнее докажите индукцией по n.)

(7) Пусть $n = 3$. Будем писать X, Y, Z вместо X_1, X_2, X_3. Тогда примером к предыдущему могут служить ряды:

$$f(X, Y, Z) = \sum_{i=1}^{\infty} (-1)^{i+1} \left(\frac{X^i}{i} + \frac{Y^i}{i} - \frac{Z^i}{i} \right),$$

$$g_1(X, Y, Z) = X, \quad g_2(X, Y, Z) = Y, \quad g_3(X, Y, Z) = X + Y + XY.$$

Приведем еще один пример для $n = 2$:

$$f(X, Y) = \left(\sum_{i=1}^{\infty} (-1)^{i+1} X^i / i \right) - Y,$$

$$g_1(X, Y) = \sum_{i=1}^{\infty} \frac{X^i}{i!}, \quad g_2(X, Y) = X.$$

Объясните, как можно воспользоваться результатами пункта (6) при доказательстве основных свойств элементарных p-адических степенных рядов. (Постройте соответствующие f и g_j в одной или двух конкретных ситуациях.)

§ 3. МНОГОУГОЛЬНИКИ НЬЮТОНА В СЛУЧАЕ МНОГОЧЛЕНОВ

Пусть $f(X) = 1 + \sum_{i=1}^{n} a_i X^i \in 1 + X\Omega[X]$ — многочлен степени n с коэффициентами в Ω и постоянным членом 1. Рассмотрим на вещественной координатной плоскости последовательность точек

$$(0, 0), (1, \operatorname{ord}_p a_1), (2, \operatorname{ord}_p a_2), \ldots$$
$$\ldots, (i, \operatorname{ord}_p a_i), \ldots, (n, \operatorname{ord}_p a_n.)$$

(Если $a_i = 0$, то соответствующая точка пропускается либо считается лежащей «бесконечно» высоко над горизонтальной осью.) *Многоугольником Ньютона* многочлена $f(X)$ называется «выпуклая оболочка» этого множества точек, а именно самая высокая из выпуклых вниз ломаных, соединяющих точки $(0, 0)$ и $(n, \operatorname{ord}_p a_n)$ и проходящих ниже всех точек $(i, \operatorname{ord}_p a_i)$ или через них. «Механически» эта выпуклая оболочка строится

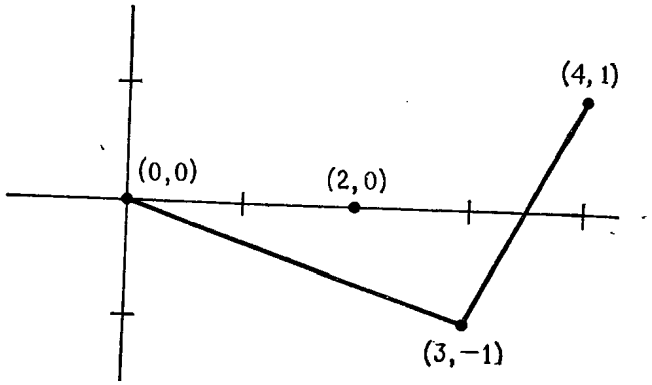


Рис. IV.1.

так. Возьмем вертикальную прямую, проходящую через точку $(0, 0)$, и начнем вращать ее вокруг $(0, 0)$ против часовой стрелки до тех пор, пока она не пройдет через одну из точек $(i, \operatorname{ord}_p a_i)$ с $i > 0$. Выберем среди таких точек последнюю[1]) $(i_1, \operatorname{ord}_p a_{i_1})$ и соединим ее отрезком с $(0, 0)$. Так находится первая сторона многоугольника Ньютона. Затем продолжим вращение этой линии вокруг точки $(i_1, \operatorname{ord}_p a_{i_1})$ до тех пор, пока она снова не пройдет через одну из последующих точек $(i, \operatorname{ord}_p a_i)$ $(i > i_1)$, выберем последнюю из этих точек $(i_2, \operatorname{ord}_p a_{i_2})$ и соединим ее отрезком с $(i_1, \operatorname{ord}_p, a_{i_1})$. Это вторая сторона искомого многоугольника. Далее продолжим вращение вокруг $(i_2, \operatorname{ord}_p a_{i_2})$ и т. д., пока не дойдем до $(n, \operatorname{ord}_p a_n)$.

На рис. 1 изображен пример многоугольника Ньютона для $f(X) = 1 + X^2 + {}^1/_3 X^3 + 3X^4$ в $\mathbb{Q}_3[X]$.

[1]) В смысле порядка индексов. — *Прим. перев.*

Вершинами многоугольника Ньютона называются точки $(i_j, \operatorname{ord}_p a_{i_j})$, в которых изменяется наклон. По определению наклон отрезка, соединяющего вершины (i, m) и (i', m'), равен отношению $(m' - m)/(i' - i)$. Под *«длиной наклона»* понимается разность $i' - i$, т. е. длина проекции соответствующей стороны многоугольника на горизонтальную ось.

Лемма 4. *В тех же обозначениях, что и выше, пусть* $f(X) = (1 - X/\alpha_1)\dots(1 - X/\alpha_n)$ *— разложение многочлена* $f(X)$ *на множители, где* $\alpha_i \in \Omega$ *— его корни. Положим* $\lambda_i = \operatorname{ord}_p 1/\alpha_i$. *Пусть* λ *— некоторый наклон соответствующего многоугольника Ньютона, имеющий длину* l. *Тогда среди всех чисел* λ_i *имеется в точности* l *равных* λ.

Иначе говоря, наклоны (длины наклонов) многоугольника Ньютона многочлена $f(X)$ равны p-адическим порядкам (кратностям) обратных корней для $f(X)$.

Доказательство. После подходящей нумерации корней можно считать, что $\lambda_1 \leqslant \lambda_2 \leqslant \dots \leqslant \lambda_n$. Пусть $\lambda_1 = \lambda_2 = \dots = \lambda_r < \lambda_{r+1}$. Тогда прежде всего утверждается, что первая сторона многоугольника Ньютона совпадает с отрезком, соединяющим $(0, 0)$ и $(r, r\lambda_1)$. Как известно, каждое a_i представимо в виде умноженного на $(-1)^i$ i-го симметрического многочлена от $1/\alpha_1, 1/\alpha_2, \dots, 1/\alpha_n$, т. е. суммы всевозможных произведений по i элементов из множеств чисел $1/\alpha_i$. Так как любое такое произведение имеет p-адический порядок не меньше $i\lambda_1$, то это верно и для a_i. Значит, каждая точка $(i, \operatorname{ord}_p a_i)$ находится либо *выше* точки $(i, i\lambda_1)$, либо совпадает с ней, т. е. лежит или выше, или на прямой, соединяющей точки $(0, 0)$ и $(r, r\lambda_1)$.

Рассмотрим теперь a_r. Существует единственное произведение из r чисел $1/\alpha_i$ с p-адическим порядком $r\lambda_1$, а именно $1/(\alpha_1 \alpha_2 \dots \alpha_r)$. Все остальные произведения из r элементов имеют p-адический порядок $> r\lambda_1$, так как в эти произведения входит по крайней мере один из элементов $\lambda_{r+1}, \lambda_{r+2}, \dots, \lambda_n$. Таким образом, a_r равно сумме числа с порядком $r\lambda_1$ и чисел с порядком $> r\lambda_1$. Поэтому $\operatorname{ord}_p a_r = r\lambda_1$ по «принципу равнобедренного треугольника».

Пусть теперь $i > r$. Как и выше, мы устанавливаем, что все произведения по i чисел из $1/\alpha_i$ имеют порядок $> i\lambda_1$. Следовательно, $\operatorname{ord}_p a_i > i\lambda_1$. Если вспомнить теперь, как строится многоугольник Ньютона, то сразу станет ясно, что его первая сторона совпадает с отрезком, соединяющим точки $(0, 0)$ и $(r, r\lambda_1)$.

Если $\lambda_s < \lambda_{s+1} = \lambda_{s+2} = \ldots = \lambda_{s+r} < \lambda_{s+r+1}$, то совпадение отрезка, соединяющего $(s, \lambda_1 + \lambda_2 + \ldots + \lambda_s)$ и $(s+r, \lambda_1 + \lambda_2 + \ldots + \lambda_s + r\lambda_{s+1})$, с одной из сторон многоугольника Ньютона, доказывается точно так же, и мы оставляем доказательство читателю. □

§ 4. МНОГОУГОЛЬНИКИ НЬЮТОНА В СЛУЧАЕ СТЕПЕННЫХ РЯДОВ

Пусть теперь $f(X) = 1 + \sum_{i=1}^{\infty} a_i X^i \in 1 + X\Omega[[X]]$ — некоторый степенной ряд[1]. Многочлен $f_n(X) = 1 + \sum_{i=1}^{n} a_i X^i \in 1 + X\Omega[X]$ называется n-й частичной суммой ряда $f(X)$. Многоугольник Ньютона для $f(X)$ определяется как «предел» многоугольников Ньютона для $f_n(X)$. Точнее, этот многоугольник строится по тому же рецепту, что и в случае многочленов: наносим на плоскость точки $(0, 0)$, $(1, \operatorname{ord}_p a_1), \ldots, (i, \operatorname{ord}_p a_i), \ldots$; вращаем вертикальную прямую вокруг $(0, 0)$, пока она не пройдет через некоторую точку $(i, \operatorname{ord}_p a_i)$, затем продолжаем вращение вокруг последней из этих точек и т. д. При этом возможны следующие три случая[2]).

(1) Получается многоугольник с бесконечным числом сторон конечной длины. Таков, например, многоугольник Ньютона ряда $f(X) = 1 + \sum_{i=1}^{\infty} p^{i^2} X^i$; он представляет собой ломаную, вписанную в правую половину параболы $y = x^2$ (рис. 2).

(2) Вращаемая прямая попадает в такое положение, при котором на ней оказывается сразу бесконечно много точек $(i, \operatorname{ord}_p a_i)$. В этом случае многоугольник Ньютона имеет конечное число сторон конечной длины и одну, а именно последнюю, — бесконечной длины. Например, многоугольник Ньютона ряда $f(X) = 1 + \sum_{i=1}^{\infty} X^i$ состоит из одного бесконечно длинного горизонтального луча из точки $(0, 0)$.

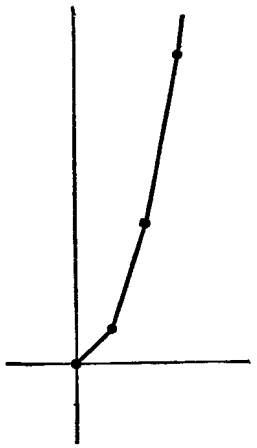


Рис. IV.2.

(3) Сама прямая, вращаемая вокруг некоторой точки, в какой-то момент еще не содержит ни одной из последующих точек $(i, \operatorname{ord}_p a_i)$, но при сколь угодно малом дальнейшем повороте она уже пройдет над некоторой из этих точек $(i, \operatorname{ord}_p a_i)$. Один из простейших примеров такого сорта дает ряд $f(X) = 1 + \sum_{i=1}^{\infty} pX^i$. В этом случае вертикаль, проходящую через $(0, 0)$, можно повернуть до горизонтального положения, но при любом дальнейшем вращении она пройдет над некоторыми точками $(i, 1)$. В подобных ситуациях в качестве последнего наклона многоугольника Ньютона берется точная верхняя грань всех наклонов, для которых соответствующая прямая проходит ниже всех последующих $(i, \operatorname{ord}_p a_i)$. В рассмотренном примере этот наклон равен 0 и многоугольник Ньютона состоит из одного горизонтального луча (рис. 3).

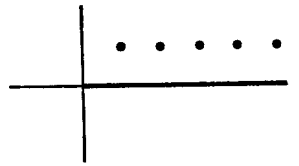


Рис. IV.3.

[1]) В этом параграфе ряды предполагаются отличными от многочленов, т. е. имеющими бесконечно много ненулевых коэффициентов. — *Прим. перев.*

[2]) Ниже всегда предполагается, что f имеет нетривиальный ($\neq \{0\}$) диск сходимости. — *Прим. перев.*

Многоугольник Ньютона в случае многочленов позволяет быстро определить, на каких радиусах расположены обратные корни. Ниже будет показано, что аналогично по многоугольнику Ньютона степенного ряда $f(X)$ можно судить о расположении нулей $f(X)$. Но вначале рассмотрим один особенно яркий пример.

Пусть

$$f(X)=1+\frac{X}{2}+\frac{X^2}{3}+\ldots+\frac{X^i}{i+1}+\ldots=-\frac{1}{X}\log_p(1-X).$$

Многоугольник Ньютона для $f(X)$ (см. рис. 4 в случае $p=3$) — это ломаная, последовательно соединяющая вершины $(0, 0)$, $(p-1, -1)$, $(p^2-1, -2)$, ..., $(p^j-1, -j)$, ... (На нем реализуется возможность (1)

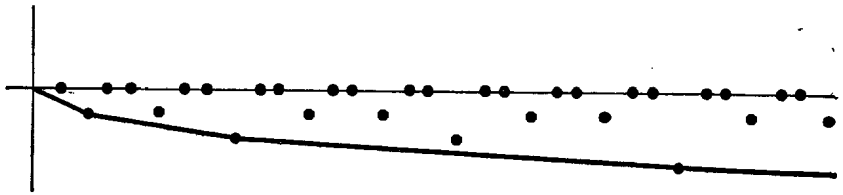


Рис. IV.4.

из приведенного выше списка.) Предположим, что для степенных рядов верен аналог леммы 4 из § 3. Тогда по виду этого многоугольника Ньютона следовало бы ожидать, что $f(X)$ имеет ровно $p^{j+1}-p^j$ нулей с p-адическим порядком $1/(p^{j+1}-p^j)$.

Но посмотрим, каковы же в действительности нули $-\log_p(1-X)/X$? Прежде всего, если $x=1-\zeta$, где ζ — примитивный корень из 1 степени p^{j+1}, то, как мы знаем из упр. 7 к § III. 4, $\mathrm{ord}_p x=1/(p^{j+1}-p^j)$. Отсюда $\log_p(1-x)=\log_p\zeta=0$ (см. обсуждение $\log_p$ в § 1). Тем самым найдены все предсказанные нули, так как существует $p^{j+1}-p^j$ примитивных корней степени p^{j+1} из 1. Имеет ли $f(X)$ нули еще где-нибудь на $D(1^-)$?

Пусть $x\in D(1^-)$ — один из таких нулей. Тогда для любого j точка $x_j=1-(1-x)^{p^j}\in D(1^-)$ также будет нулем, поскольку $\log_p(1-x_j)=p^j\log_p(1-x)=0$. Но при достаточно большом j справедливо включение $x_j\in D(p^{-1/(p-1)-})$, откуда $1-x_j=\exp_p(\log_p(1-x_j))=$

$=\exp_p 0=1$. Следовательно, $(1-x)^{p^j}=1$ и x совпадает с одним из рассмотренных выше нулей. Таким образом, форма многоугольника Ньютона полностью соответствует нашей информации о нулях ряда $\log_p(1-X)$.

Перейдем теперь к доказательству того, что многоугольник Ньютона играет для степенных рядов такую же роль, как и для многочленов. Но вначале установим один гораздо более простой результат, согласно которому по виду многоугольника Ньютона можно сразу узнать радиус сходимости соответствующего степенного ряда.

Лемма 5. *Пусть b — точная верхняя грань множества всех наклонов многоугольника Ньютона ряда $f(X)=1+\sum_{i=1}^{\infty}a_iX^i\in 1+X\,\Omega[[X]]$. Тогда его радиус сходимости равен p^b (b может быть бесконечным, и в этом случае $f(X)$ сходится на всем Ω).*

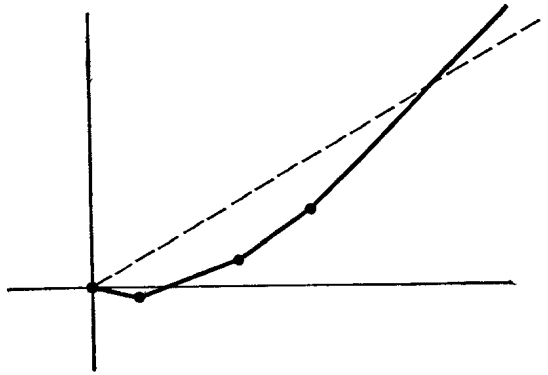


Рис. IV.5.

Доказательство. Пусть вначале $|x|_p<p^b$, т. е. $\mathrm{ord}_p x>-b$. Положим $\mathrm{ord}_p x=-b'$. Тогда $b'<b$ и $\mathrm{ord}_p(a_ix^i)=\mathrm{ord}_p a_i-ib'$. Но, очевидно (см. рис. 5), для достаточно больших i точка $(i, \mathrm{ord}_p a_i)$ лежит сколь угодно выше точки $(i, b'i)$. Иначе говоря, $\mathrm{ord}_p(a_ix^i)\to\infty$ и $f(X)$ сходится для таких $X=x$.

Пусть теперь $|x|_p>p^b$, т. е. $\mathrm{ord}_p x=-b'<-b$. Тогда по тем же соображениям имеется бесконечно

много значений i, для которых $\operatorname{ord}_p(a_i x^i) = \operatorname{ord}_p a_i - b'i$ отрицательно. Поэтому $f(x)$ не сходится. Отсюда мы заключаем, что радиус сходимости ряда $f(X)$ равен в точности p^b. □

Замечание. Эта лемма ничего не утверждает о сходимости или расходимости в точках, где $|x|_p = p^b$. Легко понять, что сходимость для таких x (т. е. «на граничной окружности») возможна лишь тогда, когда реализуется третий из перечисленных выше случаев, причем сходимость имеет место тогда и только тогда, когда расстояние по вертикали от $(i, \operatorname{ord}_p a_i)$ до последней (бесконечной) стороны стремится к ∞ при $i \to \infty$. Пример такого поведения дает ряд $f(X) = 1 + \sum_{i=1}^{\infty} p^i X^{p^i}$, многоугольник Ньютона которого совпадает с горизонтальным лучом из точки (0, 0). Этот ряд сходится, если $\operatorname{ord}_p x = 0$.

Прежде чем приступить к доказательству аналога леммы 4 для степенных рядов, сделаем одно заключительное замечание. Пусть $c \in \Omega$, $\operatorname{ord}_p c = \lambda$ и $g(X) = f(X/c)$. Тогда многоугольник Ньютона для g получается из соответствующего многоугольника для f поточечным вычитанием графика линейной функции $y = \lambda x$, т. е. прямой, проходящей через точку (0, 0) с наклоном λ. Действительно, если $f(X) = 1 + \sum a_i X^i$, а $g(X) = 1 + \sum b_i X^i$, то $\operatorname{ord}_p b_i = \operatorname{ord}_p (a_i/c^i) = \operatorname{ord}_p a_i - \lambda i$.

Лемма 6. *Предположим, что λ_1 — первый наклон многоугольника Ньютона ряда $f(X) = 1 + \sum_{i=1}^{\infty} a_i X^i \in 1 + X\,\Omega\,[[X]]$. Пусть $c \in \Omega$, $\operatorname{ord}_p c = \lambda \leqslant \lambda_1$. Предположим также, что $f(X)$ сходится на замкнутом диске $D(p^\lambda)$ (по лемме 5 это выполнено автоматически, если $\lambda < \lambda_1$ или многоугольник Ньютона для $f(X)$ имеет более одной стороны). Пусть*

$$g(X) = (1 - cX) f(X) \in 1 + X\,\Omega\,[[X]].$$

Тогда многоугольник Ньютона для $g(X)$ получается добавлением к отрезку, соединяющему точки (0, 0) и (1, λ), многоугольника Ньютона для $f(X)$, сдвинутого на 1 по горизонтали и на λ по вертикали. Иначе говоря, многоугольник Ньютона ряда $g(X)$ получается «присоединением» многоугольника Ньютона степенного ряда $f(X)$ к многоугольнику Ньютона многочлена $(1 - cX)$. Кроме того, если $f(X)$ имеет последний наклон λ_f и сходится на $D(p^{\lambda_f})$, то g также сходится на $D(p^{\lambda_f})$.

Доказательство. Прежде всего сведем доказательство к разбору специального случая $c = 1$, $\lambda = 0$. Предположим, что для этого случая лемма уже установлена и мы имеем $f(X)$ и $g(X)$, удовлетворяющие условиям. Тогда для $f_1(X) = f(X/G)$ и $g_1(X) = (1 - X) f_1(X)$ выполнены все те же условия, но с 1, 0, $\lambda_1 - \lambda$ вместо c, λ, λ_1 (см. замечание, непосредственно предшествующее формулировке леммы). По предположению, для f_1 и g_1 лемма верна, откуда мы находим форму многоугольника Ньютона для $g_1(X)$ (и устанавливаем сходимость g_1 на $D(p^{\lambda_f - \lambda})$, если f сходится на $D(p^{\lambda_f})$). Так как $g(X) = g_1(cX)$, то можно еще раз воспользоваться упомянутым замечанием, получить требуемое утверждение о многоугольнике Ньютона для $g(X)$ (см. рис. 6).

Итак, лемму 6 достаточно доказать при $c = 1$, $\lambda = 0$. Пусть $g(X) = 1 + \sum_{i=1}^{\infty} b_i X^i$. Тогда в силу равенства $g(X) = (1 - X) f(X)$ имеем $b_{i+1} = a_{i+1} - a_i$ для $i \geqslant 0$ ($a_0 = 1$). Поэтому

$$\operatorname{ord}_p b_{i+1} \geqslant \min(\operatorname{ord}_p a_{i+1}, \operatorname{ord}_p a_i),$$

причем имеет место равенство, если $\operatorname{ord}_p a_{i+1} \neq \operatorname{ord}_p a_i$ (по принципу равнобедренного треугольника). Так как обе точки $(i, \operatorname{ord}_p a_i)$ и $(i, \operatorname{ord}_p a_{i+1})$ лежат на или над стороной многоугольника Ньютона для $f(X)$, то же самое справедливо и для $(i, \operatorname{ord}_p b_{i+1})$. Если $(i, \operatorname{ord}_p a_i)$ — вершина, то $\operatorname{ord}_p a_{i+1} > \operatorname{ord}_p a_i$, а потому $\operatorname{ord}_p b_{i+1} = \operatorname{ord}_p a_i$. Отсюда следует, что многоугольник Ньютона имеет требуемый вид вплоть до своей последней вершины. Таким образом, остается разобрать случай, когда многоугольник Ньютона для $f(X)$ содержит последнюю бесконечно длинную сторону наклона λ_f, и показать, что в этом случае то же самое верно для $g(X)$; более

того, если $f(X)$ сходится на $D(p^{\lambda_f})$, то $g(X)$ сходится там же. В силу неравенства $\operatorname{ord}_p b_{i+1} \geqslant \min(\operatorname{ord}_p a_{i+1}, \operatorname{ord}_p a_i)$ из сходимости $f(X)$ немедленно следует сходимость $g(X)$ в той же области. Итак, необходимо исключить возможность, что многоугольник Ньютона ряда $g(X)$ имеет

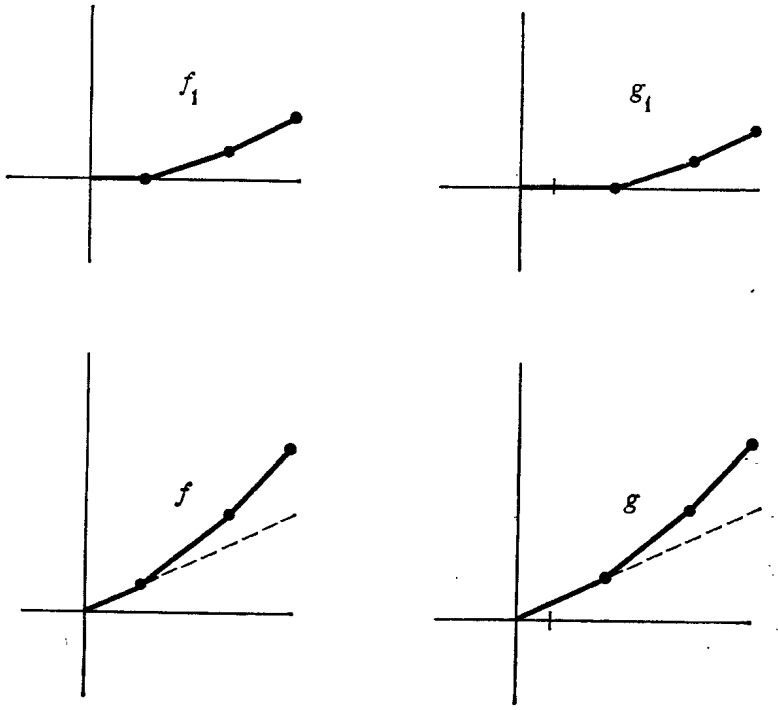


Рис. IV.6.

больший наклон λ_g, чем λ_f. Если бы это выполнялось, то при некотором достаточно большом i точка $(i+1, \operatorname{ord}_p a_i)$ лежала бы ниже соответствующей точки многоугольника Ньютона для $g(X)$. Поэтому мы имели бы $\operatorname{ord}_p b_j > \operatorname{ord}_p a_i$ для всех $j \geqslant i+1$. Из этого, во-первых, следует равенство $\operatorname{ord}_p a_{i+1} = \operatorname{ord}_p a_i$, потому что $a_{i+1} = b_{i+1} + a_i$; затем по тем же соображениям $\operatorname{ord}_p a_{i+2} = \operatorname{ord}_p a_{i+1}$ и т. д., $\operatorname{ord}_p a_j = \operatorname{ord}_p a_i$ для всех $j > i$. Но это противоречит предполагаемой сходимости $f(X)$ на $D(1)$. □

Лемма 7. *Пусть λ_1 — первый наклон многоугольника Ньютона ряда $f(X) = 1 + \sum_{i=1}^{\infty} a_i X^i \in 1 + X\Omega[[X]]$. Предположим, что $f(X)$ сходится на замкнутом диске $D(p^{\lambda_1})$, а, кроме того, линия, проходящая через (0, 0) с наклоном λ_1, содержит некоторую точку $(i, \operatorname{ord}_p a_i)$. (Оба эти условия автоматически выполнены, если многоугольник Ньютона имеет более одного наклона.) Тогда существует число $x \in \Omega$, для которого $\operatorname{ord}_p x = -\lambda_1$, а $f(x) = 0$.*

Доказательство. Для простоты рассмотрим вначале случай $\lambda_1 = 0$, а затем сведем доказательство леммы к этому случаю. Итак, пусть $\lambda_1 = 0$. Тогда $\operatorname{ord}_p a_i \geqslant 0$ для всех i и $\operatorname{ord}_p a_i \to \infty$ при $i \to \infty$. Пусть $N \geqslant 1$ равно наибольшему i, для которого $\operatorname{ord}_p a_i = 0$. (Очевидно, N есть длина первой стороны многоугольника Ньютона ряда $f(X)$, за исключением случая, когда этот многоугольник совпадает с горизонтальным лучом.) Пусть $f_n(X) = 1 + \sum_{i=1}^{n} a_i X^i$. По лемме 4 многочлен $f_n(X)$ при $n \geqslant N$ имеет в точности N корней $x_{n,1}, \ldots, x_{n,N}$ с $\operatorname{ord}_p x_{n,i} = 0$. Пусть $x_N = x_{N,1}$, а x_{n+1} при $n \geqslant N$ — любой из элементов $x_{n+1,1}, \ldots, x_{n+1,N}$ с минимальной нормой разности $|x_{n+1,i} - x_n|_p$. Утверждается, что $\{x_n\}$ — последовательность Коши и ее предел x обладает нужными свойствами.

Для $n \geqslant N$ обозначим через S_n множество корней многочлена $f_n(X)$ (с учетом их кратностей). Тогда при $n \geqslant N$ имеем

$$|f_{n+1}(x_n) - f_n(x_n)|_p = |f_{n+1}(x_n)|_p =$$

(так как $f_n(x_n) = 0$)

$$= \prod_{x \in S_{n+1}} \left|1 - \frac{x_n}{x}\right|_p = \prod_{i=1}^{N} \left|1 - \frac{x_n}{x_{n+1,i}}\right|_p =$$

(так как $|1 - x_n/x|_p = 1$, если $x \in S_{n+1}$ и $\operatorname{ord}_p x < 0$)

$$= \prod_{i=1}^{N} |x_{n+1,i} - x_n|_p \geqslant$$

(так как $|x_{n+1,i}|_p = 1$)

$$\geqslant |x_{n+1} - x_n|_p^N$$

в силу выбора x_{n+1}. Поэтому

$$|x_{n+1} - x_n|_p^N \leqslant |f_{n+1}(x_n) - f_n(x_n)|_p = |a_{n+1}x_n^{n+1}|_p = |a_{n+1}|_p.$$

Поскольку $|a_{n+1}|_p \to 0$ при $n \to \infty$, $\{x_n\}$ является последовательностью Коши. Пусть $x_n \to x \in \Omega$. Тогда $f(x) = \lim\limits_{n\to\infty} f_n(x)$. Но

$$|f_n(x)|_p = |f_n(x) - f_n(x_n)|_p = \\ = |x - x_n|_p \left| \sum_{i=1}^{n} a_i \frac{x^i - x_n^i}{x - x_n} \right|_p \leqslant |x - x_n|_p,$$

потому что $|a_i|_p \leqslant 1$ и $\left|(x^i - x_n^i)/(x - x_n)\right|_p = |x^{i-1} + x^{i-2}x_n + x^{i-3}x_n^2 + \ldots + x_n^{i-1}|_p \leqslant 1$. Следовательно, $f(x) = \lim\limits_{n\to\infty} f_n(x) = 0$. Это доказывает лемму при $\lambda_1 = 0$. Теперь легко вывести общий случай. Пусть $\pi \in \Omega$ — произвольное число с $\operatorname{ord}_p \pi = \lambda_1$. Заметим, что такое π существует: можно взять, например, корень степени i из a_i, для которого $(i, \operatorname{ord}_p a_i)$ лежит на прямой с наклоном λ_1, проходящей через $(0, 0)$. Пусть теперь $g(X) = f(X/\pi)$. Тогда $g(X)$ удовлетворяет условиям леммы с $\lambda_1 = 0$. Таким образом, по только что доказанному существует x_0 с $\operatorname{ord}_p x_0 = 0$, и $g(x_0) = 0$. Пусть $x = x_0/\pi$. Тогда $\operatorname{ord}_p x = -\lambda_1$ и $f(x) = f(x_0/\pi) = g(x_0) = 0$. □

Лемма 8. *Пусть ряд* $f(X) = 1 + \sum\limits_{i=1}^{\infty} a_i X^i \in 1 + X\Omega[[X]]$ *сходится к нулю при некотором* α. *Тогда ряд* $g(X) = 1 + \sum\limits_{i=1}^{\infty} b_i X^i$, *полученный делением ряда* $f(X)$ *на* $(1 - X/\alpha)$, *или, что то же самое, умножением на ряд* $1 + X/\alpha + X^2/\alpha^2 + \ldots + X^i/\alpha^i + \ldots$, *сходится на* $D(|\alpha|_p)$.

Доказательство. Пусть $f_n(X) = 1 + \sum\limits_{i=1}^{n} a_i X^i$. Очевидно,

$$b_i = 1/\alpha^i + a_1/\alpha^{i-1} + a_2/\alpha^{i-2} + \ldots + a_{i-1}/\alpha + a_i,$$

откуда

$$b_i\alpha^i = f_i(\alpha).$$

Следовательно, $|b_i\alpha^i|_p = |f_i(\alpha)|_p \to 0$ при $i \to \infty$, потому что $f(\alpha) = 0$. □

Теорема 14 (*p*-адическая подготовительная теорема Вейерштрасса). *Предположим, что ряд* $f(X) = 1 + \sum\limits_{i=1}^{\infty} a_i X^i \in 1 + X\Omega[[X]]$ *сходится на* $D(p^\lambda)$. *Пусть* N — *общая длина, если она конечна (т. е. если многоугольник Ньютона ряда* $f(X)$ *не имеет последней бесконечнодлинной стороны наклона* λ), *проекции на горизонтальную ось всех сторон с наклоном* $\leqslant \lambda$. *Если же многоугольник Ньютона для* $f(X)$ *имеет последний наклон* λ, *то положим* N *равным наибольшему* i, *для которого* $(i, \operatorname{ord}_p a_i)$ *лежит на последней стороне (существование такого* i *следует из сходимости* $f(X)$ *на* $D(p^\lambda)$). *Тогда найдутся такой многочлен* $h(X) \in 1 + X\Omega[X]$ *степени* N *и такой степенной ряд* $g(X) = 1 + \sum\limits_{i=1}^{\infty} b_i X^i$, *сходящийся и не обращающийся в нуль на* $D(p^\lambda)$, *что*

$$h(X) = f(X) \cdot g(X).$$

Многочлен $h(X)$ *определен однозначно этими свойствами, а его многоугольник Ньютона совпадает с многоугольником Ньютона ряда* $f(X)$ *вплоть до точки* $(N, \operatorname{ord}_p a_N)$.

Доказательство. Применим индукцию по N. Пусть вначале $N = 0$. Тогда нужно установить существование ряда $g(X)$, обратного к $f(X)$, его сходимость и необращение в нуль на $D(p^\lambda)$. Это утверждение было частью упр. 3 к § 2, но в силу его важности мы приведем здесь его доказательство для тех, кто пропустил это упражнение. Как обычно (см. доказательства лемм 6 и 7, а также замечание, предшествующее формулировке леммы 6), доказательство можно свести к случаю $\lambda = 0$.

Итак, пусть $f(X) = 1 + \sum a_i X^i$, $\operatorname{ord}_p a_i > 0$, $\operatorname{ord}_p a_i \to \infty$, $g(X) = 1 + \sum b_i X^i$. Из соотношения $f(X)\,g(X) = 1$ получается рекуррентная формула

$$b_i = -(b_{i-1}a_1 + b_{i-2}a_2 + \ldots + b_1 a_{i-1} + a_i), \quad i \geqslant 1,$$

из которой индукцией по i легко вывести неравенства $\mathrm{ord}_p b_i > 0$. Поэтому осталось показать, что $\mathrm{ord}_p b_i \to \infty$ при $i \to \infty$. Возьмем достаточно большое M. Выберем затем такое m, что $\mathrm{ord}_p a_i > M$ при $i > m$. Пусть

$$\varepsilon = \min(\mathrm{ord}_p a_1, \mathrm{ord}_p a_2, \ldots, \mathrm{ord}_p a_m) > 0.$$

Тогда утверждается, что $\mathrm{ord}_p b_i > \min(M, n\varepsilon)$ при $i > nm$. Отсюда, конечно, получается требуемое соотношение $\mathrm{ord}_p b_i \to \infty$. Утверждение докажем индукцией по n. Для $n = 0$ оно очевидно. Предположим, что $n \geqslant 1$, $i > nm$. По рекуррентной формуле

$$b_i = -(b_{i-1}a_1 + \ldots + b_{i-m}a_m + b_{i-(m+1)}a_{m+1} + \ldots + a_i).$$

Для членов $b_{i-j}a_j$ с $j > m$ имеет место неравенство $\mathrm{ord}_p(b_{i-j}a_j) \geqslant \mathrm{ord}_p a_j > M$, в то время как $\mathrm{ord}_p(b_{i-j}a_j) \geqslant \mathrm{ord}_p b_{i-j} + \varepsilon > \min(M, (n-1)\varepsilon) + \varepsilon$ при $j \leqslant m$ по индуктивному предположению (так как $i - j > (n-1)m$) и по определению ε. Поэтому все слагаемые в формуле для b_i имеют $\mathrm{ord}_p > \min(M, n\varepsilon)$. Это доказывает утверждение, а следовательно, и теорему при $N = 0$.

Предположим теперь, что $N \geqslant 1$ и теорема уже доказана для $N - 1$. Пусть $\lambda_1 \leqslant \lambda$ — первый наклон многоугольника Ньютона ряда $f(X)$. Применяя лемму 7, найдем α, для которого $f(\alpha) = 0$ и $\mathrm{ord}_p \alpha = -\lambda_1$. Положим

$$f_1(X) = f(X)\left(1 + \frac{X}{\alpha} + \frac{X^2}{\alpha^2} + \ldots + \frac{X^i}{\alpha^i} + \ldots\right) = 1 + \sum a_i' X^i \in 1 + X\Omega[[X]].$$

По лемме 8 ряд $f_1(X)$ сходится на $D(p^{\lambda_1})$. Пусть $c = 1/\alpha$, так что $f(X) = (1 - cX) f_1(X)$. Если бы первый наклон λ_1' многоугольника Ньютона для $f_1(X)$ был меньше λ_1, то по лемме 7 ряд $f_1(X)$ обладал бы корнем с p-адическим порядком $-\lambda_1'$, а тогда то же самое выполнялось бы и для $f(X)$, но, как легко проверить, это невозможно. Следовательно, $\lambda_1' \geqslant \lambda_1$ и мы находимся в условиях леммы 6 (с f_1, f, λ_1' и λ_1 вместо f, g, λ_1 и λ соответственно). Тогда по этой лемме $f_1(X)$ имеет тот же многоугольник Ньютона, что и $f(X)$, если только исключить у последнего сторону, соединяющую (0, 0) и $(1, \lambda_1)$. В частности, f и f_1 имеют одинаковые радиусы сходимости. Кроме того, даже в том случае, когда λ совпадает с последним наклоном многоугольника Ньютона ряда f (а поэтому и f_1), ряд f_1 сходится на $D(p^{\lambda})$, поскольку f сходится на $D(p^{\lambda})$ по предположению [1]).

Итак, $f_1(X)$ удовлетворяет требованиям теоремы с $N - 1$ вместо N. По индуктивному предположению можно найти такой многочлен $h_1(X) \in 1 + X\Omega[X]$ степени $N - 1$ и такой ряд $g(X) \in 1 + X\Omega[[X]]$, сходящийся и не обращающийся в нуль на $D(p^{\lambda})$, что

$$h_1(X) = f_1(X) \cdot g(X).$$

Умножим обе части последнего равенства на $(1 - cX)$ и положим $h(X) = (1 - cX) h_1(X)$. Тогда

$$h(X) = f(X) \cdot g(X)$$

и $h(X)$ и $g(X)$ обладают нужными свойствами.

Наконец, так как f имеет в точности N нулей в $D(p^{\lambda})$, из этого немедленно следует, что $h(X)$ единствен. Действительно, этот многочлен имеет степень N, постоянный член 1 и все N нулей ряда $f(X)$ являются также его нулями [2]). □

Следствие. *Если сторона многоугольника Ньютона ряда $f(X) \in 1 + X\Omega[[X]]$ имеет конечную длину N и наклон λ, то существует в точности N значений x [3]), для которых $f(x) = 0$ и $\mathrm{ord}_p x = -\lambda$.*

В качестве другого следствия теоремы 14 можно установить, что любой всюду сходящийся степенной ряд разлагается в бесконечное произведение линейных множителей $(1 - X/r)$ по всем своим нулям r. В частности, всюду сходящийся и нигде не обращающийся в нуль ряд должен быть постоянным (см. ниже упр. 13). В отличие от этого в вещественном и комплексном случае существуют непостоянные ряды без нулей, напри-

---

[1]) Это утверждение, обратное к сформулированному в конце леммы 6, доказывается по существу тем же методом. — *Прим. перев.*

[2]) Это рассуждение проходит, если все корни различны. Аккуратное доказательство требует индукции. — *Прим. перев.*

[3]) С учетом кратностей, которые позволяет определить предыдущая теорема. — *Прим. перев.*

мер ряд функции e^x (или более общий ряд $e^{h(x)}$, где h — любой всюду сходящийся степенной ряд). В комплексном анализе разложение в бесконечное произведение всюду сходящегося степенного ряда по его нулям сложнее, чем в p-адическом случае; при этом для получения «произведения Вейерштрасса» «целой» функции комплексного переменного необходимо вводить дополнительные экспоненциальные множители.

Таким образом, простой вид разложения в бесконечное произведение в p-адическом случае, существование которого следует из теоремы 14, возможен благодаря отсутствию всюду сходящихся экспоненциальных функций. Значит, тут нам с плохой сходимостью $\exp_p$ крупно повезло. Но в других обстоятельствах, скажем в теории p-адических дифференциальных уравнений, отсутствие хорошо сходящейся экспоненты очень усложняет жизнь.

Упражнения

1. Найдите многоугольник Ньютона для следующих многочленов:

(i) $1-X+pX^2$; (ii) $1-X^3/p^2$; (iii) $1+X^2+pX^4+p^3X^6$;

(iv) $\sum_{i=1}^{p} iX^{i-1}$; (v) $(1-X)(1-pX)(1-p^3X)$ (двумя способами);

(vi) $\prod_{i=1}^{p^2}(1-iX)$.

2. (a) Пусть $f(X)\in 1+X\mathbb{Z}_p[X]$ — многочлен, многоугольник Ньютона которого состоит из одного отрезка, соединяющего точки (0, 0) и (n, m). Покажите, что $f(X)$ неразложим в произведение двух многочленов положительной степени с коэффициентами в $\mathbb{Z}_p$, если n и m взаимно просты.

(b) Используя пункт (a), дайте другое доказательство критерия неприводимости Эйзенштейна (см. упр. 13 к § 1.5).

(c) Верно ли обратное к (a), т. е. всякий ли неприводимый многочлен имеет многоугольник Ньютона указанного типа (докажите или постройте контрпример)?

3. Пусть $f(X)\in 1+X\mathbb{Z}_p[X]$ — многочлен степени $2n$. Пусть нам известно, что для всякого обратного корня α многочлена $f(X)$ обратным корнем является также p/α (с той же кратностью). Что можно сказать о форме многоугольника Ньютона в этом случае?

Нарисуйте все возможные виды многоугольников Ньютона для таких $f(X)$ при $n=1, 2, 3, 4$.

4. Найдите многоугольники Ньютона следующих степенных рядов:

(i) $\sum_{i=0}^{\infty} X^{p^i-1}/p^i$; (ii) $\sum_{i=0}^{\infty}((pX)^i+X^{p^i})$;

(iii) $\sum_{i=0}^{\infty} i!X^i$; (iv) $\sum_{i=0}^{\infty} X^i/i!$;

(v) $(1-pX^2)/(1-p^2X^2)$; (vi) $(1-p^2X)/(1-pX)$;

(vii) $\prod_{i=0}^{\infty}(1-p^iX)$; (viii) $\sum_{i=0}^{\infty} p^{[i\sqrt{2}]}X^i$.

5. Покажите, что все наклоны сторон конечной длины многоугольника Ньютона для степенного ряда являются рациональными числами, но что наклон последней бесконечной стороны (если она существует) не обязательно таков (постройте пример).

6. Покажите, построив контрпример, что лемма 7 не верна, если опустить условие существования точки $(i, \operatorname{ord}_p a_i)$ с $i>0$ на прямой, проходящей через (0, 0) с наклоном λ_1.

7. Покажите, построив контрпример, что лемма 6 не верна, если опустить условие сходимости $f(X)$ на $D(p^\lambda)$.

8. Пусть $f(X)=1+\sum_{i=1}^{\infty} a_iX^i\in 1+X\Omega[[X]]$ — ряд, сходящийся на $D(p^\lambda)$. Докажите, что $\max_{x\in D(p^\lambda)}|f(x)|_p$ достигается на множестве точек x с $|x|_p=p^\lambda$, т. е. на «граничной окружности», и что p-адический порядок этого максимума равен

$$\min_{i=0,\,1,\,\ldots}(\operatorname{ord}_p a_i - i\lambda),$$

т. е. минимальному «расстоянию» по вертикали (которое может быть отрицательным) от прямой, проходящей через (0, 0) с наклоном λ, до точки $(i, \operatorname{ord}_p a_i)$.

9. Пусть $f(X)=\sum_{i=0}^{\infty} a_iX^i\in\mathbb{Z}_p[[X]]$. Предположим, что $f(X)$ сходится в *замкнутом* единичном диске $D(1)$. Кроме того, предположим, что по крайней мере два коэффициента a_i не делятся на p. Докажите, что $f(X)$ имеет нуль на $D(1)$.

10. Пусть $f(X)$ — степенной ряд сходящийся и имеющий бесконечно много нулей на $D(r)$. Покажите, что тогда $f(X)$ тождественно равен нулю.

11. Докажите, что $E_p(X)$ сходится только на $D(1^-)$ (т. е. не на всем $D(1)$). (*Указание*: воспользуйтесь упр. 9 и 10 и покажите, что если E_p имеет хотя бы один нуль, то их бесконечно много.)

12. Пусть $g(X)=h(X)/f(X)$, где $g(X)\in 1+X\Omega[[X]]$ и все коэффициенты этого ряда лежат в $D(1)$, а $h(X)$ и $f(X)\in 1+X\Omega[X]$ — два многочлена, не имеющие общих корней. Докажите, что все коэффициенты $h(X)$ и $f(X)$ также лежат в $D(1)$.

13. Пусть $f(X)\in 1+X\Omega[[X]]$ сходится всюду на Ω. Для любого вещественного λ обозначим через $h_\lambda(X)$ многочлен $h(X)$ из теоремы 14. Докажите, что $h_\lambda\to f$ при $\lambda\to\infty$ (т. е. каждый коэффициент многочлена h_λ стремится к соответствующему коэффициенту ряда f). Докажите, что если f не многочлен, то он имеет бесконечное число нулей (но не более чем счетное: $r_1, r_2, \ldots$) и $f(X)=\prod_{i=1}^{\infty}(1-X/r_i)$. В частности, не существует всюду сходящихся и нигде не обращающихся в нуль степенных рядов, кроме констант (в противоположность комплексному и вещественному случаям, где степенной ряд $e^{h(X)}$ всюду сходится и не имеет нулей для любого всюду сходящегося степенного ряда $h(X)$).

Глава V

РАЦИОНАЛЬНОСТЬ ДЗЕТА-ФУНКЦИИ СИСТЕМЫ ПОЛИНОМИАЛЬНЫХ УРАВНЕНИЙ НАД КОНЕЧНЫМ ПОЛЕМ

§ 1. ГИПЕРПОВЕРХНОСТИ И ИХ ДЗЕТА-ФУНКЦИИ

Пусть F — некоторое поле. Через $\mathbb{A}_F^n$ обозначим *n-мерное аффинное пространство над* F, т. е. множество упорядоченных наборов $(x_1, \ldots, x_n)$ по n элементов x_i из F. Пусть $f(X_1, \ldots, X_n)\in F[X_1, \ldots, X_n]$ — некоторый многочлен от n переменных $X_1, \ldots, X_n$. Под *аффинной гиперповерхностью*, заданной уравнением $f=0$, понимается множество

$$H_f \overset{\text{def}}{=} \{(x_1, \ldots, x_n)\in \mathbb{A}_F^n \mid f(x_1, \ldots, x_n)=0\}.$$

Число $n-1$ называется *размерностью* гиперповерхности H_f. Если H_f одномерна, т. е. $n=2$, она называется *аффинной кривой*.

Сопутствующим к понятию аффинного пространства является *проективное пространство*. Проективное пространство над F размерности n обозначается $\mathbb{P}_F^n$ и определяется как множество классов эквивалентности элементов из $\mathbb{A}_F^{n+1}-\{(0, 0, \ldots, 0)\}$ по отношению эквивалентности $(x_0, x_1, \ldots, x_n)\sim(x_0', x_1', \ldots, x_n')\Leftrightarrow\exists\lambda\in F^\times$, для которого $x_i'=\lambda x_i$, $i=0, \ldots, n$. Иначе говоря, множество $\mathbb{P}_F^n$ есть множество всех прямых в $\mathbb{A}_F^{n+1}$, проходящих через начало координат.

Пространство $\mathbb{A}_F^n$ можно вложить в $\mathbb{P}_F^n$ при помощи отображения $(x_1, \ldots, x_n)\longmapsto(1, x_1, \ldots, x_n)$. Образ $\mathbb{A}_F^n$ при этом отображении состоит из всех точек $\mathbb{P}_F^n$, лежащих вне «бесконечно удаленной гиперплоскости», которая есть множество классов эквивалентности упорядоченных наборов по $n+1$ элементов с нулевой x_0-координатой.

Эту гиперплоскость можно рассматривать как копию пространства $\mathbb{P}_F^{n-1}$ в силу взаимно однозначного соот-

11. Докажите, что $E_p(X)$ сходится только на $D(1^-)$ (т. е. не на всем $D(1)$). (*Указание*: воспользуйтесь упр. 9 и 10 и покажите, что если E_p имеет хотя бы один нуль, то их бесконечно много.)

12. Пусть $g(X)=h(X)/f(X)$, где $g(X)\in 1+X\Omega[[X]]$ и все коэффициенты этого ряда лежат в $D(1)$, а $h(X)$ и $f(X)\in 1+X\Omega[X]$ — два многочлена, не имеющие общих корней. Докажите, что все коэффициенты $h(X)$ и $f(X)$ также лежат в $D(1)$.

13. Пусть $f(X)\in 1+X\Omega[[X]]$ сходится всюду на Ω. Для любого вещественного λ обозначим через $h_\lambda(X)$ многочлен $h(X)$ из теоремы 14. Докажите, что $h_\lambda\to f$ при $\lambda\to\infty$ (т. е. каждый коэффициент многочлена h_λ стремится к соответствующему коэффициенту ряда f). Докажите, что если f не миогочлен, то он имеет бесконечное число нулей (но не более чем счетное: $r_1, r_2, \ldots$) и $f(X)=\prod_{i=1}^{\infty}(1-X/r_i)$. В частности, не существует всюду сходящихся и нигде не обращающихся в нуль степенных рядов, кроме констант (в противоположность комплексному и вещественному случаям, где степенной ряд $e^{h(X)}$ всюду сходится и не имеет нулей для любого всюду сходящегося степенного ряда $h(X)$).

Глава V

РАЦИОНАЛЬНОСТЬ ДЗЕТА-ФУНКЦИИ СИСТЕМЫ ПОЛИНОМИАЛЬНЫХ УРАВНЕНИЙ НАД КОНЕЧНЫМ ПОЛЕМ

§ 1. ГИПЕРПОВЕРХНОСТИ И ИХ ДЗЕТА-ФУНКЦИИ

Пусть F — некоторое поле. Через $\mathbb{A}_F^n$ обозначим *n-мерное аффинное пространство над F*, т. е. множество упорядоченных наборов $(x_1, \ldots, x_n)$ по n элементов x_i из F. Пусть $f(X_1, \ldots, X_n)\in F[X_1, \ldots, X_n]$ — некоторый многочлен от n переменных $X_1, \ldots, X_n$. Под *аффинной гиперповерхностью*, заданной уравнением $f=0$, понимается множество

$$H_f \overset{\text{def}}{=} \{(x_1, \ldots, x_n)\in \mathbb{A}_F^n \mid \quad f(x_1, \ldots, x_n)=0\}.$$

Число $n-1$ называется *размерностью* гиперповерхности H_f. Если H_f одномерна, т. е. $n=2$, она называется *аффинной кривой*.

Сопутствующим к понятию аффинного пространства является *проективное пространство*. Проективное пространство над F размерности n обозначается $\mathbb{P}_F^n$ и определяется как множество классов эквивалентности элементов из $\mathbb{A}_F^{n+1}-\{(0, 0, \ldots, 0)\}$ по отношению эквивалентности $(x_0, x_1, \ldots, x_n)\sim(x_0', x_1', \ldots, x_n')\Leftrightarrow\exists\lambda\in F^\times$, для которого $x_i'=\lambda x_i$, $i=0, \ldots, n$. Иначе говоря, множество $\mathbb{P}_F^n$ есть множество всех прямых в $\mathbb{A}_F^{n+1}$, проходящих через начало координат.

Пространство $\mathbb{A}_F^n$ можно вложить в $\mathbb{P}_F^n$ при помощи отображения $(x_1, \ldots, x_n)\longmapsto(1, x_1, \ldots, x_n)$. Образ $\mathbb{A}_F^n$ при этом отображении состоит из всех точек $\mathbb{P}_F^n$, лежащих вне «бесконечно удаленной гиперплоскости», которая есть множество классов эквивалентности упорядоченных наборов по $n+1$ элементов с нулевой x_0-координатой.

Эту гиперплоскость можно рассматривать как копию пространства $\mathbb{P}_F^{n-1}$ в силу взаимно однозначного соот-

ветствия

$$\text{класс } (0, x_1, \ldots, x_n) \longmapsto \text{класс } (x_1, \ldots, x_n).$$

(Например, если $n=2$, то проективная плоскость $\mathbb{P}^2_F$ представляется в виде объединения аффинной плоскости и «бесконечно удаленной проективной прямой».) Продолжая этот процесс, можно разложить $\mathbb{P}^n_F$ в несвязное объединение

$$\mathbb{A}^n_F \cup \mathbb{A}^{n-1}_F \cup \mathbb{A}^{n-2}_F \cup \ldots \cup \mathbb{A}^1_F \cup \text{точка}.$$

Однородным многочленом $\tilde{f}(X_0, \ldots, X_n) \in F[X_0, \ldots, X_n]$ степени d называется линейная комбинация мономов *одной и той же полной степени* d. Например, $X_0^3 + X_0^2X_1 - 3X_1X_2X_3 + X_3^3$ — однородный многочлен степени 3. Под *однородным пополнением* $\tilde{f}(X_0, X_1, \ldots, X_n)$ заданного многочлена $f(X_1, \ldots, X_n) \in F[X_1, \ldots, X_n]$ степени d понимается многочлен

$$X_0^d f(X_1/X_0, \ldots, X_n/X_0),$$

который, очевидно, однороден и имеет степень d. Например, однородное пополнение для $X_3^3 - 3X_1X_2X_3 + X_1 + 1$ совпадает с приведенным выше примером однородного многочлена степени 3.

Если $\tilde{f}(X_0, \ldots, X_n)$ однороден и $\tilde{f}(x_0, \ldots, x_n) = 0$, то $\tilde{f}(\lambda x_0, \ldots, \lambda x_n) = 0$ для любого $\lambda \in F^\times$. Поэтому можно говорить о множестве точек (классов эквивалентности упорядоченных наборов из $n+1$ элементов) пространства $\mathbb{P}^n_F$, в которых $\tilde{f}$ обращается в нуль. Это множество точек $\tilde{H}_{\tilde{f}}$ называется *проективной гиперповерхностью*, заданной однородным уравнением $\tilde{f} = 0$ в $\mathbb{P}^n_F$.

Пусть $\tilde{f}(X_0, \ldots, X_n)$ — однородное пополнение многочлена $f(X_1, \ldots, X_n)$. Тогда $\tilde{H}_{\tilde{f}}$ называется *проективным замыканием* гиперповерхности H_f. С интуитивной точки зрения $\tilde{H}_{\tilde{f}}$ получается из H_f «присоединением точек, к которым H_f стремится на бесконечности». Например, если H_f — гипербола ($F = \mathbb{R}$)

$$\frac{X_1^2}{a^2} - \frac{X_2^2}{b^2} = 1,$$

то $\tilde{f}(X_0, X_1, X_2) = X_1^2/a^2 - X_2^2/b^2 - X_0^2$ и $\tilde{H}_{\tilde{f}}$ отождествляется с

$$\{(1, X_1, X_2) \mid X_1^2/a^2 - X_2^2/b^2 = 1\} \cup \{(0, 1, X_2) \mid X_2 = \pm b/a\},$$

т. е. это H_f плюс точки бесконечно удаленной прямой, соответствующие наклонам асимптот кривой H_f.

Пусть теперь K — произвольное поле, содержащее F. Если коэффициенты некоторого многочлена лежат в F, то они лежат и в K. Поэтому можно рассмотреть «K-точки» гиперповерхности H_f, т. е. множество

$$H_f(K) \overset{\text{def}}{=} \{(x_1, \ldots, x_n) \in \mathbb{A}^n_K \mid f(x_1, \ldots, x_n) = 0\}.$$

Аналогично определяется $\tilde{H}_{\tilde{f}}(K)$ для однородного многочлена $\tilde{f}(X_0, \ldots, X_n)$.

Далее мы работаем с конечными полями $F = \mathbb{F}_q$ и их конечными расширениями $K = \mathbb{F}_{q^s}$. В этой ситуации множества $H_f(K)$ и $\tilde{H}_{\tilde{f}}(K)$ конечны, так как $\mathbb{A}^n_K$ (и $\mathbb{P}^n_K$) состоят лишь из конечного числа точек. Для $\mathbb{A}^n_K$ это число наборов по n элементов из K, и оно равно q^{sn}. Фиксируем H_f (или $\tilde{H}_{\tilde{f}}$). В этом случае определена последовательность натуральных чисел $N_1, N_2, N_3, \ldots$, равных числу $\mathbb{F}_q$-точек, $\mathbb{F}_{q^2}$-точек, $\mathbb{F}_{q^3}$-точек, ... гиперповерхности H_f (или $\tilde{H}_{\tilde{f}}$), т. е.

$$N_s \overset{\text{def}}{=} \#(H_f(\mathbb{F}_{q^s})).$$

По любой заданной последовательности целых чисел, которая, как $\{N_s\}$, имеет геометрический или теоретико-числовой смысл, можно построить «производящую функцию», а именно некоторый степенной ряд, кодирующий всю информацию о данной последовательности $\{N_s\}$. Это так называемая «дзета-функция», определяемая как формальный степенной ряд

$$\exp\left(\sum_{s=1}^{\infty} N_s T^s/s\right) \in \mathbb{Q}[[T]].$$

Будем обозначать ее через $Z(H_f/\mathbb{F}_q; T)$, где $\mathbb{F}_q$ указывает на основное поле определения. Очевидно, постоянный член степенного ряда $Z(H_f/\mathbb{F}_q; T)$ равен 1.

Прежде чем перейти к примерам, докажем две элементарные леммы.

Лемма 1. *Коэффициенты ряда* $Z(H_f/\mathbb{F}_q; T)$ *лежат в* $\mathbb{Z}$.

Доказательство. Сопоставим каждой K-точке $P = (x_1, \ldots, x_n)$ из H_f (K — конечное расширение поля $\mathbb{F}_q$) наименьший показатель $s = s_0$, при котором все $x_i \in \mathbb{F}_{q^{s_0}}$. Пусть $P_j = (x_{1j}, \ldots, x_{nj})$, $j = 1, \ldots, s_0$, — все «сопряженные» с P точки, т. е. $x_{i1}, \ldots, x_{is_0}$ сопряжены с $x_i = x_{i1}$ над $\mathbb{F}_q$. Тогда точки P_j различны. Действительно, если все x_i остаются неподвижными при некотором нетривиальном автоморфизме σ поля $\mathbb{F}_{q^{s_0}}$ над $\mathbb{F}_q$, то они принадлежат меньшему полю (а именно полю σ-инвариантов $\{x \in \mathbb{F}_{q^{s_0}} \mid \sigma(x) = x\}$).

Вычислим теперь вклад точек $P_1, \ldots, P_{s_0}$ в $Z(H_f/\mathbb{F}_q; T)$. Каждая из них является $\mathbb{F}_{q^s}$-точкой в H_f тогда и только тогда, когда $\mathbb{F}_{q^s} \supset \mathbb{F}_{q^{s_0}}$, т. е. когда $s_0 \mid s$ (см. упр. 1 к § III.1). Итак, они вносят вклад, равный s_0, в N_{s_0}, N_{2s_0}, N_{3s_0}, ... Поэтому общий вклад этих точек в $Z(H_f/\mathbb{F}_q; T)$ равен

$$\exp\left(\sum_{j=1}^{\infty} s_0 T^{js_0}/js_0\right) = \exp(-\log(1-T^{s_0})) = \frac{1}{1-T^{s_0}} = \sum_{j=0}^{\infty} T^{js_0}.$$

Полная же дзета-функция представима в виде произведения рядов такого вида (причем лишь конечное число из них имеет нетривиальный T-член степени $\leqslant s_0$), а поэтому ее коэффициенты — целые числа. □

Замечание. Из доказательства видно, что эти коэффициенты, кроме того, неотрицательны.

Лемма 2. *Коэффициент при* T^j *в* $Z(H_f/\mathbb{F}_q; T)$ *не превосходит* q^{nj}.

Доказательство. Максимальное значение N_s равно $q^{ns} = \# \mathbb{A}^n_{q^s}$. Очевидно, все коэффициенты ряда $Z(H_f/\mathbb{F}_q; T)$ не превосходят соответствующих коэффициентов ряда,

полученного подстановкой в него q^{ns} вместо N_s. Но

$$\exp\left(\sum_{s=1}^{\infty} q^{ns}T^s/s\right) = \exp(-\log(1-q^nT)) = 1/(1-q^nT) = \sum_{j=0}^{\infty} q^{nj}T^j. \quad \square$$

В качестве простого примера рассмотрим вычисление дзета-функции аффинной прямой $L = H_{X_1} \subset \mathbb{A}^2_{\mathbb{F}_q}$. Очевидно, $N_s = q^s$, поэтому

$$Z(L/\mathbb{F}_q; T) = \exp\left(\sum q^sT^s/s\right) = \exp(-\log(1-qT)) = \frac{1}{1-qT}.$$

Аналогично определяется дзета-функция проективной гиперповерхности, только при этом используется последовательность чисел

$$\tilde{N}_s \overline{\text{def}} \# \left(\tilde{H}_{\tilde{f}}(\mathbb{F}_{q^s})\right).$$

Так, например, для проективной прямой $\tilde{L}$ мы имеем $\tilde{N}_s = q^s + 1$, поэтому

$$Z(\tilde{L}/\mathbb{F}_q; T) = \exp(\sum (q^sT^s/s + T^s/s)) = \exp(-\log(1-qT) - \log(1-T)) = \frac{1}{(1-T)(1-qT)}.$$

Оказывается, гораздо естественнее работать с проективными гиперповерхностями, чем с аффинными.

Возьмем, например, единичную окружность $X_1^2 + X_2^2 = 1$, проективное замыкание которой $\tilde{H}_{\tilde{f}}$ задается уравнением $\tilde{f} = X_1^2 + X_2^2 - X_0^2 = 0$. В этом случае проще вычислить $Z(\tilde{H}_{\tilde{f}}/\mathbb{F}_q; T)$, чем $Z(H_f/\mathbb{F}_q; T)$, где $f = X_1^2 + X_2^2 - 1$. (Будем предполагать, что $p = \operatorname{char} \mathbb{F}_q \neq 2$.) Почему же это проще? А потому, что существует взаимно однозначное соответствие между $\tilde{H}_{\tilde{f}}(K)$ и $\tilde{L}(K)$ ($\tilde{L}$ обозначает проективную прямую). Для конструкции такого отображения рассмотрим проектирование из «южного полюса» на прямую $X_2 = 1$, как показано на рис. 1.

После несложных вычислений получается: $x_1 = 4t/(4+t^2)$, $x_2 = (4-t^2)/(4+t^2)$, а $t = 2x_1/(x_2+1)$. При переходе от t к x это отображение имеет неопределенность для $t^2 = -4$, т. е. для двух значений t в случае $q^s \equiv 1 \pmod 4$, а если $q^s \equiv 3 \pmod 4$, то таких значений t нет (см. упр. 8 к § III.1). Для обратного отображения тоже

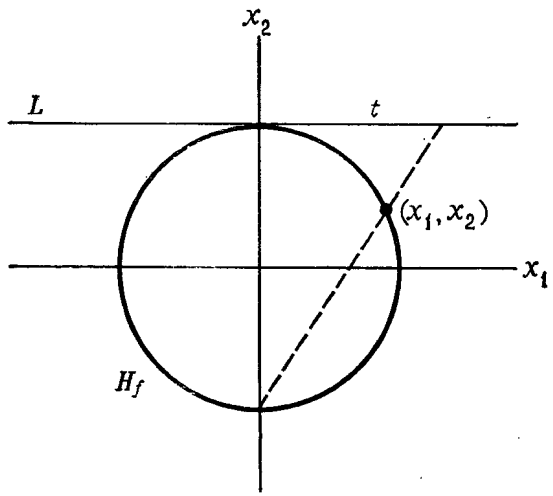


Рис. V.1.

возникает точка неопределенности с $x_2 = -1$ и $x_1 = 0$. Однако при переходе к проективным замыканиям окружности и прямой получается всюду определенное взаимно однозначное соответствие, задаваемое в однородных координатах (X_0, X_1, X_2) и (X_0', X_1') следующим образом:

$$(x_0', x_1') \longmapsto (4x_0'^2 + x_1'^2,\ 4x_0'x_1',\ 4x_0'^2 - x_1'^2);$$

$$(x_0, x_1, x_2) \longmapsto \begin{cases} (x_2 + x_0, 2x_1), & \text{если } (x_2 + x_0, 2x_1) \neq (0, 0), \\ (0, 1), & \text{если } (x_2 + x_0, 2x_1) = (0, 0). \end{cases}$$

Читателю рекомендуется аккуратно проверить, что это действительно взаимно однозначное соответствие между проективной прямой и множеством классов эквивалентности упорядоченных троек (x_0, x_1, x_2), удовлетворяющих уравнению $x_1^2 + x_2^2 - x_0^2 = 0$. Итак, поскольку $\tilde{N}_s$ одно и то же для $\tilde{H}_{\tilde{f}}$ и $\tilde{L}$, имеем

$$Z(\tilde{H}_{\tilde{f}}/\mathbb{F}_q;\ T) = Z(\tilde{L}/\mathbb{F}_q;\ T) = 1/[(1-T)(1-qT)].$$

Если же мы хотим найти $Z(H_f/\mathbb{F}_q;\ T)$, $f = X_1^2 + X_2^2 - X_0^2$, следует вычесть из $\tilde{N}_s$ все точки «на бесконечности» для $\tilde{H}_{\tilde{f}}$, т. е. те, для которых $x_1^2 + x_2^2 = x_0^2$ и $x_0 = 0$. Таких точек ровно две, если -1 имеет квадратный корень в $\mathbb{F}_{q^s}$, и ни одной в противном случае.

Случай (1). Пусть $q \equiv 1 \pmod 4$. Тогда -1 всегда имеет квадратный корень в $\mathbb{F}_{q^s}$ (см. упр. 8 к § III.1), и $N_s = \tilde{N}_s - 2$,

$$Z(H_f/\mathbb{F}_q;\ T) = \frac{Z(\tilde{H}_{\tilde{f}}/\mathbb{F}_q;\ T)}{\exp\left(\sum_{s=1}^{\infty} 2T^s/s\right)} = \frac{1/[(1-T)(1-qT)]}{1/(1-T)^2} = \frac{1-T}{1-qT}.$$

Случай (2). Пусть $q \equiv 3 \pmod 4$. Тогда, как легко показать, $N_s = \tilde{N}_s$ при нечетных s и $N_s = \tilde{N}_s - 2$ при четных s. Поэтому

$$Z(H_f/\mathbb{F}_q;\ T) = \frac{Z(\tilde{H}_f/\mathbb{F}_q;\ T)}{\exp\left(\sum_{s=1}^{\infty} 2T^{2s}/2s\right)} = \frac{1/[(1-T)(1-qT)]}{1/(1-T^2)} = \frac{1+T}{1-qT}.$$

Заметим, что во всех примерах, как ниже в примерах из упражнений, дзета-функция оказывается рациональной функцией, т. е. отношением двух многочленов. Это важный общий факт. Его впервые доказал Дворк в 1960 г., остроумно применив методы p-адического анализа.

Теорема (Дворк). *Дзета-функция любой аффинной* (или проективной, см. ниже упр. 5) *гиперповерхности является отношением двух многочленов с коэффициентами в* $\mathbb{Q}$ (и даже в $\mathbb{Z}$ и постоянным членом 1, см. ниже упр. 13).

Оставшаяся часть главы посвящена доказательству этой теоремы, принадлежащему Дворку.

Отметим, что определение дзета-функции, данное выше для гиперповерхностей, допускает обобщение на более широкий класс объектов, включающий аффинные и проективные «алгебраические многообразия», которые определяются подобно гиперповерхностям, только уже не одним, а несколькими полиномиальными уравнениями. Теорема Дворка верна также и для алгебраических многообразий (см. ниже упр. 4).

Теорема Дворка имеет глубокие конкретные следствия в теории систем полиномиальных уравнений над конечными полями. Из нее следует существование такого конечного набора комплексных чисел $\alpha_1, \ldots, \alpha_t, \beta_1, \ldots, \beta_u$, что $N_s = \sum_{i=1}^{t} \alpha_i^s - \sum_{i=1}^{u} \beta_i^s$ для *любого* $s = 1, 2, 3, \ldots$ (см. ниже упр. 6). Иначе говоря, зная конечный набор данных (α_i и β_i), а эти данные определяются уже конечным набором чисел N_s, мы получаем простую формулу, предсказывающую *все* остальные N_s. Правда, для практического применения этой формулы необходимо знать верхнюю границу степени числителя и знаменателя нашей рациональной функции $Z(H/\mathbb{F}_q; T)$ (подробности см. ниже в упр. 7—9). На самом деле во всех важных случаях степень числителя и знаменателя дзета-функции известна, как и многое другое. Эта информация содержится в знаменитых гипотезах А. Вейля[1]) (недавно доказанных, но доказательство которых даже в простейших случаях выходит далеко за рамки этой книги).

Рациональность дзета-функции была частью серии гипотез, сформулированных Вейлем в 1949 г. Данное Дворком доказательство рациональности представляло собой первый важный шаг на пути к доказательству этих гипотез. Последний шаг в этом направлении — полученное в 1973 г. Делинем доказательство так называемой «гипотезы Римана» для алгебраических многообразий над конечным полем — явился кульминацией четвертьвековых напряженных исследований в этой области.

[1]) В настоящей книге речь идет исключительно о гипотезах Вейля, относящихся к случаю многообразий над конечным полем. — *Прим. перев.*

В случае *гладкой* проективной гиперповерхности $\tilde{H}_{\tilde{f}}$ (т. е. когда все частные производные $\tilde{f}$ по всем переменным не обращаются в нуль одновременно) гипотезы Вейля утверждают следующее:

(i) $Z(\tilde{H}_{\tilde{f}}/\mathbb{F}_q; T) = P(T)^{\pm 1}/((1-T)(1-qT)(1-q^2T)\ldots(1-q^{n-1}T))$, где $P(T) \in 1 + T\mathbb{Z}[T]$ имеет степень β, а β — число, определяемое «топологией» данной гиперповерхности (оно называется ее числом Бетти; если $\tilde{H}_{\tilde{f}}$ — кривая, то это удвоенный род («число ручек») соответствующей римановой поверхности). Здесь ± 1 означает, что мы берем $P(T)$ для четного n и $1/P(T)$ для нечетного n.

(ii) Если α — обратный корень многочлена $P(T)$, то тем же свойством обладает q^{n-1}/α.

(iii) Абсолютная величина каждого из обратных корней многочлена $P(T)$ равна $q^{(n-1)/2}$. (Это утверждение называется «гипотезой Римана» по аналогии с классической гипотезой Римана о нулях дзета-функции Римана; см. по этому поводу ниже упр. 15.)

Упражнения

1. Какова дзета-функция точки? Какова $Z\left(\mathbb{A}^n_{\mathbb{F}_q}/\mathbb{F}_q; T\right)$?

2. Вычислите $Z\left(\mathbb{P}^n_{\mathbb{F}_q}/\mathbb{F}_q; T\right)$.

3. Пусть $f(X_1, \ldots, X_n) = X_n + g(X_1, \ldots, X_{n-1})$, где $g \in \mathbb{F}_q[X_1, \ldots, X_{n-1}]$. Докажите, что

$$Z(H_f/\mathbb{F}_q; T) = Z\left(\mathbb{A}^{n-1}_{\mathbb{F}_q}/\mathbb{F}_q; T\right).$$

4. Пусть $f_1(X_1, \ldots, X_n), f_2(X_1, \ldots, X_n), \ldots, f_r(X_1, \ldots, X_n) \in \mathbb{F}_q[X_1, \ldots, X_n]$, а $H_{\{f_1, f_2, \ldots, f_r\}}(\mathbb{F}_{q^s}) \subset \mathbb{A}^n_{\mathbb{F}_{q^s}}$ — множество наборов по n элементов из $\mathbb{F}_{q^s}$, которые удовлетворяют *всем* уравнениям $f_i = 0$, $i = 1, 2, \ldots, r$:

$$H_{\{f_1, f_2, \ldots, f_r\}}(\mathbb{F}_{q^s}) \overset{\text{def}}{=} \{(x_1, \ldots, x_n) \in \mathbb{A}^n_{\mathbb{F}_{q^s}} \mid f_1(x_1, \ldots, x_n) = \ldots = f_r(x_1, \ldots, x_n) = 0\}.$$

Такое H называется (аффинным) алгебраическим многообразием. Пусть $N_s = \#H(\mathbb{F}_{q^s})$ (где H — сокращенное обозначение для

$H_{\{f_1, \ldots, f_r\}}$). Определим дзета-функцию, как и выше: $Z(H/\mathbb{F}_q; T) \underset{\text{def}}{=} \exp\left(\sum_{s=1}^{\infty} N_s T^s/s\right)$. Докажите, что из теоремы Дворка для аффинных гиперповерхностей следует теорема Дворка для аффинных алгебраических многообразий. (*Указание.* Пусть, скажем, $r=2$. Покажите, что тогда $\#H_{\{f_1,f_2\}}(\mathbb{F}_{q^s}) = \#H_{f_1}(\mathbb{F}_{q^s}) + \#H_{f_2}(\mathbb{F}_{q^s}) - \#H_{f_1 f_2}(\mathbb{F}_{q^s})$, где $H_{f_1 f_2}$ — гиперповерхность, заданная уравнением $f_1 \cdot f_2 = 0$.)

5. Докажите, что если теорема Дворка верна для аффинных гиперповерхностей, то она верна и для проективных гиперповерхностей.

6. Докажите, что теорема Дворка эквивалентна следующему утверждению: существует набор алгебраических комплексных чисел $\alpha_1, \ldots, \alpha_t, \beta_1, \ldots, \beta_u$, для которого каждое из α_i при сопряжении переходит в некоторое α_j, а каждое из β_i — в некоторое β_k и

$$N_s = \sum_{i=1}^{t} \alpha_i^s - \sum_{i=1}^{u} \beta_i^s \text{ для всех } s = 1, 2, 3, \ldots.$$

7. Известно, что дзета-функция гладкой проективной кубической кривой $\tilde{E} = \tilde{H}_{\tilde{f}}$ ($\dim \tilde{E} = 1$, $\deg \tilde{f} = 3$; $\tilde{E}$ называется *эллиптической кривой*) всегда представима в виде $(1 + aT + qT^2)/[(1-T)(1-qT)]$ для некоторого $a \in \mathbb{Z}$. Покажите, что если известно число точек в $\tilde{E}(\mathbb{F}_q)$, то можно найти: (1) a и (2) $\#\tilde{E}(\mathbb{F}_{q^s})$ при всех s.

8. Используя факт, сформулированный в предыдущем упражнении, найдите $Z(\tilde{H}_{\tilde{f}}/\mathbb{F}_q; T)$ для $f(X_1, X_2)$, равного:

(i) $X_2^3 - X_1^3 - 1$ и $q \equiv 2 \pmod 3$;
(ii) $X_2^2 - X_1^3 + X_1$ и $q \equiv 3 \pmod 4$, а также для $q = 5$, 13 и 9.

9. Предположим, что рациональность функции $Z(H/\mathbb{F}_q; T)$ уже известна. Пусть m и n — степени ее числителя и знаменателя соответственно. Докажите, что числа $N_s = \#H(\mathbb{F}_{q^s})$ для $s = 1, 2, 3, \ldots, m+n$ однозначно определяют все остальные N_s. (То есть две такие рациональные функции $\exp\left(\sum_{s=1}^{\infty} N_s T^s/s\right)$ и $\exp\left(\sum_{s=1}^{\infty} N'_s T^s/s\right)$, для которых $N_s = N'_s$ при $1 \leqslant s \leqslant m+n$, совпадают, а значит, и $N_s = N'_s$ для всех s.)

10. Вычислите $Z(H_f/\mathbb{F}_q; T)$ для трехмерной гиперповерхности H_f, заданной уравнением

$$X_1X_4 - X_2X_3 = 1.$$

11. Вычислите $Z(H_f/\mathbb{F}_q; T)$ и $Z(\tilde{H}_{\tilde{f}}/\mathbb{F}_q; T)$ ($\tilde{f}$ — однородное пополнение f) для кривой H_f, заданной уравнением:

(i) $X_1X_2 = 0$; (ii) $X_1X_2(X_1 + X_2 + 1) = 0$; (iii) $X_2^2 - X_1^3 = 1$;
(iv) $X_2^2 = X_1^3$; (v) $X_2^2 = X_1^3 + X_1^2$.

12. Прямые в $\mathbb{P}^3$ получаются как пересечение двух различных гиперповерхностей, т. е. прямая состоит из классов эквивалентности четверок, удовлетворяющих одновременно двум заданным однородным линейным уравнениям. Пусть N_s — число прямых в $\mathbb{P}^3\mathbb{F}_{q^s}$. Используя данное выше определение дзета-функции по последовательности чисел N_s, вычислите дзета-функцию семейства прямых на трехмерном проективном пространстве.

13. Используя упр. 12 к § IV.4, докажите, что из приведенной выше леммы 1 и теоремы Дворка «с коэффициентами в $\mathbb{Q}$» следует теорема Дворка «с коэффициентами в $\mathbb{Z}$ и постоянным членом 1».

14. Пусть H_f — кривая, заданная уравнением $X_2^3 = X_1^5 + 1$, а $p \equiv 3$ или $7 \pmod{10}$. Докажите, что

$$Z(\tilde{H}_{\tilde{f}}/\mathbb{F}_p; T) = \frac{1 + p^2T^4}{(1-T)(1-pT)}.$$

15. Пусть $\tilde{H}_{\tilde{f}}$ — гладкая проективная кривая. Предполагая справедливость гипотез Вейля для $Z(\tilde{H}_{\tilde{f}}/\mathbb{F}_q; T)$ (которые для кривых были доказаны гораздо раньше, чем в общем случае), покажите, что все нули аналитической функции

$$F(s) \underset{\text{def}}{=} Z(\tilde{H}_{\tilde{f}}/\mathbb{F}_q; q^{-s})$$

комплексного переменного s лежат на прямой $\operatorname{Re} s = 1/2$. Этот факт объясняет, почему гипотезу Вейля (iii) называют «гипотезой Римана».

§ 2. ХАРАКТЕРЫ И ИХ ПОДНЯТИЕ

Ω-значным характером на конечной группе G называется гомоморфизм группы G в мультипликативную группу $\Omega^\times$ ненулевых чисел из Ω. Так как $g^{\text{порядок элемента } g} = 1$ для любого $g \in G$, характер отображает G в множество корней из 1 поля Ω. Пусть, например, G — аддитивная группа поля $\mathbb{F}_p$, ε — корень степени p из 1 в Ω, и пусть $\tilde{a}$ — приведенный вычет

для $a \in \mathbb{F}_p$. Тогда отображение $a \longmapsto \varepsilon^{\hat{a}}$ является характером на $\mathbb{F}_p$. В дальнейшем будем писать $a \longmapsto \varepsilon^a$, опуская тильду. Если $\varepsilon \neq 1$, этот характер нетривиален, т. е. его образ состоит не только из 1.

Если $\mathbb{F}_q$ — конечное поле из $q = p^s$ элементов, то известно, что существует $s = [\mathbb{F}_q : \mathbb{F}_p]$ автоморфизмов $\sigma_0, \ldots, \sigma_{s-1}$ поля $\mathbb{F}_q$, для которых $\sigma_i(a) = a^{p^i}$, $a \in \mathbb{F}_q$ (см. упр. 6 к § III.1). Пусть $a \in \mathbb{F}_q$. *След* элемента a, обозначаемый $\operatorname{Tr} a$, определяется формулой

$$\operatorname{Tr} a \underset{\text{def}}{=} \sum_{i=0}^{s-1} \sigma_i(a) = a + a^p + a^{p^2} + \ldots + a^{p^{s-1}}.$$

Очевидно, $(\operatorname{Tr} a)^p = \operatorname{Tr}(a)$, т. е. $\operatorname{Tr} a \in \mathbb{F}_p$. Кроме того, $\operatorname{Tr}(a+b) = \operatorname{Tr} a + \operatorname{Tr} b$. Поэтому отображение

$$a \longmapsto \varepsilon^{\operatorname{Tr} a}$$

есть Ω-значный характер аддитивной группы поля $\mathbb{F}_q$.

Напомним, что каждому элементу $a \in \mathbb{F}_q$ соответствует единственный представитель Тейхмюллера $t \in \Omega$, который лежит в неразветвленном расширении K поля $\mathbb{Q}_p$, порожденном примитивным корнем из 1 степени $(q-1)$, причем $t^q = t$, а редукция t по модулю p равна a. Цель этого параграфа — найти p-адический степенной ряд $\Theta(T)$, значение которого при $T = t$ совпадало бы с $\varepsilon^{\operatorname{Tr} a}$. (Точнее, ряд $\Theta(T)\Theta(T^p)\Theta(T^{p^2})\ldots\Theta(T^{p^{s-1}})$, где $q = p^s$, будет принимать значение $\varepsilon^{\operatorname{Tr} a}$ при $T = t$.)

Фиксируем $a \in \mathbb{F}_q^\times$. Пусть $t \in K$ — соответствующий представитель Тейхмюллера. Обозначим через Tr_K отображение следа для элементов из K в $\mathbb{Q}_p$, переводящее элемент K в сумму сопряженных с ним над $\mathbb{Q}_p$. Тогда для представителя Тейхмюллера t (см. упр. 1 к § 4 ниже)

$$\operatorname{Tr}_K t = t + t^p + t^{p^2} + \ldots + t^{p^{s-1}} \in \mathbb{Z}_p,$$

а редукция $\operatorname{Tr}_K t$ по модулю p равна

$$a + a^p + a^{p^2} + \ldots + a^{p^{s-1}} = \operatorname{Tr} a \in \mathbb{F}_p.$$

Следовательно, $\varepsilon^{\operatorname{Tr} a} = \varepsilon^{\operatorname{Tr}_K t}$, поскольку возведение ε в некоторую степень из $\mathbb{Z}_p$ зависит только от класса вычетов по модулю p.

Пусть $\lambda = \varepsilon - 1$. Нам уже известно, что $\operatorname{ord}_p \lambda = 1/(p-1)$ (см. упр. 7 к § III.4). Хотим же мы найти p-адическое выражение, зависящее от t, для

$$(1+\lambda)^{t + t^p + t^{p^2} + \ldots + t^{p^{s-1}}} = \varepsilon^{\operatorname{Tr} a}.$$

Действуя наивно, можно было бы положить

$$g(T) = (1+\lambda)^T = \sum_{i=0}^{\infty} \frac{T(T-1)\ldots(T-i+1)}{i!}\lambda^i,$$

а затем построить ряд $g(T)\,g(T^p)\,g(T^{p^2})\ldots g(T^{p^{s-1}})$. Но тогда возникает следующая трудность: как придать смысл бесконечному ряду $g(T)$ для интересующих нас значений $T = t$? А именно, если $t \notin \mathbb{Z}_p$, т. е. вычет a не лежит в $\mathbb{F}_p$, то, очевидно, $|t-i|_p = 1$ для всех $i \in \mathbb{Z}$, откуда

$$\operatorname{ord}_p \frac{t(t-1)\ldots(t-i+1)}{i!}\lambda^i = i \operatorname{ord}_p \lambda - \frac{i - S_i}{p-1} = \frac{S_i}{p-1},$$

так что этот порядок не стремится к бесконечности.

Выход из положения заключается в использовании ряда $F(X, Y)$ с лучшей сходимостью, который был введен в конце § IV.2:

$$F(X, Y) = (1+Y)^X (1+Y^p)^{(X^p - X)/p} (1+Y^{p^2})^{(X^{p^2} - X^p)/p^2} \ldots$$
$$\ldots (1+Y^{p^n})^{(X^{p^n} - X^{p^{n-1}})/p^n} \ldots.$$

Напомним, что сомножители справа обозначают соответствующие биномиальные ряды из $\mathbb{Q}[[X, Y]]$. Рассмотрим теперь $F(X, Y)$ как степенной ряд от X при фиксированном Y:

$$F(X, Y) = \sum_{n=0}^{\infty} \left(X^n \sum_{m=n}^{\infty} a_{m,n} Y^m \right), \quad a_{m,n} \in \mathbb{Z}_p;$$

при этом использован тот факт, что $a_{m,n} \neq 0$ только для $m \geqslant n$. Действительно, каждое слагаемое ряда $B_{(X^{p^n} - X^{p^{n-1}})/p^n,\, p}(Y^{p^n})$, т. е.

$$\frac{X^{p^n} - X^{p^{n-1}}}{p^n}\left(\frac{X^{p^n} - X^{p^{n-1}}}{p^n} - 1\right)\ldots\left(\frac{X^{p^n} - X^{p^{n-1}}}{p^n} - i + 1\right)\frac{Y^{ip^n}}{i!}$$

после перемножения и приведения подобных членов

дает лишь члены, степень которых по X меньше или равна степени Y^{ip^n} по Y.

Напомним, что $\lambda=\varepsilon-1$, а $\operatorname{ord}_p\lambda=1/(p-1)$. Положим

$$\Theta(T)=F(T,\ \lambda)=\sum_{n=0}^{\infty}a_nT^n,$$

где $a_n=\sum_{m=n}^{\infty}a_{m,n}\lambda^m$. Очевидно, $\operatorname{ord}_p a_n\geqslant n/(p-1)$, так как каждый член в выражении для a_n делится на λ^n. В силу полноты поля $\mathbb{Q}_p(\varepsilon)=\mathbb{Q}_p(\lambda)$ имеет место включение $a_n\in\mathbb{Q}_p(\varepsilon)$, а $\Theta(T)\in\mathbb{Q}_p(\varepsilon)[[T]]$. Более того, $\Theta(T)$ сходится для всех значений $t\in D(p^{1/(p-1)}-)$, потому что $\operatorname{ord}_p a_n\geqslant n/(p-1)$.

Рассмотрим теперь для фиксированного t ряд

$$(1+Y)^{t+t^p+\ldots+t^{p^{s-1}}}\overset{\text{def}}{=}B_{t+t^p+\ldots+t^{p^{s-1}},\,p}(Y).$$

Легко доказать следующее формальное тождество в $\Omega[[Y]]$:

$$(1+Y)^{t+t^p+\ldots+t^{p^{s-1}}}=F(t,\ Y)\,F(t^p,\ Y)\ldots F\left(t^{p^{s-1}},\ Y\right).$$

В самом деле, после тривиальных сокращений правая часть приводится к виду

$$(1+Y)^{t+t^p+\ldots+t^{p^{s-1}}}(1+Y^p)^{(t^{p^s}-t)/p}\times$$
$$\times(1+Y^{p^2})^{(t^{p^{s+1}}-t^p)/p^2}(1+Y^{p^3})^{(t^{p^{s+2}}-t^{p^2})/p^3}\ldots.$$

Но $t^{p^s}=t$, и мы получаем требуемое.

Итак, при подстановке t вместо T в $\Theta(T)\,\Theta(T^p)\ldots\Theta\left(T^{p^{s-1}}\right)$ получается

$$F(t,\ \lambda)\,F(t^p,\ \lambda)\ldots F\left(t^{p^{s-1}},\ \lambda\right)=$$
$$=(1+\lambda)^{t+t^p+\ldots+t^{p^{s-1}}}=\varepsilon^{\operatorname{Tr}a}.$$

В результате мы нашли хороший p-адический степенной ряд $\Theta(T)=\sum a_nT^n\in\mathbb{Q}_p(\varepsilon)[[T]]$ с $\operatorname{ord}_p a_n\geqslant n/(p-1)$, такой, что значения характера $a\longmapsto\varepsilon^{\operatorname{Tr}a}$ на $\mathbb{F}_q$ вычисляются подстановкой поднятия Тейхмюллера для a в $\Theta(T)\,\Theta(T^p)\ldots\Theta\left(T^{p^{s-1}}\right)$. Ряд Θ можно рассматривать как «поднятие» этого характера аддитивной группы поля $\mathbb{F}_q$ до функции на Ω (точнее, на некотором диске в Ω, включающем *замкнутый* единичный диск, а следовательно, и все представители Тейхмюллера).

Такие поднятия, как Θ, важны потому, что многие понятия анализа приложимы непосредственно только к p-адическим, а не к конечным полям. Если некоторый объект, связанный с конечным полем, например дзета-функция гиперповерхности над этим полем, допускает поднятие в поле p-адических чисел, то к нему уже можно применять анализ. В заключение отметим, как важно, что наше поднятие Θ сходится по крайней мере на *замкнутом* единичном диске (а, скажем, не просто открытом единичном диске): ведь точки, которые нас больше всего интересуют, — представители Тейхмюллера — лежат как раз на единичной окружности.

§ 3. ЛИНЕЙНЫЕ ОТОБРАЖЕНИЯ НА ВЕКТОРНОМ ПРОСТРАНСТВЕ СТЕПЕННЫХ РЯДОВ

Обозначим через R кольцо формальных степенных рядов над Ω от n независимых переменных:

$$R\overset{\text{def}}{=}\Omega[[X_1,\ X_2,\ \ldots,\ X_n]].$$

Моном $X_1^{u_1}X_2^{u_2}\ldots X_n^{u_n}$ будем обозначать через X^u, где $u=(u_1,\ \ldots,\ u_n)$ — упорядоченный набор из n целых неотрицательных чисел. Тогда каждый элемент из R можно записать в виде $\sum a_uX^u$, где u пробегает множество U всех упорядоченных наборов из n целых неотрицательных чисел и $a_u\in\Omega$.

Отметим, что R — бесконечномерное векторное пространство над Ω. Для каждого $G\in R$ определим линейное отображение из R в R, обозначаемое также через G, сопоставлением

$$r\longmapsto Gr,$$

т. е. это отображение умножения степенных рядов из R на некоторый фиксированный степенной ряд G.

Кроме того, для каждого целого положительного $q>1$ (в приложениях q будет степенью простого числа p) определим линейное отображение T_q: $R\to R$, полагая

$$r=\sum a_uX^u\longmapsto T_q(r)=\sum a_{qu}X^u,$$

где qu обозначает набор $(qu_1, qu_2, \ldots, qu_n)$. Например, при $n=1$ это отображение степенных рядов, при котором стираются все X^j-члены для j, не делящихся на q, а во всех X^j-членах, где $q \mid j$, X^j заменяется на $X^{j/q}$.

Положим теперь $\Psi_{q,G} \overset{\text{def}}{=} T_q \circ G\colon R \to R$. Пусть $G = \sum_{w \in U} g_w X^w$. Тогда $\Psi_{q,G}$ — линейное отображение, задаваемое на мономах X^u формулой

$$\Psi_{q,G}(X^u) = T_q\left(\sum_{w \in U} g_w X^{w+u}\right) = \sum_{v \in U} g_{qv-u} X^v.$$

(При этом если набор $qv-u$ не лежит в U, т. е. имеет отрицательную компоненту, то считается, что соответствующее g_{qv-u} равно нулю.)

Обозначим через $G_q(X)$ степенной ряд $G(X^q) = \sum_{w \in U} g_w X^{qw}$. Легко проверить следующее соотношение (см. ниже упр. 7):

$$G \circ T_q = T_q \circ G_q = \Psi_{q,G_q}.$$

Определим на U функцию $|\ |$ формулой $|u| = \sum_{i=1}^{n} u_i$. Пусть

$$R_0 \overset{\text{def}}{=} \Big\{ G = \sum_{w \in U} g_w X^w \in R \mid \text{существует такое } M > 0, \text{ что } \operatorname{ord}_p g_w \geqslant M|w| \text{ для всех } w \in U \Big\}.$$

Нетрудно проверить замкнутость R_0 относительно умножения и инвариантность при отображении $G \longmapsto G_q$. Отметим, что каждый степенной ряд из R_0 сходится для всех значений переменных, лежащих в некотором диске, строго большем чем $D(1)$. Один из важных примеров ряда, принадлежащего R_0, дает $\Theta(aX^w)$, где a берется из $D(1)$, а X^w обозначает моном от переменных $X_1, \ldots, X_n$ (см. ниже упр. 2).

Пусть V — конечномерное векторное пространство над полем F, а $\{a_{ij}\}$ — матрица линейного отображения $A\colon V \to V$ в некотором базисе. Тогда след отображения A определяется как

$$\operatorname{Tr} A \overset{\text{def}}{=} \sum a_{ii},$$

т. е. как сумма элементов главной диагонали (эта сумма не зависит от выбора базиса; по поводу этого факта и других основных понятий и результатов линейной алгебры см. [(а) 2], гл. 6[1]). (Использование того же символа Tr, что и для следа элемента поля $\mathbb{F}_q$, не должно приводить к путанице, поскольку из контекста всегда будет ясно, о чем идет речь.) Если поле F обладает некоторой метрикой, можно ввести след *бесконечной* матрицы A, при условии что сумма $\sum_{i=1}^{\infty} a_{ii}$ сходится.

Лемма 3. *Пусть* $G \in R_0$, $\Psi = \Psi_{q,G}$. *Тогда* $\operatorname{Tr}(\Psi^s)$ *определен для* $s = 1, 2, 3, \ldots$ *и*

$$(q^s - 1)^n \operatorname{Tr}(\Psi^s) = \sum_{\substack{x \in \Omega^n, \\ x^{q^s-1} = 1}} G(x) \cdot G(x^q) \cdot G\left(x^{q^2}\right) \ldots G\left(x^{q^{s-1}}\right),$$

где $x = (x_1, \ldots, x_n)$, $x^{q^i} = \left(x_1^{q^i}, \ldots, x_n^{q^i}\right)$, *а* $x^{q^s-1} = 1$ *означает, что* $x_j^{q^s-1} = 1$ *для* $j = 1, 2, \ldots, n$.

Доказательство. Разберем прежде всего случай $s = 1$, а затем сведем к нему общий случай. Так как $\Psi(X^u) = \sum_{v \in U} g_{qv-u} X^v$, то

$$\operatorname{Tr} \Psi = \sum_{u \in U} g_{(q-1)u}$$

и ряд сходится по определению R_0.

Рассмотрим теперь правую часть равенства в лемме. Для $i = 1, 2, \ldots, n$ имеем

$$\sum_{\substack{x_i \in \Omega, \\ x_i^{q-1} = 1}} x_i^{w_i} = \begin{cases} q-1, & \text{если } q-1 \text{ делит } w_i, \\ 0 & \text{в остальных случаях} \end{cases}$$

(см. ниже упр. 6). Следовательно,

$$\sum_{\substack{x \in \Omega^n, \\ x^{q-1} = 1}} x^w = \prod_i \sum_{x_i^{q-1} = 1} x_i^{w_i} = \begin{cases} (q-1)^n, \text{ если } q-1 \text{ делит } w, \\ 0 \text{ в остальных случаях.} \end{cases}$$

[1]) См. также книгу И. М. Гельфанда [(а) 4], гл. II. — *Прим. перев.*

Отсюда

$$\sum_{x^{q-1}=1} G(x) = \sum_{w \in U} g_w \sum_{x^{q-1}=1} x^w =$$

$$= (q-1)^n \sum_{u \in U} g_{(q-1)u} = (q-1)^n \operatorname{Tr} \Psi,$$

что и доказывает лемму для $s=1$.

Предположим теперь, что $s>1$. Тогда

$$\Psi^s = T_q \circ G \circ T_q \circ G \circ \Psi^{s-2} = T_q \circ T_q \circ G_q \circ G \circ \Psi^{s-2} =$$
$$= T_{q^2} \circ G \cdot G_q \circ \Psi^{s-2} = T_{q^2} \circ T_q \circ (G \cdot G_q)_q \, G \circ \Psi^{s-3} =$$
$$= T_{q^3} \circ G \cdot G_q \cdot G_{q^2} \circ \Psi^{s-3} = \ldots = T_{q^s} \circ G \cdot G_q \cdot G_{q^2} \ldots G_{q^{s-1}} =$$
$$= \Psi_{q^s,\ G \cdot G_q \cdot G_{q^2} \ldots G_{q^{s-1}}}.$$

Итак, заменив q на q^s и G на $G \cdot G_q \cdot G_{q^2} \ldots G_{q^{s-1}}$, мы установим лемму в общем виде. □

Пусть A — некоторая $r \times r$-матрица с элементами в поле F, а T — независимая переменная. Тогда $(1-AT)$ (где 1 обозначает $r \times r$-матрицу тождественного преобразования) является $r \times r$-матрицей с элементами в кольце $F[T]$. Эта матрица играет существенную роль при изучении линейного отображения на F^r, соответствующего A, потому что ее определитель, равный $\det(1-At)$ для любого конкретного значения $t \in F$ переменной T, обращается в нуль тогда и только тогда, когда существует нетривиальный вектор $v \in F^r$, для которого $0 = (1-At)v = v - tAv$, т. е. $Av = (1/t)v$. Иначе говоря, это происходит тогда и только тогда, когда $1/t$ есть собственное значение матрицы A. Если $A = \{a_{ij}\}$, то

$$\det(1-AT) = \sum_{m=0}^{n} b_m T^m,$$

где

$$b_m = (-1)^m \sum_{\substack{1 \leqslant u_1, \ldots, u_m \leqslant r \\ \sigma\text{—перестановка этих } u_i}} \operatorname{sgn}(\sigma)\, a_{u_1, \sigma(u_1)} \times$$

$$\times a_{u_2, \sigma(u_2)} \ldots a_{u_m, \sigma(u_m)}.$$

(Функция $\operatorname{sgn}(\sigma)$ принимает значение $+1$ или -1 в соответствии с тем, является ли данная перестановка σ произведением четного или нечетного числа транспозиций.)

Предположим теперь, что $A = \{a_{ij}\}_{i,j=1}^{\infty}$ — бесконечная «квадратная» матрица, а $F = \Omega$. Тогда выражение для $\det(1-AT)$ будет иметь смысл как формальный степенной ряд в $\Omega[[T]]$, если только выражения для b_m, которые теперь являются бесконечными рядами (условие «$\leqslant r$» на u_i отбрасывается), сходятся.

Применим это понятие к случаю, когда $A = \{g_{qv-u}\}_{u,\, v \in U}$ — «матрица» отображения $\Psi = T_q \circ G$, где $G \in R_0$, т. е. $\operatorname{ord}_p g_w \geqslant M|w|$. Тогда p-адические порядки членов в выражении для b_m допускают следующую оценку:

$$\operatorname{ord}_p \left[g_{q\sigma(u_1)-u_1} \cdot g_{q\sigma(u_2)-u_2} \cdots g_{q\sigma(u_m)-u_m} \right] \geqslant$$
$$\geqslant M\left[|q\sigma(u_1) - u_1| + |q\sigma(u_2) - u_2| + \ldots + |q\sigma(u_m) - u_m| \right] =$$
$$= M\left[\sum q\,|\sigma(u_i)| - \sum |u_i| \right] = M(q-1) \sum |u_i|.$$

(Отметим, что если G — степенной ряд от n переменных, то каждое u_i есть набор n целых неотрицательных чисел: $u_i = (u_{i1}, \ldots, u_{in})$ и $|u_i| = \sum_{j=1}^{n} u_{ij}$.) Из этого видно, что

$$\operatorname{ord}_p b_m \to \infty \quad \text{при} \quad m \to \infty,$$
$$\frac{1}{m} \operatorname{ord}_p b_m \to \infty \quad \text{при} \quad m \to \infty.$$

Последнее верно, так как существует лишь конечное число n-наборов u с заданным значением $|u|$, а среднее для $|u|$ по конечному множеству *различных* u_i, т. е. $(1/m) \sum_{i=1}^{m} |u_i|$, стремится к ∞.

Это доказывает, что

$$\det(1-AT) = \sum_{m=0}^{\infty} b_m T^m$$

корректно определен (т. е. ряд, задающий каждое b_m, сходится) и его радиус сходимости бесконечен.

Докажем теперь еще один важный вспомогательный результат, сначала для конечных матриц, а затем для

$\{g_{qv-u}\}$. А именно, в $\Omega[[T]]$ имеет место следующее тождество для формальных степенных рядов:

$$\det(1-AT)=\exp_p\left(-\sum_{s=1}^{\infty}\operatorname{Tr}(A^s)\,T^s/s\right).$$

Чтобы доказать это, напомним прежде всего два факта из теории матриц (см. [(а) 2], гл. 6[1]). Определитель и след матрицы не меняются при сопряжении $A\longmapsto CAC^{-1}$ посредством обратимой матрицы C, т. е. они инвариантны относительно замены базиса. Кроме того, если основное поле алгебраически замкнуто, что верно, например, для Ω, то после подходящей замены базиса любая матрица может быть приведена к верхней треугольной матрице A (например, к канонической жордановой форме). Иначе говоря, последняя матрица не имеет ненулевых элементов ниже главной диагонали. Поэтому при доказательстве тождества без потери общности можно предполагать, что $A=\{a_{ij}\}_{i,\,j=1}^{r}$ верхняя треугольная. Тогда левая часть требуемого равенства принимает вид $\prod_{i=1}^{r}(1-a_{ii}T)$. Справа же стоит

$$\exp_p\left(-\sum_{s=1}^{\infty}\sum_{i=1}^{r}a_{ii}^sT^s/s\right)=\prod_{i=1}^{r}\exp_p\left(-\sum_{s=1}^{\infty}(a_{ii}T)^s/s\right)=$$
$$=\prod_{i=1}^{r}\exp_p(\log_p(1-a_{ii}T))=\prod_{i=1}^{r}(1-a_{ii}T),$$

поскольку $\operatorname{Tr}(A^s)=\sum_{i=1}^{r}a_{ii}^s$.

Разбор обобщения этого тождества на случай бесконечных матриц A мы оставим читателю в качестве упражнения (см. ниже упр. 8).

Резюмируем все это в следующей лемме.

Лемма 4. *Пусть* $G(X)=\sum_{w\in U}g_wX^w\in R_0$, *а* $\Psi=T_q\circ G$, *так что матрица отображения* Ψ *есть* $A=\{g_{qv-u}\}_{v,\,u\in U}$.

[1]) А также [(а) 4], гл. II и III. — *Прим. перев.*

Тогда ряд $\det(1-AT)$ *из* $\Omega[[T]]$ *корректно определен, имеет бесконечный радиус сходимости и равен*

$$\exp_p\left\{-\sum_{s=1}^{\infty}\operatorname{Tr}(A^s)\,T^s/s\right\}.$$

§ 4. *p*-АДИЧЕСКОЕ АНАЛИТИЧЕСКОЕ ВЫРАЖЕНИЕ ДЛЯ ДЗЕТА-ФУНКЦИИ

В этом параграфе будет доказано, что дзета-функция

$$Z(H_f/\mathbb{F}_q;\ T)\in\mathbb{Z}[[T]]\subset\Omega[[T]]$$

любой гиперповерхности H_f, заданной уравнением $f=0$ с $f(X_1,\ \ldots,\ X_n)\in\mathbb{F}_q[X_1,\ \ldots,\ X_n]$, является отношением двух степенных рядов из $\Omega[[T]]$ с бесконечными радиусами сходимости. (В другой терминологии: является *p*-адической *мероморфной* функцией, или является отношением двух *целых* *p*-адических функций.)

Докажем это индукцией по числу переменных n (т. е. по размерности $n-1$ гиперповерхности H_f). При $n=0$ (т. е. когда H_f пусто) утверждение тривиально. Предположим, что оно справедливо для 1, 2, ..., $n-1$ переменных. Вместо того чтобы доказывать наше утверждение для

$$Z(H_f/\mathbb{F}_q;\ T)=\exp(\textstyle\sum N_sT^s/s),$$

достаточно доказать его для

$$Z'(H_f/\mathbb{F}_q;\ T)\ \overline{\text{def}}\ \exp\left(\sum_{s=1}^{\infty}N_s'T^s/s\right),$$

где

$N_s'\ \overline{\text{def}}$ число n-наборов $(x_1,\ \ldots,\ x_n)\in\mathbb{F}_{q^s}^n$, для которых

$f(x_1,\ \ldots,\ x_n)=0$ *и* все x_i отличны от нуля $=$

$=$ число n-наборов $(x_1,\ \ldots,\ x_n)\in\mathbb{F}_{q^s}^n$, для которых

$$f(x_1,\ \ldots,\ x_n)=0,\ \text{а}\ x_i^{q^s-1}=1,\ i=1,\ \ldots,\ n.$$

Действительно, чем отличается $Z'(H_f/\mathbb{F}_q;\ T)$ от $Z(H_f/\mathbb{F}_q;\ T)$? Очевидно,

$$Z(H_f/\mathbb{F}_q;\ T)=Z'(H_f/\mathbb{F}_q;\ T)\cdot\exp(\textstyle\sum(N_s-N_s')T^s/s),$$

причем экспоненциальный множитель в правой части есть дзета-функция объединения n гиперповерхностей H_i $(i=1, \ldots, n)$ меньшей [1]) размерности $(n-2)$, заданных уравнениями $f(X_1, \ldots, X_n)=0$ и $X_i=0$. Дзета-функция такого многообразия есть произведение дзета-функций для каждой H_i, *деленное* на произведение дзета-функций попарных пересечений H_i и H_j $(i\neq j)$ (т. е. $(n-3)$-мерных гиперповерхностей, заданных системой уравнений $X_i=X_j=0$ и $f(X_1, \ldots, X_n)=0$), *умноженное* на произведение дзета-функций тройных пересечений, *деленное* на произведение дзета-функций четверных пересечений, и т. д. Все эти дзета-функции p-адически мероморфны по предположению индукции [2]). Поэтому достаточно установить p-адическую мероморфность для Z', а отсюда уже будет следовать p-адическая мероморфность Z.

Фиксируем некоторое целое $s\geqslant 1$. Пусть $q=p^r$. Напомним, что если t обозначает представитель Тейхмюллера элемента $a\in\mathbb{F}_{q^s}$, то корень степени p из 1, равный $\varepsilon^{\mathrm{Tr}\,a}$, можно выразить через t при помощи p-адически аналитической функции

$$\varepsilon^{\mathrm{Tr}\,a}=\Theta(t)\,\Theta(t^p)\,\Theta(t^{p^2})\ldots\Theta(t^{p^{rs-1}}).$$

Одно из основных и просто доказываемых свойств характеров (см. ниже упр. 3—5) заключается в следующем:

$$\sum_{x_0\in\mathbb{F}_{q^s}}\varepsilon^{\mathrm{Tr}\,(x_0u)}=\begin{cases}0, & \text{если } u\in\mathbb{F}_{q^s}^{\times},\\ q^s, & \text{если } u=0,\end{cases}$$

или, после вычитания члена с $x_0=0$,

$$\sum_{x_0\in\mathbb{F}_{q^s}^{\times}}\varepsilon^{\mathrm{Tr}\,(x_0u)}=\begin{cases}-1, & \text{если } u\in\mathbb{F}_{q^s}^{\times},\\ q^s-1, & \text{если } u=0.\end{cases}$$

[1]) Это верно лишь для достаточно общей гиперповерхности. Однако заметим, что если $\dim H_i>n-2$, то $H_i=\mathbb{A}^{n-1}_{\mathbb{F}_q}$, а в этом случае дзета-функция контролируема, так как хорошо известна. Это следует иметь в виду и в дальнейших рассуждениях. — *Прим. перев.*

[2]) Либо из их явного вида в случае многообразия $\mathbb{A}^{n-1}_{\mathbb{F}_q}$ (см. предыдущее примечание). — *Прим. перев.*

Применим это к функции $u=f(x_1, \ldots, x_n)$ и просуммируем результат по всем $x_1, \ldots, x_n\in\mathbb{F}_{q^s}^{\times}$. Получим

$$\sum_{x_0,\,x_1,\,\ldots,\,x_n\in\mathbb{F}_{q^s}^{\times}}\varepsilon^{\mathrm{Tr}\,(x_0f(x_1,\,\ldots,\,x_n))}=q^sN'_s-(q^s-1)^n.$$

Заменим теперь все коэффициенты в $X_0f(X_1, \ldots, X_n)\in\mathbb{F}_q[X_0, X_1, \ldots, X_n]$ их представителями Тейхмюллера; при этом получится многочлен $F(X_0, X_1, \ldots, X_n)=\sum_{i=1}^{N}a_iX^{w_i}\in\Omega[X_0, X_1, \ldots, X_n]$, где X^{w_i} обозначает моном $X_0^{w_{i0}}X_1^{w_{i1}}\ldots X_n^{w_{in}}$, $w_i=(w_{i0}, w_{i1}, \ldots, w_{in})$. В этом случае

$$q^sN'_s=(q^s-1)^n+\sum_{x_0,\,x_1,\,\ldots,\,x_n\in\mathbb{F}_{q^s}^{\times}}\varepsilon^{\mathrm{Tr}\,(x_0f(x_1,\,\ldots,\,x_n))}=$$

$$=(q^s-1)^n+\sum_{\substack{x_0,\,x_1,\,\ldots,\,x_n\in\Omega,\\ x_0^{q^s-1}=\ldots=x_n^{q^s-1}=1}}\prod_{i=1}^{N}\Theta(a_ix^{w_i})\times$$

$$\times\Theta(a_i^px^{pw_i})\ldots\Theta\left(a_i^{p^{rs-1}}x^{p^{rs-1}w_i}\right).$$

Заметим, что поскольку все коэффициенты многочлена $f(X_1, \ldots, X_n)$ лежат в $\mathbb{F}_q$, а $q=p^r$, то $a_i^{p^r}=a_i$. Положим теперь

$$G(X_0, \ldots, X_n)\overset{\text{def}}{=}\prod_{i=1}^{N}\Theta(a_iX^{w_i})\,\Theta(a_i^pX^{pw_i})\ldots\Theta\left(a_i^{p^{r-1}}X^{p^{r-1}w_i}\right).$$

Тогда

$$q^sN'_s=(q^s-1)^n+\sum_{\substack{x_0,\,x_1,\,\ldots,\,x_n\in\Omega\\ x_0^{q^s-1}=\ldots=x_n^{q^s-1}=1}}G(x)\cdot G(x^q)\cdot G(x^{q^2})\cdots G(x^{q^{s-1}}).$$

Так как каждый ряд $\Theta\left(a_i^{p^j}X^{p^jw_i}\right)$ принадлежит R_0 (см. ниже упр. 2), то это же справедливо для G:

$$G(X_0, \ldots, X_1)\in R_0\subset\Omega[[X_0, \ldots, X_n]].$$

Следовательно, по лемме 3

$$q^s N'_s = (q^s - 1)^n + (q^s - 1)^{n+1} \operatorname{Tr}(\Psi^s),$$

т. е.

$$N'_s = \sum_{i=0}^{n} (-1)^i \binom{n}{i} q^{s(n-i-1)} + \sum_{i=0}^{n+1} (-1)^i \binom{n+1}{i} q^{s(n-i)} \operatorname{Tr}(\Psi^s).$$

Пусть (напомним, что A — матрица отображения Ψ)

$$\Delta(T) \overset{\text{def}}{=} \det(1 - AT) = \exp_p\left\{ - \sum_{s=1}^{\infty} \operatorname{Tr}(\Psi^s) T^s/s \right\}.$$

Тогда из предыдущего видно, что

$$\begin{aligned} Z'(H_i/\mathbb{F}_q;\ T) &= \exp_p\left\{ \sum_{s=1}^{\infty} N'_s T^s/s \right\} = \\ &= \prod_{i=0}^{n} \left[\exp_p\left\{ \sum_{s=1}^{\infty} q^{s(n-i-1)} T^s/s \right\} \right]^{(-1)^i \binom{n}{i}} \times \\ &\times \prod_{i=0}^{n+1} \left[\exp_p\left\{ \sum_{s=1}^{\infty} q^{s(n-i)} \operatorname{Tr}(\Psi^s) T^s/s \right\} \right]^{(-1)^i \binom{n+1}{i}} = \\ &= \prod_{i=0}^{n} (1 - q^{n-i-1})^{(-1)^{i+1} \binom{n}{i}} \prod_{i=0}^{n+1} \Delta(q^{n-i}T)^{(-1)^{i+1} \binom{n+1}{i}}. \end{aligned}$$

Каждый член последнего «альтернированного произведения» является целой p-адической функцией по лемме 4.

На этом завершается доказательство p-адической мероморфности дзета-функции — центральный результат в доказательстве теоремы Дворка. В следующем параграфе будет установлена представимость дзета-функции в виде отношения двух многочленов.

Упражнения

1. Пусть $t \in \Omega$ — примитивный корень степени $(p^s - 1)$ из 1. Докажите, что t, t^p, t^{p^2}, ..., $t^{p^{s-1}}$ исчерпывают все элементы, сопряженные с t над $\mathbb{Q}_p$. Другими словами, сопряженные с представителем Тейхмюллера элемента $a \in \mathbb{F}_q$ совпадают с представителями Тейхмюллера сопряженных с a элементов над $\mathbb{F}_p$.

2. Пусть $a \in D(1)$, а $X^w = X_1^{w_1} \dots X_n^{w_n}$. Докажите, что $\Theta(aX^w) \in R_0$.

3. Пусть $\sigma_1, \dots, \sigma_s$ — различные автоморфизмы поля K. Докажите, что не существует нетривиальных комбинаций $\sum a_i \sigma_i$, для которых $\sum a_i \sigma_i(x) = 0$ при любом $x \in K$. (*Указание*: воспользуйтесь индукцией по числу ненулевых a_i; в случае затруднений см. книгу Ленга [(a) 3], стр. 238.) Выведите отсюда, что отображение следа Tr из $\mathbb{F}_q$ в $\mathbb{F}_p$ ненулевое.

4. Пусть $\varepsilon \in \Omega$ — примитивный корень степени p из 1. Докажите, что $\sum_{x \in \mathbb{F}_q} \varepsilon^{\operatorname{Tr} x} = 0$. (*Указание*: произведите замену $x \longmapsto x + x_0$, где $x_0 \in \mathbb{F}_p$ имеет ненулевой след.)

5. Докажите, что

$$\sum_{x \in \mathbb{F}_{q^s}^{\times}} \varepsilon^{\operatorname{Tr}(xu)} = \begin{cases} -1, & \text{если } u \in \mathbb{F}_{q^s}^{\times}, \\ q^s - 1, & \text{если } u = 0. \end{cases}$$

6. Докажите, что для любых целых положительных n и a

$$\sum_{\zeta \in \Omega,\, \zeta^n = 1} \zeta^a = \begin{cases} n, & \text{если } n \text{ делит } a, \\ 0 & \text{в противном случае.} \end{cases}$$

7. В обозначениях § 3 докажите, что $G \circ T_q = T_q \circ G_q$.

8. Распространите тождество

$$\det(1 - AT) = \exp_p\left(- \sum_{s=1}^{\infty} \operatorname{Tr}(A^s) T^s/s \right)$$

на бесконечные матрицы A при подходящих предположениях о сходимости следов.

9. *Задача на повторение.* Пусть $f(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{F}_q[X]$ — многочлен от одной переменной с коэффициентами в $\mathbb{F}_q$, $q = p^r$, и ненулевым постоянным членом. Предположим, что нам надо найти число N различных корней многочлена $f(X)$ в $\mathbb{F}_q$. Обозначим через A_i представитель Тейхмюллера элемента a_i, $i = 0, \dots, n$. Пусть $\varepsilon = 1 + \lambda$ — фиксированный примитивный корень из 1 степени p в Ω, а $\Theta(T)$ — ряд из § 2. Положим

$$G(X, Y) = \prod_{i=0}^{n} \prod_{j=0}^{r-1} \Theta\left(A_i^{p^j} X^{ip^j} Y^{p^j}\right).$$

Докажите что

$$N = \frac{q-1}{q} + \frac{1}{q} \sum_{\substack{x,\, y \in \Omega, \\ x^{q-1} = y^{q-1} = 1}} G(x, y).$$

§ 5. КОНЕЦ ДОКАЗАТЕЛЬСТВА

Теорема Дворка теперь легко выводится из следующего критерия представимости степенного ряда в виде рациональной функции.

Лемма 5. *Пусть* $F(T)=\sum_{i=0}^{\infty} a_i T^i \in K[[T]]$, *где* K — *произвольное поле. Целым числам* m, $s\geqslant 0$ *сопоставим матрицу* $A_{s,m}=\{a_{s+i+j}\}_{0\leqslant i,\ j\leqslant m}$:

$$\begin{pmatrix} a_s & a_{s+1} & a_{s+2} & \cdots & a_{s+m} \\ a_{s+1} & a_{s+2} & a_{s+3} & \cdots & a_{s+m+1} \\ a_{s+2} & a_{s+3} & a_{s+4} & \cdots & a_{s+m+2} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{s+m} & a_{s+m+1} & a_{s+m+2} & \cdots & a_{s+2m} \end{pmatrix}$$

Пусть $N_{s,m} \overset{\text{def}}{=} \det(A_{s,m})$. *Тогда ряд* $F(T)$ *равен отношению двух многочленов*

$$F(T)=\frac{P(T)}{Q(T)}, \quad P(T),\ Q(T)\in K[T],$$

в том и только том случае, когда существуют целые $m\geqslant 0$ *и* S, *для которых* $N_{s,m}=0$ *при всяком* $s\geqslant S$.

Доказательство. Предположим вначале, что $F(T)$ есть такое отношение. Пусть $P(T)=\sum_{i=0}^{M} b_i T^i$, а $Q(T)=\sum_{i=0}^{N} c_i T^i$. Тогда, приравнивая коэффициенты при T^i в соотношении $F(T)\cdot Q(T)=P(T)$ для $i>\max(M, N)$, получим

$$\sum_{j=0}^{N} a_{i-N+j}c_{N-j}=0.$$

Пусть $S=\max(M-N+1, 1)$, а $m=N$. Возьмем $s\geqslant S$ и запишем эти уравнения для $i=s+N, s+N+1, \ldots, s+2N$:

$$\begin{aligned} a_s c_N + a_{s+1}c_{N-1} + \ldots + a_{s+N}c_0 &= 0, \\ a_{s+1}c_N + a_{s+2}c_{N-1} + \ldots + a_{s+N+1}c_0 &= 0, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots & \\ a_{s+N}c_N + a_{s+N+1}c_{N-1} + \ldots + a_{s+2N}c_0 &= 0, \end{aligned}$$

Следовательно, матрица коэффициентов при c_j, равная $A_{s,N}$, имеет нулевой определитель:

$$N_{s,m}=N_{s,N}=0 \quad \text{для } s\geqslant S.$$

Обратно, предположим, что $N_{s,m}=0$ при $s\geqslant S$, где m выбрано минимальным с данным свойством: $N_{s,m}=0$ при всех $s\geqslant S$. Утверждается, что $N_{s,m-1}\neq 0$ для *всех* $s\geqslant S$.

Предположим противное. Тогда некоторая нетривиальная линейная комбинация первых m строк r_0, $r_1, \ldots, r_{m-1}$ матрицы $A_{s,m}$ обращается в нуль везде, кроме, может быть, последнего столбца. Пусть r_{i_0} — первая строка с ненулевым коэффициентом в этой линейной комбинации, т. е. i_0-я строка r_{i_0} равна

$$\alpha_1 r_{i_0+1}+\alpha_2 r_{i_0+2}+\ldots+\alpha_{m-i_0-1}r_{m-1},$$

кроме, может быть, элемента последнего столбца. Заменим r_{i_0} в $A_{s,m}$ на $r_{i_0}-(\alpha_1 r_{i_0+1}+\ldots+\alpha_{m-i_0-1}r_{m-1})$ и рассмотрим следующие две возможности:

(1) $i_0>0$. Тогда мы получаем матрицу вида

$$\left(\begin{array}{cccc} a_s & a_{s+1} & \cdots & a_{s+m} \\ \hline a_{s+1} & a_{s+2} & \cdots & a_{s+m+1} \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots\ 0 & \beta \\ \vdots & \vdots & & \vdots \\ a_{s+m} & a_{s+m+1} & \cdots & a_{s+2m} \end{array}\right)$$

и определитель выделенной матрицы равен $N_{s+1,m-1}=0$.

(2) $i_0=0$. Тогда мы получаем

$$\left(\begin{array}{cccc} 0 & 0 & \cdots\ 0 & \beta \\ \hline a_{s+1} & a_{s+2} & \cdots & a_{s+m+1} \\ \vdots & \vdots & & \vdots \\ a_{s+m} & a_{s+m+1} & \cdots & a_{s+2m} \end{array}\right)$$

В этом случае $N_{s+1,m-1}$ совпадает с определителем каждой из двух выделенных матриц. Поскольку определитель $N_{s,m}$ всей матрицы равен 0, то либо определитель нижней выделенной матрицы равен 0, либо $\beta=0$

и определитель верхней выделенной матрицы равен 0. Поэтому $N_{s+1,\,m-1}=0$.

Итак, в любом случае $N_{s+1,\,m-1}=0$. Далее по индукции легко получить, что $N_{s',\,m-1}=0$ при всех $s'\geqslant s$. Это противоречит минимальности выбранного m.

Но тогда при любом $s\geqslant S$ мы имеем $N_{s,\,m}=0$ и $N_{s,\,m-1}\neq 0$. Следовательно, существует линейная комбинация строк матрицы $A_{s,\,m}$, равная строке из нулей. Более того, у *этой комбинации коэффициент последней строки отличен от нуля*. Таким образом, последняя строка матрицы $A_{s,\,m}$ при любом $s\geqslant S$ представима в виде линейной комбинации предыдущих m строк. Поэтому всякое решение линейной системы

$$\begin{gathered}a_S u_m+a_{S+1}u_{m-1}+\ldots+a_{S+m}u_0=0,\\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\\ a_{S+m-1}u_m+a_{S+m}u_{m-1}+\ldots+a_{S+2m-1}u_0=0\end{gathered}$$

является решением уравнения

$$a_{S+m}u_m+a_{S+m+1}u_{m-1}+\ldots+a_{S+2m}u_0=0,$$

а по индукции — любого линейного уравнения

$$a_s u_m+a_{s+1}u_{m-1}+\ldots+a_{s+m}u_0=0$$

при $s\geqslant S$. Из этого, очевидно, следует, что

$$\left(\sum_{i=0}^{m}u_iX^i\right)\cdot\left(\sum_{i=1}^{\infty}a_iX^i\right)$$

— многочлен (степени $<S+m$). □

Закончим теперь доказательство теоремы, используя лемму 5. Нам понадобится «p-адическая подготовительная теорема Вейерштрасса» (теорема 14, § IV.4) в следующей форме: если $F(T)$ — целая p-адическая функция, то для любого положительного вещественного R (равного рациональной степени p) существует многочлен $P(T)$ и p-адический степенной ряд $F_0(T)\in 1+T\Omega[[T]]$, который сходится на диске $D(R)$ радиуса R *вместе со своим обратным* $G(T)$, а $F(T)=P(T)\cdot F_0(T)$. Действительно, положите в теореме 14 $p^\lambda=R$; так как F целая, она сходится на $D(p^\lambda)$.

Для краткости будем писать $\mathrm{Z}(T)$ вместо $\mathrm{Z}(H_f/\mathbb{F}_q;\,T)$. В § 4 мы выяснили, что $\mathrm{Z}(t)=A(T)/B(T)$, где $A(T)$ и $B(T)$ — две целые p-адические функции. Выберем некоторое $R>q^n$; для простоты возьмем, например, $R=q^{2n}$. Применим теперь утверждение предыдущего абзаца к $B(T)$. Получим, что $B(T)=P(T)/G(T)$, где $G(T)$ сходится на $D(R)$. Пусть $F(T)=A(T)\cdot G(T)$. Этот ряд также сходится на $D(R)$. Итак,

$$F(T)=P(T)\cdot\mathrm{Z}(T).$$

Пусть $F(T)=\sum\limits_{i=0}^{\infty}b_iT^i\in 1+T\Omega[[T]]$, $P(T)=\sum\limits_{i=0}^{e}c_iT^i\in$ $\in 1+T\Omega[T]$, $\mathrm{Z}(T)=\sum\limits_{i=0}^{\infty}a_iT^i\in 1+T\mathbb{Z}[[T]]$. По лемме 2 из § 1

$$|a_i|_\infty\leqslant q^{in}.$$

Поскольку $F(T)$ сходится на $D(R)$, то для достаточно большого i

$$|b_i|_p\leqslant R^{-i}=q^{-2ni}.$$

Фиксируем некоторое $m>2e$. Пусть $A_{s,\,m}=\{a_{s+i+j}\}_{0\leqslant i,\,j\leqslant m}$, как и выше, а $N_{s,\,m}=\det(A_{s,\,m})$. Утверждается, что для данного m мы имеем $N_{s,\,m}=0$ при всех достаточно больших s. По лемме 5 отсюда будет следовать рациональность функции $\mathrm{Z}(T)$.

Приравнивая коэффициенты в соотношении $F(T)=$ $=P(T)\mathrm{Z}(T)$, находим

$$b_{j+e}=a_{j+e}+c_1a_{j+e-1}+c_2a_{j+e-2}+\ldots+c_ea_j.$$

Добавим в матрице $A_{s,\,m}$ к каждому $(j+e)$-му столбцу, начиная с последнего и двигаясь влево до e-го столбца, линейную комбинацию e предыдущих с коэффициентом c_k при $(j+e-k)$-м столбце. Тогда получится матрица, e первых столбцов которой те же, что и у $A_{s,\,m}$, а в остальных столбцах элементы a заменены соответствующими b. Определитель этой матрицы по-прежнему равен $N_{s,\,m}$. Используя ее вид, оценим $|N_{s,\,m}|_p$.

Так как $a_i\in\mathbb{Z}$, имеем $|a_i|_p\leqslant 1$. Поэтому $|N_{s,\,m}|_p\leqslant$ $\leqslant\left(\max\limits_{j\geqslant s+e}|b_j|_p\right)^{m+1-e}<R^{-s(m+1-e)}$ для достаточно больших s. Но $R=q^{2n}$, а $m>2e$, откуда $|N_{s,\,m}|_p<q^{-ns(m+2)}$.

С другой стороны, грубая оценка прямо для матрицы $A_{s,m}$ дает неравенство $|N_{s,m}|_\infty \leqslant (m+1)!\, q^{n(s+2m)(m+1)} = (m+1)!\, q^{2nm(m+1)} q^{ns(m+1)}$. Перемножая две указанные оценки, мы видим, что произведение p-адической нормы и обычной абсолютной величины для $N_{s,m}$ ограничено сверху выражением, которое меньше 1 при достаточно больших s:

$$|N_{s,m}|_p \cdot |N_{s,m}|_\infty < q^{-ns(m+2)} \cdot (m+1)!\, q^{2nm(m+1)} q^{ns(m+1)} = \frac{(m+1)!\, q^{2nm(m+1)}}{q^{ns}} < 1$$

при достаточно больших s. Однако $N_{s,m} \in \mathbb{Z}$, а единственное целое число n с этим свойством: $|n| \cdot |n|_p < 1$, есть число $n = 0$. Следовательно, $N_{s,m} = 0$ для всех достаточно больших s.

Таким образом, $Z(T)$ — рациональная функция и теорема Дворка доказана. □

ЛИТЕРАТУРА

Порядок работ внутри каждого из следующих пунктов приблизительно соответствует возрастанию их трудности. Для книг и больших статей это весьма грубая оценка, основанная главным образом на уровне подготовки, необходимой для понимания тех разделов, которые тесно связаны с материалом одной из наших глав I — V. [Работы, отмеченные звездочкой, добавлены при переводе. — *Перев.*]

(a) Подготовительная

1. Симмонс (Simmons G.) Introduction to topology and modern analysis. — McGraw-Hill, 1963.
2. Херстейн (Herstein I.) Topics in algebra. — John Wiley and Sons, 1975.
3. Ленг С. Алгебра. Пер. с англ. — М.: Мир, 1968.
4*. Гельфанд И. М. Лекции по линейной алгебре. — М.: Наука, 1966.
5*. Рудин У. Основы математического анализа. Пер. с англ. — М.: Мир, 1966.
6*. Куратовский К. Топология. Пер. с англ. — М.: Мир, т. 1, 1966; т. 2, 1969.

(b) Общая

1. Боревич З. И., Шафаревич И. Р. Теория чисел. — М.: Наука, 1964.
2. Ленг С. Алгебраическая теория чисел. Пер. с англ. — М.: Мир, 1966.
3. Серр Ж.-П. Курс арифметики. Пер. с франц. — М.: Мир, 1972.
4. Айрленд и Розен (Ireland K. and Rosen M.) Elements of number theory, including an introduction to equations over finite fields. — Bogden and Quigley, 1972.
5. Дынкин Е. Б., Успенский В. А. Математические беседы. — М.: Гостехиздат, 1952.
6. Малер (Mahler K.) Introduction to p-adic numbers and their functions. — Cambridge University Press, 1973.
7. Бахман (Bachman G.) Introduction to p-adic numbers and valuation theory. — Academic Press, 1964.
8. Монна (Monna A. F.) Analyse non-archimédienne. — Springer-Verlag, 1970.

(c) К главе II

1. Ивасава (Iwasawa K.) Lectures on p-adic L-functions. — Princeton University Press, 1972.
2. Кубота и Леопольдт (Kubota T., Leopoldt H. W.) Eine p-adische Theorie der Zetawerte I. — *J. Reine Angew. Math.*, 214/215 (1964), 328—339.
3. Катц (Katz N.) p-adic L-functions via moduli of elliptic curves. — Proceedings A. M. S. Summer Institute of Alg. Geom. at Arcata, Calif., 1974.
4. Ленг С. Введение в теорию модулярных форм. Пер. с англ. — М.: Мир, 1979.
5. Серр (Serre J.-P.) Formes modulaires et fonctions zêta p-adiques.

С другой стороны, грубая оценка прямо для матрицы $A_{s,m}$ дает неравенство $|N_{s,m}|_\infty \leqslant (m+1)!\, q^{n(s+2m)(m+1)} = (m+1)!\, q^{2nm(m+1)} q^{ns(m+1)}$. Перемножая две указанные оценки, мы видим, что произведение p-адической нормы и обычной абсолютной величины для $N_{s,m}$ ограничено сверху выражением, которое меньше 1 при достаточно больших s:

$$|N_{s,m}|_p \cdot |N_{s,m}|_\infty < q^{-ns(m+2)} \cdot (m+1)!\, q^{2nm(m+1)} q^{ns(m+1)} = \frac{(m+1)!\, q^{2nm(m+1)}}{q^{ns}} < 1$$

при достаточно больших s. Однако $N_{s,m} \in \mathbb{Z}$, а единственное целое число n с этим свойством: $|n| \cdot |n|_p < 1$, есть число $n = 0$. Следовательно, $N_{s,m} = 0$ для всех достаточно больших s.

Таким образом, $Z(T)$ — рациональная функция и теорема Дворка доказана. □

ЛИТЕРАТУРА

Порядок работ внутри каждого из следующих пунктов приблизительно соответствует возрастанию их трудности. Для книг и больших статей это весьма грубая оценка, основанная главным образом на уровне подготовки, необходимой для понимания тех разделов, которые тесно связаны с материалом одной из наших глав I — V. [Работы, отмеченные звездочкой, добавлены при переводе. — *Перев.*]

(a) Подготовительная

1. Симмонс (Simmons G.) Introduction to topology and modern analysis. — McGraw-Hill, 1963.
2. Херстейн (Herstein I.) Topics in algebra. — John Wiley and Sons, 1975.
3. Ленг С. Алгебра. Пер. с англ. — М.: Мир, 1968.
4*. Гельфанд И. М. Лекции по линейной алгебре. — М.: Наука, 1966.
5*. Рудин У. Основы математического анализа. Пер. с англ. — М.: Мир, 1966.
6*. Куратовский К. Топология. Пер. с англ. — М.: Мир, т. 1, 1966; т. 2, 1969.

(b) Общая

1. Боревич З. И., Шафаревич И. Р. Теория чисел. — М.: Наука, 1964.
2. Ленг С. Алгебраическая теория чисел. Пер. с англ. — М.: Мир, 1966.
3. Серр Ж.-П. Курс арифметики. Пер. с франц. — М.: Мир, 1972.
4. Айрленд и Розен (Ireland K. and Rosen M.) Elements of number theory, including an introduction to equations over finite fields. — Bogden and Quigley, 1972.
5. Дынкин Е. Б., Успенский В. А. Математические беседы. — М.: Гостехиздат, 1952.
6. Малер (Mahler K.) Introduction to p-adic numbers and their functions. — Cambridge University Press, 1973.
7. Бахман (Bachman G.) Introduction to p-adic numbers and valuation theory. — Academic Press, 1964.
8. Монна (Monna A. F.) Analyse non-archimédienne. — Springer-Verlag, 1970.

(c) К главе II

1. Ивасава (Iwasawa K.) Lectures on p-adic L-functions. — Princeton University Press, 1972.
2. Кубота и Леопольдт (Kubota T., Leopoldt H. W.) Eine p-adische Theorie der Zetawerte I. — *J. Reine Angew. Math.*, 214/215 (1964), 328—339.
3. Катц (Katz N.) p-adic L-functions via moduli of elliptic curves. — Proceedings A. M. S. Summer Institute of Alg. Geom. at Arcata, Calif., 1974.
4. Ленг С. Введение в теорию модулярных форм. Пер. с англ. — М.: Мир, 1979.
5. Серр (Serre J.-P.) Formes modulaires et fonctions zêta p-adiques.

In: Modular functions of one variable III (Lecture Notes in Math. 350). — Springer-Verlag, 1973.

6. Манин Ю. И. Периоды параболических форм и p-адические ряды Гекке. — *Матем. сб.*, **92** (1973), № 3, 378—400. (Особо отметим § 8.)

7. Вишик М. М. Неархимедовы меры, связанные с рядами Дирихле. — *Матем. сб.*, **99** (141) (1976), № 2, 248—266.

8. Амис и Велю (Amice Y., Vélu J.) Distributions p-adiques associées aux séries de Hecke. — Journées arithmétiques, 1974.

9. Катц (Katz N.) p-adic properties of modular schemes and modular forms. In: Modular functions of one variable III (Lecture Notes in Math. 350). — Springer-Verlag, 1973.

10. Катц (Katz N.) The Eisenstein measure and p-adic interpolation. — *Amer. J. Math.*, **99** (1977), 238—311.

11. Катц (Katz N.) p-adic interpolation of real analytic Eisenstein series. — *Ann. of Math.*, **104** (1976), 459—571.

12. Мазур и Суинертон-Дайер (Mazur B., Swinnerton-Dyer S.) Arithmetic of Weil curves. — *Invent. Math.*, **25** (1974), 1—61.

(d) К главе IV

1. Дворк (Dwork B.) § 1 из: On zeta function of a hypersurface. — *Publ. Math. I. H. E. S.*, **12** (1962), 7—17.

2. Амис (Amice Y.) Les nombres p-adiques. — Presses Universitaires de France, 1975.

(e) К главе V

1. Вейль (Weil A.) Number of solutions of equations in finite fields. — *Bull. Amer. Math. Soc.*, **55** (1949), 497—508.

2. Серр (Serre J.-P.) Rationalité des fonctions ζ des variétés algébriques (d'aprés Bernard Dwork). — Séminaire Bourbaki, No. 198, February 1960.

3. Дворк Б. О рациональности дзета-функции алгебраического многообразия. Пер. с англ. — Сб. *Математика*, **5:6** (1961), 55—72.

4. Монски (Monsky P.) p-adic analysis and zeta functions. Lectures at Kyoto University. — Kinokuniya Book Store, Tokyo, or Brandeis Univ. Math. Dept., 1970.

5. Катц (Katz N.) Une formule de congruence pour la fonction ζ. — S. G. A. 7 II (Lecture Notes in Math. 340), Springer-Verlag, 1973.

6. Дворк (Dwork B.) On the zeta function of a hypersurface. — *Publ. Math. I. H. E. S.*, **12** (1962), 5—68.

7. Дворк (Dwork B.) On the zeta function of a hypersurface II. — *Ann. of Math.*, **80** (1964), 227—299.

8. Дворк (Dwork B.) A deformation theory for the zeta function of a hypersurface. — Proc. Int. Cong. Math. 1962 Stockholm, 247—259.

9. Катц Н. Работы Дворка. Пер. с франц. — Сб. *Математика*, **18:6** (1974), 3—19.

noise. Acta Math., 1964, **112**, № 1-2, 99—143 (РЖМат, 1965, 6В60)
36. **Rozanov Yu. A.**, Some approximation problems in the theory of stationary processes. J. Multivar. Anal. 1972, 2, № 2, 135—144 (РЖМат, 1972, 11В80)
37. —, Innovation processes and non-anticipative processes. J. Multivar. Anal., 1973, 3
38. **Shepp L. A.**, Radon—Nicodym derivaties of Gaussian measures. Ann. Math. Statist., 1966, **37**, № 2, 321—354 (РЖМат, 1971, 10В155)
39. **Stone M. H.**, Linear transformations in Hilbert space. N.-Y., 1932
40. **Wiener N.**, Masani P., The prediction theory of multivariate stochastic processes. II. The linear predictor. Acta Math, m 1958, **99**, № 1-2, 93—137 (РЖМат, 1960, 1919)

СОДЕРЖАНИЕ

Технический редактор *Л. И. Дрожилова*

Подписано в печать 26/II-1974 г. Формат бумаги 60×90¹/₁₆ Тираж 1200 экз.
Печ. л. 16,25 Уч.-изд. л. 13,98 Цена 1 р. 56 к. Заказ 7374

Производственно-издательский комбинат ВИНИТИ, Люберцы, Октябрьский пр., 403

Опечатки к сборнику «Итоги науки и техники» выпуск «СОВРЕМЕННЫЕ ПРОБЛЕМЫ МАТЕМАТИКИ. Т. 3»

Стр.	Строка	Напечатано	Следует читать
33	18 сверху	$I(g)\,1^{<}$	$I(g)^{<}$
	19 сверху	$I(g^{-1})\,1^{<}$	$I(g^{-1})^{<}$
72	2 снизу	X^{p_1}	X^{p_2}
77	19 сверху	$\Gamma/\Omega.$	$\Gamma\setminus\Omega$
	20 сверху	сроении	строении
	21 сверху	явлтяется	является
89	10 снизу	Γ/Δ_Γ	$\Gamma\setminus\Delta_\Gamma$
95	19 сверху	$U_0(t)=e^{-iH^0t},$	$U_0(t)=e^{-iH_0t},$
100	17 сверху	$\gamma=\pm\,\dddot{.}$	$\gamma=\pm 1:$
114	10 сверху	$s_{22}(k)=s_{11}(k).$	$\widetilde{s}_{22}(k)=s_{11}(k).$
145	4 снизу	$\{f,\ g=\}f^{(1)}g^2-f^{(2)}g^{(1)}.$	$\{f,\ g\}=f^{(1)}g^{(2)}-f^{(2)}g^{(1)}.$
220	4 снизу	$\int_{-\infty}^{\infty}\frac{\log f_\alpha}{1+\lambda^2}\,d\lambda>cI,$	$\int_{-\infty}^{\infty}\frac{\log f(\lambda)}{1+\lambda^2}\,d\lambda>-cI,$

Содержится подробный обзор ряда важных и интересных результатов в современной теории случайных процессов 2-го порядка (в частности нестационарных), изложенне принадлежащей автору концепции, с позиции которой эти результаты переосмыслены и которая позволила автору получить новые теоремы.

Технический редактор *Л. И. Дрожилова*

Подписано в печать 26/II-1974 г. Формат бумаги 60×90¹/₁₆ Тираж 1200 экз.
Печ. л. 16,25 Уч.-изд. л. 13,98 Цена 1 р. 56 к. Заказ 7374

Производственно-издательский комбинат ВИНИТИ, Люберцы, Октябрьский пр., 403

Опечатки к сборнику «Итоги науки и техники» выпуск «СОВРЕМЕННЫЕ ПРОБЛЕМЫ МАТЕМАТИКИ. Т. 3»

Стр.	Строка	Напечатано	Следует читать
33	18 сверху	$I(g)\,1^{<}$	$I(g)^{<}$
	19 сверху	$I(g^{-1})\,1^{<}$	$I(g^{-1})^{<}$
72	2 снизу	X^{p_1}	X^{p_2}
77	19 сверху	$\Gamma/\Omega.$	$\Gamma\setminus\Omega$
	20 сверху	строении	строении
	21 сверху	являтяется	является
89	10 снизу	Γ/Δ_Γ	$\Gamma\setminus\Delta_\Gamma$
95	19 сверху	$U_0(t)=e^{-iH^0t},$	$U_0(t)=e^{-iH_0t},$
100	17 сверху	$\gamma=\pm\,\dddot{.}$	$\gamma=\pm 1:$
114	10 сверху	$s_{22}(k)=s_{11}(k).$	$\widetilde{s}_{22}(k)=s_{11}(k).$
145	4 снизу	$\{f,\ g=\}f^{(1)}g^2-f^{(2)}g^{(1)}.$	$\{f,\ g\}=f^{(1)}g^{(2)}-f^{(2)}g^{(1)}.$
220	4 снизу	$\int_{-\infty}^{\infty}\frac{\log f_\alpha}{1+\lambda^2}\,d\lambda>cI,$	$\int_{-\infty}^{\infty}\frac{\log f(\lambda)}{1+\lambda^2}\,d\lambda>-cI,$

Содержится подробный обзор ряда важных и интересных результатов в современной теории случайных процессов 2-го порядка (в частности нестационарных), изложенне принадлежащей автору концепции, с позиции которой эти результаты переосмыслены и которая позволила автору получить новые теоремы.

СЕРИЯ

СОВРЕМЕННЫЕ ПРОБЛЕМЫ МАТЕМАТИКИ

Выпуск «Современные проблемы математики. Том 3» состоит из трех статей.

В статье *Ю. И. Манина* «*p*-аднческие автоморфные функции» дается системное изложение *p*-адических аналогов классических автоморфных функций Якоби, Абеля и Шоттки. Рассматривается функциональный и алгебро-геометрический аспекты теории. Строится аналог решетки периодов для алгебраических кривых униформизируемых *p*-адическими дискретными группами.

В статье *Л. Д. Фаддеева* «Обратная задача квантовой теории рассеяния. Излагается развитие проблемы о восстановлении потенциала в операторе Шрёдингера по амплитуде рассеяния в течение последних 15 лет

В статье *Ю. А. Розанова* «Обновляющие процессы и проблема факторизации» содержится подробный обзор ряда важных и интересных результатов современной теории случайных процессов 2-го порядка (в частности нестационарных), изложение принадлежащей автору концепции, которая позволила ему получить новые теоремы.

Выпуск рассчитан на работников научно-исследовательских институтов, преподавательский состав, аспирантов и студентов высших учебных заведений.

ОТ РЕДАКЦИИ

Выпуси «Современные проблемы математики. Т. 3» охватывает в основном литературу, прореферированную в Реферативном журнале «Математика» за 1953—1973 гг. К каждой статье прилагается библиография вопроса со ссылкой на реферат.

Редакция обращается ко всем читателям с просьбой прислать свои отзывы и пожелания в отношении дальнейшей формы и содержания выпусков «Итоги науки и техники» по адресу: *Москва, 125219, Балтийская ул., 14, ВИНИТИ, Отдел математики.*

Авторы:
проф. *Ю. И. Манин*, проф. *Л. Д. Фаддеев*, проф. *Ю. А. Розанов*

УДК 517.862.3

p-АДИЧЕСКИЕ АВТОМОРФНЫЕ ФУНКЦИИ

Ю. И. Манин

ВВЕДЕНИЕ

Классические автоморфные функции появляются в следующей ситуации: дана комплексная область D, на которой действует дискретная группа Γ; рассматриваются функции на D, обладающие определенными свойствами аналитичности и предписанным поведением под действием Γ. Простейший случай — Γ-периодичность; типичный случай — появление «множителей автоморфности».

Алгебраическая геометрия с самого начала служила богатым источником задач и мотивировок этой теории. Действительно, классические автоморфные функции одной переменной — это прообразы мероморфных функций и дифференциалов римановой поверхности на универсальной накрывающей $D \longrightarrow X$.

Роль Γ играет фундаментальная группа X (или некоторая ее факторгруппа). Аналогично, абелевы функции — это аналитические функции с $2n$ комплексными периодами от n переменных, то есть рациональные функции на алгебраическом торе.

В последние годы и на эту ветвь классического анализа распространились тенденции к алгебраизации и связанные с этим попытки рассматривать неархимедовы пополнения поля рациональных чисел на равных правах с архимедовыми R и C.

Эти обобщения оказались успешными и уже привели к ясной картине p-адической униформизации алгебраических кривых и абелевых многообразий. Новая p-адическая теория сама по себе отличается внутренней красотой и получила важные арифметические приложения (см., например, Серр [23]).

В этом обзоре предпринята попытка изложить основные известные факты теории, дополнив их некоторыми новыми результатами. Опишем кратко план работы.

Пусть K — конечное расширение поля p-адических чисел Q_p. Мы рассматриваем три пары p-адических объектов {область, группа автоморфизмов}, с которыми связаны автоморфные функции.

В главе I это мультипликативная группа K^* и ее дискретная циклическая подгруппа $\Gamma=(q^n)\subset K^*$, $|q|<1$. Автоморфные функции — это всюду сходящиеся ряды Лорана или их отношения с естественными свойствами периодичности относительно умножения аргумента на q. Основной результат: поле инвариантных функций является полем функций на эллиптической кривой над K с группой точек $K^*/(q^n)$.

Этот случай был впервые рассмотрен Тэйтом (детали опубликованы в [23], [21]; см. также [22]) и лег в основу дальнейших обобщений.

В главе II рассмотрено обобщение на случай группы $(K^*)^n$ с дискретной подгруппой B ранга n. Аналитическая теория приводит к конструкции абелева многообразия с группой точек $(K^*)^n/B$. Возможность такого построения была непосредственно видна после работы Тэйта; публикации Морикавы [17], Герритцена [3, 4], Рейно [20] исследуют различные аспекты задачи; Мамфорд [19] внес в эту проблему новые идеи.

Глава III посвящена значительно более неожиданному обобщению теории Тэйта на случай униформизации кривых рода >1. Это обобщение принадлежит также Мамфорду [18]. В нем роль Γ играет так называемая группа Шоттки — свободная дискретная подгруппа ранга $n\geqslant 1$ в группе дробно-линейных преобразований $\mathrm{PGL}(2, K)$. Она действует дискретно на некоторой области $\Omega\subset P_K{}^1$, дополнение к которой при $n\geqslant 2$ является дисконтинуумом Кантора. Фактор $\Gamma\backslash\Omega$ можно снабдить структурой алгебраической кривой рода n над K, и автоморфные функции относительно Γ определяют эту структуру.

В этой главе содержатся основные новые результаты настоящей работы. Дело в том, что Мамфорд ввел в теорию чрезвычайно сильный и плодотворный метод формальных схем, очень прояснивший геометрический аспект задачи. Однако функциональные аспекты при этом остаются в тени, будучи скрыты в общих когомологических теоремах Гротендика. Наш подход состоит в явном построении соответствующих автоморфных функций по образцу теории Тэйта. В результате оказалось возможным также дать прямую аналитическую конструкцию многообразия Якоби (для кривых Шоттки — Мамфорда) и отображения кривой в свой якобиан. Получившиеся формулы для «мультипликативных абелевых интегралов», кажется, не рассматривались в классическом случае и имеют интересную структуру.

Наконец, глава IV содержит обзор общей теории p-адических аналитических пространств и ее приложений к задачам алгебраизма аналитических объектов, построенных в предыдущих главах. Основы этой теории были также заложены Тэйтом [28]; наиболее важные из последующих работ — статьи Киля [12], [13], работа Герритцена и Грауэрта [7] и неопубликованный препринт Рейно о связи с формальными схемами. К сожалению, систематического изложения основ этой теории с полными доказательствами до сих пор нет. Кроме того, отсутствует исследование фундаментальной группы аналитических пространств, что особенно катастрофично для общей теории униформизации и автоморфных функций. Это обусловило несколько отрывочный характер изложения в четвертой главе. В предшествующих главах все основные факты доказаны.

Глава I

ФУНКЦИИ ЯКОБИ-ТЭЙТА

§ 1. ОСНОВНЫЕ СОГЛАШЕНИЯ

1.1. На протяжении всей работы p-фиксированное простое число, Q_p — поле p-адических чисел. Поле K обычно означает некоторое конечное расширение Q_p, K — алгебраическое замыкание K. В следующем параграфе этой главы K может быть пополнением алгебраического замыкания Q_p.

В большинстве случаев результаты работы остаются верными также для дискретно нормированных полных полей конечной характеристики, а иногда и для любых полных нормированных неархимедовых полей. Однако на этих обобщениях мы не останавливались. Алгебро-геометрические аспекты теории в такой (и большей) общности изучены Мамфордом [18, 19].

Символ $O\subset K$ означает кольцо целых чисел поля K $m\subset O$ — максимальный идеал, $k=O/m$ — поле классов вычетов. Символом $\mathrm{ord}: K\to Z$ мы обозначим показатель: $\mathrm{ord}\,\pi=1$, если $m=O\pi$. Иногда удобно нормировать его, полагая (для конечных расширений L поля K) $\mathrm{ord}(\pi_L)=\frac{1}{e_{L/K}}$, где $m_L=O_L\pi_L$, $e_{L/K}$ — индекс ветвления L над K. Это дает распространение ord на K. В других случаях удобно полагать $\mathrm{ord}\,\pi_L=1$, меняя значение ord на K; мы будем оговаривать выбор, когда возможна двусмысленность.

Иногда удобно рассматривать неархимедову норму $|\ |: K \to R$, полагая $|a| = c^{\operatorname{ord} a}$, где $0 < c < 1$. В качестве c можно взять, скажем, p^{-1}. Норма определяет топологию K, так что условие $a_i \to 0$ равносильно условию $\operatorname{ord} a_i \to \infty$.

1.2. Ссылка типа «см. п. 2.3» означает подпункт 3 из § 2 той главы, в которой находится ссылка. При отсылке в другую главу ее номер указывается явно. Значок ■ отмечает конец доказательства или его отсутствие.

§ 2. p-АДИЧЕСКИЕ РЯДЫ ЛОРАНА

2.1. В этом параграфе $[K : Q_p] < \infty$ или же K-пополнение алгебраического замыкания поля Q_p.

Рассмотрим некоторый формальный ряд Лорана над K: $f(z) = \sum_{-\infty}^{\infty} a_i z^i$. Он сходится в точке $z_0 \in \overline{K}^*$, если и только если $\lim |a_i z_0^i| \to 0$ при $i \to \pm\infty$ или, что то же, если $\operatorname{ord} a_i + i \operatorname{ord} z_0 \to \infty$ при $i \to \pm\infty$.

Предположим, что f сходится при всех z с $0 < r \leqslant |z| \leqslant s$. Назовем точку $t \in [r, s]$ критической (для f), если существуют такие $i \neq j$, что $|a_i| t^i = |a_j| t^j = \max\limits_{k \in Z} |a_k| t^k$ (максимум существует, ибо $|a_k| t^k \to 0$ при $k \to \pm\infty$). Ниже мы будем работать также с показателем вместо модуля; так как $\operatorname{ord} a = \log_c |a|$, интервал $[r, s]$ перейдет в $[\log s, \log r]$ и точки $\log t$, отвечающие критическим t, мы тоже будем называть критическими.

Следующая основная теорема в этом параграфе дает качественное описание f как функции от $z \in \overline{K}$.

2.2. Теорема. а) f имеет только конечное число критических точек на $[r, s]$. Пусть это будут точки $t_0 = r \leqslant t_1 < t_2 < \ldots < t_l \leqslant s = t_{l+1}$ (возможно, за исключением r, s).

б) Вне критических значений $|z|$ модуль $|f(z)|$ зависит только от $|z|$. Эта зависимость кусочно-степенная, непрерывная, с растущими показателями степени: при $t_1 < |z| = t < t_{i+1}$, $|f(z)| = |a_{m_i}| t^{m_i} = \max\limits_k |a_k| t^k$. Здесь $m_0 < m_1 < \ldots < m_l$ и левый предел $|f(z)|$ в $|z| = t_i$ совпадает с правым пределом.

в) Все t_i принадлежат $|\overline{K}| = \{|z| \mid z \in \overline{K}\}$. На множестве $z \in K$ с $|z| = t_i$ имеем $\sup |f(z)| = \max\limits_{z \in K} |f(z)| = \max\limits_k |a_k| t_i^k$, если поле классов вычетов K достаточно велико и $t_i \in |K|$; $\inf |f(z)| = \min |f(z)| = 0$. В частности, $|f(z)|$ имеет нули при $|z| = t_i$, а также принимает любые допустимые значения между 0 и $\max |a_k| t_i^k$.

г) Число нулей $f(z)$ на $|z| = t_i$ конечно и равно (с учетом надлежаще определенных кратностей) $m_i - m_{i-1}$.

2.3. Примеры. а) $f(z) = \frac{1}{1-z} = 1 + z + z^2 + \ldots$. Ряд сходится при $0 \leqslant |z| < 1$; критических точек нет; $|f(z)| = 1$. Таким образом, по графику модуля нельзя определить, что в точке $z = 1$ есть полюс. Все дело, конечно, в неархимедовости: «окружность» $|z| = 1$ на самом деле открыта, так что существует фиксированная окрестность полюса $|z - 1| < r < 1$, в которую нельзя попасть, оставаясь внутри единичного круга.

б) $\theta(z) = \prod\limits_{n>0} (1 - q^n z) \prod\limits_{n \geqslant 0} (1 - q^n z^{-1})$, $|q| < 1$. Это более интересный случай. Прежде всего, нетрудно убедиться, что это произведение разлагается во всюду сходящийся ряд Лорана. Далее, имеет место функциональное уравнение

$$\theta(qz) = -(qz)^{-1}\theta(z). \tag{1}$$

Критические точки: $t = |q|^n$, $n \in Z$; в них нули кратности единица. Чтобы построить график $\operatorname{ord} \theta(z)$ (вместо модуля), положим $z^* = \operatorname{ord} z$, $q^* = \operatorname{ord} q$, $\theta^* = \operatorname{ord} \theta(z) = \theta^*(z^*)$ (в некритических z^*). Из уравнения (1) находим

$$\theta^*(z^* + q^*) = \theta^*(z^*) - z^* - q^*.$$

Такому же уравнению удовлетворяет функция $-\frac{z^{*2}}{2q^*} - \frac{z^*}{2}$. Поэтому

$$\theta^*(z^*) = -\frac{z^{*2}}{2q^*} - \frac{z^*}{2} + q^* \quad (q^* \text{ — периодическая функция}).$$

Значение остатка вычисляется по периодичности из того, что $\theta^*(z^*) = 0$ при $-q^* < z^* < 0$.

в) Пользуясь доказательством теоремы, легко построить пример ряда Лорана, сходящегося в открытом интервале $0 < |r| < |z| < s$ и имеющего в нем бесконечно много критических точек.

2.4. Доказательство теоремы 2.2.

Критические точки и график $|f(z)|$. Ясно, что если $|z| = t$ не критична, то $|f(z)| = |a_m| t^m = \max\limits_k |a_k z^k|$. Начертим для каждого $i \in Z$ график Γ_i, изображающий $\operatorname{ord}(a_i z^i)$ как функцию от $\operatorname{ord} z$. Это прямая с угловым коэффициентом i. Далее, в некритических $|z|$

$$\operatorname{ord}(|f(z)|) = \min_k (\operatorname{ord}(a_k) + k \operatorname{ord}(z)),$$

так что график $\operatorname{ord}(|f(z)|)$ есть граница пересечения полуплоскостей под всеми Γ_i. Так как $|a_i| r^i \to 0$, $|a_i| s^i \to 0$ при $|i| \to \infty$ (сходимость $f(z)$ на границе), имеем $\operatorname{ord} a_i + i \log_c r \to$

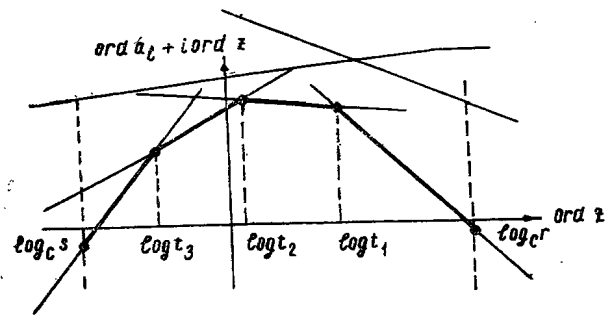


Рис. 1

$\to\infty$ и аналогично для s при $|i|\to\infty$, то есть лишь конечное число Γ_i участвует в образовании границы в интересующей нас конечной полосе между $\log_c s$ и $\log_c r$. Таким образом, график $\operatorname{ord}(|f(z)|)$ вне критических точек кусочно-линейный, выпуклый вверх и имеет лишь конечное число угловых точек — как раз при критических ord z, когда $\min\limits_k(\operatorname{ord} a_k + k \operatorname{ord} z)$ достигается по крайней мере при двух разных значениях k. Выпуклость вверх равносильна возрастанию угловых коэффициентов m_i линейных кусков графика при движении от $\log_c r$ к $\log_c s$. Это доказывает утверждения а) и б) теоремы.

Дальше мы займемся поведением $f(z)$ в критических точках.

2.5. Достижение максимума. Пусть t критична, $t\in|K|$. Заменив z на bz, а $f(z)$ на $dz^k f(z)$ при подходящих $b, d\in K$, $k\in Z$, мы можем считать, что $t=1$ и далее $|a_0|=1$, $|a_k|<1$ при $k<0$, $|a_k|\leqslant 1$ при $k>0$, то есть самый первый из максимальных членов ряда постоянен и по модулю равен 1 в $|z|=t=1$. Но это означает, что все коэффициенты $f(z)$ целые, а его редукция по модулю максимального идеала в кольце целых чисел из K является нулевым многочленом. Если поле классов вычетов K достаточно велико, эта редукция принимает ненулевое значение в какой-то точке; поднимая эту точку в K, получаем значение $f(z_0)$ с $|f(z_0)|=1=|a_0|=\max\limits_k|a_k|t^k$. Обратные замены, очевидно, сохраняют справедливость утверждения $\max|f(z_0)|=\max\limits_k|a_k|t^k$.

Чтобы доказать утверждение о нулях, мы сначала рассмотрим простой частный случай.

2.6. График модуля многочлена. Пусть $f(z)=\prod(z-z_i^{(j)})$, где $|z_i^{(j)}|=t_i$, $t_0<t_1<\ldots<t_m$. Тогда при $t_i<|z|<t_{i+1}$ имеем

$$|z-z_j^{(k)}|=\begin{cases}|z|, & \text{если } k\leqslant i;\\ |z_k^{(j)}|, & \text{если } k\geqslant i+1.\end{cases}$$

Отсюда

$$\left.\begin{aligned}&|f(z)|=b|z|^m \text{ при } t_i<|z|<t_{i+1},\\ &m \text{ равно числу нулей } f(z) \text{ с } |z|\leqslant t_i;\\ &b=\prod_{k>i}|z_k^{(j)}| \text{ (произведение по нулям правее } t_i).\end{aligned}\right\}\qquad(2)$$

В частности, при переходе через $|z|=t_i$ показатель m возрастает как раз на количество нулей f с $|z|=t_i$ и t_i являются в точности критическими значениями для f. Таким образом, для многочленов теорема окончательно доказана.

2.7. Конструкция одного корня. Пусть теперь снова $f(z)=\sum\limits_{-\infty}^{\infty}a_i z^i$. Как выше, достаточно разобрать случай, когда критическое значение есть $t=1$, и $|a_k|<1$ при $k<0$, $|a_0|=|a_d|=1$, $|a_k|<1$ при $k>d$. Будем приближать $f(z)$ многочленами $f_j(z)=z^j\sum\limits_{-j}^{j}a_i z^i$ и считать, что K алгебраически замкнуто.

2.8. Лемма. а) При $j\geqslant d$ у $f_j(z)$ имеется j корней $z_1,\ldots,z_j$ с $|z_k|<1$, d корней $z_{j+1},\ldots,z_{j+d}$ с $|z_k|=1$, $j-d$ корней $z_{j+d+1},\ldots,z_{2j}$ с $|z_k|>1$. б) $|a_j|\prod\limits_{k\geqslant 1}|z_{j+d+k}|=1$.

2.9. Доказательство леммы. При $|z|=1-\varepsilon$, $\varepsilon>0$ мало, имеем $|f_j(z)|=|z|^j$ (доминирует a_0); при $|z|=1+\varepsilon$ имеем $|f_j(z)|=|z|^{j+d}$ (доминирует a_d) в силу предположений об a_i. Пользуясь (2), получаем, что при $|z|<1$ у f имеется j нулей, а при $|z|=1$ еще d. Утверждение б) получается сразу же из (1), если учесть, что в (2) старший коэффициент f равен 1, а у нас a_j.

2.10. Теперь покажем, что из нулей $f_j(z)$, по модулю равных 1, при $j\to\infty$ можно выбрать сходящуюся последовательность, предел которой есть нуль $f(z)$.

Это легко сделать, если коэффициенты f порождают конечное расширение Q_p: в силу леммы, все такие нули лежат в расширениях $Q_p(\ldots a_i\ldots)$ степени $\leqslant d$, и, значит, в группе единиц некоторого конечного расширения Q_p, которая компактна.

В общем случае пусть $z_{j,1},\ldots,z_{j,d}$ — нули $f_j(z)$ с $|z_{j,k}|=1$. Положим $y_d=z_{d,1}$ и индукцией по j выберем $y_j\in(z_{j,1},\ldots,z_{j,d})$ так, чтобы $|y_{j+1}-y_j|\to 0$. Чтобы установить возможность этого выбора, вычислим двумя способами $|f_{j+1}(y_j)|$:

$$|f_{j+1}(y_j)|=|f_j(y_j)\,y_j+a_{-(j+1)}+a_{(j+1)}y_{j+1}^{2j}|\leqslant$$
$$\leqslant\max(|a_{-(j+1)}|,|a_j|)\to 0;$$

$$|f_{j+1}(y_j)| = |a_{j+1}| \prod_{i=1}^{d} |y_j - z_{j,i}| \prod_{|z_j^{(k)}|>1} |z_j^{(k)}|.$$

В силу леммы $|a_{j+1}| \prod |z_j^{(k)}| = 1$; значит, множители $|y_j - z_{j,i}|$ не могут быть ограничены от нуля при $j \to \infty$, откуда и следует существование y_{j+1} с $|y_{j+1} - y_j| \to 0$.

Очевидно, предел y_j есть корень $f(z)$. Он лежит в конечном расширении поля $Q_p(\ldots a_i \ldots)$, если это поле конечно над Q_p, и в дополнении его замыкания в противном случае.

2.11. Конец доказательства. Нам осталось проверить, что число корней f в критической точке вычисляется так же, как для многочлена, — как разность левого и правого угловых коэффициентов в графике $\operatorname{ord}(f(z))$.

Прежде всего, если $f(a) = 0$, то $f(z) = (a - z)g(z)$, где $g(z)$ — ряд Лорана с той же областью сходимости. Для доказательства достаточно рассмотреть случай $a = 1$ и построить g. Сначала вычислим g формально:

$$g(z) = \frac{f(z)}{1-z} = f(z)(1 + z + z^2 + \ldots) = \sum_{-\infty}^{\infty} b_j z^j,$$

где $b_j = a_j + a_{j-1} + a_{j-2} + \ldots$ сходится, потому что $a_j \to 0$ при $j \to -\infty$ ($f(z)$ сходится в $z = 1$).

Теперь проверим сходимость $g(z)$ в точках сходимости $f(z)$. Если $|z| = t < 1$, то

$$b_j t^j \to 0 \quad \text{при} \quad j \to \infty, \quad \text{ибо} \quad |b_j| \leqslant \max_k |a_k|, \quad |t|^j \to 0;$$

$$b_j t^j \to 0 \quad \text{при} \quad j \to -\infty, \quad \text{ибо} \quad |b_j t^j| \leqslant \max_{k<j} |a_k t^k| \to 0$$

в силу сходимости f.

Если же $|z| = t \geqslant 1$, то

$$b_j t^j \to 0 \quad \text{при} \quad j \to -\infty, \quad \text{ибо} \quad |b_j| \leqslant \max_k |a_k|, \quad t^j \to 0;$$

$$b_j t^j \to 0 \quad \text{при} \quad j \to \infty, \quad \text{ибо} \quad |b_j| = |f(1) - (a_{j+1} + a_{j+2} + \ldots)| =$$
$$= |a_{j+1} + a_{j+2} + \ldots| \leqslant \max_{k>j} |a_k|.$$

Значит, мы доказали, что существование нуля у $f(z)$ позволяет выделить линейный множитель.

Пусть теперь $|z| = t$ — критическая точка, $d_t(f)$ равно разности угловых коэффициентов графика $\operatorname{ord} f(z)$ в t, равно расстоянию между крайними максимальными членами (fz.) в $|z| = t$. (Второе равенство следует из рассмотрений п. 2.4). Покажем, что если $|a| = t$, то

$$d_t((z-a)f(z)) = d_t(f) + 1.$$

Для этого достаточно рассмотреть случай, когда $t = |a| = 1$,

коэффициенты f целые, и $|a_0| = 1$. Но в этом случае $d_t(f)$ совпадает со степенью редукции $f(z)$, и все становится очевидным.

Окончательно, функция $d_t(f)$ совпадает с числом корней f при $|z| = t$, потому что:

а) обе функции равны нулю, если корней нет (потому что тогда t — не угловая точка, и в ней $|f(z)| = bt^m \neq 0$);

б) обе функции увеличиваются на единицу при переходе от f к $(z-a)f$, $|a| = t$. ■

2.12. Дивизоры. Пусть теперь K — конечное расширение Q_p. Назовем K-дивизором функцию на $\overline{K}^*$ со значениями в Z: $z \mapsto n_z$ со следующими свойствами:

а) для любых $0 < r < s$ существует лишь конечное число $z \in \overline{K}^*$ таких, что $r \leqslant |z| \leqslant s$ и $n_z \neq 0$;

б) $n_{z_1} = n_{z_2}$, если z_1 и z_2 сопряжены над K. K-дивизоры мы будем записывать также в виде (бесконечной) суммы $\sum n_z z$. Дивизор эффективен, если $n_z \geqslant 0$ для всех z; конечен, если $n_z \neq 0$ лишь для конечного числа z. K-дивизоры образуют группу $\mathcal{D}(K^*)$ (записываемую аддитивно), а эффективные дивизоры — полугруппу $\mathcal{D}^+(K^*)$.

Пусть $f(z) = \sum_{-\infty}^{\infty} a_i z^i$ — некоторый ряд Лорана, $a_i \in K$ для всех i. Предположим, что f сходится при $r \leqslant |z| \leqslant s$. Тогда с f можно сопоставить конечный эффективный K-дивизор $\sum n_i z_i$, где z_i — нули $f(z)$ с $r \leqslant |z_i| \leqslant s$, а n_i — их кратности (см. п. п. 2.8 — 2.11). Если $f(z)$ сходится при всех $0 < |z| < \infty$, то, устремляя r к нулю, а s к ∞, мы получаем полный дивизор $\operatorname{div} f$, который остается эффективным, но может перестать быть конечным. Примеры: $\operatorname{div} \theta(z) = \sum_{n \in Z} (q^n)$, $\operatorname{div}(z^n) = 0$.

Обозначим через $\mathcal{L}$ пространство рядов Лорана над K, сходящихся при всех $z \in \overline{K}^*$. Пусть $U = (cz^n)$, $n \in Z$, $c \in K^*$; $\mathcal{L}^\times$ — множество ненулевых элементов $\mathcal{L}$.

2.13. Теорема. а) $\mathcal{L}$ является кольцом без делителей нуля, а U — его подгруппа единиц.

б) Отображение $\operatorname{div}: \mathcal{L}^\times \to \mathcal{D}^+(K^*)$ индуцирует изоморфизм полугруппы $\mathcal{L}^\times / U$ с полугруппой эффективных K-дивизоров.

Доказательство. а) Пусть $f = \sum a_i z^i$, $g = \sum b_i z^i$ — ненулевые элементы $\mathcal{L}$. Тогда при $|i| \to \infty$ коэффициенты a_i и b_i стремятся к нулю быстрее любой геометрической прогрессии. В частности, существуют $c_n = \sum_{i=-\infty}^{\infty} a_i b_{n-i}$, и ряд Ло-

рана $\sum c_n z^n$, как нетрудно видеть, сходится всюду и представляет произведение f_g. Согласно теореме 2.2 б) вне критических значений $|z|$, которые расположены дискретно, f и g не обращаются в нуль; поэтому и fg не обращается там в нуль.

Предположим, что ряд f обратим в $\mathscr{L}$. Тогда он не имеет нулей в $\bar{K}^*$ и, значит, для f нет критических значений $|z|$. Пусть cz^m — максимальный член f, один и тот же всюду. Тогда $f(cz^m)^{-1}=1+g$, где в любой точке $\bar{K}^*$ все члены g по модулю меньше 1. Но это возможно лишь при $g=0$, ибо $|az^n|$ при $a\neq 0$ стремится к ∞ при $|z|\to\infty$. Значит, $f=cz^m$.

б) Пусть $D=\sum_{i=-\infty}^{\infty} n_i z_i \in \mathscr{D}^+(K^*)$ — эффективный K-дивизор. Прежде всего, нетрудно построить ряд Лорана с таким дивизором. Положим, по образцу конструкции θ,

$$W_D(z)=\prod_{|z_i|>1}(1-zz_i^{-1})^{n_i}\prod_{|z_i|<1}(1-z^{-1}z_i)^{n_i}.$$

При фиксированном z и $|i|\to\infty$ члены этого произведения Вейерштрасса стремятся к 1, по свойству а) дивизора, поэтому оно сходится поточечно. Отсюда же видно, что последовательность частичных произведений $W_D(z)$ — конечных рядов Лорана — сходится покоэффициентно к некоторому ряду Лорана. Его коэффициенты лежат в K в силу свойства б) дивизора, так что $W_D(z)\in\mathscr{L}$. Легко видеть, что $\operatorname{div} W_D(z)=D$.

Таким образом, отображение $\operatorname{div}:\mathscr{L}^\times\to\mathscr{D}^+(K^*)$ сюръективно. Предположим теперь, что $f\in\mathscr{L}^\times$ — другой ряд Лорана с $\operatorname{div} f=D$, и покажем, что $f=az^m W_D(z)$ для некоторых $a\in K^*$ и $m\in Z$.

Действительно, прежде всего функция

$$f(z)\prod_{1<|z_i|\leqslant s}(1-zz_i^{-1})^{-n_i}\prod_{r\leqslant|z_i|<1}(1-z^{-1}z_i)^{-n_i}$$

для всех $0<r<s$ есть ряд Лорана над K, не имеющий нулей при $r\leqslant|z|\leqslant s$ в силу пп. 2.8—2.11. Последовательность таких рядов, которая получается при $r\to 0$ и $s\to\infty$, сходится к элементу из $\mathscr{L}$, как показывает несложный анализ по образцу п. 2.11. Ее предел не имеет нулей и потому, как в пункте а), принадлежит U. Окончательно, $\operatorname{div} f=D\Leftrightarrow f=az^m W_D(z)$, что завершает доказательство. ■

Изложенная теория рядов Лорана является классической: см., например, [11]. Вопросы теории дивизоров для других полей K исследованы Лазаром [15].

2.14. Из теоремы 2.13 видно, что мы можем построить поле отношений $\mathscr{M}$ кольца $\mathscr{L}$ и поставить в соответствие каждому элементу $\mathscr{M}$ его дивизор из группы $\mathscr{D}(K^*)$. Далее, имеет место точная последовательность

$$1\to U\to\mathscr{M}^*\to\mathscr{D}(K^*)\to 0.$$

Естественно называть элементы из $\mathscr{L}$ голоморфными K-функциями на $\bar{K}^*$, а элементы из $\mathscr{M}$ — мероморфными K-функциями. Следующий параграф будет посвящен исследованию поля периодических (относительно $z\mapsto qz$) мероморфных K-функций и доказательству того, что это поле эллиптических функций над K. Основную роль будет играть простое соображение, что у периодической функции должен быть периодический дивизор.

§ 3. ФУНКЦИИ ЯКОБИ — ТЭЙТА

3.1. В этом параграфе по-прежнему K — конечное расширение Q_p, $\mathscr{M}$ — поле мероморфных K-функций на $\bar{K}^*$. Пусть $q\in K^*$, $|q|<1$; положим $\Gamma=(q^n)$, $n\in Z$. Это циклическая группа, действующая сдвигами на $\bar{K}^*$, $\mathscr{L}$, $\mathscr{M}$ и на дивизоры $\mathscr{D}(\bar{K}^*)$.

3.2. Теорема. Пусть $d\in\mathscr{D}(\bar{K}^*)^\Gamma$ — Γ-инвариантный K-дивизор. Пусть $f\in\mathscr{M}$ и предположим, что $\operatorname{div} f=d$. Тогда справедливы следующие утверждения:

а) $f(qz)=a(-z)^{-m}f(z)$ для некоторых $a\in K^*$, $m\in Z$.

б) $\operatorname{Класс}(aq^n)_{n\in Z}=\Gamma a$ и число m зависят лишь от d, но не от f. Более точно:

в) $m=\deg d$ — разность числа нулей и полюсов d в фундаментальной области для Γ: $|q|<|z|\leqslant 1$; $a \bmod\Gamma=$(произведение нулей и полюсов d в той же фундаментальной области) $\bmod\Gamma=j(d)$ (образ Якоби).

Доказательство. а) По предположению, $\operatorname{div} f(z)=\operatorname{div} f(qz)=d$. Из теоремы 2.13 тогда следует, что $f(z)/f(qz)=a(-z)^m$ для некоторых $a\in K^*$, $m\in Z$.

б) Если $g\in\mathscr{M}$ — другая функция с $\operatorname{div} g=d$, то $g=bz^n f$, откуда

$$g(qz)=b(qz)^n f(qz)=bz^n f(z)\,q^n a(-z)^m,$$

так что m не меняется, а a заменяется на aq^n.

в) Для явного вычисления m и a заметим прежде всего, что они аддитивно (соответственно мультипликативно) зависят от d — это ясно из определения. Далее, группа Γ-инвариантных $\bar{K}$-дивизоров имеет, очевидно, следующую систему образующих:

$$d_a=\sum_{n=-\infty}^{\infty}(aq^n),\quad |q|<|a|\leqslant 1,\quad a\in\bar{K}.$$

Применяя лемму 3.5 к нашему кольцу $\bigoplus_{m=0}^{\infty} A_n$ и пользуясь тем, что $\dim_K A_m = m$, сразу находим $\deg \mathrm{tr}_K \mathcal{M}^\Gamma \leqslant 1$. С другой стороны, в $\mathcal{M}^\Gamma$ есть непостоянные элементы (например, $\theta_{\sqrt{q}}\theta_{-\sqrt{q}}\theta_1^{-2}$), так что $\deg \mathrm{tr}_K \mathcal{M}^\Gamma = 1$. Значит, по утверждению б) леммы, $\mathcal{M}^\Gamma$ конечно порождено над K. Легко убедиться, что K алгебраически замкнуто в $\mathcal{M}$ и тем более в $\mathcal{M}^\Gamma$. Значит, $\mathcal{M}^\Gamma$ — поле алгебраических функций на некоторой K-кривой X.

Легко видеть, что отображение «сдвига аргумента» дает вложение группы $K^*/(q^n)$ в группу автоморфизмов поля $\mathcal{M}^\Gamma/K$. Таким образом, род X может быть лишь 0 или 1. Если считать уже известным, что отображение $K^*/(q^n) \to X(K)$ («значение функции в точке») является изоморфизмом, то эта альтернатива немедленно разрешается в пользу рода 1, ибо у этой группы автоморфизмов нет неподвижной точки на $X(K)$. Дифференциалы первого рода на X тогда отождествляются с образами $Kz^{-1}dz$, ибо в $\mathcal{L}d\mathcal{L}$ больше нет Г-инвариантных дифференциалов с тривиальным дивизором.

Таким образом, осталось отождествить K-точки кривой X с $K^*/(q^n)$.

Это можно сделать, например, так. Обозначим через S множество локальных колец в $\mathcal{M}^\Gamma$, отвечающих простым Г-инвариантным K-дивизорам: (простой дивизор d) $\mapsto$ ($f \in \mathcal{M}^\Gamma$, f не имеет полюса в d) $\in S$. Очевидно, это отображение доставляет вложение (простые дивизоры) $\subset\!\!\to$ (локальные кольца X). Это вложение переводит аналитически определенную функцию «порядок f в простом дивизоре» в такую же алгебраически определенную функцию, а дивизоры степени 1 — в локальные кольца K-точек X.

Наконец, аналитический «порядок f в d» удовлетворяет «формуле произведения» $\sum_{d \in S} \mathrm{ord}_d(f) = 0$. Совершенно такой же формуле удовлетворяет алгебраический порядок. Классическое рассуждение Артина — Уэйплса показывает, что если бы образ S пропускал некоторые локальные кольца, то можно было бы построить функцию f, часть дивизора которой была бы сосредоточена в пропущенных кольцах, так, чтобы $\sum_{d \in S} \mathrm{ord}_d(f)$ оказалась $\neq 0$. ■

3.7. В заключение приведем без доказательства два эквивалентных описания множества эллиптических кривых над K, допускающих униформизацию описанного типа.

а) Инвариантное описание. Это те кривые, у которых существует гладкая собственная модель над целыми числами $O \subset K$, замкнутый слой которой состоит из n проективных прямых P_k^1, пересекающихся «колесом» при $n \geqslant 2$ (подробнее см. п. 9.3 главы III) или является кривой рода 0 с одной двойной точкой с разделенными касательными, определенными над k. (Подробнее см. главу III и работу Мамфорда [18]).

б) Описание с помощью уравнений (см. Рокетт [21]). Это те кривые, которые можно задать над K уравнением Вейерштрасса вида $y^2 = 4x^3 - g_2 x - g_3$ с условиями

$$б_1)\ |j| > 1, \text{ где } j = 12^3 g_2^3 (g_2^3 - 27 g_3^2);$$

$$б_2)\ -\frac{1}{2} g_2 g_3^{-1} \in (K^*)^2.$$

Самое простое доказательство: задать x, y, g_2, g_3 явными формулами классической теории, рассматривая необходимые тождества между ними как формальные. Важнейшие тождества:

$$j = \frac{\left(1 + 240 \sum_{m=1}^{\infty} \frac{m^3 q^m}{1-q^m}\right)^3}{q \prod_{m=1}^{\infty} (1-q^m)^{24}},$$

$$g_2 = \frac{1}{12} + 20 \sum_{m=1}^{\infty} \frac{m^3 q^m}{1-q^m},$$

$$g_3 = -\frac{1}{216} + \frac{7}{3} \sum_{m=1}^{\infty} \frac{m^5 q^m}{1-q^m},$$

$$x = x(z) = \frac{1}{12} - 2 \sum_{m=1}^{\infty} \frac{m q^m}{1-q^m} + \sum_{m=-\infty}^{\infty} \frac{q^m z}{(1-q^m z)^2},$$

$$y = y(z) = \sum_{m=-\infty}^{\infty} \frac{q^m z + q^{2m} z^2}{(1-q^m z)^2}.$$

Глава II

АБЕЛЕВЫ ФУНКЦИИ

§ 1. РЯДЫ ЛОРАНА ОТ МНОГИХ ПЕРЕМЕННЫХ

1.1. В этой главе $[K:Q_p] < \infty$. Мы начнем с распространения результатов главы I на ряды Лорана от многих переменных

$$\sum_{i_1, \ldots, i_n=-\infty}^{\infty} a_{i_1 \ldots i_n} z_1^{i_1} \ldots z_n^{i_n}, \quad a_{i_1 \ldots i_n} \in K.$$

Удобно несколько изменить обозначения. Пусть H — мультипликативная свободная абелева группа одночленов $z_1^{i_1} \ldots z_n^{i_n}$; ее элементы мы будем обозначать буквами χ, η с индексами. Каждый элемент $\chi \in H$ будем рассматривать как элемент кольца схемы $T = \operatorname{Spec} K[H]$. Для любой K-алгебры A имеем

$$T(A) = \operatorname{Hom}_K(K[H], A) = \operatorname{Hom}(H, A^*) \cong (A^*)^n.$$

Таким образом, T есть групповая схема, изоморфная $G_{m,K}^n$, то есть n-мерный тор. Элементы $\chi \in H$ превращаются в функции на $T(A)$ для всех A; в частности, в функции на $T(\bar{K})$. Их принято называть характерами тора T.

Ряды Лорана $\sum_{\chi \in H} a_\chi \chi$ мы будем рассматривать как функции на подмножествах $T(\bar{K})$, на которых эти ряды сходятся.

1.2. Положим $H^* = \operatorname{Hom}(H, R)$; мы будем представлять H^* как R-линейное пространство и записывать аддитивно. Каждая точка $u \in T(\bar{K})$ определяет точку $u^* \in H^*$ по формуле

$$u^*(\chi) = \operatorname{ord} \chi(u), \quad \chi \in H.$$

Пусть $f = \sum a_\chi \chi$, $a_\chi \in K$ — некоторый ряд Лорана. Пусть $U^* \subset H^*$ — некоторый замкнутый параллелепипед в H^* (в любом базисе и метрике). Предположим, что f сходится в тех точках $u \in T(\bar{K})$, для которых $u^* \in U^*$.

Назовем точку $v^* \in U^*$ критической для f, если существуют такие $\chi_1 \neq \chi_2$, что

$$\operatorname{ord} a_{\chi_1} + v^*(\chi_1) = \operatorname{ord} a_{\chi_2} + v^*(\chi_2) = \min_{\chi \in H} (\operatorname{ord} a_\chi + v^*(\chi))$$

(минимум по χ достигается из-за предположения о замкнутости U^* и о том, что $\operatorname{ord} a_\chi + u^*(\chi) \to \infty$ по χ для $u^* \in U^*$. Действительно, множество точек, пришедших из $T(\bar{K})$, которые лежат в U^*, плотно).

Положим $f^*(v^*) = \min_{\chi \in H} (\operatorname{ord} a_\chi + v^*(\chi))$.

Следующая теорема параллельна теореме 2.2 главы 1:

1.3. Теорема. а) В условиях п. 1.2 критические точки f в U^* образуют $(n-1)$-мерный остов некоторого конечного полиэдрального разбиения.

б) Если $u \in T(\bar{K})$, $u^* \in U^*$, u^* не критична для f, то

$$f^*(u^*) = \operatorname{ord} f(u).$$

График функции $u^* \mapsto f^*(u^*)$ в $U^* \times R$ непрерывный, выпуклый вверх, кусочно линейный, и проекция множества его угловых точек на U^* совпадает с множеством критических точек для f.

в) На множестве точек $u \in T(\bar{K})$, для которых $u^* \in U^*$ — фиксированная критическая точка, $\operatorname{ord} f(u)$ принимает все рациональные значения между ∞ и $f^*(u^*)$.

Доказательство. Рассуждения полностью аналогичны тем, которые проводились в одномерном случае. Рассмотрим для каждого $\chi \in H$ график $\Gamma_\chi \subset U^* \times R$, изображающий $\operatorname{ord} a_\chi + u^*(\chi)$ как функцию от $u^* \in U^*$. Мы получим счетную систему гиперплоскостей. В точках границы $u^* \in \partial U^*$ имеем $\min_{u^*} (\operatorname{ord} a_\chi + u^*(\chi)) \to \infty$ по фильтру дополнений к конечным множествам χ. Значит, график $v^* \mapsto f^*(v^*)$ есть граница пересечения конечного числа полупространств в $U^* \times R$, лежащих ниже конечного числа графиков Γ_χ. Точки, принадлежащие по крайней мере двум Γ_χ на этой границе, по определению, проектируются как раз в критические точки f на U^*. Это доказывает утверждения а) и б).

Доказательство в) легко получается редукцией к одномерному случаю. Действительно, в обозначениях начала п. 1.1 задача выглядит так: дан ряд $f = \sum a_{i_1 \ldots i_n} z_1^{i_1} \ldots z_n^{i_n}$, дано множество точек с $(\operatorname{ord} z_1, \ldots, \operatorname{ord} z_n) = u^*$, в которых у ряда есть по крайней мере два разных максимальных члена. Мы хотим доказать, что модуль ряда принимает в этих точках все значения, промежуточные между нулем и максимальным. Достаточно подобрать конкретные значения $(\bar{z}_i)$, $i \neq i_0$, в этом множестве такие, чтобы при подстановке в ряд z_i вместо z_i у получившегося ряда от z_{i_0} по-прежнему было не меньше двух максимальных членов, и затем применить теорему главы I. Это нетрудно сделать. ■

1.4. Теорема. Множество $\mathscr{L}$ рядов Лорана $\sum a_\chi \chi$, сходящихся во всех точках $u \in T(\bar{K})$, является кольцом без делителей нуля. Его группа единиц есть $K^* H$.

Доказательство. Первое утверждение легко следует из теоремы 1.3, как соответствующий одномерный факт. Аналогично обстоит дело со вторым утверждением: если $f = \sum a_\chi \chi$ обратим, то f не имеет нулей, и $v^* \mapsto f^*(v^*)$ есть линейная функция. Тогда у f имеется единственный член $a_\chi \chi$, максимальный во всех точках, так что $f a_\chi^{-1} \chi^{-1}$ во всех точках имеет вид $1 + g$, $|g| < 1$. Это возможно лишь при $g = 0$. ■

1.5. Дивизоры. В многомерном случае мы не можем получить о дивизорах функций $f \in \mathscr{L}$ столь же полное представление, как в одномерном, однако теоремы 1.3 и 1.4 дают

о них полезную наглядную информацию. Поступим следующим образом.

По аналогии с одномерным случаем, где полугруппа эффективных дивизоров апостериори отождествлялась с $\mathscr{L}^\times/(K^*z^i)$, мы можем ее здесь определить как $\mathscr{L}^\times/(K^*H)$: это пригодится в следующем параграфе при выборе определения тэта-функций.

Множество критических точек функции $f\in\mathscr{L}$, которое, согласно теореме 1.3 а), образует $(n-1)$-мерные «полиэдральные соты» в H^*, служит некоторым геометрическим образом дивизора f, ибо нули f проектируются в него при отображении $u\mapsto u^*$. См. примеры в конце следующего параграфа.

§ 2. ПЕРИОДЫ, ПОЛЯРИЗАЦИИ, ТЭТА-ФУНКЦИИ

2.1. Мы сохраняем обозначения § 1. Пусть дополнительно дана некоторая подгруппа «периодов» $B\subset T(K)$. Позже мы будем предполагать, что она дискретна ранга $n=\dim T$; это аналог подгруппы $(q^n)\subset K^*$ главы I.

2.2. Определение. Тэта-функцией (относительно B) называется любая функция $\theta\in\mathscr{L}$, дивизор которой инвариантен относительно сдвигов на периоды $b\in B$.

Расшифруем определение: согласно п. 1.5 и 1.4, дивизор $\theta(u)$ есть класс $\theta \bmod K^*H$; отсюда следует, что если θ — тэта-функция, то существует такое отображение $\varphi\colon B\to H$, $b\mapsto\chi_b$ и такие константы $\lambda_b\in K^*$, что

$$\theta(bu)=\lambda_b\chi_b(u)^{-1}\theta(u) \text{ для всех } b\in B,\ u\in T(\overline{K}). \qquad (1)$$

2.3. Предложение. В условиях (1) имеем следующие тождества:

а) Отображение $b\mapsto\chi_b$ является гомоморфизмом; кроме того, $\chi_{b_2}(b_1)=\chi_{b_1}(b_2)$, так что обе части бимультипликативны и симметричны по b_1, b_2.

б) $\dfrac{\lambda_{b_1}\lambda_{b_2}}{\lambda_{b_1b_2}}=\chi_{b_1}(b_2)$; b_1, $b_2\in B$.

в) Предположим, что существует такое симметричное бимультипликативное спаривание $[,]\colon B\times B\to K^*$, что $[b_1, b_2]^2=\chi_{b_1}(b_2)$ для всех b_1, $b_2\in B$. Тогда существует однозначно определенный гомоморфизм $\psi\colon B\to K^*$ такой, что $\lambda_b=[b,b]^{-1}\psi(b)$ для всех $b\in B$.

Доказательство. Записывая (1) для $b=b_1b_2$ двумя способами, находим

$$\lambda_{b_1b_2}\chi^{-1}_{b_1b_2}(u)=\lambda_{b_1}\lambda_{b_2}\chi^{-1}_{b_1}(b_2)\chi^{-1}_{b_1}(u)\chi^{-1}_{b_2}(u).$$

Отсюда видно, прежде всего, что χ_b мультипликативен по b, так что отображение $\varphi\colon B\to H$ является гомоморфизмом. Отсюда же следуют остальные утверждения а) и б). Из б) легко увидеть, что $\psi(b)=\lambda_b[b,b]$ является гомоморфизмом $B\to K^*$. ■

2.4. В дальнейшем мы будем всегда предполагать, что для рассматриваемых θ-функций условие в) выполнено. Этого можно добиться, перейдя от K к конечному расширению $K(\sqrt{K^*})$: матрицу $[,]$ в некотором базисе (b_i) группы B можно тогда найти, извлекши квадратные корни из элементов матрицы $(\chi_{b_i}(b_j))$. Другой вариант — перейти от гомоморфизма φ к φ^2; ср. ниже. Вместо $[b_1, b_2]$ мы будем писать дальше $\chi_{b_1}(b_2)^{\frac{1}{2}}$ (считая выбор $[,]$ фиксированным). Окончательно, уравнение θ-функции будет записываться в виде:

$$\theta(bu)=\psi(b)\chi_b(b)^{-\frac{1}{2}}\chi_b(u)^{-1}\theta(u). \qquad (2)$$

Типом тэта-функции, удовлетворяющей (2), называется тройка $(\varphi, \psi, [,])$, где

$$\varphi\colon B\to H,\ b\mapsto\chi_b;\ \psi\colon B\to K^*;\ [b_1, b_2]^2=\chi_{b_1}(b_2).$$

Произведение двух тэта-функций также является тэта-функцией; их типы перемножаются очевидным образом.

Начнем с выяснения того, как устроены тэта-функции одного типа, и насколько их много.

2.5. Лемма. Пусть $\theta=\sum a_\chi\chi$ — формальный ряд Лорана. Предположим, что он формально удовлетворяет уравнению (2). Тогда

$$a_\chi=\psi(b)^{-1}\chi_b(b)^{-\frac{1}{2}}\chi(b)a_{\chi\chi_b^{-1}};\ \chi\in H,\ b\in B. \qquad (3)$$

Доказательство. Запишем явно левую и правую части (2):

$$\theta(bu)=\sum_{\chi\in H}a_\chi\chi(b)\chi(u)=\sum_{\chi\chi_b^{-1}\in H}a_{\chi\chi_b^{-1}}(\chi\chi_b^{-1})(b)(\chi\chi_b^{-1})(u),$$

$$\psi(b)\chi_b(b)^{-\frac{1}{2}}\chi_b(u)^{-1}\theta(u)=\sum_{\chi\in H}a_\chi\psi(b)\chi_b(b)^{-\frac{1}{2}}(\chi\chi_b^{-1})(u).$$

Сравнивая коэффициенты, находим требуемое. ■

2.6. Теорема. а) Формальные ряды $\sum a_\chi\chi$, удовлетворяющие функциональному уравнению (2), образуют линейное пространство размерности $[H:\varphi(B)]$.

б) Описанное пространство целиком состоит из рядов, сходящихся в любой точке $T(\overline{K})$, в том и только том случае, когда $[H:\varphi(B)]<\infty$ и форма

$$\varphi(B)\times\varphi(B)\to Z\colon (\chi_{b_1}, \chi_{b_2})\mapsto \operatorname{ord}\chi_{b_1}(b_2)$$

положительно определена.

в) Если условия б) выполнены, и B не имеет кручения, то $B \subset T(K)$ — дискретная подгруппа максимального ранга, а ядро $\varphi: B \to H$ тривиально.

Доказательство. а) Из уравнений (3) нетрудно усмотреть, что все коэффициенты a_χ однозначно определяются, если произвольно заданы их значения на любой системе представителей смежных классов $H/\varphi(B)$ (явные формулы см. ниже). В частности, если $[H:\varphi(B)]=\infty$, то существуют ряды, для которых a_χ не стремятся к нулю по χ. Эти ряды не могут сходиться всюду на $T(\overline{K})$.

б) Пусть теперь $[H:\varphi(B)]<\infty$. Чтобы исследовать сходимость рядов, напишем формулы для a_χ явно. Начнем с простейшего типа, где положение дел яснее всего.

Тип $\psi\equiv 1$, $H=\varphi(B)$. Любой $\chi\in H$ имеет вид χ_b для некоторого b. Легко видеть, что все решения уравнения (3) записываются в виде

$$a_{\chi_b} = a_1 \chi_b(b)^{\frac{1}{2}}, \quad a_1 \in K. \tag{4}$$

Необходимое условие, чтобы ряд всюду сходился: $\operatorname{ord}\chi_b(b)\to\infty$. Так как H — свободная абелева группа конечного ранга, а $\operatorname{ord}\chi_b(b)$ — целозначная квадратичная форма на ней, это возможно только тогда, когда форма положительно определена. Это же условие и достаточно для сходимости, потому что при фиксированной точке $u\in T(\overline{K})$ и переменной χ_b $\operatorname{ord}\chi_b(u)$ является линейной функцией от χ_b, так что

$$\operatorname{ord}(a_{\chi_b}\chi_b(u)) = \tfrac{1}{2}\operatorname{ord}\chi_b(b) + \operatorname{ord}\chi_b(u) + \operatorname{ord}a_1 \to \infty$$

(по (4)).

Тип $\psi\equiv 1$, $[H:\varphi(B)]<\infty$ — любой. Формулы (4) остаются верными на единичном смежном классе $\varphi(B)$, а на общем классе $\chi_0\varphi(B)$ приобретают вид

$$a_{\chi_0\chi_b} = a_{\chi_0}\chi_0(b)\,\chi_b(b)^{\frac{1}{b}}, \quad a_{\chi_0}\in K. \tag{5}$$

Дальше применимы те же рассуждения, что и в предыдущем случае.

Общий тип. Случай произвольного гомоморфизма $\psi: B\to K^*$ сводится к $\psi\equiv 1$ сдвигом аргумента. Если $\theta(u)$ удовлетворяет (2), то для любой точки $u_0\in T(\overline{K})$ ряд $\theta(u_0 u)$ удовлетворяет такому же уравнению, но с $\psi(b)\chi_b(u_0)^{-1}$ вместо $\psi(b)$. Если $[H:\varphi(B)]<\infty$ и B не имеет кручения, то точку u_0, для которой $\chi_b(u_0)=\psi(b)$ при всех $b\in B$ подобрать можно (разбор более общего случая мы опускаем, он нетруден и не интересен). В самом деле, тогда $\operatorname{Ker}\varphi=\{1\}$, потому что, если $b_0\in\operatorname{Ker}\varphi$, то $\chi_{b_0}(b)=1$ при всех $b\in B$, откуда по

2.3 а), $\chi_b(b_0)=1$. Но если все характеры из подгруппы конечного индекса обращаются в 1 в точке тора, то это точка конечного порядка.

Итак, φ вкладывает B в H; тогда любой гомоморфизм $\psi: B\to K^*$, очевидно, продолжается до гомоморфизма $\overline{\varphi}: H\to\overline{K}^*$, который и доставляет требуемую точку.

Сдвиг на нее сводит общий случай к уже разобранному.

в) Мы уже доказали, что φ вкладывает B в H. Осталось проверить, что $B\subset T(K)$ дискретна. Допустим, что $b=\lim b_i$, $b_i\in B$, и покажем, что последовательность (b_i) тогда стабилизируется. Действительно, для всех $i\geqslant i_0$ и всех $\lambda\in H$ имеем тогда $\operatorname{ord}\chi(b)=\operatorname{ord}\chi(b_i)$ (это ясно для базиса и затем по аддитивности). В частности, $\operatorname{ord}\chi_b(b_i)=\operatorname{ord}\chi_b(b_j)$ для всех $b\in B$ и $i,j\geqslant i_0$. Из невырожденности формы $\operatorname{ord}\chi_b(b)$, очевидно, следует тогда, что $b_i=b_j$. ■

2.7. Если группа периодов $B\subset T(K)$ дискретна и свободна максимального ранга, а гомоморфизм $\varphi: B\to H$, $b\mapsto\chi_b$ удовлетворяет условиям

$$[H:\varphi(B)]<\infty;$$

$$\chi_{b_1}(b_2)=\chi_{b_2}(b_1) \text{ для всех } b_1, b_2\in B;$$

$$\operatorname{ord}\chi_b(b)>0 \text{ для всех } b\in B,\ b\neq 1,$$

то мы будем называть φ поляризацией. Поляризация называется главной, если $\varphi(B)=H$. Типу с главной поляризацией отвечает по существу одна тэта-функция. Мы подробнее рассмотрим ее ниже.

2.8. Фиксируем некоторую главную поляризацию $\varphi: B\to H$ и изучим график модуля (точнее, показателя ord) тэта-функции

$$\theta = \sum_{b\in B} \chi_b(b)^{\frac{1}{2}}\chi_b,$$

(ср. (4)), как в § 1.

Напомним, что этот график лежит в пространстве $H^*\times R$, где $H^*=\operatorname{Hom}(H,R)$, а критические точки θ — образ дивизора нулей θ — образуют некоторые $(n-1)$-мерные соты в H^*.

В нашей ситуации на H^* есть дополнительные структуры:

а) $B^*=\{b^*\mid b\in B\}\subset H^*$. Напомним, что $b^*(\chi)=\operatorname{ord}\chi(b)$ (п. 1.2). Легко видеть, что B^* — решетка максимального ранга в H^*.

б) Евклидова норма на H^*, которая на решетке B^* индуцирует скалярное произведение

$$(b_1^*, b_2^*) = \operatorname{ord}\chi_{b_1}(b_2), \quad \|b^*\| = (b^*, b^*)^{\frac{1}{2}}.$$

Определим еще функцию $\theta^*: H^*\to R$:

$$\theta^*(u^*)=\begin{cases}\operatorname{ord}\theta(u), & \text{если } u\in T(\overline{K}),\ u^* \text{ не критична;}\\ \text{по непрерывности,} & \text{если } u^* \text{ критична.}\end{cases}$$

(См. теорему 1.3).

Чтобы сформулировать следующую теорему, напомним еще понятие разбиения Вороного. Пусть в евклидовом пространстве E дано некоторое дискретное множество точек C. Для каждой точки $c\in C$ положим

$$P_c=\{x\in E \mid \|x-c\|\leqslant\|x-d\| \text{ для всех } d\in C\}.$$

Это (замкнутые) полиэдры максимальной размерности n. Их грани коразмерности $k-1$ имеют вид

$$P_{c_1\ldots c_k}=\bigcap_{i=1}^{k}P_{c_i}=\{x\in E \mid \|x-c_1\|=\ldots=\|x-c_k\|\leqslant$$

$$\leqslant\|x-d\| \text{ для всех } d\in C\}.$$

2.9. Теорема. а) В условиях п. 2.9 имеем $\theta^*(u^*)=-\frac{1}{2}\|u^*\|^2+B^*$ (B^* — периодическая функция). б) Критические точки θ в H^* образуют $(n-1)$-мерный остов разбиения Вороного, отвечающего решетке $B^*\subset H^*$.

Доказательство. а) Уравнение (2) в применении к θ^* превращается в уравнение

$$\theta^*(u^*+b^*)=\theta^*(u^*)-(u^*,\ b^*)-\frac{1}{2}(b^*,\ b^*) \text{ для всех } b^*\in B^*.$$

Так как функция $u^*\mapsto-\frac{1}{2}\|u^*\|^2$ удовлетворяет тому же уравнению, разность $\theta^*(u^*+b^*)+\frac{1}{2}\|u^*\|^2$ периодична. б) Пусть $u^*\in H^*$. Исследуем, каковы максимальные члены ряда $\sum a_x\chi$ в соответствующих точках $T(\overline{K})$. Имеем

$$\operatorname{ord}a_{x_b}+\operatorname{ord}u^*(\chi_b)=\frac{1}{2}(b^*,\ b^*)+(u^*,\ b^*)=$$

$$=\frac{1}{2}\|u^*+b^*\|^2-\frac{1}{2}\|u^*\|^2.$$

Значит, при фиксированном u^* минимум этого выражения достигается при тех χ_b, для которых b^* лежит к $-u^*$ ближе, чем остальные точки B^*. Таким образом, внутренность n-мерных полиэдров соответствующего разбиения Вороного состоит в точности из некритических точек (максимальный член определяется по u^* однозначно). Грани коразмерности k отвечают точкам, в которых имеется $k+1$ максимальный член.

2.10. Пример. Рассмотрим случай $n=\dim T=2$. Выберем в H^* базис, в котором метрика $\|\ \|^2$ записывается в виде суммы квадратов.

Разбиения Вороного (на чертеже жирные линии), отвечающие решетке $B^*\subset H^*$, бывают двух типов: прямоугольные (если B^* прямоугольная) и шестиугольные (в остальных случаях):

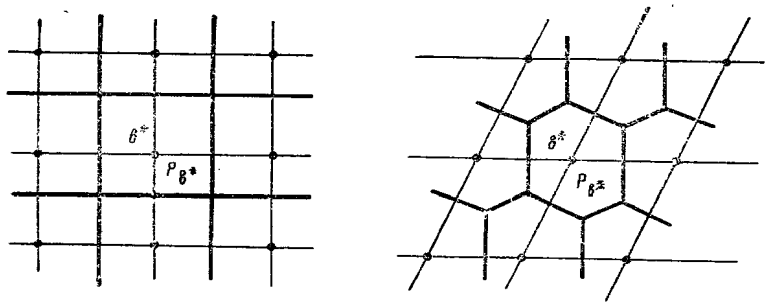


Рис. 2

Напомним, что вещественный тор H^*/B^* является некоторым «изображением» p-адического пространства $T(\overline{K})/B$, так что границы многогранников Вороного $\bmod B^*$ изображают тэта-дивизор.

График $\operatorname{ord}\theta(u)$ (точнее, $\theta^*(u^*)$), согласно теореме 2.9 а), асимптотически ведет себя как купол — параболоид вращения

$$z=-\frac{1}{2}(x^2+y^2)$$

(x, y — декартовы координаты в H^*). Однако этот график кусочно-плоский: он вымощен четырехугольной или шестиугольной черепицей; проекция этого замощения на $(x,\ y)$-плоскость составляет разбиение Вороного.

§ 3. ПОЛЕ АБЕЛЕВЫХ ФУНКЦИЙ

3.1. Пусть T — n-мерный тор над K, как в § 2, с группой характеров H. Пусть дана также свободная дискретная подгруппа периодов $B\subset T(K)$ ранга n.

В этом параграфе мы будем считать, что множество поляризаций $\varphi: B\to H$ непусто. Согласто п. 2.7, множество типов $(\varphi,\ \psi,\ [\ ,\ ])$, где φ пробегает всевозможные поляризации, образует полугруппу.

Назовем абелевой функцией на T (с периодами B) нуль или отношение двух тэта-функций одного и того же типа, отвечающего какой-нибудь поляризации. Из предыдущего замечания следует, что абелевы функции с периодами B образуют поле. Обозначим его $\mathcal{M}^B$.

Фиксируем некоторую поляризацию φ. Обозначим через $A_m(\varphi)$ пространство всех тэта-функций типа $(\varphi^{2m}, 1, \chi_{b_1}(b_2)^m)$ при $m \geqslant 1$ и K при $m=0$. Положим $A(\varphi) = \bigoplus_{m=0}^{\infty} A_m(\varphi)$. Это градуированное кольцо. Обозначим через $\mathcal{M}(\varphi)$ его поле частных нулевой степени. Очевидно, $\mathcal{M}(\varphi) \subset \mathcal{M}^B$.

Основной целью этого параграфа будет доказательство следующей теоремы:

3.2. Теорема. а) Поле $\mathcal{M}(\varphi)$ совпадает с полем абелевых функций $\mathcal{M}^B$, в частности, не зависит от поляризации φ. Оно инвариантно относительно сдвига аргументов на точки из $T(K)$, так что группа $T(K)/B$ действует на это поле.

б) $\mathcal{M}^B$ конечно порождено над K; его степень трансцендентности равна n; K алгебраически замкнуто в $\mathcal{M}^B$.

в) Если $[L:K] < \infty$, то $A_L(\varphi) = A(\varphi) \underset{K}{\otimes} L$ и $\mathcal{M}_L^B = \mathcal{M}^B L$ — композит $\mathcal{M}^B$ и L над K. Здесь кольцо $A_L(\varphi)$ построено для тора $T_L = \operatorname{Spec} L[H]$ так же, как $A(\varphi)$ для K.

Доказательство. а) Пусть $\theta_1\theta_2^{-1} \in \mathcal{M}^B$, где θ_1, θ_2 — тэта-функции типа $(\varphi_1, \psi, [\ ,\ ])$, φ_1 — некоторая поляризация. Мы покажем, что θ_1 и θ_2 можно умножить на одну и ту же тэта-функцию такого типа, что получившиеся произведения будут лежать в $A_N(\varphi)$ для подходящего N. Отсюда будет следовать, что $\mathcal{M}^B \subset \mathcal{M}(\varphi)$ и, значит, $\mathcal{M}^B = \mathcal{M}(\varphi)$.

Прежде всего, легко добиться того, чтобы $\psi \equiv 1$: достаточно умножить θ_1 и θ_2 на ненулевую тэта-функцию типа $(\varphi, \psi^{-1}, [\ ,\ ])$, которая существует по теореме 2.6. Мы получим функции типа $(\varphi_1^2, 1, [\ ,\ ]_1)$.

Для дальнейшей редукции важен следующий факт: существует такое $N \geqslant 1$, и поляризация φ_2, что $\varphi^N = \varphi_1\varphi_2$.

Действительно, гомоморфизму $\varphi^N\varphi_1^{-1} : B \to H$ отвечает симметричная билинейная форма:

$$B \times B \to Z : (b_1, b_2) \mapsto N \operatorname{ord} \varphi(b_1)[b_2] - \operatorname{ord} \varphi_1(b_1)[b_2] \qquad (6)$$

(раньше вместо $\varphi(b_1)$ мы всегда писали χ_{b_1}). Форма $\operatorname{ord}\varphi(b_1)[b_2]$ положительно определена. Так как пространство таких форм открыто, для достаточно большого N форма (6) также положительно определена. Из ее невырожденности следует, что $\varphi^N\varphi_1^{-1}$ имеет тривиальное ядро. Из теоремы 2.6 в) тогда вытекает, что $\varphi^N\varphi_1^{-1} = \varphi_2$ является поляризацией.

Умножив теперь θ_1 и θ_2 на тэта-функцию типа $(\varphi_2^2, 1, [\ ,\ ]_2)$, мы получим тэта-функции типа $(\varphi^{2N}, 1, [\ ,\ ]_3)$, где $[\ ,\ ]_3$ еще может отличаться от $(\chi_{b_1}(b_2))^N$ знаком для некоторых значений b_1, b_2. Умножив еще раз числитель и знаменатель, скажем, на числитель, мы попадем, наконец, в $A_{2N}(\varphi)$.

Итак, $\mathcal{M}^B = \mathcal{M}(\varphi)$. Инвариантность $\mathcal{M}^B$ относительно сдвигов на точки из $T(K)$ проверяется с помощью замечания в

доказательстве теоремы 2.6 б): сдвиг тэта-функции меняет в ее типе только ψ, но не соответствующую поляризацию.

б), в). Пользуясь определением кольца $A(\varphi)$ и теоремой 2.6, получаем

$$\dim_K A_m(\varphi) = [H : \varphi^{2m}(B)] = cm^n, \quad c = [H : \varphi^2(B)].$$

Лемма 3.5 а) главы I показывает тогда, что $\deg \operatorname{tr}_K \mathcal{M}(\varphi) \leqslant n$. Вторая часть этой же леммы даст то, что нам нужно, если мы найдем n алгебраически независимых функций в поле $\mathcal{M}(\varphi)$. Мы воспользуемся тем, что $\mathcal{M}(\varphi) = \mathcal{M}^B$, и будем искать n независимых абелевых функций. Удобно будет строить их в $\mathcal{M}^B L$ для достаточно большого $L \supset K$, поэтому проверим сначала последние утверждения теоремы 3.2. Это легко: каноническое отображение $A(\varphi) \underset{K}{\otimes} L \to A_L(\varphi)$ является изоморфизмом, ибо размерности однородных компонент над L у колец слева и справа одинаковы. В частности, при тензорном умножении на L не появляется делителей нуля. Отсюда следует, что K алгебраически замкнуто в L и что $\mathcal{M}_L^B = \mathcal{M}^B L$.

Окончательно, нам осталось доказать следующую лемму:

3.3. Лемма. Пусть φ — некоторая поляризация. Существует такая тэта-функция $\theta(u)$ типа $(\varphi, 1, [\ ,\ ])$ и такие точки $u_1, \ldots, u_n \in T(\overline{K})$, что функции

$$\frac{\theta(u_i^2 u)\,\theta(u_i^{-1}u)^2}{\theta(u)^3}, \quad i = 1, \ldots, n \qquad (7)$$

принадлежат $\mathcal{M}^B\overline{K}$ и алгебраически независимы над K.

Доказательство. Положим $\theta = \sum a_\chi \chi$, где $a_\chi = \chi_b(b)^{\frac{1}{2}}$, если $\chi \in \varphi(B)$, $a_\chi = 0$, если $\chi \notin \varphi(B)$. Тогда $\varphi(B)^* \subset H^*$ — решетка максимального ранга. Относительно нее $\theta(u)$ ведет себя так, как если бы поляризация была главной, и мы можем пользоваться теоремой 2.9 и вычислениями, полученными в ходе ее доказательства.

Функции (7), очевидно, лежат в $\mathcal{M}^B\overline{K}$ для любого выбора u_i. Допустим, что между ними имеется полиномиальное соотношение степени N. Освобождаясь от знаменателя, приходим к соотношению вида

$$\sum a_{i_0 \ldots i_n} \theta(u)^{3i_0} \left[\theta(u_1^2 u)\,\theta(u_1^{-1}u)^2\right]^{i_1} \ldots \left[\theta(u_n^2 u)\,\theta(u_n^{-1}u)^2\right]^{i_n} = 0, \qquad (8)$$

где суммирование распространено на (i_k) с $i_0 + \ldots + i_n = N$.

Переходя к ord и учитывая, что в левой части (8) при всех u в окрестности 1 должна быть фиксированная пара максимальных одночленов, получаем из (8) некоторое соотношение вида

$$\left.\begin{aligned} &3j_0\theta^*(u^*)+\sum_{i=1}^{n} j_k\left(\theta^*(u^*+2u_i^*)+2\theta^*(u^*-u_i^*)=\text{const},\right.\\ &j_0+\ \dots\ +j_n=0 \end{aligned}\right\} \quad (9)$$

(не все j_i равны нулю).

Подберем u_i так, чтобы вычисление (9), как в теореме 2.9, привело к противоречию.

Для этого достаточно, чтобы 0 была единственной точкой решетки $\varphi(B)^*$, ближайшей к каждой из точек u_i^*, и в то же время, чтобы точки $b_i^* \in \varphi(B)$ $(i=1, \dots, n)$, ближайшие к $-2u_i^*$, были линейно независимы в H^*. (В существовании таких u_i легко убедиться). Тогда находим по п. 2.9 (для u^* в окрестности нуля):

$$\theta^*(u^*+2u_i^*)=(u^*,\ b_i^*)+\text{const}_i,$$

$$\theta^*(u^*-u_i^*)=\text{const}_i,$$

$$\theta^*(u^*)=\text{const}.$$

Подставляя в (9), получаем

$$\begin{cases} \sum_{i=1}^{n} j_i(u_i^*,\ b_i^*)=\text{const},\\ j_0+\ \dots\ +j_n=0. \end{cases} \quad (10)$$

Так как b_i^* независимы, находим $\text{const}=j_1=\ \dots\ =j_n=0$ из первого соотношения и затем $j_0=0$ из второго, что противоречит конструкции j_i. ■

3.4. В заключение приведем без доказательства некоторые дополнительные сведения. Часть из них можно было бы, вероятно, установить «элементарно», имитируя соответствующие доказательства в комплексном случае. Другую часть естественно рассматривать средствами главы IV.

Прежде всего, для любой поляризации φ кольцо $A(\varphi)$ конечно порождено, и проективный спектр $X=\text{Proj}\,A(\varphi)$ является абелевым многообразием над K, не зависящим от φ. Это каноническая модель поля $\mathcal{M}^B$. Для любого конечного расширения $L \supset K$, имеет место естественный изоморфизм $X(L)=T(L)/B$. Множество абелевых многообразий над K, являющихся моделями $\mathcal{M}^B$, должно допускать такое же описание, как в п. 3.7 а) главы I, но подробного изложения в литературе нет.

Типы тэта-функций и поляризации интерпретируются в терминах групп когомологий и группы Пикара многообразия X. Можно дать также описание двойственного многообразия $\hat{X}$, указав явно соответствующую группу периодов $\hat{B}$ в торе $\hat{T}$. Подробности см. в работах Герритцена [3] и [4].

Очень важная работа Мамфорда [19], в которой X строится как алгебраизация некоторой формальной схемы, а тэта-функции появляются лишь как особые переменные в градуированных кольцах, проливает новый свет на эти конструкции и содержит существенно новые идеи.

Глава III

ГРУППЫ И ФУНКЦИИ ШОТТКИ

§ 1. ГРУППЫ ШОТТКИ

1.1. В этой главе $[K:Q_p]<\infty$, $\text{PGL}(2, K)=\text{GL}(2, K)/K^*$ — группа дробно-линейных преобразований одной переменной над K. Она, естественно, действует слева на проективную прямую P_K^1 с выделенной системой координат: если $g=\begin{pmatrix} a & b \\ c & d \end{pmatrix} \bmod K^*$, то

$$g(z)=\frac{az+b}{cz+d},\ z \in \overline{K}.$$

В дальнейшем мы будем писать просто $g=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ (опуская $\bmod K^*$).

Группой Шоттки $\Gamma \subset \text{PGL}(2, K)$ называется любая дискретная подгруппа без кручения с конечным числом образующих.

Элемент $g \in \text{PGL}(2, K)$ называется гиперболическим, если он представлен матрицей, собственные значения которой по модулю не совпадают.

Следующий результат дает полезные варианты определения групп Шоттки.

1.2. Предложение. Следующие три свойства подгруппы $\Gamma \subset \text{PGL}(2, K)$ эквивалентны:

а) Γ является группой Шоттки.

б) Γ имеет конечное число образующих и все ее элементы, кроме единицы, гиперболичны.

в) Γ имеет конечное число образующих, не содержит кручения и дискретно действует в какой-то точке $z \in P^1(\overline{K})$.

Доказательство. а) $\Rightarrow$ б). Достаточно проверить, что если в Γ есть негиперболический элемент бесконечного порядка, то она недискретна. Действительно, такой элемент сопряжен

$$\left.\begin{aligned} &3j_0\theta^*(u^*)+\sum_{i=1}^{n} j_k\left(\theta^*(u^*+2u_i^*)+2\theta^*(u^*-u_1^*)=\text{const},\right.\\ &j_0+\ \ldots\ +j_n=0 \end{aligned}\right\} \quad (9)$$

(не все j_i равны нулю).

Подберем u_i так, чтобы вычисление (9), как в теореме 2.9, привело к противоречию.

Для этого достаточно, чтобы 0 была единственной точкой решетки $\varphi(B)^*$, ближайшей к каждой из точек u_i^*, и в то же время, чтобы точки $b_i^*\in\varphi(B)$ $(i=1, \ldots, n)$, ближайшие к $-2u_i^*$, были линейно независимы в H^*. (В существовании таких u_i легко убедиться). Тогда находим по п. 2.9 (для u^* в окрестности нуля):

$$\theta^*(u^*+2u_i^*)=(u^*,\ b_i^*)+\text{const}_i,$$

$$\theta^*(u^*-u_i^*)=\text{const}_i,$$

$$\theta^*(u^*)=\text{const}.$$

Подставляя в (9), получаем

$$\begin{cases}\sum_{i=1}^{n} j_i(u_i^*,\ b_i^*)=\text{const},\\ j_0+\ \ldots\ +j_n=0.\end{cases} \quad (10)$$

Так как b_i^* независимы, находим $\text{const}=j_1=\ \ldots\ =j_n=0$ из первого соотношения и затем $j_0=0$ из второго, что противоречит конструкции j_i. ■

3.4. В заключение приведем без доказательства некоторые дополнительные сведения. Часть из них можно было бы, вероятно, установить «элементарно», имитируя соответствующие доказательства в комплексном случае. Другую часть естественно рассматривать средствами главы IV.

Прежде всего, для любой поляризации φ кольцо $A(\varphi)$ конечно порождено, и проективный спектр $X=\text{Proj}\,A(\varphi)$ является абелевым многообразием над K, не зависящим от φ. Это каноническая модель поля $\mathcal{M}^B$. Для любого конечного расширения $L\supset K$, имеет место естественный изоморфизм $X(L)=T(L)/B$. Множество абелевых многообразий над K, являющихся моделями $\mathcal{M}^B$, должно допускать такое же описание, как в п. 3.7 а) главы I, но подробного изложения в литературе нет.

Типы тэта-функций и поляризации интерпретируются в терминах групп когомологий и группы Пикара многообразия X. Можно дать также описание двойственного многообразия $\hat{X}$, указав явно соответствующую группу периодов $\hat{B}$ в торе $\hat{T}$. Подробности см. в работах Герритцена [3] и [4].

Очень важная работа Мамфорда [19], в которой X строится как алгебраизация некоторой формальной схемы, а тэта-функции появляются лишь как особые переменные в градуированных кольцах, проливает новый свет на эти конструкции и содержит существенно новые идеи.

Глава III

ГРУППЫ И ФУНКЦИИ ШОТТКИ

§ 1. ГРУППЫ ШОТТКИ

1.1. В этой главе $[K:Q_p]<\infty$, $\text{PGL}(2, K)=\text{GL}(2, K)/K^*$ — группа дробно-линейных преобразований одной переменной над K. Она, естественно, действует слева на проективную прямую P_K^1 с выделенной системой координат: если $g=\begin{pmatrix}a & b\\ c & d\end{pmatrix} \bmod K^*$, то

$$g(z)=\frac{az+b}{cz+d},\ z\in\overline{K}.$$

В дальнейшем мы будем писать просто $g=\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ (опуская $\bmod K^*$).

Группой Шоттки $\Gamma\subset\text{PGL}(2, K)$ называется любая дискретная подгруппа без кручения с конечным числом образующих.

Элемент $g\in\text{PGL}(2, K)$ называется гиперболическим, если он представлен матрицей, собственные значения которой по модулю не совпадают.

Следующий результат дает полезные варианты определения групп Шоттки.

1.2. Предложение. Следующие три свойства подгруппы $\Gamma\subset\text{PGL}(2, K)$ эквивалентны:

а) Γ является группой Шоттки.

б) Γ имеет конечное число образующих и все ее элементы, кроме единицы, гиперболичны.

в) Γ имеет конечное число образующих, не содержит кручения и дискретно действует в какой-то точке $z\in P^1(\overline{K})$.

Доказательство. а) $\Rightarrow$ б). Достаточно проверить, что если в Γ есть негиперболический элемент бесконечного порядка, то она недискретна. Действительно, такой элемент сопряжен

в $\mathrm{PGL}(2,\overline{K})$ либо с элементом вида $g=\begin{pmatrix}1 & \lambda\\ 0 & 1\end{pmatrix}$, либо с элементом вида $h=\begin{pmatrix}1 & 0\\ 0 & \mu\end{pmatrix}$ с $|\mu|=1$. В первом случае $g^{p^n}\to e$ при $n\to\infty$, во втором случае $h^{(q-1)p^n}\to e$ при $n\to\infty$, где q — число классов вычетов поля $K(\mu)$. Поэтому единица в Γ является предельной точкой степеней негиперболического элемента.

б) $\Rightarrow$ а). Если Γ удовлетворяет условию б), то она, очевидно, не имеет кручения. Если бы она не была дискретна, то некоторая последовательность (g_i) ее элементов сходилась бы к e и, значит, начиная с некоторого i характеристические корни g_i должны были бы стать по модулю одинаковыми, что противоречит условию гиперболичности.

в) $\Rightarrow$ а). Очевидно.

а) $\Rightarrow$ в). Предположим, что группа Шоттки Γ ни в какой точке $z\in P^1(\overline{K})$ не действует дискретно. Возьмем три разных, но сопряженных над K точки $z^{(1)}$, $z^{(2)}$, $z^{(3)}$. Пусть $(g_i)\subset\Gamma$ — такая последовательность элементов, что $g_i z^{(1)}\to z^{(1)}$ при $i\to\infty$. Тогда $g_i z^{(j)}\to z^{(j)}$ для всех $j=1, 2, 3$, ибо сопряжение непрерывно. Но тогда $g_i\to e$, что противоречит дискретности Γ в $\mathrm{PGL}(2, K)$. ■

1.3. Пример. Пусть Γ — группа Шоттки ранга 1 с образующей g. Характеристические корни любой матрицы в классе g разные по модулю и потому определены над K. Значит, у g есть две неподвижные точки, также определенные над K. Выберем систему координат, в которой одна неподвижная точка есть 0, а другая ∞. В этой системе координат g представлен диагональной матрицей $\begin{pmatrix}q & 0\\ 0 & 1\end{pmatrix}$. Можно считать, что $|q|<1$ (иначе нужно поменять местами 0 и ∞). Тогда

$$0=\lim_{n\to\infty} g^n z \text{ для любой } z\neq\infty,$$

$$\infty=\lim_{n\to-\infty} g^n z \text{ для любой } z\neq 0.$$

Γ действует дискретно вне двух своих неподвижных точек.

В дальнейшем мы для любого гиперболического элемента g и любой точки z, не являющейся неподвижной, будем писать:

$$z_g^+=\lim_{n\to\infty} g^n z,$$

$$z_g^-=\lim_{n\to-\infty} g^n z.$$

Из предыдущего обсуждения ясно, что эти пределы существуют, не зависят от z и являются неподвижными точками

g, — притягивающей (z_g^+) и отталкивающей (z_g^-) соответственно.

1.4. Пусть $g=\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ — такой элемент $\mathrm{PGL}(2, K)$, что $c\neq 0$, то есть ∞ не является неподвижной точкой g. Положим

$$j_g(z)=\frac{d}{dz}\frac{az+b}{cz+d}=\frac{ad-bc}{(cz+d)^2}$$

и определим изометрическую окружность g как множество точек $z\in P^1(\overline{K})$ вида

$$I(g)^{=}=\{z\mid |j_g(z)|=1\}.$$

Аналогично, $I(g)^{>}$ будет определяться условием $|j_g(z)|>1$ и т. п.

1.5. Лемма. Если g гиперболичен, то

а) $I(g)^{<}\cap I(g^{-1})^{<}=\varnothing$;

б) $g(I(g)^{=})=I(g^{-1})^{=}$, $g(I(g)^{>})=I(g^{-1})^{<}$;

в) $z_g^+\in I(g^{-1})^{<}$, $z_g^-\in I(g)^{<}$.

Доказательство. а) Перейдя в случае нужды к квадратичному расширению K, мы можем считать, что $ad-bc=1$. Тогда $|\mathrm{Tr}\,g|=|a+d|>1$, потому что $a+d$ есть сумма двух неравных по модулю характеристических корней g, произведение которых есть 1. Точка $-\frac{d}{c}$ лежит в $I(g)1^{<}$, а $\frac{a}{c}$ лежит в $I(g^{-1})1^{<}$; радиусы кругов $I(g)$ и $I(g^{-1})$ равны $\frac{1}{|c|}$. Так как расстояние $\left|\frac{a}{c}+\frac{d}{c}\right|=\frac{|a+d|}{|c|}$ больше радиусов, эти круги не пересекаются. (Напомним, что в неархимедовой геометрии круги с границей либо не пересекаются, либо целиком содержатся один внутри другого!).

б) $z\in I(g)^{=}\Leftrightarrow |cz+d|=1$; аналогично, $g(z)\in I(g^{-1})^{=}\Leftrightarrow$ $\Leftrightarrow |cg(z)-a|=1$. Но

$$|cg(z)-a|=\left|c\frac{az+b}{cz+d}-a\right|=\frac{1}{|cz+d|}.$$

Поэтому g переводит $I(g)$ в $I(g^{-1})$, а внешность $I(g)$ во внутренность $I(g^{-1})$.

в) Пусть $z\in I(g)^{>}$; тогда в силу б) и а), $g(z)\in I(g^{-1})^{<}\subset I(g)^{>}$. Иными словами, g переводит любую точку z, лежащую вне своего изометрического круга, внутрь изометрического круга обратного преобразования, и при последующих применениях g она остается там. Следовательно, $z_g^+=\lim\limits_{n\to\infty} g^n z\in I(g^{-1})$. Аналогично проверяется второе включение.

1.6. Предложение. Пусть Γ — группа Шоттки и пусть система координат в P^1 выбрана так, что в ∞ Γ действует дискретно. Тогда множество неподвижных точек элементов

Γ ограничено, а радиусы изометрических окружностей стремятся к нулю (по фильтру дополнений к конечным подмножествам Γ).

Доказательство. Множество $\Gamma_\infty - (\infty)$ лежит вне некоторой окрестности ∞, то есть ограничено. Любая неподвижная точка лежит в его замыкании (ибо имеет вид $\lim g^n(\infty)$), которое также ограничено.

Для проверки утверждения об изометрических окружностях достаточно считать, что все элементы $g \in \Gamma$ представлены матрицами с определителем 1 (этого можно добиться, присоединив к K все $\sqrt{\det g}$, что дает конечное расширение). Пусть $g = \begin{pmatrix} a_g & b_g \\ c_g & d_g \end{pmatrix}$, $\det = 1$; тогда $r_g = $ радиус $I(g) = \frac{1}{|c_g|}$. Предположим, что для некоторого $C > 0$ и бесконечно многих $g \in \Gamma$ имеем $|c_g| < C$ (то есть r_g не стремятся к нулю). Так как по доказанному $|g(\infty)| = \left|\frac{a_g}{c_g}\right| < R$ для некоторого R, на этом же множестве $|a_g| < RC$; аналогично, $|d_g| < RC$, ибо $|g^{-1}(\infty)| = \left|\frac{d_g}{c_g}\right| < R$. Значит, на этом множестве $|b_g| \to \infty$ (иначе Γ не была бы дискретной), а так как $ad - bc = 1$, то с необходимостью $|c_g| \to 0$.

Выведем из этого противоречие, установив, что $|c_g|$ ограничены снизу во всей группе Γ. Это вытекает из следующего простого тождества. Пусть $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, $h = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $g \neq h^{-1}$ — два элемента из Γ, представленные матрицами из SL. Тогда

$$r_h^2 = \frac{1}{|c|^2} = |(gh)^{-1}(\infty) - h^{-1}(\infty)|\,|h(\infty) - g^{-1}(\infty)| < R^2.$$

Проверка тождества:

$$gh = \begin{pmatrix} \alpha a + \beta c & \alpha b + \beta d \\ \gamma a + \delta c & \gamma b + \delta d \end{pmatrix};$$

$$gh^{-1}(\infty) = -\frac{\gamma b + \delta d}{\gamma a + \delta c};$$

$$h^{-1}(\infty) = -\frac{d}{c}; \quad h(\infty) = \frac{a}{c}; \quad g^{-1}(\infty) = -\frac{\delta}{\gamma};$$

$$-\frac{\gamma b + \delta d}{\gamma a + \delta c} + \frac{d}{c} = \frac{\gamma}{c(\gamma a + \delta c)};$$

$$\frac{a}{c} + \frac{\delta}{\gamma} = \frac{\gamma a + \delta c}{\gamma c}. \blacksquare$$

Это доказательство в комплексном случае принадлежит Форду [2]. Можно дать совсем другой вывод этого и следующего результатов, пользуясь методами §§ 4—6.

1.7. Теорема. Пусть $\Gamma \subset PGL(2, K)$ — группа Шоттки, $z \in P^1(K)$ — некоторая точка. Следующие три свойства равносильны.

а) z является точкой накопления некоторой орбиты Γz_0, где Γ действует в z_0 дискретно;

б) z является точкой накопления семейства неподвижных точек неединичных элементов Γ;

в) Γ не действует в z дискретно.

Множество Σ таких точек z замкнуто, содержит все неподвижные точки элементов Γ и называется множеством предельных точек Γ.

Доказательство. а) $\Leftrightarrow$ б). Выберем систему координат, в которой z_0 есть ∞. Для любого $g \in \Gamma$, $g \neq e$ по лемме 1.5 имеем $z_g^- \in I_g^{\leq}$ и $g^{-1}(\infty) \in I(g)^<$. Поэтому $|z_g^- - g^{-1}(\infty)| < r_g \to 0$ по предложению 1.6. Значит, любая точка накопления орбиты $\Gamma(\infty)$ будет в то же время точкой накопления семейства неподвижных точек z_g^-, и наоборот.

а) $\Leftrightarrow$ в). Очевидно. ■

1.8. Пример: специальные группы Шоттки.

Пользуясь установленными фактами, мы построим сейчас явные примеры групп Шоттки любого ранга, задавая их образующими.

Пусть $n \geqslant 1$. Выберем в конечной части прямой $P^1(K)$ круги $I_1, \ldots, I_n$ (с границей) и $I_1', \ldots, I_n'$ (без границы) со следующими свойствами:

а) радиус I_k = радиус $I_k' = r_k \in |K|$, $k = 1, \ldots, n$; все круги попарно не пересекаются, даже если к I_k' добавить их границы.

Далее, выберем такие элементы $c_k \in K$, что

б) $r_k = \frac{1}{|c_k|}$;

наконец, выберем по очереди такие элементы $a_k, d_k, b_k \in K$, что

в) $-\frac{d_k}{c_k} \in I_k$; $\frac{a_k}{c_k} \in I_k'$, $a_k d_k - b_k c_k = 1$.

Положим $g_k = \begin{pmatrix} a_k & b_k \\ c_k & d_k \end{pmatrix}$.

1.9. Предложение. а) Элементы $g_1, \ldots, g_n$ порождают свободную подгруппу Γ в $PGL(2, K)$, которая является группой Шоттки; $I_k = I(g_k)^<$, $I_k' = I(g_k^{-1})^<$.

б) Область $D = \bigcap_{k=1}^{n} (I(g_k)^> \cap I(g_k^{-1})^>)$ является фундаментальной областью для Γ в $\Omega = P^1 \setminus \Sigma$.

Замечание. Позже будет доказано, что любая группа Шоттки свободна.

Доказательство. а) Пусть $g = g_{i_m}^{\varepsilon_m} \ldots g_{i_1}^{\varepsilon_1}$ — приведенная запись элемента из Γ: $\varepsilon_k = \pm 1$ и если $i_r = i_{r+1}$, то $\varepsilon_r = \varepsilon_{r+1}$. Индукцией по $m \geqslant 1$ покажем, что $D \cap gD = \varnothing$. Отсюда будет следовать, что $g \neq 1$, так что Γ свободна и действует

дискретно в точках D. Поэтому Γ является группой Шоттки в силу предложения 1.2 в).

Пусть сначала $m>1$. Как в доказательстве леммы 1.5 а), легко убедиться, что g_k гиперболичны, потому что I_k — изометрический круг g_k, I_k' — то же для g_k^{-1}, а расстояние между ними больше их общего радиуса, так что $|\operatorname{Tr} g_k| = |a_k+d_k|>1$. Учитывая еще $\det g_k=1$, получаем гиперболичность g_k.

Любая точка $z\in D$ лежит в $I(g_k)^>$, поэтому по лемме 1.5 б) $g_k(z)\in I(g_k^{-1})^< \not\subset D$ по определению D.

Переход от m к $m+1$. Индуктивное предположение: если $z\in D$, то

$$g_{i_m}^{\varepsilon_m}\dots g_{i_1}^{\varepsilon_1}(z)\in I\left(g_{i_m}^{-\varepsilon_m}\right)^< \not\subset D.$$

Для $m=1$ оно уже проверено. Проверим его для $m+1$, положив $g=g_{i_{m+1}}^{\varepsilon_{m+1}}\dots g_{i_1}^{\varepsilon_1}(z)$. Если $i_{m+1}\neq i_m$, то по предположению

$$g_{i_m}^{\varepsilon_m}\dots g_{i_1}^{\varepsilon_1}(z)\in I\left(g_{i_m}^{-\varepsilon_m}\right)^<\subset I\left(g_{i_{m+1}}^{\varepsilon_{m+1}}\right)^>$$

(ибо круги попарно не пересекаются), и по лемме 1.5 б),

$$g(z)\in g_{i_{m+1}}\left(I\left(g_{i_{m+1}}^{\varepsilon_{m+1}}\right)^>\right)\subset I\left(g_{i_{m+1}}^{-\varepsilon_{m+1}}\right)^<,$$

что и нужно было доказать.

Если же $i_{m+1}=i_m$, то обязательно $\varepsilon_{m+1}=\varepsilon_m$, так что по-прежнему $I\left(g_{i_m}^{-\varepsilon_m}\right)^<\subset I\left(g_{i_m}^{\varepsilon_m}\right)^> = I\left(g_{i_{m+1}}^{\varepsilon_{m+1}}\right)^>$, и рассуждение продолжается, как выше.

б) Мы уже установили, что разные точки D неэквивалентны относительно Γ. Для проверки того, что D — фундаментальная область, остается проверить, что $P^1(\bar K)\setminus \bigcup_{g\in\Gamma} gD=\Sigma$ (предельные точки Γ). В самом деле, обозначая штрихом дополнение в $P^1(\bar K)$, имеем

$$\left(\bigcup_g gD\right)' = \bigcap_g (gD)' = \bigcap_g gD' = \bigcap_g g\left(\bigcup_{k=1}^n I(g_k)^< \cup I\left(g_k^{-1}\right)^<\right).$$

Поменяем в последнем равенстве местами объединение и пересечение по формуле $\bigcap_{i\in I}\left(\bigcap_{j\in J(i)} M_{ij}\right)=\bigcup_f\left(\bigcap_i M_{i,f(i)}\right)$, где f пробегает множество наборов $(f(i))_{i\in I}$, $f(i)\in J(i)$. Тогда мы получим, что $(\cup gD)'$ есть объединение множеств, каждое из которых является бесконечным пересечением вида

$$M=\bigcap_{g\in\Gamma_1} g\left(I_{k_1(g)}\right)\bigcap_{g\in\Gamma_2} g\left(I'_{k_2(g)}\right),$$

где $\Gamma=\Gamma_1\cup\Gamma_2$, $\Gamma_1\cap\Gamma_2=\varnothing$; $k_i:\Gamma_i\to[1,\dots,n]$. Покажем, что

если такое пересечение непусто, то оно целиком лежит в Σ. Действительно, либо k_1, либо k_2 бесконечно много раз принимает одно и то же значение. Пусть, скажем, k_1 равно 1 на бесконечном подмножестве $\Gamma_0\subset\Gamma$. Тогда

$$M\subset\bigcap_{g\in\Gamma_0} g\ (I_1).$$

Покажем, что любая $\bar K$-точка из $\bigcap_{g\in\Gamma_0} g^{-1}(I_1)$ принадлежит Σ. Пусть это не так; тогда в этом пересечении есть точка z, не являющаяся, в частности, неподвижной точкой элементов Γ. Пусть $z=g(z_g)$, $z_g\in I_1$, $g\in\Gamma_0$. Выберем из множества (z_g) предельную точку z_∞ (это возможно в силу того, что $z_g\in I_1(K(z))$), а это множество компактно). Тогда z является предельной точкой орбиты Γz_∞. ■

1.9. Аналогия с комплексным полем. Область D для комплексной группы Шоттки, построенной, как в п. 1.8, имеет такой вид, как на рис. 3. Склеив границы кругов I_k, I_k', мы получим риманову поверхность рода n — сферу с n ручками. Ниже будет показано, что $\Gamma\backslash\Omega$ и в

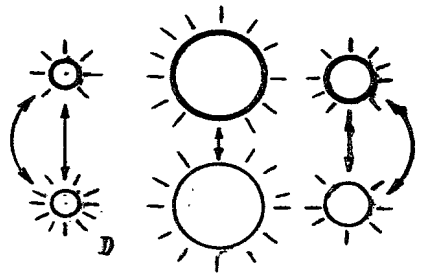


Рис. 3

p-адическом случае представляет кривую рода n. Всякая ли группа Шоттки имеет фундаментальную область такого вида кажется, не известно.

§ 2. ДИВИЗОРЫ И АВТОМОРФНЫЕ ФУНКЦИИ

2.1. Дивизоры. В этом параграфе мы построим для фиксированной группы Шоттки $\Gamma\subset \mathrm{PGL}(2,K)$ произведения Вейерштрасса, аналогичные θ-функциям главы I, и исследуем их свойства.

Пусть $\Omega=P^1(\bar K)\setminus\Sigma$ — множество точек, где Γ действует дискретно. Назовем K-дивизором d на Ω функцию $\Omega(\bar K)\to Z: z\mapsto n_z$ со следующими свойствами:

а) Множество $\operatorname{supp}(d)=\{z|n_z\neq 0\}$ не имеет предельных точек в Ω.

б) Существует такое конечное расширение $L\supset K$, что если $n_z\neq 0$, то $z\in\Omega(L)$.

в) $n_{z_1}=n_{z_2}$, если z_1 и z_2 сопряжены над K. Как в главе I, мы пишем $d=\Sigma n_z z$. Носитель $\operatorname{supp}(d)$ — это множество $\{z|n_z\neq 0\}$. Дивизор конечен, если $\operatorname{supp}(d)$ конечен.

Группа Γ действует на группе K-дивизоров $\mathscr{D}_\Omega(K)$ слева. Опишем сначала Γ-инвариантные K-дивизоры.

2.2. Предложение. а) Группа Γ-инвариантных K-дивизоров состоит в точности из дивизоров вида $\sum\limits_{g\in\Gamma} g(d)$, где d может быть любым конечным K-дивизором на Ω.

б) $\Sigma g(d)=0$ для конечного K-дивизора d, если и только если он может быть представлен в виде

$$d=\sum_{i=1}^{k}(1-g_i)\,d_i,$$

где $g_i\in\Gamma$, d_i — некоторые конечные K-дивизоры на Ω.

Доказательство. а) Если d конечен, то формальная сумма $\Sigma g(d)$ является дивизором: условие а) выполняется в силу теоремы 1.7, а условия б) и в) очевидны.

Наоборот, пусть $D\in\mathscr{D}_\Omega(K)^\Gamma$. Чтобы построить d с $D=\sum\limits_{g\in\Gamma} g(d)$, воспользуемся следующим фактом, который будет доказан ниже, в § 6: существует такая область $S\subset\Omega$, что $\Omega=\bigcup\limits_{g\in\Gamma} gS$ и $S(L)$ компактно для всех конечных расширений $L\supset K$. (На самом деле в качестве S можно взять конечное объединение конечных пересечений колец с границей, где каждое кольцо с границей определено условиями $|a|\leqslant|f|\leqslant|b|$, a, $b\in K$, f — некоторая координатная функция на P^1 с дивизором в Σ: см. теорему 6.10).

Итак, пусть даны $D\in\mathscr{D}_\Omega(K)^\Gamma$ и область S. Множество $\operatorname{supp} D$ разбивается только на конечное число Γ-орбит: иначе пересечение $\operatorname{supp} D\cap S$ было бы бесконечно и содержалось бы в $S(L)$ для конечного $L\supset K$ по свойству б) дивизора; тогда оно имело бы предельную точку в $S(L)\subset\Omega$ в силу компактности $S(L)$, что противоречит свойству а) дивизора. Далее, точки в одной орбите не могут быть сопряжены над K: у точек z и gz в системе координат с нулем z_g^+ и полюсом z_g^- не совпадают модули (их отношение есть $|q|<1$, если $g=\left(\begin{smallmatrix} q & 0\\ 0 & 1\end{smallmatrix}\right)$). Поэтому мы можем написать $D=\sum\limits_{z\in E} n_z\left(\sum\limits_{g\in\Gamma} gz\right)$, где E — конечный набор представителей Γ-орбит в $\operatorname{supp} D$,

содержащий вместе с каждой точкой сопряженную к ней. Полагая $d=\sum\limits_{z\in E} n_z z$, находим требуемое.

б) Пусть $d=\Sigma m_i z_i$, $\sum\limits_{g\in\Gamma} g(d)=0$. Положим $|d|=\Sigma|m_i|$ и проведем индукцию по $|d|$. Если $|d|\leqslant 1$, то, очевидно, $d=0$. Если $|d|\geqslant 2$, должны найтись такие $z_i\neq z_j$, что $m_i>0$, $m_j<0$ и $\Gamma z_i=\Gamma z_j$. Тогда $z_i-z_j=(1-g)z_i$ для некоторого $g\in\Gamma$ и $d=(1-g)z_i+d'$, где $|d'|<|d|$ и $\sum\limits_g g(d')=0$. Если z_i не определена над K, d_0 — сумма сопряженных к z_i, то как нетрудно видеть, $d=(1-g)d_0+d''$, где $|d''|<|d|$ и $\Sigma g(d'')=0$. Это завершает доказательство.

Следствие. Существует гомоморфизм «степень»:

$$\mathscr{D}_\Omega(K)^\Gamma\xrightarrow{\deg} Z\colon \sum_{g\in\Gamma} g\left(\sum_{i=1}^{k} m_i z_i\right)\mapsto\sum_{i=1}^{k} m_i.$$

В самом деле, из 2.2 видно, что разные представления дивизора в виде $\sum g(d)$ дают одно и то же значение правой части. Мы также будем говорить о степени конечного дивизора в обычном смысле; очевидно, это не может привести к путанице.

2.3. Произведения Вейерштрасса. Пусть дан некоторый конечный K-дивизор d. Мы построим сейчас некоторую мероморфную функцию на Ω с Γ-инвариантным дивизором $\sum\limits_{g\in\Gamma} g(d)$.

Так как d — конечный K-дивизор нулевой степени, на P^1 существует K-рациональная функция $w_d(z)$ с дивизором d. Выберем точку $z_0\in\Omega\setminus\bigcup\limits_g g(\operatorname{supp}(d))$ и положим формально:

$$W_{d,z_0}(z)=\prod_{h\in\Gamma}\frac{w_d(hz)}{w_d(hz_0)}. \tag{1}$$

2.4. Предложение. Произведение (1) сходится в любой точке $z\in\Omega$, если исключить из него конечное число членов, имеющих нуль или полюс в этой точке. При другом выборе z_0 оно умножается на константу.

Доказательство. Пусть $h=\left(\begin{smallmatrix} a & b\\ c & d\end{smallmatrix}\right)$; имеем, прежде всего,

$$h(z)-h(z_0)=\frac{az+b}{cz+d}-\frac{az_0+b}{cz_0+d}=\frac{z-z_0}{c^2\left(z+\frac{d}{c}\right)\left(z_0+\frac{d}{c}\right)},$$

откуда

$$|h(z)-h(z_0)|=|z-z_0|\cdot r_h^2\cdot\frac{1}{|z-\text{центр } I(h)|\,|z_0-\text{центр } I(h)|}$$

(здесь r_h — радиус изометрического круга $I(h)$ для h; координата z выбрана так, что $z_0\neq\infty$ и $\infty\in\Omega$, как в § 1). Внутри $I(h)$ находится неподвижная точка $z_h\in\Sigma$, а $r_h\to 0$ по фильтру дополнений к конечным множествам в Γ; поэтому $I(h)$ для всех h, кроме конечного числа, лежат в маленькой окрестности множества предельных точек Σ, так что при фиксированных z и $z_0\in\Omega$ расстояния $|z-\text{центр } I(h)|$, $|z_0-\text{центр } I(h)|$ отграничены от нуля (на почти всех h). Значит, $|h(z)-h(z_0)|\to 0$ по h. Кроме того, поскольку $\operatorname{supp}(d)\subset\Omega$, существует такая окрестность $\operatorname{supp}(d)$, что $h(z)$ и $h(z_0)$ для почти всех h находятся вне этой окрестности. Таким образом, $\frac{w_d(hz)}{w_d(hz_0)}$ есть отношение значений рациональной функции w_d в переменной паре точек, расстояние между которыми стремится к нулю и которые остаются вне окрестности нулей и полюсов w_d. Значит, $\frac{w_d(hz)}{w_d(hz_0)}\to 1$ по h. В силу неархимедовости K, этого достаточно для сходимости произведения (1). Последнее утверждение очевидно. ■

В § 6 мы докажем, что (1) сходится равномерно, если z остается вне Γ-инвариантной окрестности $\operatorname{supp}(d)\cup\Omega$. Мы воспользуемся этим в главе IV, где нужно будет знать, что W — мероморфные «жестко аналитические» функции.

Теперь исследуем множители автоморфности для $W_{d,z_0}(z)$. Интуитивно, $W_{d,z_0}(z)$ имеет Γ-инвариантный дивизор и потому при сдвиге на элемент $g\in\Gamma$ должна умножаться на обратимую в Ω голоморфную функцию; на самом деле эта функция оказывается константой.

2.5. Предложение. В условиях 2.4 для всех $g\in\Gamma$ имеем

$$W_{g,z_0}(gz)=\mu_d(g)\,W_{d,z_0}(z), \tag{2}$$

где $\mu_d(g)\in K^*$ и $\mu_d(g)$ мультипликативно зависит от d и g, но не зависит от z_0.

Доказательство. Имеем в силу (1):

$$W_{d,z_0}(gz)=\prod_{h\in\Gamma}\frac{w_d(hgz)}{w_d(hz_0)}=\prod_{h\in\Gamma}\frac{w_d(hz)}{w_d(hg^{-1}z_0)}.$$

Деля на $W_{d,z_0}(z)$, находим

$$\mu_d(g)=\prod_{h\in\Gamma}\frac{w_d(hz_0)}{w_d(hg^{-1}z_0)}. \tag{3}$$

Независимость от z_0 следует из того, что при изменении z_0 функция W_{d,z_0} умножается на константу. Мультипликативность по d следует из того, что W_{d,z_0} мультипликативны

по d, а мультипликативность по g очевидна из (2). Наконец, если $z_0\in\Omega(K)$, то $\mu_d(g)\in K^*$ в силу (3), а если $\Omega(K)$ пусто, то $\mu_d(g)$ все равно $\operatorname{Gal}(\bar{K}/K)$-инвариантно, ибо не зависит от $z_0\in\Omega(\bar{K})$. ■

Особый интерес представляет случай, когда дивизор d таков, что $\sum_{g\in\Gamma}g(d)=0$, так что функция $W_{d,z_0}(z)$ естественно доопределяется до голоморфной и голоморфно обратимой функции на всем Ω (в точке носителя $\bigcup_g\operatorname{supp}(d)$ нужно собрать в произведении (1) конечное число членов, обращающихся в 0 или ∞ в этой точке; эти нули и полюса взаимно уничтожаются). Чтобы исследовать этот случай, достаточно в силу предложения 2.5 б) ограничиться дивизорами вида $(e-1)z_1$, где $e\in\Gamma$, $z_1\in\Omega$.

2.6. Теорема. Положим $H=\Gamma/[\Gamma,\Gamma]$. Пусть $g,e\in\Gamma$, χ,ε — классы g,e в H. Положим

$$\langle\chi,\varepsilon\rangle=\mu_{(e-1)z_1}(g),$$

где $z_1\in\Omega$, $z_1\notin\Gamma(\infty)$. Тогда $\langle\chi,\varepsilon\rangle$ зависит только от χ, ε (а не от g, h в классах χ, ε и не от z_1). Кроме того,

$$\langle\ ,\ \rangle: H\times H\to K^*$$

есть мультипликативное симметричное скалярное произведение на группе H.

Доказательство. Прежде всего, $w_{(e-1)z_1}=\frac{z-ez_1}{z-z_1}$. Далее, для любой точки $z_0\in\Omega$, $z_0\notin\Gamma\infty\cup\Gamma z_1$ имеем в силу (3)

$$\mu_{(e-1)z_1}(g)=\prod_{h\in\Gamma}\frac{hz_0-ez_1}{hz_0-z_1}\,\frac{hg^{-1}z_0-z_1}{hg^{-1}z_0-ez_1}. \tag{4}$$

В члене, отвечающем данному h, поменяем местами знаменатели, а также знаки всех числителей и знаменателей:

$$\mu_{(e-1)z_1}(g)=\prod_{h\in\Gamma}\frac{ez_1-hz_0}{ez_1-hg^{-1}z_0}\,\frac{z_1-hg^{-1}z_0}{z_1-hz_0}. \tag{4'}$$

Теперь этот член представлен в виде двойного отношения четырех точек $(ez_1,\ z_1,\ hz_0,\ hg^{-1}z_0)$. Двойное отношение проективно инвариантно; применив к этим четырем точкам h^{-1}, получим

$$\mu_{(e-1)z_1}(g)=\prod_{h\in\Gamma}\frac{h^{-1}ez_1-z_0}{h^{-1}ez_1-g^{-1}z_0}\,\frac{h^{-1}z_1-g^{-1}z_0}{h^{-1}z_1-z_0}=$$

$$=\prod_{h\in\Gamma}\frac{w_{g^{-1}z_0-z_0}(h^{-1}z_1)}{w_{g^{-1}z_0-z_0}(h^{-1}ez_1)}=\mu_{(g^{-1}-1)z_0}(e^{-1}).$$

Из этого равенства

$$\mu_{(e-1)z_1}(g)=\mu_{(g^{-1}-1)z_0}(e^{-1}) \qquad (5)$$

уже следует все, что нам нужно. В самом деле, левая часть не зависит от z_0 и мультипликативна по g, а правая не зависит от z_1 и мультипликативна по e в силу предложения 2.5. Значит, обе части не зависят ни от z_0, ни от z_1 и бимультипликативны по e, g. Так как их значения принадлежат абелевой группе K^*, то на самом деле они зависят только от $\chi=g \bmod [\Gamma,\Gamma]$, $\varepsilon=e \bmod [\Gamma,\Gamma]$, так что оправдано обозначение $\langle \chi,\varepsilon\rangle$. Формула (5) тогда превращается в $\langle \chi,\varepsilon\rangle = \langle \varepsilon^{-1},\chi^{-1}\rangle = \langle \varepsilon,\chi\rangle$ (по бимультипликативности). ■

Введенное в теореме 2.6 скалярное произведение $\langle , \rangle$: $H\times H\to K^*$ очень важно: как мы покажем, оно определяет поляризацию на торе, связанном с группой H, и является p-адическим аналогом классической формы Римана для якобиана кривой $\Gamma\backslash\Omega$.

Формула (4), однако, не очень удобна для работы с этим произведением, ибо она содержит точки z_0, z_1, от которых на самом деле $\langle , \rangle$ не зависит. Сейчас мы покажем, как устранить этот недостаток. Начнем с несложной технической леммы. Чтобы содержание накладываемых ограничений было яснее, напомним, что позже будет установлено, что группа Γ свободна, и, значит, H свободная абелева.

2.7. Лемма. а) Пусть g, $e\in\Gamma$ — такие элементы, что их образы в $H=\Gamma/[\Gamma,\Gamma]$ независимы, т. е. порождают свободную абелеву подгруппу ранга 2. Пусть $C(e\,|\,g)$ означает некоторое полное множество представителей двусторонних смежных классов $(e^m)\backslash\Gamma/(g^n)$. Тогда любой элемент группы Γ однозначно представляется в виде $e^m h g^n$, где $m, n\in Z$, $h\in C(e\,|\,g)$.

б) Пусть $g\in\Gamma$ — элемент, образ которого имеет бесконечный порядок и не делим в группе H, и пусть $C_0(g\,|\,g)$ означает некоторое полное множество представителей всех двусторонних смежных классов $(g^m)\backslash\Gamma/(g^n)$, кроме единичного. Тогда любой элемент в Γ однозначно представляется либо в виде g^m, либо в виде $g^m h g^n$, где $m, n\in Z$, $h\in C_0(g\,|\,g)$.

Доказательство. а) Представления одного и того же элемента в виде $e^m h g^n$ с разными h невозможны в силу выбора $C(e\,|\,g)$, а с одним и тем же h — потому, что в факторе по коммутанту равенство этих двух представлений привело бы к соотношению между образами g и e.

б) Как и выше, достаточно установить однозначность представления в виде $g^m h g^n$. Иначе имеется соотношение вида $g^m h g^n = h$. Рассматривая его в факторе по коммутанту, получаем $m+n=0$, откуда $g^m h = h g^m$. Теперь нетрудно установить, что g^m и h содержатся в общей циклической подгруппе в Γ.

В самом деле, выберем систему координат, в которой g^m представлен матрицей $\begin{pmatrix} q & 0 \\ 0 & 1 \end{pmatrix}$, $|q|<1$. Тогда сразу видно, что коммутирующие с g^m дробнолинейные преобразования h также представлены диагональными матрицами. Значит, g^m и h порождают дискретную подгруппу без кручения в K^* (или в K_1^*, где K_1 — конечное расширение K, в котором g^m приводится к диагональному виду). Но из точной последовательности

$$1\to U\to K^*\xrightarrow{\text{ord}} Z\to 0,$$

где U — компактная группа единиц, сразу видно, что любая дискретная подгруппа без кручения в K^* циклична.

Окончательно, если элемент e из Γ представляется в виде $g^m h g^n$ двумя разными способами, то g^m и h лежат в одной циклической подгруппе, которая должна быть порождена g ибо образ g в H не делим, а стационарная подгруппа в Γ точек $z^{\pm}_{g^m}=z^{\pm}_g$ циклична. Но тогда $h=g^r$, и элемент h лежит в единичном двойном классе. ■

2.8. Теорема. а) В условиях леммы 2.7 а) положим $\chi=g \bmod [\Gamma,\Gamma]$, $\varepsilon=e \bmod [\Gamma,\Gamma]$. Тогда

$$\langle \varepsilon,\chi\rangle = \prod_{h\in C(e|g)} \frac{w_{z_e^+-z_e^-}(hz_g^+)}{w_{z_e^+-z_e^-}(hz_g^-)}. \qquad (6)$$

б) В условиях леммы 2.7 б) положим $\chi=g \bmod [\Gamma,\Gamma]$. Тогда

$$\langle \chi,\chi\rangle = q_g \prod_{h\in C_0(g|g)} \frac{w_{z_g^+-z_g^-}(hz_g^+)}{w_{z_g^+-z_g^-}(hz_g^-)}, \qquad (7)$$

где g представлен матрицей, сопряженной с $\begin{pmatrix} q_g & 0 \\ 0 & 1 \end{pmatrix}$ в $GL(2,\overline{K})$, $|q_g|<1$.

2.9. Пояснения. Чтобы лучше представить себе структуру формул (6) и (7), заметим, что фигурирующие в них w являются координатными функциями с нулями и полюсами в Σ, то есть единицами на Ω. Значение этих функций берется в паре точек (hz_g^+, hz_g^-), которые также лежат в Σ. Расстояние между ними стремится к нулю (как в доказательстве предложения 2.4), однако они бесконечно часто попадают в сколь угодно малые окрестности носителя дивизора w, так что с первого взгляда даже сходимость (6) и (7) не очевидна; она будет установлена в ходе доказательства.

Укажем еще более явный вид (7) в подходящей системе координат. Пусть g записывается в этой системе в виде $\begin{pmatrix} q & 0 \\ 0 & 1 \end{pmatrix}$, $|q|<1$. Тогда $z_g^+=0$, $z_g^-=\infty$ и можно положить $w_{z_g^+-z_g^-}(z)=z$. Далее, если $h=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, то $h(z_g^+)=\frac{b}{d}$, $h(z_g^-)=\frac{a}{c}$. Окончательно:

$$\langle \chi, \chi \rangle = q \prod_{\binom{a\ b}{c\ d} \in C_0(g|g)} \frac{bc}{ad}. \tag{8}$$

2.10. Доказательство теоремы 2.8. а) Для вычисления $\langle \chi, \varepsilon \rangle$ воспользуемся формулой (4′):

$$\langle \chi, \varepsilon \rangle = \prod_{h \in \Gamma} \frac{ez_1 - hz_0}{ez_1 - hg^{-1}z_0} \frac{z_1 - hg^{-1}z_0}{z_1 - hz_0}.$$

Соберем воедино члены, отвечающие элементам одного смежного класса $e^{-m}hg^n$, $h \in C(e|g)$, как в лемме 2.7 а), и будем вычислять произведение в следующем порядке:

$$\langle \chi, \varepsilon \rangle = \prod_{h \in C(e|g)} \prod_{m=-\infty}^{\infty} \prod_{n=-\infty}^{\infty} \frac{ez_1 - e^{-m}hg^n z_0}{ez_1 - e^{-m}hg^{n-1}z_0} \frac{z_1 - e^{-m}hg^{n-1}z_0}{z_1 - e^{-m}hg^n z_0}.$$

Покажем сначала, как сворачивается внутреннее произведение, при фиксированных m, h. Обозначим его n-й член через $\frac{\alpha_n}{\alpha_{n-1}} \frac{\beta_{n-1}}{\beta_n}$ в очевидных сокращениях. Тогда

$$\prod_{n=-N}^{N} \frac{\alpha_n}{\alpha_{n-1}} = \frac{\alpha_N}{\alpha_{-N-1}}, \quad \prod_{n=-N}^{N} \frac{\beta_{n-1}}{\beta_n} = \frac{\beta_{-N-1}}{\beta_N}.$$

Поэтому, полагая $\alpha_\infty = \lim\limits_{N\to\infty} \alpha_N$ и т. д., имеем

$$\prod_{n=-\infty}^{\infty} = \frac{\alpha_\infty}{\alpha_{-\infty}} \frac{\beta_{-\infty}}{\beta_\infty} = \frac{ez_1 - e^{-m}hz_g^+}{ez_1 - e^{-m}hz_g^-} \frac{z_1 - e^{-m}hz_g^-}{z_1 - e^{-m}hz_g^+},$$

поскольку $z_g^+ = \lim\limits_{N\to\infty} g^N z_0$, $z_g^- = \lim\limits_{N\to\infty} g^{-N} z_0$.

Теперь, прежде чем сворачивать произведение по m, воспользуемся инвариантностью этого двойного отношения при сдвиге на e^m. Это дает:

$$\prod_{n=-\infty}^{\infty} = \frac{e^{m+1}z_1 - hz_g^+}{e^{m+1}z_1 - hz_g^-} \frac{e^m z_1 - hz_g^-}{e^m z_1 - hz_g^+} = \frac{\gamma_{m+1}}{\delta_{m+1}} \frac{\delta_m}{\gamma_m}.$$

Теперь в точности, как выше, получаем:

$$\prod_{m=-\infty}^{\infty} \prod_{n=-\infty}^{\infty} = \frac{\gamma_\infty}{\gamma_{-\infty}} \frac{\delta_{-\infty}}{\delta_\infty} = \frac{z_e^+ - hz_g^+}{z_e^- - hz_g^+} \frac{z_e^- - hz_g^-}{z_e^+ - hz_g^-} = \frac{w_{z_e^+ - z_e^-}(hz_g^+)}{w_{z_e^+ - z_e^-}(hz_g^-)},$$

что доказывает формулу (6).

б) В формуле (7) члены, отвечающие $h \in C_0(g|g)$, вычисляются точно так же, как общий член в (6), и получаются формальной подстановкой $e=g$ в (6). Первый же множитель должен отвечать единичному двойному классу (см. лемму 2.7 б)). Таким образом, мы должны вычислить часть произведения (4′), отвечающую случаю $e=g$ и $h \in (g^n)$, $n \in Z$; она получается, если в самом первом вычислении положить формально $e^{-m}h=id$:

$$\prod_{n=-\infty}^{\infty} \frac{gz_1 - g^n z_0}{gz_1 - g^{n-1}z_0} \frac{z_1 - g^{n-1}z_0}{z_1 - g^n z_0} = \frac{gz_1 - z_g^+}{gz_1 - z_g^-} \frac{z_1 - z_g^-}{z_1 - z_g^+} = \frac{w_{z_g^+ - z_g^-}(gz_1)}{w_{z_g^+ - z_g^-}(z_1)}$$

Вычислим это отношение в системе координат, в которой $g=\begin{pmatrix} q & 0 \\ 0 & 1 \end{pmatrix}$, $|q|<1$. Тогда $z_g^+=0$, $z_g^-=\infty$, $w_{z_g^+ - z_g^-}(z)=z$, $gz_1=qz_1$, так что это отношение есть просто q, что доказывает (7). ■

Наш последний результат дает явные формулы для дифференциалов первого рода на кривой, униформируемой группой Шоттки (ср. следующий параграф).

2.11. Теорема. а) Пусть $g \in \Gamma$, $g \neq id$. Функция $W_{(g-1)z_1,z_0}(z)$ (см. (1)) может быть представлена формулой

$$W_{(g-1)z_1,z_0}(z) = \prod_{h \in C(|g)} \frac{w_{hz_g^+ - hz_g^-}(z)}{w_{hz_g^+ - hz_g^-}(z_0)},$$

где $C(|g)$ — некоторое множество представителей классов $\Gamma/(g^n)$. В частности, она не зависит от z_1 и не имеет нулей и полюсов в Ω.

б) $W_{(g-1)z_1,z_0}(z)$ мультипликативно зависит от g.

Следствие. Для каждого $g \in \Gamma$

$$\omega_g = d \log W_{(g-1)z_1,z_0} \tag{9}$$

есть Γ-инвариантный дифференциал без полюсов на Ω. Отображение $g \mapsto \omega_g$ индуцирует гомоморфизм групп

$$H \to \begin{pmatrix} \text{группа } \Gamma\text{-инвариантных дифференциалов} \\ \text{без полюсов на } \Omega \end{pmatrix}.$$

Доказательство. а) Имеем, пользуясь определением и инвариантностью двойного отношения:

$$W_{(g-1)z_1,z_0} = \prod_{h \in \Gamma} \frac{w_{(g-1)z_1}(h^{-1}z)}{w_{(g-1)z_1}(h^{-1}z_0)} = \prod_{h \in \Gamma} \frac{w_{(hg-h)z_1}(z)}{w_{(hg-h)z_1}(z_0)} =$$

$$= \prod_{h\in C(lg)} \prod_{n=-\infty}^{\infty} \frac{w_{(hg^{n+1}-hg^n)z_1}(z_1)}{w_{(hg^{n+1}-hg^n)z_1}(z_0)} = \prod_{h\in C(lg)} \frac{w_{\left(hz_g^+-hz_g^-\right)}(z)}{w_{\left(hz_g^+-hz_g^-\right)}(z_0)}.$$

Сворачивание внутреннего произведения делается, как выше. Независимость от z_1 становится очевидной.

б) Имеем

$$(g_1g_2-1)\,z_1=(g_1-1)(g_2z_1)+(g_2-1)\,z_1.$$

Записывая мультипликативность W_{d,z_0} по d с этими дивизорами и учитывая независимость $W_{(g-1)z_1,z_0}$ от z_1, немедленно получаем мультипликативность $W_{(g-1)z_1,z_0}$ по g. ■

§ 3. АНАЛИТИЧЕСКИЙ ЯКОБИАН ГРУППЫ ШОТТКИ

3.1. Пусть $[K:Q_p]<\infty$, $\Gamma\subset \mathrm{PGL}(2,K)$ — некоторая группа Шоттки. В этом параграфе мы введем набор объектов, конструируемых «аналитически» (над K) по Γ, которые, как будет показано впоследствии, допускают однозначную алгебро-геометрическую интерпретацию.

а) Аналитическая кривая X_{an}, униформизируемая группой Шоттки Γ.

По определению, это функтор на категории конечных расширений K:

$$L\mapsto \Gamma\backslash\Omega(L)=X_{\mathrm{an}}(L),$$

где $\Omega\subset P^1_K$ — множество, где Γ действует дискретно.

б) Группа аналитических дивизоров $\mathscr{D}_{\mathrm{an}}$ (нулевой степени) на кривой X_{an}.

Это функтор $L\to\mathscr{D}_{\mathrm{an}}(L)=L$-дивизоры нулевой степени на Ω, инвариантные относительно Γ. (см. п. 2.1).

в) Группа главных аналитических дивизоров $\mathscr{D}^0_{\mathrm{an}}\subset\mathscr{D}_{\mathrm{an}}$.

Дивизор $D\in\mathscr{D}_{\mathrm{an}}(L)$ называется главным, если существует такое его представление $D=\sum\limits_{g\in\Gamma} g(d)$, где d — конечный L-дивизор нулевой степени, что

$$\mu_d(g)=1 \text{ для всех } g\in\Gamma,$$

то есть $W_{d,z_0}(z)$ — Γ-инвариантная функция, которая, следовательно, спускается на X_{an}.

г) Аналитический якобиан J_{an} кривой X_{an}.

Прежде всего, построим тор $T=\mathrm{Spec}\,K[H]$ (здесь снова используется, что H — свободная абелева группа, что будет доказано позже).

Одна K-точка T — это гомоморфизм $H\to K^*$. В частности, для $g\in\Gamma$, $z_1\in\Omega(\bar K)$ отображение $h \bmod [\Gamma,\Gamma]\mapsto\mu_{(g-1)z_1}(h)$ является таким гомоморфизмом.

Полученные таким образом точки образуют подгруппу в $T(K)$, которая называется группой периодов B:

$$B=\{\text{множество точек } h \bmod[\Gamma,\Gamma]\mapsto\mu_{(e-1)z_1}(h)\}=$$
$$=\left\{\begin{array}{l}\text{множество точек } \chi\mapsto\langle\chi,\varepsilon\rangle\\ \text{для всех } \varepsilon\in H\end{array}\right\}\subset T(K).$$

Ниже будет доказано, что B — дискретная подгруппа ранга n. Вместе с B определяется гомоморфизм

$$\varphi^{-1}: H\to B,\quad \varphi^{-1}(\varepsilon)=\langle\cdot,\varepsilon\rangle,$$

относительно которого позже будет доказано, что он есть изоморфизм, обратный к которому является поляризацией (определение см. в § 2 главы II).

Окончательно, аналитический якобиан J_{an} кривой X_{an} определяется как функтор на конечных расширениях $L\supset K$ вида

$$L\mapsto T(L)/B.$$

д) Аналитические отображения Якоби.

Их два: это морфизмы функторов

$$j_1:\mathscr{D}_{\mathrm{an}}/\mathscr{D}^0_{\mathrm{an}}\to J_{\mathrm{an}},$$
$$j: X_{\mathrm{an}}\to J_{\mathrm{an}}.$$

Определение j_1:

$$j_1\left(\text{класс}\sum_{g\in\Gamma} g(d) \bmod \mathscr{D}^0_{\mathrm{an}}\right)=\mu_d(\cdot) \bmod B,$$

где $\mu_d(\cdot)$ есть гомоморфизм $h \bmod[\Gamma,\Gamma]\mapsto\mu_d(h)$ группы H в $K(d)^*$, рассматриваемый как $K(d)$-точка тора T. Очевидно, он мультипликативен по d. Кроме того, определение корректно, что показывают следующие соображения. Если

$$\sum_{g\in\Gamma} g(d)\in\mathscr{D}^0_{\mathrm{an}}(K(d)),$$

то в силу определения $\mathscr{D}^0_{\mathrm{an}}$ существует такой конечный дивизор d', что $\sum\limits_{g\in\Gamma} g(d)=\sum\limits_{g\in\Gamma} g(d')$ и $\mu_{d'}(\cdot)=1$. В силу предложения 2.2, поскольку $\sum\limits_{g\in\Gamma} g(d-d')=0$, имеем

$$d-d'=\sum_{i=1}^{k}(1-g_i)\,d_i.$$

Поэтому точка тора T

$$\mu_d(\cdot)=\mu_d(\cdot)\mu_{d'}^{-1}(\cdot)=\mu_{d-d'}(\cdot)=\prod_{i=1}^{k}\mu_{(1-g_i)d_i}(\cdot)$$

принадлежит подгруппе периодов B.

Определение j. Чтобы определить j, выберем точку $z_0\in\Omega(K)$, которая перейдет в нуль якобиана, и положим для $z_1\in\Omega(K)$

$$j(\Gamma z_1)=\mu_{z_1-z_0}(\cdot)\bmod B.$$

Корректность определения j видна из того, что

$$\frac{\mu_{gz_1-z_0}(\cdot)}{\mu_{z_1-z_0}(\cdot)}=\mu_{(g-1)z_1}(\cdot)\in B.$$

Если $\Omega(K)$ пусто, то j нельзя определить над K, а лишь над конечным расширением K, где X_{an} приобретает точку.

е) Аналитические дифференциалы первого рода.

Это дифференциалы ω_g для $g\in\Gamma$, определенные формулой (8). Теперь мы можем дать для них более прозрачное выражение. Пусть $\chi=g\bmod[\Gamma,\Gamma]$ и $\bar{j}:\Omega\to T$, $\bar{j}(z)=\mu_{z-z_0}(\cdot)$, как в пункте д). Тогда

$$\omega_g=\bar{j}^*(\chi^{-1}d\chi). \qquad (8')$$

Мы докажем даже, что $W_{(g-1)z_1,z_0}(z)=\bar{j}^*(\chi)$. Действительно, это равенство эквивалентно такому:

$$W_{(g-1)z_1,z_0}(z)=\chi(\bar{j}(z))=\mu_{z-z_0}(g).$$

Пользуясь (1) и (3) (с gz_1, вместо z_0), находим

$$W_{(g-1)z_1,z_0}(z)=\prod_{h\in\Gamma}\frac{hz-gz_1}{hz-z_1}\frac{hz_0-z_1}{hz_0-gz_1},$$

$$\mu_{z-z_0}(q)=\prod_{h\in\Gamma}\frac{hgz_1-z}{hgz_1-z_0}\frac{hz_1-z_0}{hz_1-z}$$

и равенство становится очевидным с учетом инвариантности двойного отношения.

На этом заканчиваются аналитические конструкции. Теперь мы сформулируем их основные свойства, которые будут доказаны позже (частично в главе IV).

3.2. Теорема. Множество Γ-инвариантных функций $W_{d,z_0}(z)$, построенных для главных K-дивизоров d, вместе с нулем, образует поле функций на алгебраической кривой X рода n над K. Существует единственный изоморфизм функторов («алгебраизация»)

$$\alpha: X_{\text{an}}\xrightarrow{\sim}X,$$

сохраняющий значения функций в точках. При замене поля K на $L\supset K$ кривая X переходит в $X\otimes L$. ■

3.3. Теорема. Изоморфизм α с помощью очевидного переноса структур определяет также изоморфизмы следующих алгебраических объектов с аналитическими:

а) аналитические L-дивизоры$\leftrightarrow$дивизоры нулевой степени на X, рациональные над L.

б) Главные аналитические L-дивизоры$\leftrightarrow$дивизоры рациональных функций на $X\otimes L$.

в) Аналитические дифференциалы первого рода на $X_{\text{an}}\leftrightarrow$ некоторая Z-решетка ранга n в пространстве дифференциалов первого рода на X.

г) Аналитический якобиан J_{an} и отображения Якоби j, $j_1\leftrightarrow$ $\leftrightarrow$алгебраическийя кобиан J кривой X и соответствующие отображения Якоби (как функторы на расширениях K). ■

3.4. Теорема. а) $B\subset T(K)$ есть дискретная подгруппа ранга n, а φ^{-1}: $H\to B$ есть изоморфизм, обратный к которому является поляризацией.

б) Структура абелева многообразия на T/B, определенная с помощью конструкций главы II, совпадает с алгебраической структурой на J_{an}, индуцированной изоморфизмом, существование которого утверждается теоремой 3.3 г). ■

Ближайшие параграфы будут посвящены развитию техники, нужной для доказательства первой части теоремы 3.4 (и утверждения о свободе Γ). Эта же техника позволяет построить алгебраическую кривую X вместе с естественным изоморфизмом $X_{\text{an}}\xrightarrow{\sim}X$, который, однако, устанавливается геометрическими приемами, а не работой с полем инвариантных функций. Первоначально строится формальное пополнение $\hat{X}$ как фактор по Γ некоторой формальной схемы над кольцом целых чисел в K. Алгебраизация $\hat{X}$ затем производится с помощью основных теорем Гротендика в формальной геометрии, где функции участвуют неявно.

Естественный подход к доказательству остальных результатов, сформулированных в этом параграфе, доставляет методы жесткой аналитической геометрии Тэйта—Киля, которые будут обсуждены в следующей главе.

§ 4. ДЕРЕВО ГРУППЫ PGL (2)

4.1. В § 1 мы изучали группы Шоттки $\Gamma\subset\mathrm{PGL}(2)$ вместе с их действием на P^1—естественном однородном пространстве для PGL (2). Существует, однако, еще одно важное однородное пространство, геометрия которого дает существенную информацию о Γ-факторе PGL (2) по максимальной компактной подгруппе. Его естественная реализация имеет струк-

туру вершин некоторого бесконечного дерева, изученного Брюа и Титсом [1], Серром [24] и Мамфордом [17]. Эту структуру мы сейчас и начнем описывать.

4.2. Итак, пусть $[K:Q_p]<\infty$, V — двумерное векторное пространство над K, $P^1(K)$ — множество K-прямых, проходящих через начало координат в V; $G=\mathrm{PGL}(2, K)$ — группа автоморфизмов $P^1(K)$.

Пусть $O\subset K$ — кольцо целых чисел в K, $m\subset O$ — максимальный идеал, $k=O/m$. Будем рассматривать свободные O-модули ранга два $M\subset V$. Назовем два таких модуля эквивалентными, $M_1\sim M_2$, если существует такой элемент $a\in K^*$, что $M_1=aM_2$. Группа $\mathrm{GL}(V)$ линейных автоморфизмов V действует на множество таких модулей слева: $gM=\{g(m)\,|\,m\in M\}$, $g\in\mathrm{GL}(V)$. Условие $M_1\sim M_2$ равносильно тому, что M_1 и M_2 принадлежат одной орбите центра $K^*\subset\mathrm{GL}(V)$. Поэтому $G=\mathrm{GL}(V)/K^*$ действует слева на множестве классов эквивалентных модулей M.

Пусть Δ^0 — это множество классов; будем обозначать класс M через $\{M\}$.

4.3. Определение-лемма. Пусть $\Lambda_1, \Lambda_2\in\Delta^0$, $\Lambda_i=\{M_i\}$ и пусть $M_1\supset M_2$. Если

$$M_1/M_2\cong O/m^r\oplus O/m^s$$

как O-модуль (это всегда так, ибо O — кольцо главных идеалов, а M_1 имеет две образующих), то положим

$$d(\Lambda_1, \Lambda_2)=|r-s|.$$

Число $d(\Lambda_1, \Lambda_2)$ определено корректно и однозначно для любых Λ_1, Λ_2.

Доказательство. Пусть Λ_1, Λ_2 даны; выберем M_1 в классе Λ_1 как угодно. Если M_2' лежит в классе Λ_2, то элементы базиса M_2' выражаются в виде линейных комбинаций с коэффициентами в K через базис M_1. Умножая M_2' на общий знаменатель этих коэффициентов, получаем M_2 в классе Λ_2 такой, что $M_2\subset M_1$. Если $M_1\supset M_2$ даны, то умножения M_1 и M_2 на элементы поля K, сохраняющие включение, очевидно, не меняют $|r-s|$. ■

4.4. Определение. Графом Δ (группы $\mathrm{PGL}(2)$ над K) называется (бесконечный) граф с множеством вершин Δ^0, у которого две вершины Λ_1, Λ_2 соединены ребром, если и только если $d(\Lambda_1, \Lambda_2)=1$. Такие вершины будем называть соседними.

4.5. Теорема. а) Граф Δ связан и не имеет петель, то есть является деревом, из каждой вершины которого исходит $q+1$ ребер, где $q=\mathrm{card}\,O/m$.

б) $d(\Lambda_1, \Lambda_2)$ есть длина (т. е. число ребер) кратчайшего пути без возвращений от Λ_1 к Λ_2 в графе Δ.

в) Группа G действует на Δ слева, транзитивно на вершинах, сохраняя естественную метрику d.

Доказательство. Связность Δ следует из того, что если $M_1\supset M_2$, то M_1/M_2 имеет конечную длину, так что существует ряд O-свободных подмодулей $M_1=M^{(1)}\supset M^{(2)}\supset\ldots\supset M^{(k)}=M_2$ такой, что $M^{(i)}/M^{(i+1)}\cong O/m$, так что $d(M^{(i)}, M^{(i+1)})=1$.

Ребра Δ, исходящие из вершины Λ-класса M, находятся во взаимно однозначном соответствии с подмодулями $N\subset M$ такими, что $M/N\cong O/m$, т. е. с прямыми, проходящими через начало в k-плоскости M/mM, число которых $q+1$.

Действительно, если $d(\Lambda, \Lambda')=1$, то Λ' всегда можно представить таким подмодулем $N\subset M$ (ср. лемму 2.3), а два разных подмодуля такого вида не могут быть эквивалентны.

Для доказательства отсутствия петель в Δ достаточно проверить, что если последовательность модулей $M_0\supset M_1\supset\ldots\supset M_n$ представляет все вершины пути без возвращений в Δ, то $M_0\neq M_n$.

Для этого достаточно установить, что $M_n\not\subset mM_0$, потому что тогда $M_0/M_n\cong A/m^n$, так что M_0 и M_n не могут быть эквивалентны.

Проведем индукцию по n. На рисунке ребра означают включения (не все они — ребра графа Δ!). Факторы, отвечающие нижним перечеркнутым ребрам, не совпадают — иначе мы

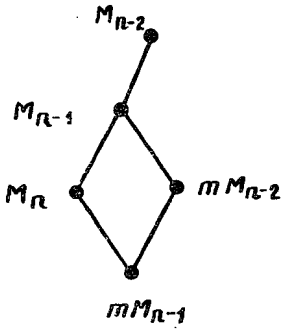


Рис. 4

бы имели $M_n=mM_{n-2}$ так, что в нашем пути было бы возвращение (от Λ_{n-2} к Λ_{n-1} и затем назад к Λ_{n-2}). Так, $\dim_k M_{n-1}/mM_{n-1}=2$, отсюда следует, что эти факторы порождают это двумерное пространство. Таким образом, $M_n+mM_{n-2}=M_{n-1}$, откуда $M_n\equiv M_{n-1}\bmod mM_0$, а в силу индуктивного предположения $M_{n-1}\not\equiv 0\bmod mM_0$.

Все остальные утверждения теоремы очевидным образом следуют из уже доказанных. ■

4.6. Теперь мы займемся связями между Δ и P^1. Напомним прежде всего, что концом дерева Δ называется класс бесконечных в одну сторону путей с конечным числом возвращений по ребрам Δ: два пути принадлежат одному классу, если они отличаются лишь конечным числом ребер.

Пусть $\partial\Delta$ — «граница Δ» — множество концов Δ.

4.7. Теорема. Пусть $\Lambda_0 \in \Delta^0$ — вершина, представленная модулем M. Рассмотрим два отображения:

$$\left\{\begin{array}{l}\text{пути с конечным числом}\\ \text{возвращений } M_0 \supset M_1 \supset M_2 \supset \ldots,\\ M_i/M_{i+1} \cong O/m \text{ при } i > i_0\end{array}\right\} \underset{\beta}{\overset{\alpha}{\rightleftarrows}} \left\{\begin{array}{l}\text{прямые через 0}\\ \text{в } V\end{array}\right\},$$

$$(M_0 \supset M_1 \supset M_2 \supset \ldots) \overset{\alpha}{\mapsto} K\left(\bigcap_{i=0}^{\infty} M_i\right) \subset V,$$

$$(\ldots \supset M_0 m^i + M_0 \cap L \supset M_0 m^{i+1} + M_0 \cap L \supset \ldots) \overset{\beta}{\leftarrow} L \subset V.$$

Они определены корректно и доставляют взаимно обратные изоморфизмы G-множеств $\partial\Delta \leftrightarrow P^1(K)$, не зависящие ни от каких произвольных выборов (Λ_0, M_0, представитель конца и т. п.).

Доказательство. а) Пусть дан некоторый конец Δ, представленный последовательностями $M_0 \supset M_1 \supset M_2 \supset \ldots$ и $N_0 \supset N_1 \supset N_2 \supset \ldots$ такими, что $M_i/M_{i+1} \cong N_j/N_{j+1} \cong O/m$ при $i, j \gg 0$. Тогда (класс M_r) = (класс N_{r+s}) для некоторого s и всех $r \geqslant r_0$, откуда индукцией по r легко получаем, что $M_r = aN_{r+s}$ для некоторого $a \in K^*$ и всех $r \geqslant r_0$. Следовательно,

$$K\left(\bigcap_{i=1}^{\infty} M_i\right) = K\left(\bigcap_{i=1}^{\infty} N_i\right).$$

Далее, пересечение $\bigcap_{i=1}^{\infty} M$ является свободным O-модулем ранга 1, потому что если путь, представленный $M_0 \supset M_1 \supset \ldots$, не имеет возвращений (а это так, начиная с некоторого места), то $M_0/M_i \cong O/m^i$ (см. доказательство теоремы 2.5) и, значит, $M/\bigcap_{i=1}^{\infty} M_i \cong \varprojlim O/m^i \cong O$. Отсюда видно, что $K\left(\bigcap_{i=1}^{\infty} M_i\right)$ является прямой в V, которая зависит только от класса $(M_0 \supset M_1 \supset \ldots)$ в $\partial\Delta$.

Значит, α определяет отображение $\partial\Delta \to P^1(K)$, которое мы также обозначим α.

б) Пусть дана прямая $L \subset V$ и модуль M_0. Легко видеть, что $M' = L \cap M_0$ является свободным подмодулем ранга 1 в M_0, который выделяется прямым слагаемым: $M_0 = M' \oplus M''$. Тогда

$$(M_0 + M_0 \cap L)/(M_0 m^i + M_0 \cap L) \cong M''/m^i M'' \cong O/m^i.$$

Значит, $\beta(L)$ есть последовательность модулей, представляющая вершины пути без возвращений в Δ.

Покажем, что класс $\beta(L)$ в $\partial\Delta$ не зависит от выбора M_0. Выберем вместо M_0 другой модуль N_0; не меняя класса пути, построенного по N_0, мы можем умножить N_0 на элемент из K^* так, что после этого будет $M_0 \cap L = N_0 \cap L = Ox$, $x \in V$. Пусть тогда

$$M_0 = Ox \oplus Oy,\ N_0 = Ox + Oz,\ z = ax + by;\ a, b \in K.$$

Если i настолько велико, что $m^i a \subset O$, $m^i b \subset O$, то

$$N_0 m^i + N_0 = Ox + Om^i(ax + by) = Ox + Om^i by = Ox + Om^{i-j} y = M_0 \oplus m^{i-j} M_0,$$

где $bm^i = m^{i-j}$. Значит, начиная с некоторого места, пути, построенные по M_0 и по N_0, совпадают (сдвиг нумерации несуществен). Таким образом, β определяет отображение $P^1(K) \to \partial\Delta$, которое мы также обозначим β.

в) $\alpha \circ \beta = id$ (на $P^1(K)$). Это очевидно, ибо

$$\bigcap_{i=0}^{\infty} (M_0 m^i + M_0 \cap L) = M_0 \cap L,\ K(M_0 \cap L) = L.$$

г) $\beta \circ \alpha = id$ (на $\partial\Delta$). Действительно, пусть $M_0 \supset M_1 \supset \ldots$ путь без возвращений; тогда $M_i = Ox + m^i y$ для некоторых $x, y \in V$, как выше; тогда α-образ этого пути есть Kx, и затем

$$M_0 m^i + M_0 \cap Kx = Ox + m^i y = M_i.$$

Наконец, совместимость α и β с действием G ясна из определения. ■

4.8. Расширение основного поля. Пусть $L \supset K$ — конечное расширение, O_K, O_L и т. п. — связанные с ними кольца целых чисел и т. п.; $e_{L/K}$ — индекс ветвления. Чтобы проследить за связью Δ_L с Δ_K, начнем с конструкции естественных отображений, совместимых с вложением $G_K = \mathrm{PGL}(2, K) \subset \mathrm{PGL}(2, L) = G_L$.

а) Если $G_K = \mathrm{Aut}_K V$, то $G_L = \mathrm{Aut}_L(V \underset{K}{\otimes} L)$.

б) Пусть $M \subset V$ — свободный O_L-модуль ранга 2; тогда $M \underset{O_K}{\otimes} O_L \subset V \underset{K}{\otimes} L$ есть свободный O_L-модуль ранга 2. Эквивалентные модули остаются эквивалентными. Это определяет естественное отображение $\Delta_K^0 \to \Delta_L^0$. Легко видеть, что оно является вложением.

2) Вложение $\Delta_K^0 \to \Delta_L^0$ не сохраняет, однако, расстояние: оно умножается на $e_{L/K}$, потому что

$$(O_K/m_K^r) \otimes O_L \cong O_L/m_L^{re_{L/K}}.$$

Чтобы избавиться от этого неудобства, естественно ввести на графах Δ_L для всех $L \supset K$ K-нормированное расстояние, положив

$$d_K(\{M_1\}, \{M_2\}) = \frac{1}{e_{L/K}} d_L(\{M_1\}, \{M_2\}); \; M_1, M_2 \subset V \otimes L.$$

(Можно даже провести абсолютную нормировку, деля на e_{L/Q_p}).

Тогда отображение $\Delta_L^0 \to \Delta_K^0$ станет изометричным. Соседние в Δ_K^0 вершины, однако, перестанут быть соседними, если L/K разветвлено: между ними разместится $e_{L/K} - 1$ новых вершин. Кроме того, из каждой (старой и новой) вершины будет исходить $q^f + 1$, а не $q + 1$ ребер, длины $\frac{1}{e_{L/K}}$ каждое, $f = [L:K]\, e_{L/K}^{-1}$.

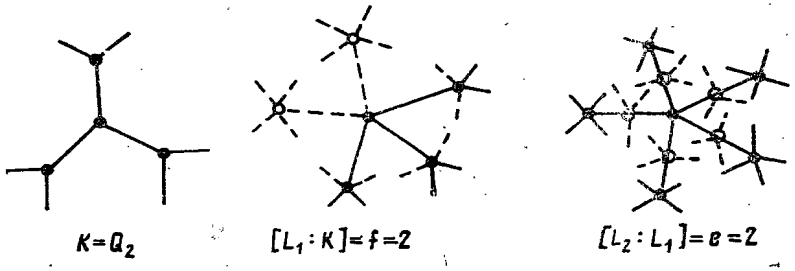


Рис. 4а

Пунктирами (соотв. кружочками) обозначены новые ребра (соотв., новые вершины) на рис. 4а.

Полезно ввести понятие «K-направление выхода из вершины $\Lambda \in \Delta_K^0$», которое было бы инвариантно относительно описанных отображений $\Delta_K^0 \to \Delta_L^0$. Интуитивно, это есть «бесконечно малый отрезок одного из ребер, выходящих из Λ в Δ_K^0». Формально это есть класс ребер, по одному в каждом Δ_L, выходящих из Λ и имеющих попарно непустое пересечение.

Если дан путь без возвращений, выходящий из вершины $\Lambda \in \Delta_K^0$, то он однозначно определяет путь без возвращений в каждом из графов Δ_L, выходящий из Λ, и направление выхода этого пути из Λ не зависит от выбора L. Это отображение путей отвечает, конечно, естественному вложению $P^1(K) \subset P^1(L)$.

§ 5. КООРДИНАТЫ, КРУГИ, ДВОЙНЫЕ ОТНОШЕНИЯ

5.1. В этом параграфе мы интерпретируем в терминах графа Δ понятия, связанные с выбором координатной функции на $P^1(K)$. Это позволит, в частности, описать в следующем параграфе действие гиперболических автоморфизмов на Δ и дать геометрическую интерпретацию модулю двойного отношения точек, что понадобится нам дальше.

Итак, пусть z — координатная функция на $P^1(K)$. Она определяет три точки с z-координатами $0, 1, \infty$ и сама однозначно определяется этими тремя точками. Удобным эквивалентом z в графе является поэтому следующий геометрический объект.

5.2. Определение. Пусть $z_0, z_1, z_2 \in P^1(K)$ — три разных точки. Перекрестком z_0, z_1, z_2 называется единственная вершина в Δ такая, что пути без возвращений из нее к z_0, z_1, z_2 начинаются с разных направлений. (Путь к z — это путь класса z).

Пояснения. Существование перекрестка легко следует из связности графа: нужно начать с трех любых путей в классах z_0, z_1, z_2, включить их в связный подграф, а потом

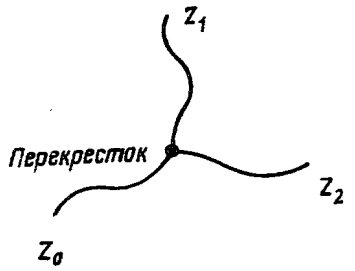


Рис. 5

убрать лишние ребра. Получится фигура, подобная изображенной на рис. 5. Никакая вторая точка не может быть перекрестком: если она лежит вне этой фигуры, то пути без возвращений от нее к z_0, z_1, z_2 начинаются все с одного направления, а если она лежит только на одном из «лучей», то с двух направлений.

5.3. Лемма. Пусть $\bar{z}_0, \bar{z}_1, \bar{z}_2 \in V$ — ненулевые векторы с условием $\bar{z}_0 + \bar{z}_1 + \bar{z}_2 = 0$; $z_1, z_2, z_3 \in P^1(K)$ — точки, отвечающие прямым $K\bar{z}_i$. Тогда перекресток (z_0, z_1, z_2) есть класс $(O\bar{z}_0 + O\bar{z}_1 + O\bar{z}_2) \in \Delta^0$.

Доказательство. Рассмотрим последовательность модулей

$$M_i^{(0)} = O\bar{z}_0 + m^i\bar{z}_1 + m^i\bar{z}_2 = O\bar{z}_0 + m^i\bar{z}_1, \; i \geqslant 0.$$

Очевидно, она определяет бесконечный путь без возвращений с началом Λ=класс $(O\bar{z}_0 + O\bar{z}_1 + O\bar{z}_2)$. По теореме 4.7, класс этого пути в $P^1(K)$ есть $K\left(\bigcap_{i=0}^{\infty} M_i^{(0)}\right) = K\bar{z}_0 = z_0$. Аналогично строятся пути без возвращений $(M_i^{(1)})$, $(M_i^{(2)})$ из Λ к z_1 и z_2. Ближайшие к Λ вершины на этих трех путях попарно различны. Действительно, скажем, модуль $M_1^{(0)}$ содержит $\bar{z}_0$, но не $\bar{z}_1$ и $\bar{z}_2$, а $M_1^{(1)}$ содержит $\bar{z}_1$, но не $\bar{z}_0$ и $\bar{z}_2$, так что эти модули не могут быть эквивалентны. ■

Геометрический смысл показателя. Назовем осью в Δ бесконечный в обе стороны путь без возвращений.

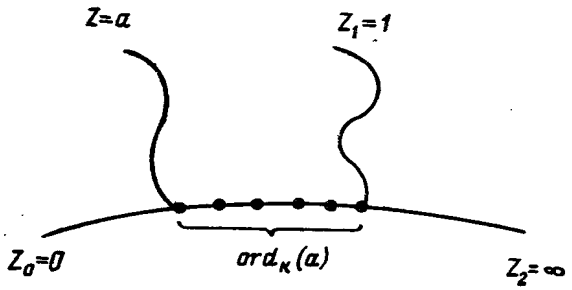


Рис. 6

Любые две точки $z_0, z_2 \in P^1(K)$ однозначно определяют соединяющую их ось, концы которой лежат в классах z_0, z_2. В частности, координатная функция z определяет ось $(0, \infty)$ — объединение двух соответствующих путей от перекрестка $(0, 1, \infty)$.

5.4. Лемма. Для любой точки $a \in P^1(K)$, $a \neq 0, \infty$ перекресток $(0, a, \infty)$ лежит на оси $(0, \infty)$. Показатель $\mathrm{ord}_K(a)$ равен расстоянию от перекрестка $(0, a, \infty)$ до перекрестка $(0, 1, \infty)$, если ориентация этого пути между перекрестками совпадает с ориентацией оси от 0 к ∞. В противном случае показатель равен расстоянию с обратным знаком.

Доказательство. Первое утверждение геометрически очевидно. Для проверки второго выберем в V базис e_1, e_2, согласованный с координатной функцией z в том смысле, что z — координата точки, отвечающей прямой $K(ae_1 + be_2)$, равна $\frac{a}{b} \in K \cup \infty$. Тогда получаем следующее соответствие между точками и прямыми:

точки:	прямые:
0	$Ke_2 = K(-e_2)$
∞	$Ke_1 = K(-ae_1)$
1	$K(e_1 + e_2)$
a	$K(ae_1 + e_2)$

По лемме 5.3 имеем отсюда:

перекресток $(0, 1, \infty)$ = класс $Oe_1 + Oe_2$

перекресток $(0, a, \infty)$ = класс $Oae_1 + Oe_2$

Значит, расстояние между перекрестками равно $|\mathrm{ord}_K(a)|$. Знак же показателя $\mathrm{ord}_K(a)$ определяется тем, что $a \to 0$, когда $\mathrm{ord}_K a \to \infty$ и $a \to \infty$, когда $\mathrm{ord}_K a \to -\infty$.

5.5. Круги, кольца, топология. Пусть P — некоторый отрезок в графе Δ_K, включающий конечные точки или нет, конечный или бесконечный; конечные точки его не обязаны быть вершинами Δ_K^0. Как видно из обсуждения в п. 4.8, этот отрезок однозначно определяет отрезок в Δ_L для любого конечного расширения $L \supset K$, который мы будем также обозначать P.

Назовем щеткой с базой P в Δ_L объединение носителей всех путей без возвращений, бесконечных в одну сторону и начинающихся в вершинах из P по направлениям, не лежа-

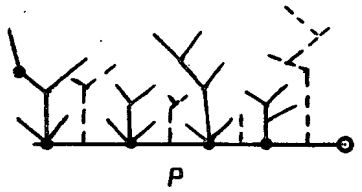


Рис. 7

щим в P. Из леммы 5.4 сразу же вытекают следующие факты. (Показатель $\mathrm{ord} z$ нормирован относительно K).

а) Круг с границей $\mathrm{ord} z \leqslant \mathrm{ord} a$ $(a \in \bar{K})$ есть множество концов некоторой щетки, база P которой в одну сторону бесконечна, а в другую включает конечную точку, вершину из $\Delta_{K(a)}^0$.

Наоборот, концы таких щеток суть круги в некоторой системе координат на $P^1(K)$ (взять класс конца P в качестве нуля координатной функции, а ∞ выбрать так, чтобы ось $(0, \infty)$ содержала P).

Оба эти утверждения универсальны по L, то есть сохраняют смысл и верны во всех графах Δ_L и соответствующих множествах $P^1(K)$. То же относится к последующим формулировкам.

б) Кольцо с границами $\operatorname{ord} b \leqslant \operatorname{ord} z \leqslant \operatorname{ord} a$, $a, b \in \bar{K}$ есть множество концов некоторой щетки с конечной базой P, включающей конечные точки.

Чтобы получить круг или кольцо без границы, нужно исключить в базе соответствующие конечные точки.

в) Топология. Пусть Λ — некоторая вершина, из которой выходит путь без возвращений P к точке $z \in P^1(K)$. Пусть $z_1, \ldots, z_n, \ldots \in P^1(K)$ — некоторая последовательность точек; $P_1, \ldots, P_n, \ldots$ — пути без возвращений из Λ к $z_1, \ldots, z_n, \ldots$ соответственно.

Обозначим через $\Lambda_i \in P \cap P_i$ самую далекую от Λ вершину, лежащую одновременно на P и P_i: до Λ_i пути P и P_i идут вместе, а затем расходятся.

Тогда сходимость z_i к z равносильна тому, что $d(\Lambda_i, \Lambda) \to \infty$.

5.6. Лемма о двойном отношении. Пусть z_1, z_2, a_1, a_2 — z-координаты четырех разных точек в $P^1(K)$. Тогда показатель двойного отношения

$$\operatorname{ord}\left(\frac{z_1-a_1}{z_1-a_2}\,\frac{z_2-a_2}{z_2-a_1}\right) = \operatorname{ord}\frac{w_{(a_1)-(a_2)}(z_1)}{w_{(a_1)-(a_2)}(z_2)}$$

равен индексу перекрытия ориентированных осей (z_1, z_2) и (a_1, a_2) соответственно, т. е. числу общих ребер у этих осей или этому числу с обратным знаком, в зависимости от того, совпадают или различны ориентации, индуцированные на этих ребрах осями.

Доказательство. Как двойное отношение, так и индекс перекрытия осей инвариантны относительно действия $G = \mathrm{PGL}(2)$ и, значит, выбора системы координат. Поэтому достаточно разобрать случай, когда четверка (z_1, z_2, a_1, a_2) имеет вид $(0, \infty, a, 1)$. В этом случае $w_{(a_1)-(a_2)}(z) = \frac{z-a}{z-1}$,

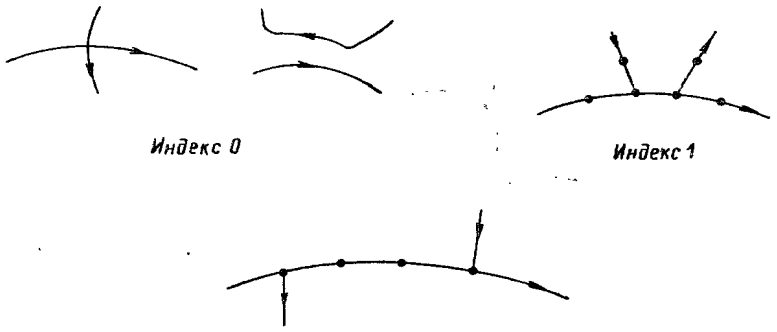


Рис. 8

так что соответствующее двойное отношение равно $\frac{-a}{-1}\cdot 1 = a$. Значит, нужно проверить, что $\operatorname{ord}_K a$ есть индекс перекрытия осей $(0, \infty)$ и $(a, 1)$ с надлежащим знаком; но в точности это утверждает лемма 5.4, потому что пересечение этих осей есть кратчайший путь между перекрестками $(0, a, \infty)$ и $(0, 1, \infty)$, как видно из рисунков. ■

§ 6. ДЕЙСТВИЕ ГРУППЫ ШОТТКИ НА ДЕРЕВО

6.1. Лемма. Пусть $g \in \mathrm{PGL}(2)$ — гиперболический элемент. Тогда существует единственная g-инвариантная ось в дереве Δ. Элемент g действует на ней сдвигом; она называется осью g. Если g сопряжен с $\begin{pmatrix} q & 0 \\ 0 & 1 \end{pmatrix}$, $|q| < 1$, то сдвиг по оси происходит на расстояние $\operatorname{ord} q$.

Доказательство. Если ось g-инвариантна, то ее концы должны быть неподвижными точками g. Существует единственная ось, соединяющая две неподвижные точки. Ее g-образ имеет те же концы и потому должен совпадать с ней, ибо в Δ нет циклов. Значит, g действует на ней сдвигом.

Пусть z — координатная функция, имеющая 0 в z_g^+ и ∞ в z_g^-; тогда перекресток $(0, 1, \infty)$ отстоит от перекрестка $(0, g(1) = q, \infty)$ на $\operatorname{ord} q$ по лемме 5.4, так что g производит сдвиг по оси на $\operatorname{ord} q$ в сторону z_g^+. ■

Из этой леммы видно, что гиперболические элементы не имеют в Δ инвариантных вершин или ребер.

6.2. Теорема. Любая группа Шоттки $\Gamma \subset \mathrm{PGL}(2)$ свободна.

Мы докажем более общий факт:

6.3. Теорема. Группа Γ, действующая на некотором дереве Δ без инвариантных вершин и ребер, свободна.

6.4. Доказательство частного случая теоремы 6.3. Разберем сначала случай, когда Γ транзитивна на множестве вершин Δ^0 дерева Δ. Фиксируем некоторую вершину $\Lambda \in \Delta^0$; пусть $(\Lambda_i)_{i \in I}$ — все ее соседи и пусть $\Lambda_i = h_i \Lambda$, $h_i \in \Gamma$.

Для любого i вершина $h_i^{-1}\Lambda$ также является соседом Λ, ибо $d(\Lambda, h_i^{-1}\Lambda) = d(h_i\Lambda, \Lambda) = 1$. Поэтому для каждого $i \in I$ существует такой $j \in I$, что $h_i^{-1}\Lambda = h_j\Lambda$. При этом $h_i \neq h_j$, иначе h_i переводил бы ребро $(\Lambda, h_i\Lambda)$ в себя, вопреки предположению.

Из каждой пары индексов (i, j) с $h_i^{-1}\Lambda = h_j\Lambda$ выберем один и обозначим через J множество выбранных индексов.

Мы докажем, что (h_i), $i \in J$, составляют свободную систему образующих группы Γ.

а) (h_i) порождают Γ. Действительно, пусть $g \in \Gamma$. Положим $l(g) = d(\Lambda, g(\Lambda))$ (расстояние в графе Δ). Индукцией по $l(g)$ покажем, что g содержится в подгруппе, порожденной (h_i), $i \in J$. В самом деле, если $l(g) = 0$, то это так, ибо тогда $g(\Lambda) = \Lambda$ и, значит, $g = id$, ибо неединичные элементы не имеют инвариантных вершин. Пусть для $l(h) \leqslant d$ это доказано и пусть $l(g) = d + 1$. Тогда $d(\Lambda, g(\Lambda)) = d + 1$, откуда для некоторых $i \in J$, $\varepsilon = \pm 1$, $d(h_i^{\varepsilon}\Lambda, g(\Lambda)) = d$ (взять в качестве $h_i^{\varepsilon}\Lambda$ ближайшую к Λ вершину на пути без возвращений от Λ к $g(\Lambda)$). Но отсюда следует, что $d(\Lambda, h_i^{-\varepsilon} g(\Lambda)) = d$, так что $h_i^{-\varepsilon} g$ содержится в подгруппе, порожденной (h_i), $i \in J$.

б) Множество (h_i) свободно. Предположим, что это не так. Тогда существует наименьшее r и $\varepsilon_1, \ldots, \varepsilon_r = \pm 1$ такие, что $h_{i_1}^{\varepsilon_1} \ldots h_{i_r}^{\varepsilon_r} = id$; $\varepsilon_k = \varepsilon_{k+1}$, если $i_k = i_{k+1}$, $i_k \in J$. Ясно, что $r \geqslant 3$. Положим $\Lambda_0 = \Lambda$, $\Lambda_k = h_{i_1}^{\varepsilon_1} \ldots h_{i_k}^{\varepsilon_k}\Lambda$, $k \leqslant r$. Так как мы выбрали соотношение наименьшей длины, все $\Lambda_0, \ldots, \Lambda_{r-1}$ попарно различны; $(\Lambda_k, \Lambda_{k+1})$ — соседи для всех $k \leqslant r-1$; наконец, ребро $(\Lambda_{r-1}, \Lambda_r = \Lambda_0)$ отличается от всех предыдущих ребер, так как $r \geqslant 3$. Таким образом, $\Lambda_0, \ldots, \Lambda_{r-1}$ являются вершинами цикла — это противоречит предположению о том, что Δ дерево.

6.5. Редукция общего случая к разобранному. Теперь мы не будем предполагать, что Γ транзитивна на множестве вершин Δ, но, исходя из Δ, построим новое дерево $\overline{\Delta}$, на котором Γ будет действовать, как в п. 6.4. Дерево $\overline{\Delta}$ получится из Δ факторизацией — стягиванием некоторых специальных поддеревьев Δ в точки — вершины $\overline{\Delta}$. Интуитивно ясно, какие поддеревья надо стягивать, — те, которые инъективно вкладываются в фактор $\Gamma \backslash \Delta$ — они как раз и мешают действию Γ на Δ^0 быть транзитивным. Проведем теперь конструкцию подробно.

а) Построим фактор $\Gamma \backslash \Delta$: множество его вершин (соотв. ребер) является фактором множества вершин Δ (соотв. ребер Δ) под действием Γ. (На рисунке Γ порождена сдвигом на расстояние 2 вдоль оси).

б) Выберем в графе $\Gamma \backslash \Delta$ некоторое максимальное (по включению) поддерево $S \subset \Delta$. (На рисунке достаточно выбросить перечеркнутое ребро).

Оно существует в силу леммы Цорна. Оно содержит все вершины $\Gamma \backslash \Delta$: иначе в силу связности $\Gamma \backslash \Delta$ существовал бы путь без возвращений от не входящей в S вершины к S; его последнее ребро, не входящее в S, можно было бы добавить к S, оставив S деревом, что противоречит максимальности.

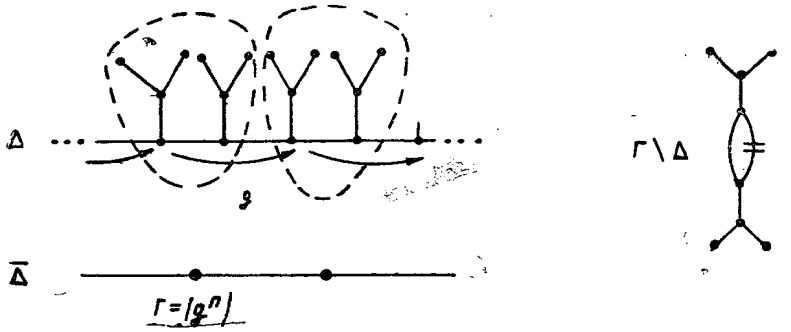


Рис. 9

(В этом рассуждении $\Gamma \backslash \Delta$ может быть любым связным графом).

в) Поднимем максимальное поддерево $S \subset \Gamma \backslash \Delta$ до поддерева $S' \subset \Delta$ (на рисунке два подъема S' заключены в пунктирные рамки).

Чтобы показать существование S', обозначим через W множество всех тех поддеревьев в Δ, которые инъективно отображаются в S. По лемме Цорна, в W есть максимальный элемент. Пусть $S_0 \subset S$ — его образ. Покажем, что S_0 совпадает с S.

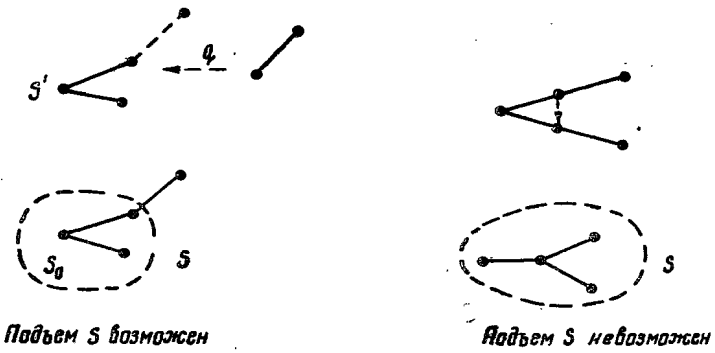


Рис. 10

Иначе в S существовало бы ребро, один конец которого лежал бы в S_0, а другой нет. Поднимем это ребро как угодно в Δ, затем с помощью подходящего элемента $g \in \Gamma$ сдвинем этот подъем так, чтобы его конец, попадающий в S, перешел в подходящую вершину S'. Объединение S' с этим новым ребром дает элемент W, что противоречит максимальности S'.

В этом рассуждении существенно используется то обстоятельство, что проекция $\Delta \to \Gamma \backslash \Delta$ есть факторизация под действием группы. На чертеже показан случай простого отображения графов, при котором подъем максимального дерева невозможен.

г) Пусть $S' \subset \Delta$ — подъем максимального поддерева в $\Gamma \backslash \Delta$. Так как S содержит все вершины $\Gamma \backslash \Delta$, S' содержит представителей всех классов эквивалентности вершин Δ относительно Γ по одному разу. Поэтому $S' \cap g(S') = \varnothing$ при $g \neq id$. Построим граф $\bar{\Delta}$, вершины которого взаимно однозначно соответствуют $g(S')$, $g \in \Gamma$, а две вершины соединены ребром, если в Δ есть ребро, соединяющее соответствующие поддеревья. Легко видеть, что $\bar{\Delta}$ — дерево (цикл в $\bar{\Delta}$ позволил бы построить цикл в Δ). Далее, Γ действует на $\bar{\Delta}$, транзитивна на вершинах и не имеет инвариантных вершин и ребер. ■

На протяжении пп. 6.3—6.5 дерево Δ и группа Γ были любыми. Теперь мы снова возвращаемся к случаю дерева Δ группы $\mathrm{PGL}(2, K)$ и группы Шоттки Γ. Опишем в терминах Δ множества Σ и Ω в $P^1(K)$, связанные с группой Γ.

Пусть даны две оси в Δ. Перемычкой между ними назовем путь без возвращений, начинающийся на одной оси, кончающийся на другой и не имеющий общих ребер с осями. Перемычка может состоять из одной точки; если это не так, то она определена однозначно.

6.6. Определение-лемма. Деревом $\Delta_\Gamma \subset \Delta$ называется подграф, допускающий следующие равносильные описания:

а) Δ_Γ состоит из осей элементов Γ и перемычек между ними.

б) Δ_Γ — максимальный связный подграф, содержащий оси элементов Γ. ■

6.7. Теорема. а) $\{\text{Концы } \Delta_\Gamma\} = \Sigma \subset P^1(K)$ (предельные точки Γ).

б) Группа Γ переводит Δ_Γ в себя, и фактор $\Gamma \backslash \Delta_\Gamma$ конечен.

Доказательство. а) Сначала проверим, что $\Sigma \subset \{\text{концы } \Delta_\Gamma\}$.

В Σ входят неподвижные точки элементов Γ; они являются концами осей элементов Γ и потому концами Δ_Γ. Кроме того, в Σ входят предельные точки множества неподвижных точек. Пусть некоторый бесконечный в одну сторону путь без возвращений L представляет такую предельную точку: $z = \lim z_i$. Обсуждение в пункте 5.5в) тогда показывает, что имеет место один из двух случаев: либо существует последовательность осей элементов Γ, пересекающих L как угодно далеко от начала, либо такой последовательности нет, но существует последовательность осей элементов Γ, таких, что перемычки, соединяющие эти оси с L в Δ, пересекают L как угодно далеко от начала.

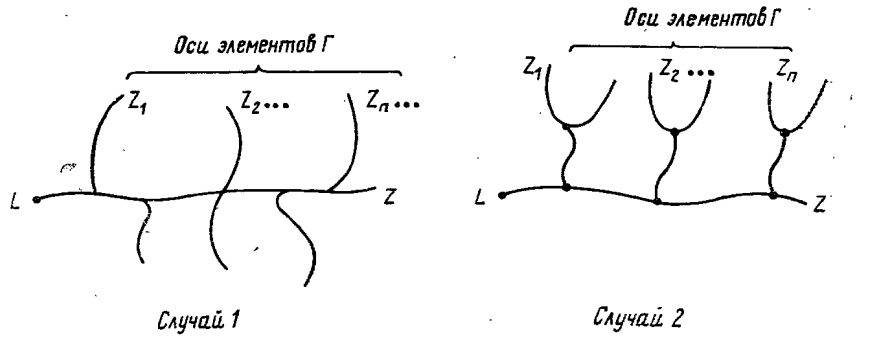


Рис. 11

В обоих случаях та часть L, которая находится дальше первого пересечения L с осью или перемычкой, принадлежит Δ_Γ, потому что она составлена из перемычек (соотв. частей перемычек) между осями элементов Γ, которые принадлежат Δ_Γ в силу 6.6 а). Значит, конец L является концом Δ_Γ.

Теперь установим обратное включение

$$\{\text{концы } \Delta_\Gamma\} \subset \Sigma.$$

Рассмотрим бесконечный в одну сторону путь без возвращений L в Δ_Γ. Если, начиная с некоторого места, он совпадает с осью некоторого элемента Γ, то его класс является неподвижной точкой Γ и потому принадлежит Σ. В противном случае L должен как угодно далеко содержать куски перемычек между осями элементов Γ. Последовательность неподвижных точек этих элементов тогда сходится к концу L (снова в силу 5.5 в)), потому что пути от начала L к этим неподвижным точкам будут расходиться с L как угодно далеко от начала.

б) Чтобы проверить, что Γ действует на Δ_Γ, достаточно установить, что Γ переводит оси в оси. Действительно, $g(\text{ось } h) = \text{ось } ghg^{-1}$, потому что аналогичное соотношение выполняется для неподвижных точек.

Для доказательства конечности графа $\Gamma \backslash \Delta_\Gamma$ выберем свободную систему образующих $h_1, \ldots, h_n$ группы Γ и вершину Λ дерева Δ_Γ. Обозначим, далее, через S подграф в Δ_Γ, состоящий из путей без возвращений от Λ ко всем $h_i\Lambda$. Мы покажем, что $\bigcup_{g \in \Gamma} g(S) = \Delta_\Gamma$; отсюда, очевидно, будет следовать конечность фактора, ибо отображение $S \to \Gamma \backslash \Delta_\Gamma$ окажется сюръективным.

Так как $S \subset \Delta_\Gamma$ (ибо $\Lambda, h_i \Lambda \in \Delta_\Gamma^0$ и Δ_Γ связен), достаточно проверить включение $\Delta_\Gamma \subset \bigcup_{g \in \Gamma} g(S)$.

Граф $\bigcup g(S)$ связен: если $g = h_{i_1}^{e_1} \ldots h_{i_r}^{e_r}$ в приведенной записи, то вершина x связана с вершиной gx путем, который проходит через вершины $h_{i_1}^{e_1} x$, $h_{i_1}^{e_1} h_{i_2}^{e_2} x$, ..., $h_{i_1}^{e_1} \ldots h_{i_r}^{e_r} x$. Последовательные вершины соединены сдвигами путей от x до $h_{i_k}^{e_{i_k}} x$, и эти сдвиги принадлежат путям $\bigcup g(S)$ по определению S.

Кроме того, для любого $g \in \Gamma$ ось g содержится в Δ_Γ. Действительно, наименьший связный подграф, содержащий орбиту $(g^n x)$, содержится в Δ_Γ в силу связности Δ_Γ. С другой стороны, он содержит ось g, ибо путь от $g^n x$ до $g^{n+1} x$ идет сначала до оси g, затем проходит фундаментальную область g на оси, затем уходит с оси и возвращается к $g^{n+1} x$ (см. лемму 6.1):

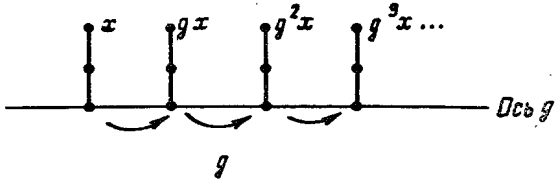


Рис. 12

Доказательство окончено. ■

6.8. Фундаментальная область для Γ в Ω. Комбинируя соображения этого параграфа и п. 5.5, мы опишем сейчас некоторый метод построения фундаментальной области для группы Шоттки Γ, действующей дискретно на $\Omega = P^1 \setminus \Sigma$.

Геометрическое описание. По теореме 6.7 K-точки Ω находятся во взаимно однозначном соответствии с теми концами Δ, которые не являются концами Δ_Γ. Назовем дорогой к точке $z \in \Omega(K)$ из Δ_Γ единственный бесконечный путь без возвращений в классе z, который начинается вершиной из Δ_Γ и выходит из нее по направлению, не принадлежащему Δ_Γ (см. конец п. 4.8).

Выберем теперь в Δ_Γ два подмножества $\overline{U} \subset \overline{V}$, удовлетворяющие следующим условиям.

$\overline{V}$ — конечное поддерево Δ_Γ, множество ребер которого содержит по одному разу представителей каждого класса ребер Δ_Γ по модулю Γ. Оно существует в силу теоремы 6.7 б). Дерево $\overline{V}$ является фундаментальной областью для Γ на Δ_Γ в слабом смысле слова: некоторые его вершины могут быть Γ-эквивалентными.

$\overline{U} = \overline{V} \setminus$ (конечное множество вершин); оставшиеся в $\overline{U}$ вершины должны содержать по одному разу представителей каждого класса вершин $\overline{V}$ по модулю Γ. Таким образом, $\overline{U}$ есть фундаментальная область для Γ на Δ_Γ в строгом смысле слова: $\Delta_\Gamma = \bigcup_{g \in \Gamma} g(\overline{U})$, $\overline{U} \cap g(\overline{U}) = \varnothing$, если $g \neq id$.

Положим, далее,

U (соответственно V) = точки $z \in \Omega$, дороги к которым начинаются в точках $\overline{U}$ (соответственно $\overline{V}$).

Левая и правая части суть функторы на конечных расширениях $L \supset K$: все конструкции согласованы с вложениями $\Delta_K \subset \Delta_L$, описанными в п. 4.8, в частности, потому, что образ $\Delta_\Gamma \subset \Delta_K$ при таком вложении равен $\Delta_\Gamma \subset \Delta_L$, и $\overline{U}$ (соответственно $\overline{V}$) удовлетворяют в Δ_L тем же условиям, которым они удовлетворяли в Δ_K.

Мы будем называть V (соответственно U) канонической фундаментальной областью для Γ на Ω (соответственно такой областью в строгом смысле слова), связанной с $\overline{V}$ (соответственно $\overline{U}$). Название оправдано тем, что для всех $L \supset K$ множество $U(L) \subset \Omega \subset P^1(L)$ открыто и содержит представителей всех классов $\Gamma \setminus \Omega(L)$ по одному разу. Множество $V(L)$ не удовлетворяет последнему условию, но оно тоже открыто и $\Omega(L) = \bigcup_{g \in \Gamma} g(V(L))$.

Чтобы лучше разобраться в структуре U и V, разобьем сначала $\overline{U}$ в конечное объединение отрезков (с конечными точками или без), $\overline{U} = \bigcup_{i=1}^{m} \overline{U}_i$, так, чтобы выполнялись следующие условия:

а) $\overline{U}_i \cap \overline{U}_j = \varnothing$ при $i \neq j$ (конечная точка, лежащая в замыкании нескольких $\overline{U}_i$, присоединяется лишь к одному из них);

б) конечные точки $\overline{U}_i$ являются вершинами Δ_K;

в) если $x \in \overline{U}_i$ — внутренняя точка, то из x выходят только два направления, принадлежащие Δ_Γ, — те, которые лежат в $\overline{U}_i$.

Такое разбиение назовем допустимым; например, в качестве конечных точек $\overline{U}_i$ можно взять все вершины $\overline{V}$ в Δ_K.

По каждому допустимому разбиению $\overline{U} = \bigcup_{i=1}^{m} \overline{U}_i$ можно построить разбиение $\overline{V} = \bigcup_{i=1}^{m} \overline{V}_i$, положив $\overline{V}_i$-замыкание $\overline{U}_i = \overline{U}_i \cup$ (конечные точки $\overline{U}_i$). Так получающиеся разбиения мы также назовем допустимыми.

Каждому такому разбиению отвечают разбиения фундаментальных областей

$$U=\bigcup_{i=1}^{m} U_i,\ V=\bigcup_{i=1}^{m} V_i,$$

определенные так же, как U и V.

Напомним теперь, что согласно п. 5.5 множество точек, отвечающих путям без возвращений с началом на $\overline{V}_i$, которые отходят по направлениям, не принадлежащим $\overline{V}_i$ (на концах $\overline{V}_i$ нужно исключить еще по одному направлению), образуют кольцо с границей в подходящей системе координат на P^1. Однако не все такие пути являются дорогами к точкам из Ω в смысле определения, данного в начале этого пункта: нужно исключить пути, которые начинаются в конечных точках $\overline{V}_i$ по направлениям, принадлежащим Δ_Γ, но не $\overline{V}_i$ «с продолжениями».

Чтобы описать этот процесс алгебраически, аксиоматизируем ситуацию.

Рассмотрим следующую систему данных.

$\overline{W}\subset\Delta_\Gamma$ — отрезок в Δ_K, включающий конечные точки; в каждой точке $\overline{W}$ отмечены запрещенные направления — те, которые принадлежат Δ_Γ; во внутренних точках их ровно два. Далее, $W\subset P^1$ — множество классов путей без возвращений, выходящих из точек $\overline{W}$ по незапрещенным направлениям. В этих условиях справедлива

6.9. Лемма. На P^1_K существует такое конечное число координатных функций $z_0, z_1, \ldots, z_n$ с дивизорами в Σ, что для некоторых элементов $a, b\in\overline{K}$ имеем:

$$W=\bigcap_{i=1}^{n}(|z_i|=1)\cap(|a|\leqslant|z_0|\leqslant|b|).$$

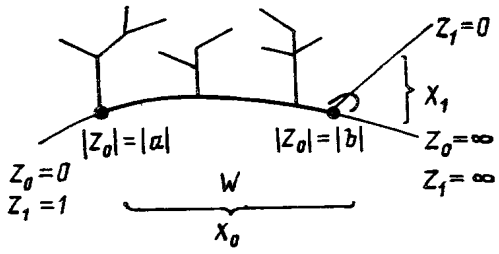


Рис. 13

Можно взять даже $a, b\in K$, если концы W лежат в Δ. В частности, W есть пересечение конечного числа колец с границей. Эти утверждения верны универсально по $L\supset K$.

Доказательство. Продолжим $\overline{W}$ до некоторой оси X_0, целиком лежащей в Δ_Γ. Выберем z_0 так, чтобы один конец этой оси был нулем Z_0, а другой полюсом. Выберем a, $b\in\overline{K}$ так, чтобы дорога к точке $z_0=a\in\Omega(K)$ начиналась в одной конечной точке $\overline{W}$, а дорога к $z_0=b$ — в другой.

Тогда множество $|a|\leqslant|z_0|\leqslant|b|$ представлено всеми путями без возвращений, начинающимися в точках $\overline{W}$ по направлениям, не принадлежащим выбранной оси. Допустим, что в конечной точке $\overline{W}$ имеется еще одно запрещенное направление. Построим тогда ось X_1, лежащую в Δ_Γ, одна половина которой выходит из этой конечной точки по этому запрещенному направлению, а другая половина совпадает с частью оси X_0, начинающейся в той же конечной точке и не содержащей $\overline{W}$ (см. чертеж). Построим координатную функцию z_1, нулем которой является конец оси X_1, выходящий в запрещенном направлении; полюсом — другой конец оси X_1; наконец, точкой $z_1=1$ — оставшийся конец оси X_0. Тогда кольцо $|z_1|=1$, согласно пп. 5.3—5.5, представлено путями без возвращений, которые начинаются в рассматриваемой конечной точке $\overline{W}$ и отходят не по направлениям из X_1. Из чертежа видно, что все точки кольца $|a|\leqslant|z_0|\leqslant|b|$ представлены такими путями, кроме тех, пути к которым отходят по запрещенному направлению.

Если имеется (на этой же или другой конечной точке $\overline{W}$) еще одно запрещенное направление, построим аналогично функцию z_2 и кольцо $|z_2|=1$ и т. п. ■

Объединяя теперь лемму 6.9 с конструкцией п. 6.8, получаем алгебраическое описание фундаментальной области Γ в Ω:

6. 10. Теорема. а) Каноническая фундаментальная область V является конечным объединением конечных пересечений колец с границей, уравнения которых являются единицами в Ω (лемма 6. 9).

б) Фундаментальная область U в строгом смысле слова получается из V, если у некоторых фигурирующих в описании колец удалить (одну или обе) компоненты границы. ■

В заключение этого параграфа мы займемся вопросом о равномерной сходимости произведения Вейерштрасса (1), введенного в конце п. 2.3 и докажем следующий факт:

6. 11. Предложение. В условиях пп. 2.3, 2.4 произведение $W_{d,z_0}(z)$ равномерно сходится для точек z, остающихся вне любой фиксированной Γ-инвариантной окрестности множества $\operatorname{supp}(d)\cup\Sigma$.

Доказательство. Разобьем рассуждение на несколько этапов.

а) Достаточно разобрать случай, когда $w_d = w$ — координатная функция с нулем и полюсом в Ω. Действительно, если перейти от K к конечному расширению, то любая w_d разобьется в конечное произведение таких координатных функций.

б) Пусть $G_0 = \mathrm{PGL}(2, O)$ — компактная группа дробно-линейных преобразований с коэффициентами из O и определителем из O^* (в w-координате). На P^1_k существует G_0-инвариантная метрика δ. Ее логарифм по какому-нибудь основанию $0 < c < 1$ можно описать так:

$$\log_\delta(z_1, z_2) = \begin{cases} \mathrm{ord}\,(w(z_1) - w(z_2)), & \text{если } |w(z_1)|,\ |w(z_2)| \leqslant 1, \\ \mathrm{ord}\,(w(z_1)^{-1} - w(z_2)^{-1}), & \text{если } |w(z_1),\ |w(z_2)| \geqslant 1, \\ 0 \text{ в остальных случаях.} \end{cases}$$

в) Пусть h пробегает элементы Г. Мы хотим доказать, что $\frac{w(hz)}{w(hz_0)} \to 1$ равномерно по z, когда z (и z_0) остается вне Г-инвариантной окрестности нуля и полюса w, а также Σ. В этом случае $w(hz)$ и $w(hz_0)$ отграничены от нуля и бесконечности, так что достаточно проверить, что $w(z)^{\pm 1} - w(z_0)^{\pm 1} \to 0$ равномерно по z. Чтобы проверить это, интерпретируем $\log \delta(z, z_0)$ в терминах графов Δ и Δ_Γ.

г) Пусть Λ — вершина Δ, являющаяся перекрестком точек $0, 1, \infty$ в w-координате. Тогда $\mathrm{PGL}(2, O)$ является стационарной подгруппой Λ в $\mathrm{PGL}(2, K)$. Поэтому функция $(z_1, z_2) \mapsto$ (длина общей части путей без возвращений от Λ к z_1 и к z_2) $\mathrm{PGL}(2, O)$ — инвариантна. Нетрудно убедиться, что она как раз совпадает с $\log \delta(z_1, z_2)$.

д) Рассмотрим ось (zz_0). Когда точка z остается вне фиксированной Г-инвариантной окрестности Δ_Γ, длина пересечения (ось $zz_0) \cap \Delta_\Gamma$ остается ограниченной, как видно из пункта 5.5. Это пересечение, если оно непусто, содержит фиксированную точку на Δ_Γ, из которой выходит путь без возвращений к z_0. Поэтому пересечение целиком содержится в фиксированном ограниченном подмножестве Δ_Γ.

е) Рассмотрим теперь пути от Λ к hz и к hz_0 соответственно. Построим сначала такие пути: от Λ до ближайшей к Λ вершине $\Lambda_1 \in \Delta_\Gamma$ без возвращений; от Λ_1 до ближайшей к Λ_1 вершине Λ_2 пересечения ось $(hz, hz_0) \cap \Delta_\Gamma$ без возвращений; пути без возвращений от Λ_2 к hz и к hz_0. Легкие геометрические рассуждения показывают, что общая длина возвращений на этих путях равномерно ограничена, а длина их пересечений на равномерно ограниченную величину отличается от длины отрезка $\Lambda_1\Lambda_2$. Наконец, из пп. 6.4 и 6.5 видно, что длина отрезка $\Lambda_1\Lambda_2$ стремится к бесконечности так:

a^- длина $h + b^- \leqslant$ длина $\Lambda_1\Lambda_2 \leqslant a^+$ длина $h + b^+$,

где $a^\pm > 0$, $b^\pm$ — некоторые константы, а длина h — это длина приведенного разложения h в каком-нибудь базисе Г. ■

§ 7. ПОЛЯРИЗАЦИЯ АНАЛИТИЧЕСКОГО ЯКОБИАНА ГРУППЫ ШОТТКИ

7.1. Мы получили уже достаточно много информации о группах Шоттки Г, чтобы доказать часть результатов, сформулированных в § 4, к теме которого мы возвращаемся.

Прежде всего, Г свободна (теорема 6.2); пусть n — ее ранг. Поэтому группа H свободная абелева, и $T = \mathrm{Spec}\, K[H]$ есть n-мерный тор с группой характеров H. На группе H задано скалярное произведение $\langle\ ,\ \rangle$ (конструкция в § 2), которое симметрично и принимает значения в K^*. Основным результатом этого параграфа будет следующая теорема (а также ее уточнение, сформулированное ниже):

7.2. Теорема (В. Дринфельд). Если $\chi \in H$, $\chi \neq 1$, то $|\langle \chi, \chi \rangle| < 1$.

Прежде, чем доказывать ее, сформулируем некоторые следствия.

7.3. Следствие. Форма $\langle\ ,\ \rangle$ невырождена; более того, форма

$$H \times H \to Z : (\chi, \varepsilon) \mapsto \mathrm{ord}\,\langle \chi, \varepsilon \rangle$$

положительно определена.

7.4. Следствие. а) Группа периодов $B \subset T(K)$, определенная в п. 3.1 д), дискретна и свободна ранга n.

б) Гомоморфизм $\varphi^{-1}: H \to B$, описанный там же, является изоморфизмом, а обратный к нему изоморфизм есть поляризация в смысле п. 1.1 главы II.

Доказательство. Напомним, что $\varphi^{-1}(\varepsilon) = \langle \cdot, \varepsilon \rangle \in \mathrm{Hom}(H, K^*)$. Так как $\langle\ ,\ \rangle$ невырождена, ядро φ^{-1} тривиально. С другой стороны, сюръективность φ^{-1} следует из определения B. Значит, φ^{-1} — изоморфизм. Обратный изоморфизм

$$\varphi : B \to H,\ d \mapsto \chi_d$$

(обозначения § 1 главы II) обладает свойствами поляризации:

$$\chi_d(d') = \chi_{d'}(d),$$

потому что $\chi_d(d') = \langle d, d' \rangle$ по определению φ и B;

$$|\chi_d(d)| < 1,\ d \neq 1,$$

в силу теоремы 7.2. Окончательно, лемма 1.3 главы II показывает, что B дискретна, так что φ действительно является поляризацией. ■

Таким образом, из теоремы 7.2 следует часть а) теоремы 3.4 этой главы.

7.5. Доказательство теоремы 7.2 будет основано на явном вычислении формы ord $\langle\ ,\ \rangle$ в терминах графа $\Gamma\backslash\Delta_\Gamma$.

Чтобы сформулировать результат этого вычисления, введем некоторые новые понятия.

Пусть $C_1(\Gamma\backslash\Delta_\Gamma)$ — группа целочисленных одномерных цепей графа $\Gamma\backslash\Delta_\Gamma$: ее элементами являются целочисленные линейные комбинации ориентированных ребер графа (над K). Если e — ребро, то $-e$ означает то же геометрическое ребро с противоположной ориентацией. Введем на $C_1(\Gamma\backslash\Delta_\Gamma)$ скалярное произведение $[,]$ «индекс перекрытия»:

$$[e, e]=1;\quad [e, f]=0,\quad \text{если}\quad e\neq\pm f,$$

где e, f — ребра. Индекс перекрытия, очевидно, является положительно определенной целочисленной симметричной формой.

Пусть $\chi\in H$, $\chi\neq 1$, $\chi=g \bmod [\Gamma,\Gamma]$, $g\in\Gamma$. Рассмотрим ось X_g элемента g в графе Δ_Γ. Ориентируем X_g направлением от z_g^+ к z_g^-. Пусть $e_1, \ldots, e_r$ — ребра на X_g, ориентированные, как X_g, по одному для каждого класса эквивалентности ребер X_g относительно группы $(g^n)_{n\in Z}$. Обозначим через $\pi(e_i)$ их образы в $\Gamma\backslash\Delta_\Gamma$ при естественной проекции $\pi\colon \Delta_\Gamma\to\Gamma\backslash\Delta_\Gamma$. Положим, наконец,

$$c_\chi=\sum_{i=1}^{r}\pi(e_i)\in C_1(\Gamma\backslash\Delta_\Gamma).$$

Цепь c_χ является циклом, класс гомологий которого в $H\cong H_1(\Gamma\backslash\Delta_\Gamma, Z)$ совпадает с классом χ при естественном гомоморфизме $\pi_1(\Gamma\backslash\Delta_\Gamma)=\Gamma\to H_1=H$. Так как $\Gamma\backslash\Delta_\Gamma$ одномерен, группа его 1-циклов совпадает с H_1, так что c_χ зависит только от χ, но не от выбора g в классе χ и не от $e_1, \ldots, e_r$. Кроме того, c_χ аддитивна по χ.

Теорема 7.2 теперь будет вытекать из следующего результата:

7.6. Теорема. Для любых $\chi, \varepsilon\in H$ имеем

$$\operatorname{ord}\langle\chi,\varepsilon\rangle=[c_\chi, c_\varepsilon].$$

Доказательство. Обе части формулы являются билинейными симметричными формами по χ, ε. Поэтому достаточно установить их совпадение в случае, когда $\chi=\varepsilon$ и χ неделим в группе H. Для вычисления ord $\langle\chi,\chi\rangle$ в этом случае мы применим теорему 2.8 б) и лемму 5.6.

Согласно теореме, имеем

$$\langle\chi,\chi\rangle=q\prod_{h\in C_0(g|g)}\frac{w_{z^+-z^-}(hz^+)}{w_{z^+-z^-}(hz^-)},$$

где $\chi=g \bmod [\Gamma,\Gamma]$ представлен матрицей, сопряженной $\begin{pmatrix} q & 0\\ 0 & 1\end{pmatrix}$, $|q|<1$, z^+, z^- — неподвижные точки g.

По лемме 5.6 тогда

$$\operatorname{ord}\langle\chi,\chi\rangle=\operatorname{ord} q+\sum_{h\in C_0(g|g)}(\text{индекс перекрытия осей } (z^+, z^-), (hz^+, hz^-)).$$

В Δ_Γ мы будем рассматривать бесконечные цепи, но перекрытия их всегда будут конечными, поэтому мы без дальнейших оговорок будем применять те же обозначения, что и для $C_1(\Gamma\backslash\Delta_\Gamma)$.

Пусть $e_1, \ldots, e_r$ — ребра оси X_g, как в п. 7.5. Согласно лемме 6.1 $r=\operatorname{ord} q$. Далее,

$$\text{цепь оси } X_g=\sum_{n\in Z}\sum_{i=1}^{r}g^n e_i,$$

$$\text{цепь оси } hX_g=\sum_{m\in Z}\sum_{j=1}^{r}hg^m e_j.$$

Поэтому

$$\operatorname{ord}\langle\chi,\chi\rangle=r+\sum_{h\in C_0(g|g)}\sum_{m,n}\sum_{i,j=1}^{r}[g^n e_i, hg^m e_j]=$$

$$=r+\sum_{h\in C_0(g|g)}\sum_{m,n}\sum_{i,j=1}^{r}[e_i, g^{-n}hg^m e_j]=$$

$$=r+\sum_{h\in\Gamma\backslash(g^n)}\sum_{i,j=0}^{r}[e_i, he_j]=\sum_{h\in\Gamma}\sum_{i,j=0}^{r}[e_i, he_j].$$

Переход от второй строчки к третьей учитывает, что $g^{-n}hg^m$ пробегает все элементы Γ, кроме степеней g^n, по определению $C_0(g|g)$. Последняя строка получается, если учесть, что $\sum_{n=-\infty}^{\infty}[e_i, g^n e_j]=r$ по выбору $e_1, \ldots, e_r$. Теперь остается отождествить $\sum_{h\in\Gamma}\sum_{i,j=1}^{r}[e_i, he_j]$ с $[c_\chi, c_\chi]=\sum_{i,j=1}^{r}[\pi(e_i), \pi(e_j)]$.

В самом деле,

$$[\pi(e_i), \pi(e_j)]=\begin{cases}[e_i, he_j], & \text{если существует (обязательно один) элемент } h\in\Gamma \text{ с } he_i=\pm e_j;\\ 0 & \text{в противном случае.}\end{cases}$$

Это завершает доказательство. ■

§ 8. СХЕМЫ МАМФОРДА

8. 1. В этом параграфе мы изложим метод Мамфорда для конструкции алгебраической кривой, представляющей фактор $\Gamma\backslash\Omega$. Естественный объект, который строится этим способом, представляет собой формальную схему над O-кольцом целых чисел поля K. Последующее доказательство ее алгебраичности «неэлементарно» в том смысле, что требует применения когомологической теории Гротендика; идейно оно близко к соответствующим рассуждениям для жестких пространств, и мы отложим обсуждение этой темы до следующей главы.

8. 2. Пусть V — двумерное пространство над полем K, $G=(\mathrm{Aut}V)/K^*$. Поставим в соответствие двумерному свободному подмодулю $M\subset V$ схему над O

$$P(M)=S(\mathrm{Hom}_o(M,O))\cong P^1_o.$$

Здесь S — симметрическая алгебра O-модуля. Общие слои этих схем $P(M)\underset{o}{\otimes}K$ канонически изоморфны P^1_K (функтор прямых в V). Это означает, что между любыми двумя схемами $P(M_1)$ и $P(M_2)$ существует бирациональное соответствие (индуцирующее канонический изоморфизм на общем слое). Пусть вообще X, Y — целостные схемы над O и пусть $\varphi: X\to Y$ — бирациональ-

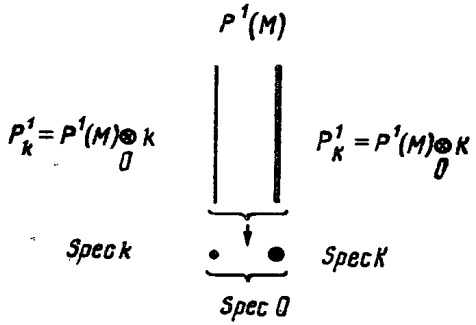


Рис. 14

ное отображение над O. Рассмотрим какие-нибудь плотные открытые подсхемы $X_0\subset X, Y_0\subset Y$, на которых φ индуцирует изоморфизм, обозначим через $\Gamma_\varphi\subset X_0\times Y_0\subset X\underset{o}{\times}Y$ график φ и положим

$$X\vee Y=\text{замыкание } \Gamma_\varphi \text{ в } X\underset{O}{\times}Y.$$

Схема $X\vee Y$ называется соединением X и Y (относительно φ). Она не зависит от выбора X_0, Y_0. Существуют канонические проекции $X\xleftarrow{p_1}X\vee Y\xrightarrow{p_2}Y$, которые являются бирациональными морфизмами над O; при этом $\varphi=p_2\circ p_1^{-1}$. Аналогично определяется соединение конечного числа схем, связанных согласованными бирациональными отображениями и проекцией. Изучим, как устроены соединения схем $P(M)$. Прежде всего, если $M_1=aM_2$, $a\in K^*$, то $P(M_1)=P(M_2)$, так что $P(M)$ зависит лишь от вершины графа Δ, сопоставляемой с M; наоборот, если $P(M_1)=P(M_2)$, то M_1 и M_2 эквивалентны. Далее, пусть вершины M_1 и M_2 — соседи; скажем, $M_1\subset M_2$ и $M_2/M_1\cong k$. Тогда $M_1 \bmod mM_2$ есть прямая в $M_2 \bmod mM_2$, то есть точка на замкнутом слое $P(M_2)\otimes k$. Если менять M_1 и M_2 в своих классах эквивалентности, то, как легко видеть, эта точка останется неизменной. Эта конструкция определяет изоморфизм

$$\{\text{соседи класса } M \text{ в } \Delta\}\leftrightarrow\{k\text{-точки } P(M)\otimes k\}.$$

Окончательно, мы получаем следующие два отображения:

вершины графа Δ ↔ схемы $P(M)$;

(ребра графа Δ) → (пары k-точек на замкнутых слоях схем, отвечающих соседним вершинам).

Теперь мы можем сформулировать

8.3. Предложение. Пусть M_1 и M_2 представляют соседние вершины. Тогда проекция

$$p_i: P(M_1)\vee P(M_2)\to P(M_i),\ i=1,2,$$

представляет собой моноидальное преобразование схемы $P(M_i)$ с центром в замкнутой точке замкнутого слоя, отвечающей соседней вершине $\{M_j\}$. ■

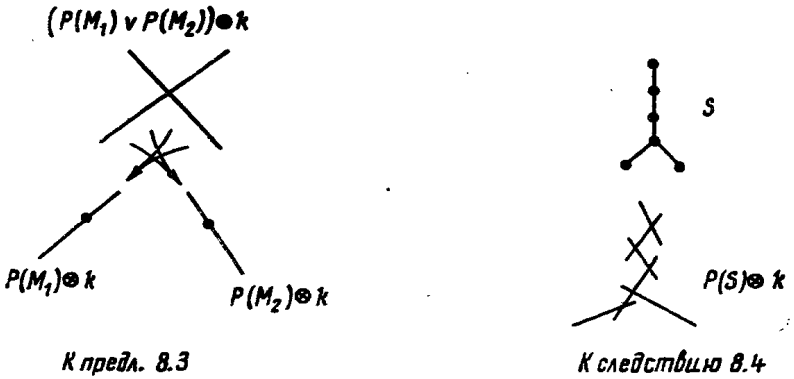
8.4. Следствие. Пусть $S\subset\Delta$ — конечное поддерево с множеством вершин S^0. Тогда

а) Соединение $P(S)=\bigvee\limits_{\{M\}\in S^0}P(M)$ есть целостная схема над O, общий слой которой изоморфен P^1_K, а замкнутый слой состоит из компонент P^1_k, связанных, как дерево S.

б) Проекция $P(S)=\bigvee\limits_{\{M\}\in S^0}P(M)\to P(N)$ для $\{N\}\in S^0$ стягивает все компоненты замкнутого слоя, кроме той, которая отвечает $\{N\}$. Точка на слое $P(N)\otimes k$, в которую стягивается $P(M)\otimes k$, отвечает последнему ребру на пути без возвращений от $\{M\}$ к $\{N\}$ в графе Δ. ■

Предложение 8.3 устанавливается прямым сопоставлением определений, а следствие получается из 8.3 индукцией по числу вершин. Мы опускаем эти простые, но кропотливые проверки.

8.5. Основная цель введения схем $P(M)$ и их соединений состоит в том, чтобы построить схему над O, на которую данная группа Шоттки Γ действовала бы бирегулярно, а не только бирационально. Интуитивно ясно, однако, что конечными соединениями нельзя обойтись: элемент $g\in\Gamma$ переводит $\{M\}$ в $\{gM\}$, и орбита $\{M\}$ бесконечна, так что «разрешение



К предл. 8.3 *К следствию 8.4*

Рис. 15

особенностей» требует раздувания все новых и новых замкнутых точек. Чтобы определить необходимый предельный переход, введем следующие вспомогательные схемы.

Пусть $S \subset \Delta_\Gamma$ — конечное поддерево. На замкнутом слое $P(S) \otimes k$ отметим те точки, которые отвечают принадлежащим Δ_Γ, но не S, направлениям выхода из вершин S. Обозначим через $P(S)'$ дополнение к этим точкам. Если T — другое поддерево Δ_Γ, $S \subset T$, то естественное отображение проекции $P(T) \xrightarrow{p} P(S)$ индуцирует изоморфизм $p^{-1}(P(S)') \xrightarrow{\sim} \xrightarrow{\sim} P(S)'$ в силу следствия 8.4 б) (точнее, его легкого обобщения): при переходе от $P(S)$ к $P(T)$ раздуваются только

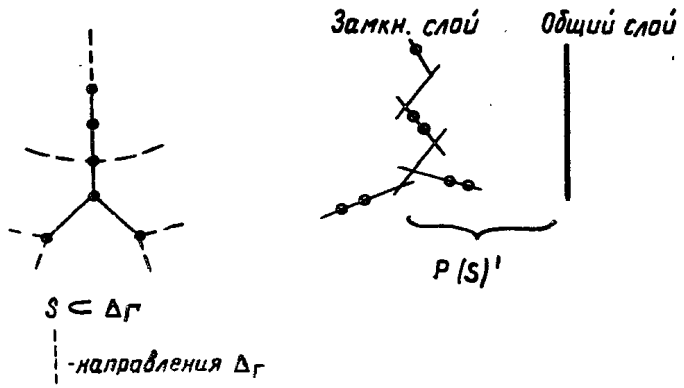


Рис. 16

выколотые точки и точки, лежащие над ними. Кроме того, $p^{-1}(P(S)') \subset P(T)'$. Таким образом, вложение деревьев $S \subset T$ определяет естественное вложение схем $P(S)' \subset P(T)'$.

Положим

$$P(\Delta_\Gamma) = \lim_{S \rightrightarrows \Delta_\Gamma} P(S)' = \bigcup_{S \subset \Delta_\Gamma} P(S)'.$$

Это целостная схема локально конечного типа над кольцом O. Ее общий слой по-прежнему изоморфен P^1_K, тогда как замкнутый слой состоит из бесконечного множества компонент P^1_k, связанных, как вершины дерева Δ_Γ.

Она является полезным алгебро-геометрическим объектом, на котором действует Γ:

8.6. Предложение. а) Группа Γ действует на $P(\Delta_\Gamma)$ бирегулярно.

б) Множество O-сечений $\operatorname{Spec} O \to P(\Delta_\Gamma)$ находится во взаимно-однозначном соответствии с множеством точек $\Omega(K) \subset P^1(K)$, в которых Γ действует дискретно.

Доказательство. а) Любой элемент g определяет изоморфизм $S \xrightarrow{\sim} g(S)$ и, значит, изоморфизм $P(S) \xrightarrow{\sim} P(g(S))$. Если $S \subset \Delta_\Gamma$, то и $g(S) \subset \Delta_\Gamma$ (теорема 6.7); по этой же причине $P(S)' \xrightarrow{\sim} P(g(S))'$. Значит, g действует на элементах покрытия $\bigcup_{S \subset \Delta_\Gamma} P(S)'$, определяющего $P(\Delta_\Gamma)$; очевидно, что это действие согласовано со склейками.

б) Пусть $z \in P^1(K)$. Для любого $M \subset V$ определена точка $z_0 \in P(M) \otimes k$ — «редукция z»; если z есть класс пути без возвращений с началом $\{M\}$, то z_0 отвечает первому ребру этого пути, как это описано в п. 8.2.

Точно также, для любого конечного дерева $S \subset \Delta_\Gamma$ точка z определяет точку $z_{0,S} \in P(S) \otimes k$ на замкнутом слое.

Предположим, что $z \in \Omega(K)$. Тогда z представлен некоторой дорогой от Δ_Γ (см. п. 6.8.). Если S содержит начало этой дороги, то $z_{0,S} \in P(S)'$ (потому что начальное направление дороги не принадлежит Δ_Γ). Значит, существует сечение $\operatorname{Spec} O \to P(S)'$, отвечающее z на общем слое; оно доставляет нужное сечение схемы $P(\Delta_\Gamma)$.

Наоборот, пусть дано сечение $\operatorname{Spec} O \to P(\Delta_\Gamma)$. Так как схемы $P(S)'$, $S \subset \Delta_\Gamma$ образуют открытое покрытие $P(\Delta_\Gamma)$, это сечение лежит в каком-то $P(S)'$ и, значит, отвечает такому пути без возвращений в графе Δ, который начинается вершиной из Δ_Γ, но выходит по направлению, не принадлежащему Δ_Γ. Стало быть, конец графа Δ, соответствующий этому пути, не является концом Δ_Γ, и потому принадлежит $\Omega(K)$ в силу теоремы 6.7. ■

8.7. Замечание. Поведение $P(\Delta_\Gamma)$ при конечных расширениях основного поля представляет некоторые особенности. Пусть $L \supset K$; будем отмечать поле определения объекта соответствующим индексом внизу.

Тогда схема $P(\Delta_\Gamma) \otimes O_L$ не изоморфна схеме $P(\Delta_\Gamma)_L$, если $L \supset K$ разветвлено: у второй больше компонент в замкну-

том слое — они отвечают новым вершинам Δ_Γ (см. п. 4.8). Более того, схема $P(\Delta_\Gamma)\otimes O_L$ не регулярна в этом случае.

Имеет место следующее: существует морфизм над O_L: $P(\Delta_\Gamma)_L \to P(\Delta_\Gamma)\otimes O_L$, который стягивает все лишние компоненты замкнутого слоя в особые точки.

Мы не будем доказывать это утверждение, ибо оно нам не понадобится.

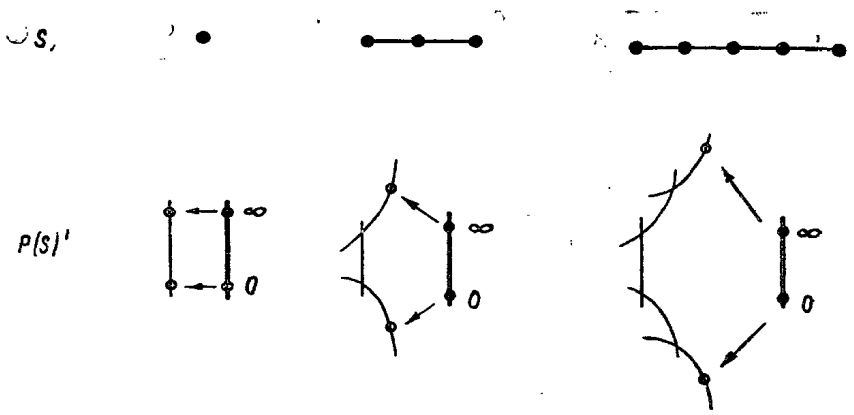


Рис. 17

8.8. Пример. $\Gamma=(g^n)$ — циклическая группа. Тогда Δ_Γ является осью в Δ; в подходящей системе координат пусть 0 — один ее конец, ∞ — другой. Конечное поддерево $S\subset\Delta_\Gamma$ является отрезком; $P(S)'$ получается выкалыванием из $P(S)$ двух точек: редукций $\bmod m$ точек 0 и ∞ общего слоя. Эти редукции лежат в двух крайних компонентах цепочки $P(S)\otimes k$. Они же раздуваются при добавлении к S двух новых ребер с двух концов.

§ 9. КОНСТРУКЦИЯ ФОРМАЛЬНЫХ ФАКТОРОВ

9.1. Факторизация замкнутого слоя схемы $P(\Delta_\Gamma)$. Пусть Γ — группа Шоттки, $P=P(\Delta_\Gamma)$ — схема, построенная в предыдущем параграфе. Так как ее общий слой есть P^1_K, построить ее фактор по Γ в каком-нибудь смысле ничуть не легче, чем факторизовать P^1 по Γ. Однако замкнутый слой $P(\Delta_\Gamma)_0=P(\Delta_\Gamma)\otimes k$ факторизовать нетрудно.

Следуя Мамфорду, сведем сначала дело к случаю, когда неединичные элементы Γ не переводят ни одну вершину в соседнюю. Этого можно добиться, либо перейдя к разветвленному квадратичному расширению основного поля, либо к некоторой нормальной подгруппе $\Gamma_0\subset\Gamma$ конечного индекса, и затем проделав дополнительную факторизацию по конечной группе.

Пусть это условие уже выполнено для Γ. Тогда Γ действует на $P(\Delta_\Gamma)_0$ дискретно в топологии Зариского. Действительно, пусть $x\in P(\Delta_\Gamma)_0$, U — компонента $P(\Delta_\Gamma)_0$, содержащая x, из которой выброшены все ее точки пересечения с другими компонентами, кроме, возможно, x. Тогда $g(U)\cap U=\varnothing$ для всех $g\in\Gamma$, $g\neq id$.

Вообще, если некоторая группа Γ действует на какой-то схеме P дискретно в топологии Зариского, то фактор $\Gamma\backslash P$ строится следующим образом. Пусть $P=\cup U_i$, где $g(U_i)\cap U_i=\varnothing$, если $g\neq id$. Тогда для любых двух индексов i, j существует не больше одного элемента g_{ij} такого, что $g_{ij}(U_i)\cap U_j\neq\varnothing$. Склеив пары U_i, U_j по этому пересечению с помощью ограничения g_{ij}, мы получим, как нетрудно видеть, фактор $\Gamma\backslash P$ в топологическом смысле.

Этот же процесс позволяет склеить структурные пучки, так что $\Gamma\backslash P$ снабжается структурой схемы.

В конечном счете $\Gamma\backslash P(\Delta_\Gamma)_0$ окажется замкнутым слоем подходящей O-модели той алгебраической кривой над K, которая представляет фактор Γ/Ω. Поэтому имеет смысл уже сейчас разобраться в геометрическом строении этого слоя.

9.2. Теорема. а) Фактор $\Gamma\backslash P(\Delta_\Gamma)_0$ являтяется связной проективной алгебраической кривой над k.

б) Компоненты $\Gamma\backslash P(\Delta_\Gamma)_0$ являются k-кривыми, нормализации которых изоморфны P^1_k; все особые точки двойные с разделенными касательными, определенными над k; на каждой компоненте есть не меньше двух ветвей, проходящих через особые точки.

в) Существуют взаимно однозначные соответствия:

$$\{\text{компоненты } \Gamma\backslash P(\Delta_\Gamma)_0\} \leftrightarrow \{\text{вершины графа } \Gamma\backslash\Delta_\Gamma\},$$
$$\{\text{двойные точки } \Gamma\backslash P(\Delta_\Gamma)_0\} \leftrightarrow \{\text{ребра графа } \Gamma\backslash\Delta_\Gamma\},$$

при которых отношение «компонента содержит двойную точку» переходит в отношение «вершина принадлежит ребру».

Доказательство. Компоненты $\Gamma\backslash P(\Delta_\Gamma)_0$ являются образами компонент $P(\Delta_\Gamma)_0$ относительно факторизации по Γ. Так как граф $\Gamma\backslash\Delta_\Gamma$ конечен, их конечное число. Каждая компонента $P(S)'_0$, которая отвечает вершине, входящей в S вместе со всеми своими соседями из Δ_Γ, изоморфна P^1_k. С ростом S все компоненты по очереди становятся такими, поэтому компоненты $\Gamma\backslash P(\Delta_\Gamma)_0$ проективны, а их нормализации изоморфны P^1_k. Из конструкции фактора видно, что неособые точки $P(\Delta_\Gamma)_0$ остаются неособыми в $\Gamma\backslash P(\Delta_\Gamma)_0$. Отображения

компоненты $P(\Delta_\Gamma)_0 \approx$ ребра $\Delta_\Gamma \to$ компоненты $\Gamma\backslash P(\Delta_\Gamma)_0$

двойные точки $P(\Delta_\Gamma)_0 \approx$ вершины $\Delta_\Gamma \to$ особые точки $\Gamma\backslash P(\Delta_\Gamma)_0$

определяют отображения пункта в). Сохранение соответствующих отношений, проверенных для Δ_Γ в § 8, без труда переносится на $\Gamma\backslash\Delta_\Gamma$. ■

9.3. Примеры. Граф $\Gamma\backslash\Delta_\Gamma$ обладает следующими свойствами, он конечен, и

а) $\pi_1(\Gamma\backslash\Delta_\Gamma)$ — свободная группа с n образующими;

б) $\Gamma\backslash\Delta_\Gamma$ не имеет концевых вершин.

Удобно сначала классифицировать (при данном n) одномерные клеточные комплексы с такими свойствами с точностью до гомеоморфизма, потом восстанавливать по ним графы (просто ставя точки на ребрах; точки кратности $\geqslant 3$,

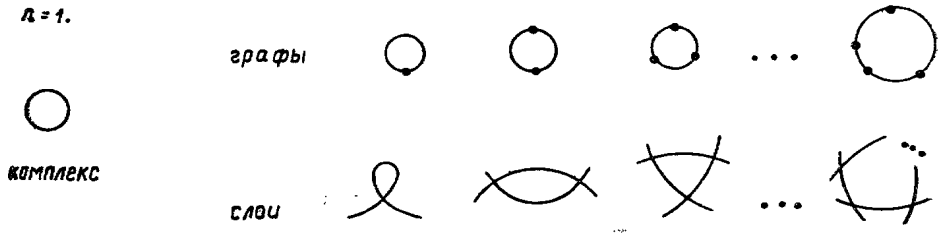


Рис. 18

конечно, должны быть вершинами всегда) и, наконец, по графам восстанавливать замкнутые слои факторов $\Gamma\backslash P(\Delta_\Gamma)_0$.

Мы получаем вырождения типа I_m, $m\geqslant 1$, в классификации вырождений эллиптических кривых по Нерону-Кодаире.

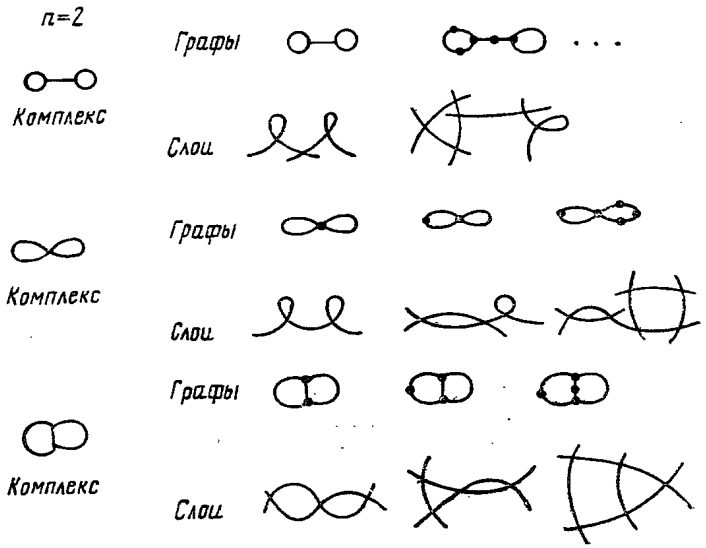


Рис. 19

(Легко видеть, что комплексы ранга 2 мы перечислили все; классификация остальных объектов после этого проводится автоматически).

Рис. 20

Этот пример характерен следующими свойствами (имеется в виду его реализация для группы Шоттки Г):

а) Фактор $\Gamma\backslash\mathrm{PGL}(2, K)$ компактен;

б) Дерево Δ_Γ совпадает с деревом Δ;

в) Множество Ω пусто.

9.4. Факторизуя по Г только замкнутый слой $P(\Delta_\Gamma)$ мы теряем много важной информации. Дело в том, что есть еще много замкнутых подсхем $P(\Delta_\Gamma)$, носителем которых является замкнутый слой. Конфинальную систему в этом множестве образуют инфинитезимальные окрестности замкнутого слоя порядка n, т. е. подсхемы $P_n = P(\Delta_\Gamma)\otimes O/m^n$. К каждой из них применима конструкция п. 9.1. Положим $X_n = \Gamma\backslash P_n$.

Если $r\geqslant s$, существует каноническое отображение $X_s \to X_r$. Оно является изоморфизмом на топологических пространствах; на пучках оно индуцирует редукцию $\bmod m^s$.

Индуктивный предел $\varinjlim X_n$ существует в категории формальных схем над O. Это окольцованное пространство $(\hat{X}, O_{\hat{X}})$, топологически совпадающее с фактором по Г замкнутого слоя $P(\Delta_\Gamma)_0$. Однако на нем имеется большой пучок колец, полных в m-адической топологии: $O_{\hat{X}} = \varprojlim O_{X_n}$.

Учет этого пучка позволяет дать формальное описание фактора $\Gamma\backslash\Omega(K)$.

9.5. Теорема. Существует изоморфизм

$$\Gamma\backslash\Omega(K) \xrightarrow{\sim} \mathrm{Hom}(\mathrm{Spf}\, O, \hat{X}) = \hat{X}(K). \blacksquare$$

Он строится в несколько шагов:

точка из $\Omega(K) \mapsto O$-сечение $P(\Delta_\Gamma) \mapsto O$-сечения $P(\Delta_\Gamma)\otimes O/m^n \mapsto$ $\mapsto O$-сечения $X_n \mapsto$ их предел по n. Первая стрелка определена в силу предложения 8.6. Доказательство сюръективности отображения и того, что в одну точку переходят лишь

Γ-эквивалентные точки, требуют привлечения алгебро-геометрических соображений, которые мы опускаем: см. Мамфорд [18], предложение 3.4 и теорема 3.5.

В заключение приведем без доказательства результаты Мамфорда об алгебраизации формальных схем $\hat{X} = \hat{X}_\Gamma$.

9.6. Теорема. а) Для любой группы Шоттки $\Gamma \subset PGL(2, K)$ существует проективная алгебраическая кривая X_Γ рода $n = rk\Gamma$ над K такая, что $\hat{X}_\Gamma$ является формальным пополнением ее минимальной гладкой модели над O (в смысле Нерона и Шафаревича; см. Лихтенбаум [16]).

б) Любая гладкая кривая X рода $n \geqslant 1$ над K, минимальная модель которой имеет стабильное k-расщепимое вырождение, изоморфна кривой вида X_Γ, где подгруппа $\Gamma \subset PGL(2, K)$ определена однозначно с точностью до сопряжения. ■

Условие, наложенное на вырождение, подробно сформулировано в теореме 9.2 б). Упомянем еще один факт относительно кривых X: все автоморфизмы X_Γ определены над K, и $\mathrm{Aut}\, X_\Gamma \cong N(\Gamma)/\Gamma$, где $N(\Gamma)$ — нормализатор Γ в $PGL(2, K)$ (см. Мамфорд [18]).

Глава IV

p-АДИЧЕСКИЕ АНАЛИТИЧЕСКИЕ ПРОСТРАНСТВА И ФОРМАЛЬНЫЕ СХЕМЫ

§ 1. АФФИНОИДНЫЕ ПРОСТРАНСТВА

1. 1. Пусть $[K : Q_p] < \infty$. Положим

$$T_n = K\langle\langle t_1, \ldots, t_n\rangle\rangle =$$

$$= \left\{ \sum_{i_k \geqslant 0} a_{i_1 \ldots i_n} t_1^{i_1} \ldots t_n^{i_n} \,\middle|\, a_{i_1 \ldots i_n} \to 0 \right\} \subset K[[t_1, \ldots, t_n]].$$

Иными словами, $K\langle\langle t_1, \ldots, t_n\rangle\rangle$ — кольцо рядов над K, сходящихся в полидиске с границей $|t_i| \leqslant 1$. Норма

$$\|f\| = \sup |a_{i_1 \ldots i_n}|, \text{ если } f = \sum a_{i_1 \ldots i_n} t_1^{i_1} \ldots t_n^{i_n}$$

определяет на T_n банахову топологию.

Назовем K-аффиноидной алгеброй любое кольцо, изоморфное фактор кольцу T_n для некоторого n. Кольца T_n и, значит, все аффиноидные алгебры нетеровы.

Следующие факты доказаны в [28].

1. 2. Теорема. а) Банахова топология на T_n однозначно определяет банаховы топологии на всех аффиноидных алгебрах, относительно которых все идеалы замкнуты, а все гомоморфизмы непрерывны.

б) Нетеровы модули над аффиноидными алгебрами однозначно снабжаются банаховыми топологиями так, что они становятся топологическими модулями. Все подмодули замкнуты и все гомоморфизмы модулей непрерывны. ■

1. 3. Пусть A — аффиноидная алгебра, $\mathrm{Max}\, A$ — множество ее максимальных идеалов. Доказывается, что любой максимальный идеал имеет конечную коразмерность A. Отсюда следует, что

$$\mathrm{Max}\, A \cong \mathrm{Hom}_k(A, \bar{K}) / \mathrm{Gal}(\bar{K}/K),$$

то есть «точки» из $\mathrm{Max}\, A$ находятся во взаимно однозначном соответствии с наборами сопряженных «геометрических точек», определенных над конечными расширениями K.

Пусть $\varphi : A \to B$ — гомоморфизм аффиноидных K-алгебр. Если на A, B заданы нормы, превращающие A, B в банаховы алгебры с канонической топологией, и $\|A\|, \|B\| \subset |K|$, то гомоморфизм φ должен быть сжимающим. (Иначе мы могли бы найти $f \in A$ с условием $\|\varphi(f)\| = 1$, $\|f\| < 1$, откуда $f^n \to 0$, но $\varphi(f)^n$ стремится к 0, в противоречие с непрерывностью φ). Применяя это к гомоморфизмам $\varphi : T_n \to L, (L : K) < \infty$, получаем $\|\varphi(z_i)\| = |\varphi(z_i)| \leqslant 1$, откуда

$$\mathrm{Max}\, T_n = \{(\zeta_i) \in \bar{K}^n \,|\, |\zeta_i| \leqslant 1\} / \mathrm{Gal}\, \bar{K}/K.$$

Значит, $\mathrm{Max}\, T_n$ представляет полидиск единичного радиуса. Аналогично, $\mathrm{Max}\, A$ представляют аналитические подмножества полидисков.

Банахова топология на T_n совпадает с топологией равномерной сходимости на $\mathrm{Max}\, T_n$. То же верно для аффиноидных алгебр A без нильпотентов.

На $\mathrm{Max}\, A$ определена топология, которую мы будем называть K-топологией: слабейшая, в которой отображения $x \mapsto |f(x)|$ непрерывны для всех $f \in A$. Множества $|f| = c$, а также $|f| < c$ для всевозможных $f \in A$, $c > 0$, образуют ее базис.

Гомоморфизм $\varphi : A \to B$ определяет отображение $\varphi^* : \mathrm{Max}\, B \to \mathrm{Max}\, A$. Пары $(\mathrm{Max}\, A, A)$, морфизмы которых отвечают гомоморфизмам аффиноидных алгебр, образуют категорию аффиноидных пространств.

Это локальные обьекты p-адической аналитической геометрии. Чтобы склеивать из них глобальные, необходимо ввести на них дополнительную структуру.

1. 4. Жесткость. Пусть X — топологическое пространство. Жесткостью на X называется набор данных следующего вида:

а) Семейство T открытых множеств на X, называемых допустимыми.

б) Для каждого $U \in T$ семейство $\mathrm{Cov}\, U$ покрытий $U = \cup U_i$,

Γ-эквивалентные точки, требуют привлечения алгебро-геометрических соображений, которые мы опускаем: см. Мамфорд [18], предложение 3.4 и теорема 3.5.

В заключение приведем без доказательства результаты Мамфорда об алгебраизации формальных схем $\hat{X} = \hat{X}_\Gamma$.

9.6. Теорема. а) Для любой группы Шоттки $\Gamma \subset PGL(2, K)$ существует проективная алгебраическая кривая X_Γ рода $n = rk\Gamma$ над K такая, что $\hat{X}_\Gamma$ является формальным пополнением ее минимальной гладкой модели над O (в смысле Нерона и Шафаревича; см. Лихтенбаум [16]).

б) Любая гладкая кривая X рода $n \geqslant 1$ над K, минимальная модель которой имеет стабильное k-расщепимое вырождение, изоморфна кривой вида X_Γ, где подгруппа $\Gamma \subset PGL(2, K)$ определена однозначно с точностью до сопряжения. ■

Условие, наложенное на вырождение, подробно сформулировано в теореме 9.2 б). Упомянем еще один факт относительно кривых X: все автоморфизмы X_Γ определены над K, и $\mathrm{Aut}\, X_\Gamma \cong N(\Gamma)/\Gamma$, где $N(\Gamma)$ — нормализатор Γ в $PGL(2, K)$ (см. Мамфорд [18]).

Глава IV

p-АДИЧЕСКИЕ АНАЛИТИЧЕСКИЕ ПРОСТРАНСТВА И ФОРМАЛЬНЫЕ СХЕМЫ

§ 1. АФФИНОИДНЫЕ ПРОСТРАНСТВА

1. 1. Пусть $[K : Q_p] < \infty$. Положим

$$T_n = K\langle\langle t_1, \ldots, t_n\rangle\rangle =$$

$$= \left\{ \sum_{i_k \geqslant 0} a_{i_1 \ldots i_n} t_1^{i_1} \ldots t_n^{i_n} \,\middle|\, a_{i_1 \ldots i_n} \to 0 \right\} \subset K[[t_1, \ldots, t_n]].$$

Иными словами, $K\langle\langle t_1, \ldots, t_n\rangle\rangle$ — кольцо рядов над K, сходящихся в полидиске с границей $|t_i| \leqslant 1$. Норма

$$\|f\| = \sup |a_{i_1 \ldots i_n}|, \text{ если } f = \sum a_{i_1 \ldots i_n} t_1^{i_1} \ldots t_n^{i_n}$$

определяет на T_n банахову топологию.

Назовем K-аффиноидной алгеброй любое кольцо, изоморфное фактор кольцу T_n для некоторого n. Кольца T_n и, значит, все аффиноидные алгебры нетеровы.

Следующие факты доказаны в [28].

1. 2. Теорема. а) Банахова топология на T_n однозначно определяет банаховы топологии на всех аффиноидных алгебрах, относительно которых все идеалы замкнуты, а все гомоморфизмы непрерывны.

б) Нетеровы модули над аффиноидными алгебрами однозначно снабжаются банаховыми топологиями так, что они становятся топологическими модулями. Все подмодули замкнуты и все гомоморфизмы модулей непрерывны. ■

1. 3. Пусть A — аффиноидная алгебра, $\mathrm{Max}\, A$ — множество ее максимальных идеалов. Доказывается, что любой максимальный идеал имеет конечную коразмерность A. Отсюда следует, что

$$\mathrm{Max}\, A \cong \mathrm{Hom}_k(A, \bar{K}) / \mathrm{Gal}(\bar{K}/K),$$

то есть «точки» из $\mathrm{Max}\, A$ находятся во взаимно однозначном соответствии с наборами сопряженных «геометрических точек», определенных над конечными расширениями K.

Пусть $\varphi : A \to B$ — гомоморфизм аффиноидных K-алгебр. Если на A, B заданы нормы, превращающие A, B в банаховы алгебры с канонической топологией, и $\|A\|, \|B\| \subset |K|$, то гомоморфизм φ должен быть сжимающим. (Иначе мы могли бы найти $f \in A$ с условием $\|\varphi(f)\| = 1$, $\|f\| < 1$, откуда $f^n \to 0$, но $\varphi(f)^n$ стремится к 0, в противоречие с непрерывностью φ). Применяя это к гомоморфизмам $\varphi : T_n \to L, (L : K) < \infty$, получаем $\|\varphi(z_i)\| = |\varphi(z_i)| \leqslant 1$, откуда

$$\mathrm{Max}\, T_n = \{(\zeta_i) \in \bar{K}^n \,|\, |\zeta_i| \leqslant 1\} / \mathrm{Gal}\, \bar{K}/K.$$

Значит, $\mathrm{Max}\, T_n$ представляет полидиск единичного радиуса. Аналогично, $\mathrm{Max}\, A$ представляют аналитические подмножества полидисков.

Банахова топология на T_n совпадает с топологией равномерной сходимости на $\mathrm{Max}\, T_n$. То же верно для аффиноидных алгебр A без нильпотентов.

На $\mathrm{Max}\, A$ определена топология, которую мы будем называть K-топологией: слабейшая, в которой отображения $x \mapsto |f(x)|$ непрерывны для всех $f \in A$. Множества $|f| = c$, а также $|f| < c$ для всевозможных $f \in A$, $c > 0$, образуют ее базис.

Гомоморфизм $\varphi : A \to B$ определяет отображение $\varphi^* : \mathrm{Max}\, B \to \mathrm{Max}\, A$. Пары $(\mathrm{Max}\, A, A)$, морфизмы которых отвечают гомоморфизмам аффиноидных алгебр, образуют категорию аффиноидных пространств.

Это локальные обьекты p-адической аналитической геометрии. Чтобы склеивать из них глобальные, необходимо ввести на них дополнительную структуру.

1. 4. Жесткость. Пусть X — топологическое пространство. Жесткостью на X называется набор данных следующего вида:

а) Семейство T открытых множеств на X, называемых допустимыми.

б) Для каждого $U \in T$ семейство $\mathrm{Cov}\, U$ покрытий $U = \bigcup U_i$,

где все $U_i \in T$. Элементы $\mathrm{Cov}\, U$ называются допустимыми покрытиями; мы пишем $\mathrm{Cov}\, T = \bigcup_{U \in T} \mathrm{Cov}\, U$.

в) Предпучок колец O_X на T, то есть набор колец $\Gamma(U, O_X)$ для всех $U \in T$ и ограничений $\Gamma(U, O_x) \to \Gamma(V, O_X)$ для всех $V \subset U$ с обычными условиями транзитивности.

Эти данные должны удовлетворять следующим аксиомам.

(I). T содержит $\varnothing, X$, образует базис топологии X и замкнуто относительно конечных пересечений.

(II). Тождественное покрытие $U \rightrightarrows U$ допустимо для $U \in T$. Если $U, V, V_i \in T$, $U \subset V = \bigcup_i V_i$ и это покрытие V допустимо, то покрытие $U = \bigcup_i (V_i \cap U)$ допустимо.

(III). Если покрытия $U = \bigcup_{i \in I} U_i$ и $U_i = \bigcup_{j \in J_i} U_{ij}$ допустимы, то покрытие $U = \bigcup_{i,j} U_{ij}$ допустимо.

(Аксиомы (I)—(III) означают, что допустимые множества и покрытия образуют предтопологию Артина—Гротендика).

(IV). Если $U \subset V = \bigcup_i V_i$; V, V_i и покрытие V допустимы и $U \cap V_i$ допустимы для всех i, то U допустимо.

(V). Предпучок O_X удовлетворяет аксиоме пучка на всех допустимых покрытиях допустимых открытых множеств.

Наконец, в приложениях будет всегда выполнена еще одна аксиома:

(VI). Слои $O_x = \varinjlim_{x \in U \in T} \Gamma(U, O_x)$ пучка O_X во всех точках $x \in X$ являются локальными кольцами.

1.5. Морфизмы пространств с жесткостью. Пусть даны пространство X с жесткостью T_X, $\mathrm{Cov}\, T_X$, O_X и Y с жесткостью T_Y, $\mathrm{Cov}\, T_Y$, O_Y.

Морфизм $f = (\varphi, \psi) : X \to Y$ состоит из следующих данных:

а) $\varphi : X \to Y$ — непрерывное отображение топологических пространств такое, что $\varphi^{-1}(T_Y) \subset T_X$, $\varphi^{-1}(\mathrm{Cov}\, T_Y) \subset \mathrm{Cov}\, T_X$.

б) $\psi = (\psi_U)$, где для каждого $U \in T_Y$ гомоморфизмы колец

$$\psi_U : \Gamma(U, O_Y) \to \Gamma(\varphi^{-1}(U), O_X)$$

совместимы с ограничениями и индуцируют локальные гомоморфизмы колец $\psi_x : O_{Y, \varphi(x)} \to O_{X,x}$.

1.6. Индуцированная жесткость. Пусть X — пространство с жесткостью T_X, $\mathrm{Cov}\, T_X$, O_X; $Y \subset X$ — допустимое открытое множество. Индуцированная жесткость на Y определяется данными:

$T_Y = \{U \in T_X \mid U \subset Y\}$;

$\mathrm{Cov}\, T_Y$ = покрытия множеств из T_Y, допустимые на X;

O_Y = ограничение O_X на Y.

1.7. Каноническая жесткость на аффиноидных пространствах. Пусть $X = (\mathrm{Max}\, A, A)$ — аффиноидное пространство. Открытое подмножество $Y \subset X$ называется аффиноидной подобластью с алгеброй A_Y, если дан гомоморфизм $\varphi : A \to A_Y$ такой, что $\varphi^*(\mathrm{Max}\, A_Y) \subset Y$ и если любой гомоморфизм $\psi : A \to B$ с $\psi^*(\mathrm{Max}\, B) \subset Y$ однозначно проводится через φ.

Следующие свойства аффиноидных подобластей доказаны в [28].

1.7.1. $\varphi : A \to A_Y$ определяется по Y однозначно, и $\varphi^* : \mathrm{Max}\, A_Y \to Y$ является гомеоморфизмом.

1.7.2. Пересечение конечного семейства аффиноидных подобластей является аффиноидной подобластью.

1.7.3. Свойство «быть аффиноидной подобластью» транзитивно.

1.7.4. Прообраз аффиноидной подобласти $U \subset X$ относительно морфизма аффиноидных пространств $Y \to X$ (см. п. 1.3) является аффиноидной подобластью.

Теперь мы можем описать каноническую жесткость на аффиноидном пространстве $X = \mathrm{Max}\,(A, A)$.

а) Открытое подмножество $U \subset X$ допустимо, если и только если существует такое его покрытие аффиноидными подобластями $U = \bigcup_i U_i$, что для любого морфизма аффиноидных пространств $\varphi : Y \to X$ с $\varphi(Y) \subset U$ существует покрытие Y, вписанное в $\bigcup_i \varphi^{-1}(U_i)$ и состоящее из конечного числа аффиноидных подобластей Y.

б) Покрытие $U = \bigcup_i U_i$ с допустимыми подмножествами U, U_i называется допустимым, если в ситуации а) покрытие $Y = \bigcup_i \varphi^{-1}(U_i)$ содержит вписанное покрытие, состоящее из конечного числа аффиноидных подобластей Y.

в) Если $U \subset X$ — аффиноидная подобласть с алгеброй A_U, то мы полагаем

$$\Gamma(U, O_X) = A_U.$$

Если $U = \bigcup U_i$ — конечное покрытие аффиноидными областями то мы полагаем

$$\Gamma(U, O_X) = \mathrm{Ker}\left(\prod_i \Gamma(U_i, O_X) \to \prod_{i,j} \Gamma(U_i \cap U_j, O_X)\right).$$

Согласно Тэйту [28], Грауэрту и Герритцену [6], результат не зависит от выбора покрытия U.

Наконец, продолжение пучка O_X на все допустимые множества осуществляется с помощью общих конструкций Гротендика—Артина, которые мы опускаем.

Мы опускаем также проверку аксиом (I) — (VI) для жесткости, в которой самыми тонкими являются аксиомы пучка O_X.

1.8. Теорема. Морфизмы аффиноидных пространств с

жесткостью $(\mathrm{Max}\,A,\ A)\to(\mathrm{Max}\,B,\ B)$ находятся во взаимно-однозначном соответствии с гомоморфизмами K-алгебр $B\to A$, в согласии с предварительным определением п. 1.3. ■

1.9. Примеры аффиноидных подобластей. Пусть $z_1, \ldots, z_m \in A$ — любые функции, $\varepsilon_i = \pm 1$. Тогда

$$Y = \bigcap_{i=1}^{m} \{|z_i|^{\varepsilon_i} \leqslant 1\} \subset X = \mathrm{Max}\,A$$

аффиноидная подобласть с кольцом

$$A_Y = A\ll Z_1, \ldots, Z_n\gg/(Z_i - z_i,\ Zz_j - 1).$$

Справа i пробегает индексы с $\varepsilon_i = 1$, а j — индексы с $\varepsilon_j = -1$

§ 2. АНАЛИТИЧЕСКИЕ ПРОСТРАНСТВА

2.1. Определение А. Топологическое пространство X с жесткостью называется жестким аналитическим пространством над полем K, если у него существует допустимое покрытие $X = \bigcup_i X_i$ такое, что жесткость, индуцированная на каждом X_i, превращает X_i в аффиноидное пространство над K с канонической жесткостью.

Это определение принадлежит Тэйту и Килю; для него в работах Киля [12], [13] доказаны аналоги некоторых основных когомологических теорем комплексного анализа. Для нас будет удобнее другое определение, данное Герритценом и Грауэртом.

2.2. Определение Б. Голоморфным пространством X с аффиноидным атласом $\{X_i\}$ называется следующий набор данных:

а) топологическое пространство X и его открытое покрытие $X = \bigcup_i X_i$.

б) Структура аффиноидного пространства на каждом X_i с алгеброй A_i.

Этот набор данных должен быть подчинен следующим условиям:

(I) $X_i \cap X_j$ пусто или является аффиноидной подобластью X_{ij} в каждом X_i, X_j с одной и той же алгеброй A_{ij}. Кроме того, A_{ij} должна быть топологически порождена образами A_i^0 и A_j^0, где

$$A_i^0 = \{f \in A_i \mid |f(x)| \leqslant 1 \text{ для всех } x \in X_i\}.$$

(II) Для каждого i есть лишь конечное число j с $X_i \cap X_j = \varnothing$.

Атлас $\{Y_j\}$ на том же пространстве X называется допустимым измельчением атласа $\{X_i\}$, если $Y_j \subset X_{\sigma(j)}$ для некоторого отображения σ множества индексов, если Y_j является аффиноидной подобластью в $X_{\sigma(j)}$, и если, кроме того, для каждого i пересечение $X_i \cap Y_j$ непусто лишь для конечного множества j.

Два атласа, имеющие общее допустимое измельчение, называются эквивалентными; можно проверить, что это действительно отношение эквивалентности.

Окончательно, голоморфным пространством X называется пространство X вместе с классом эквивалентных аффиноидных атласов на X. Каждый атлас из этого класса будет называться голоморфным; класс этих атласов называется голоморфной структурой на X.

2.3. Взаимоотношения между определениями А и Б не выяснены. Предположительно, при естественном определении морфизмов голоморфных пространств их категория окажется эквивалентной некоторой подкатегории жестких аналитических пространств. Этот факт должен основываться на конструкции жесткости по классу аффиноидных атласов.

Ниже мы будем пользоваться определением Б и принимать гипотезу о том, что некоторые основные факты, доказанные для жестких пространств, верны также для голоморфных.

2.4. Пусть $X' \subset X$ — открытое подмножество в голоморфном пространстве X. Аффиноидный атлас на X' называется индуцированным с X, если любое конечное число элементов этого атласа можно включить в голоморфный атлас на X.

X' вместе с голоморфной структурой называется голоморфной подобластью в X, если на X' существуют сколь угодно мелкие голоморфные атласы, индуцированные с X. Согласно Грауэрту и Герритцену, голоморфная структура на X' не определяется однозначно.

2.5. Замкнутые голоморфные пространства. Положим $D^n = \mathrm{Max}\,K\ll t_1, \ldots, t_n\gg$ — аффиноидная схема «n-мерный диск». Положим, далее, для $0 < \varepsilon < 1$:

$$D^n_{1-\varepsilon} = \{x \in D^n \mid \forall i,\ |t_i(x)| \leqslant 1 - \varepsilon\}.$$

Это аффиноидная подобласть в $D^n \otimes L$, если $L \supset K$ достаточно велико, так что $1 - \varepsilon \in |L|$.

Пусть X — аффиноидное пространство, $Y \subset X$ — аффиноидная подобласть. Мы говорим, что Y лежит внутри X, в записи $Y \Subset X$, если существует такое замкнутое погружение $X \subset D^n$, что $Y \subset D^n_{1-\varepsilon}$ при некотором $\varepsilon > 0$. (Замкнутое погружение $X \subset D^n$ определяется сюръективным гомоморфизмом $K\ll t_1, \ldots, t_n\gg \to A$, где $X = \mathrm{Max}\,A$).

Пусть X — голоморфное пространство с атласом $\{X_i\}$. Допустимое измельчение $\{Y_j\}$ атласа $\{X_i\}$ называется сжатием $\{X_i\}$, если существует такое отображение индексов σ, что $Y_j \Subset X_{\sigma(j)}$ для всех j.

Голоморфное пространство X называется замкнутым, если у него есть конечный (голоморфный аффиноидный) атлас, допускающий сжатие.

2.6. Примеры. Алгебраические многообразия над K здесь будут рассматриваться как множества своих замкнутых точек с K-топологией.

а) $X=P^n_K$ — n-мерное проективное пространство. Выберем систему координат $P^n_K=\mathrm{Proj}\,K[t_0, \ldots, t_n]$. Положим

$$U_i=\left\{x\in P^n_K \mid \forall k,\ \left|\frac{t_k}{t_i}(x)\right|\leqslant c\right\},\ i=0, \ldots, n,$$

где $c>1$, $c\in|K|$, и

$$V_i=\left\{x\in P^n_K \mid \forall k,\ \left|\frac{t_k}{t_i}(x)\right|\leqslant 1\right\},\ i=0, \ldots, n.$$

Введем на U_i (соответственно V_i) структуру аффиноидного пространства, положив

$$U_i=\mathrm{Max}\,K\ll\frac{t_0}{at_i}, \ldots, \frac{t_n}{at_i}\gg,$$

$$V_i=\mathrm{Max}\,K\ll\frac{t_0}{t_i}, \ldots, \frac{t_n}{t_i}\gg.$$

Тогда $\{U_i\}$ и $\{V_i\}$ образуют аффиноидные атласы на P^n_K (проверка аксиом (I) и (II) п. 2.2 легка). Они эквивалентны; более того, второе является сжатием первого. Это доставляет на P^n_K структуру голоморфного пространства, притом замкнутого.

б) $X\subset P^n_K$ — проективное алгебраическое подмногообразие. Положим $X_i=X\cap U_i$, $Y_i=X\cap V_i$, где U_i, V_i определены, как выше. X превращается в замкнутое голоморфное пространство. Согласно Герритцену и Грауэрту, эта структура голоморфного пространства не зависит от выбора проективного погружения.

в) X квазипроективное многообразие. Погрузим X в его замыкание $\hat{X}$. На $\hat{X}$ определена голоморфная структура согласно пункту б). На X существует единственная голоморфная структура, которая превращает X в голоморфную подобласть $\hat{X}$ в смысле п. 2.4 и которая обладает следующим дополнительным свойством: любой элемент любого голоморфного атласа на $\hat{X}$, содержащийся в X, пересекается лишь с конечным числом элементов любого голоморфного атласа на X.

Эта структура также не зависит от X.

§ 3. СВЯЗЬ С ФОРМАЛЬНЫМИ СХЕМАМИ

3.1. Рассмотрим кольцо $K\ll t_1, \ldots, t_n\gg$ и в нем подкольцо $O\ll t_1, \ldots, t_n\gg$, состоящее из рядов с целыми коэффициентами. Так как эти коэффициенты стремятся к нулю, редукция $\mathrm{mod}\,m^N$ любого ряда из $O\ll t_1, \ldots, t_n\gg$ является многочленом. Таким образом,

$$O\ll t_1, \ldots, t_n\gg=\varprojlim O/m^N[t_1, \ldots, t_n].$$

С другой стороны, $O/m^N[t_1, \ldots, t_n]$ суть сечения структурного пучка N-й инфинитезимальной окрестности замкнутого слоя аффинного пространства $A^n_O=\mathrm{Spec}\,O[t_1, \ldots, t_n]$ над O, а $\varprojlim O/m^N[t_1, \ldots, t_n]$ — сечения структурного пучка формального пополнения $\hat{A}^n_O$.

Если учесть, что

$$O\ll t_1, \ldots, t_n\gg=\{f\in K\ll t_1, \ldots, t_n\gg \mid \forall x\in D_n,\ |f(x)|\leqslant 1\},$$

так что это кольцо восстанавливается по $D^n=\mathrm{Max}K\ll t_1, \ldots, t_n\gg$ однозначно, — мы получаем вполне инвариантную конструкцию:

{аффиноидный полидиск D^n}$\mapsto$ {аффинная формальная схема A^n_O}.

Она распространяется на аффиноидные пространства без нильпотентов следующим образом. Пусть A — алгебра такого пространства, $A^0=\{f\in A \mid \forall x\in\mathrm{Max}\,A,\ |f(x)|\leqslant 1$. Тогда A^0 — алгебра топологически конечного типа, и соответствие

$$(A, \mathrm{Max}\,A)\mapsto(\text{формальный спектр } \mathrm{Spf}\,A^0)$$

продолжается до функтора

$$\left\{\begin{array}{l}\text{аффиноидные}\\ \text{пространства}\\ \text{без нильпотентов}\end{array}\right\}\to\left\{\begin{array}{l}\text{аффинные}\\ \text{формальные}\\ \text{схемы конечного типа над } O\end{array}\right\}.$$

Существует и естественная стрелка в обратную сторону, которая формальной схеме $\mathrm{Spf}\,A^0$ ставит в соответствие аффиноидное пространство $(\mathrm{Max}\,A^0\underset{O}{\otimes}K,\ A^0\underset{O}{\otimes}K)$. Его естественно назвать «общим слоем» схемы $\mathrm{Spf}\,A^0$.

Однако при сравнении глобальных объектов обеих категорий возникает следующая трудность. Гомоморфизм $Z_p\ll t\gg\to Z_p\ll u\gg: t\to pu$ с точки зрения аффиноидных пространств определяет вложение в D^1 аффиноидной подобласти $D^1_{p^{-1}}$, а с точки зрения формальных схем — морфизм, при котором образом всего пространства служит точка. Можно восстановить ситуацию, в которой аффинноидной подобласти будет отвечать аффинное открытое вложение, ценой проведения моноидальных преобразований формальных схем, сосредоточенных на замкнутом слое.

Подробный анализ положения дел привел М. Рейно к следующей важной теореме, подробное доказательство которой, к сожалению, еще не опубликовано:

3.2. Теорема. Существует эквивалентность следующих двух категорий:

а) Категория жестких аналитических пространств, имеющих такое конечное допустимое покрытие аффиноидами, что пересечение любой пары элементов покрытия является конечным допустимым объединением допустимых аффиноидов (условие квазиотделимости).

б) Категория формальных O-схем конечного типа, локализованная относительно моноидальных преобразований с центром в пучках идеалов, содержащих некоторую степень m.

При этой эквивалентности замкнутые пространства в смысле п. 2.4 отвечают собственным формальным схемам.

§ 4. АЛГЕБРАИЗАЦИЯ АНАЛИТИЧЕСКИХ ОБЪЕКТОВ

4.1. В этом параграфе мы дадим набросок доказательств теорем об алгебраизации 3.2—3.4 главы III. Доказательства эти неполны в двух отношениях. Во-первых, как уже было отмечено, в литературе нет подробного изложения всех нужных нам фактов, принадлежащих к основаниям теории p-адических аналитических пространств, — например, теорем типа GAGA (не говоря уже о том, что нет единого описания категории этих пространств). Во-вторых, мы сами опускаем детальную проверку ряда технических утверждений.

Тем не менее, представляется несомненным, что все пробелы можно заполнить, не вводя существенно новых идей.

Мы изложим план доказательства и прокомментируем отдельные шаги.

Ниже мы свободно пользуемся обозначениями и результатами главы III, особенно §§ 1—3,6. В частности, мы считаем что фиксирована группа Шоттки Γ, область $\Omega\subset P^1_K$, где Γ действует дискретно, и соответствующие аналитические объекты X_{an}, $\mathscr{D}^0_{\text{an}}$, $\mathscr{D}_{\text{an}}$, J_{an} и т. п.

Доказательство теорем об алгебраизации состоит из нескольких конструкций и применения общих теорем о голоморфных пространствах.

4.2. Конструкция голоморфного атласа на Ω. Проще всего взять в качестве голоморфного атласа покрытие $\Omega=\bigcup\limits_i\bigcup\limits_{g\in\Gamma} gV_i$, где $V=\bigcup V_i$ — некоторая каноническая фундаментальная область для Γ, построенная в п. п. 6.8—6.10 главы III, а V_i — пересечения колец с границей. Проверка аксиом атласа из п. 2.2 основана на следующих соображениях.

а) Кольцо с границей $|a|\leqslant|z|\leqslant|b|$ имеет структуру аффиноидной схемы с кольцом $K\ll\frac{z}{b},\frac{z}{a}\gg$; аналогично строится кольцо функций для конечного пересечения колец с границей. Поэтому V_i — аффиноиды.

б) Функции z, участвующие в уравнениях для gV_i, являются координатными функциями на P^1_K с дивизорами в Σ. Поэтому любая из них принадлежит аффиноидному кольцу любой области gV_i так, что пересечение $gV_i\cap hV_j$ является полицилиндром в каждой из областей. Кроме того, каждая из областей пересекается лишь с конечным числом других, как видно из п. 6.8. Аналогично проверяется последнее условие в определении атласа.

4.3. Конструкция фактора $\Gamma\backslash\Omega$ как замкнутого голоморфного пространства. Чтобы построить фактор $\Gamma\backslash\Omega$ с двумя атласами, один из которых является сжатием другого (см. п. 2.5), мы несколько усложним конструкцию п. 4.2, построив два атласа $\Omega=\bigcup\limits_i\bigcup\limits_g gU_i=\bigcup\limits_i\bigcup\limits_g gW_i$ со следующими свойствами:

а) $gW_i\Subset gU_i$ для всех i, $g\in\Gamma$;

б) $gU_i\cap hU_i=\varnothing$, $g\neq h$.

После этого $\Gamma\backslash\Omega$ вместе с двумя голоморфными атласами получится склейкой U_i (или W_i), как в п. 9.1 главы III.

Для конструкции U_i и W_i мы предположим, что на каждой геометрической петле графа $\Gamma\backslash\Delta_\Gamma$ лежит $\geqslant 7$ ребер, и между каждыми двумя кратными вершинами графа лежит не меньше шести вершин кратности 2. (Общий случай сводится к этому, как в п. 9.1, либо переходом к подгруппе конечного индекса в Γ, либо конечным расширением основного поля, и последующей дополнительной факторизацией по конечной группе). После этого построим U_i и W_i, как в п. 6.8, разбив фундаментальную область V для Γ на Δ_Γ на следующие части:

в) $\bar{U}_i$ — прообразы «звезд» в $\Gamma\backslash\Delta_\Gamma$, которые состоят из всех отрезков длиной в три ребра, выходящих из вершин кратности $\geqslant 3$; а также прообразы отрезков длины $\geqslant 5$, все вершины которых имеют кратность 2 в Γ/Δ_Γ, а конечные вершины являются соседями вершин кратности $\geqslant 3$.

г) $\bar{W}_i$ получаются из соответствующих $\bar{U}_i$ отбрасыванием всех конечных ребер.

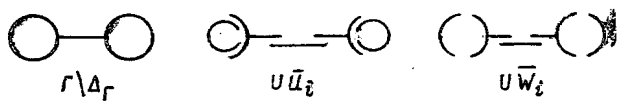


Рис. 21

Доказательство того, что W_i — пересечение колец с границей и что $W_i\Subset U_i$, проводится по образцу леммы 6.9 главы III.

4.4. Конструкция J_{an} как замкнутого голоморфного пространства. Этому посвящены работы Гер-

ритцена [3, 4], относящиеся к общему случаю фактора T/B, где T — тор над K, а $B \subset T(K)$ — подгруппа периодов

4.5. Алгебраизация $X_{an} = \Gamma \backslash \Omega$, J_{an} и морфизма $j: X_{an} \to J_{an}$. Любое одномерное замкнутое голоморф ое пространство проективно алгебраично (Герритцен и Грауэрт [6], стр. 182). Это дает K-алгебраическую структуру X_{alg} на X_{an}. Многообразие J_{an} алгебраизуется с помощь ю поляризации (см. § 7 главы III) и теории главы II; получает ся абелево многообразие J_{alg} над K. Достаточно подробное изложение с точки зрения голоморфных пространств содержится в статье Герритцена [4].

Отображение j является голоморфным: это следует из его явного описания в терминах множителей автоморфности μ и явных формул для μ типа формулы (3) из п. 2.4 главы III.

Теорема типа GAGA должна после этого гарантировать алгебраичность $j: X_{alg} \to J_{alg}$.

4.6. Морфизм $j: X_{alg} \to J_{alg}$ является каноническим морфизмом кривой в ее якобиан. Для доказательства нужно прежде всего заметить, что $X_{an} = X_{alg}$ как функтор на $L \supset K$ совпадает с функтором $\Gamma \backslash \Omega$ (Мамфорд [18] доказывает это в контексте формальных схем, и не должно быть трудным проделать то же для аналитических пространств). Это немедленно доставляет изоморфизм функторов $\mathcal{D}_{an} = \mathcal{D}_{alg}$ (алгебраические L-дивизоры нулевой степени на X_{alg}). Далее, $\mathcal{D}^0_{an} \subset \mathcal{D}^0_{alg}$ (главные L-дивизоры на X_{alg}). Действительно, по каждому главному аналитическому дивизору мы построили Γ-инвариантную мероморфную функцию на Ω; спуская ее на $\Gamma \backslash \Omega$, получаем мероморфную функцию на X_{an}; теорема типа GAGA позволяет считать, что это рациональная функция, на X_{alg}.

С другой стороны, если $D \in \mathcal{D}^0_{alg} \subset \mathcal{D}_{an}$, $D = \sum_{g \in \Gamma} g(d)$, то d как аналитический дивизор обладает тем свойством, что $\mu_d \equiv 1 \bmod B$. Действительно, $\mu_{z_1 - z_0} \bmod B$ есть $j(\Gamma z_1)$, так что μ_d получается суммированием j-образов точек из d в смысле группового закона J_{alg}. Но хорошо известно, что главные дивизоры при таком суммировании дают нулевую точку при отображении в любое абелево многообразие, в частности, в J_{alg}. Значит, $\mathcal{D}^0_{alg} \subset \mathcal{D}^0_{an}$.

Отсюда следует, что $\mathcal{D}^0_{alg} = \mathcal{D}^0_{an}$ и, значит, функторы $\mathcal{D}_{alg}/\mathcal{D}^0_{alg}$ и $\mathcal{D}_{an}/\mathcal{D}^0_{an}$ совпадают. Поэтому J_{alg} — алгебраический якобиан X.

4.7. Функции $W_{d, z_0}(z)$ (и нуль) для главных K-дивизоров d составляют поле рациональных функций на X_{alg} (поднятое на Ω). Действительно, для каждого главного K-дивизора на X_{alg} соответствующее произведение Вейерштрасса совпадает (с точностью до константы) с подъемом на Ω функции с этим дивизором, согласно п. 4.6.

4.8. Дифференциалы. Дифференциал ω_g, определенный в п. 2.11, индуцирован дифференциалом $d\chi/\chi$ на торе T, где $\chi = g \bmod [\Gamma, \Gamma] \in H$, $T = \operatorname{Spec} K[H]$ (см. 3.1 е). Такие дифференциалы индуцируют решетку дифференциалов ранга n на $J = T/B$ и, значит, решетку ранга n на X.

БИБЛИОГРАФИЯ

1. **Форд С.,** Автоморфные функции. ОНТИ, 1936
2. **Bruhat F.,** Tits J., Groupes algébriques semi-simples sur un corps local. Publ. IHES, 1972, 42
3. **Gerritzen L.,** Über Endomorphismen nichtarchimedischer holomorpher Tori. Invent. math., 1970, **11**, № 1, 27—36 (РЖМат, 1971, 5А469)
4. —, On non-archimedian representations of abelian varieties. Math. Ann., 1972, **196**, № 4, 323—346 (РЖМат, 1972, 12А362)
5. —, Die Norm der gleichmässigen Konvergenz auf reduzierten affinoiden Algebren. J. reine und angew. Math., 1968, **231**, 114—120 (РЖМат, 1969, 3Б499)
6. —, Grauert H., Die azyklizität der affinoiden Überdeckungen, in Global Analysis. Papers in honor of Kodaira, University of Tokyo Press, Princeton University Press, 1970, 159—184
7. **Grauert H.,** Remmert R., Über die Methode der diskret bewerteten Ringe in der nichtarchimedischen Analysis. Invent. math., 1966, **2**, № 2, 87—133 (РЖМат, 1968, 4А333)
8. —, —, Nichtarchimedische Funktionentheorie. Wiss., Abh. Arbeitsgemeinsch. Forsch. Landes Nordthein—Westfalen, 1966, **33**, 393—476 (РЖМат, 1967, 12А369)
9. —, —, Analytische Stellenalgebren. Berlin, Springer, 1971, 240 S. (РЖМат, 1972, 2А550К)
10. **Grothendieck A.,** Elements de géométrie algébrique. IV. Publs math. Inst. hautes études scient., 1964, № 20, 101—355 (РЖМат, 1965, 5А210)
11. **Güntzer A. U.,** Zur Funktionentheorie einer Veränderlichen über einem vollständigen nichtarchimedischen Grundkörper. Arch. Math., 1966, **17**, № 5, 415—431 (РЖМат, 1967, 5Б549)
12. **Kiehl R.,** Der Endlichkeitssatz für eigentliche Abbildungen in der nichtarchimedischen Funktionentheorie. Invent. math., 1967, **2**, № 3, 191—214 (РЖМат, 1968, 10А289)
13. —, Theorem A und theorem B in der nichtarchimedischen Funktionentheorie. Invent. Math., 1967, **2**, № 4, 256—273 (РЖМат, 1968, 10А290)
14. —, Die de Rham Kohomologie algebraischer Mannigfaltigkeiten über einem bewerteten Körper. Publs math. Inst. hautes études scient., 1967 (1968), № 33, 367—382 (РЖМат, 1969, 10А228)
15. **Lazard M.,** Les zéros d'une fonction analitique d'une variable sur un corps valué complet. Publs math. Inst. hautes études scient., 1962, № 14, 47—75
16. **Lichtenbaum S.,** Curves over discrete valuation rings. Amer. J. Math., 1968, **90**, № 2, 380—394 (РЖМат, 1969, 8А321)
17. **Morikawa Hasasi,** Theta functions and abelian varieties over valuation fields of rank one 1. Nagoya Math. J., 1962, **20**, 1—27 (РЖМат, 1966, 5А215)

18. **Mumford D.,** An analytic construction of degenerating curves over complete local rings. Compos. math., 1972, 24, № 2, 129—174 (РЖМат, 1972, 11А317)
19. —, An analytic construction of degenerating abelian varieties over complete rings. Compos. math., 1972, 24, № 3, 239—272 (РЖМат, 1973, 2А373)
20. **Raynaud M.,** Variétés abéliennes et géométrie rigide. Actes Congr. Int. mathématiciens, 1970, Vol. 1. Paris, 1971, 473—477 (РЖМат, 1972, 4А496)
21. **Roquette P.,** Analytic-theory of elliptic functions over local fields. Göttingen, 1970
22. **Serre J.-P.,** Cours Collège de France, 1961—1962
23. —, Abelian l-adic representations and elliptic curves. New York, Bengamin, 1968, 208 pp (РЖМат, 1970, 6А384 К)
24. **Serre J. P.,** Endomorphismes complètement continus des espaces de Banach p-adiques. Publs math. Inst. hautes études Scient., № 12, 69—85 (РЖМат, 1967, 8А233)
25. —, Groupes discrets. Collège de France, 1968—1969
26. —, Géométrie algébrique et géométrie analytique. Ann. Inst. Fourier, 1955—1956(1956), 6, 1—42 (РЖМат, 1958, 2405)
27. **Shafarevitch I. R.,** Lectures on minimal models and birational transformations on two dimensional schemes. Tata Institute of Fundamental research, Bombay, 1966, 175 S. (РЖМат, 1969, 8А322)
28. **Tate J.,** Rigid analytic spaces. Invent. math., 1971, 12, № 4, 257—289 (РЖМат, 1971, 11А407)