A. N. Andrianov, Singular Hecke–Shimura rings and Hecke operators on Siegel modular forms,
Algebra i Analiz, 1999, Volume 11, Issue 6, 1–68

Алгебра и анализ
Том 11 (1999), вып. 6

СИНГУЛЯРНЫЕ КОЛЬЦА ГЕККЕ–ШИМУРЫ И ОПЕРАТОРЫ ГЕККЕ НА ЗИГЕЛЕВЫХ МОДУЛЯРНЫХ ФОРМАХ

© А. Н. Андрианов

Развита теория сингулярных колец Гекке–Шимуры и операторов Гекке на зигелевых модулярных формах для групп $\Gamma_0^n(q)$. Доказано, в частности, что в случае $n = 2$ пространства новых касп-форм целых весов имеют базисы из общих собственных функций всех регулярных операторов Гекке, операторов Гекке, отвечающих элементам сингулярных неразветвленных колец и всем сингулярным элементам Фробениуса. Включен классический случай одной переменной, рассмотренный ранее Аткиным и Ленером.

Оглавление

Ключевые слова: новые зигелевы модулярные формы, сингулярные кольца Гекке–Шимуры, сингулярные операторы Гекке, старые зигелевы модулярные формы, элементы Фробениуса.

Работа выполнена при частичной поддержке РФФИ, грант 96-01 00663.

Введение

Наиболее впечатляющее приложение модулярных форм к диофантовой теории чисел в последнее десятилетие, доказательство великой теоремы Ферма Вайлсом и Тейлором было бы буквально невозможно без достаточно полной теории p-операторов Гекке на модулярных формах от одной переменной для всех простых чисел p как не делящих ступень рассматриваемых модулярных форм (*регулярные p-операторы*, рассмотренные Гекке [8] и Петерссоном [12]), так и для простых делителей ступени (*сингулярные p-операторы*, изученные Аткиным и Ленером [7], Ли [9] и др.). Без этого было бы нельзя даже определить все p-множители эйлеровых произведений, отвечающих модулярным формам и, стало быть, точно сформулировать гипотезу Шимуры–Таниямы о дзета-функциях эллиптических кривых, лежащую в основе доказательства Вайлса–Тейлора.

Вряд ли можно сомневаться, что связь дзета-функций эллиптических кривых и дзета-функций модулярных форм, известная как гипотеза Шимуры–Таниямы, является только частным случаем неких общих связей глобальных дзета-функций алгебраических многообразий и дзета-функций автоморфных форм от нескольких переменных. Говоря об абелевых многообразиях вместо эллиптических кривых, можно ожидать, что модулярные формы от одной переменной должны быть заменены зигелевыми модулярными формами для конгруэнц-подгрупп модулярной группы Зигеля $\Gamma^n = \mathrm{Sp}_n(\mathbb{Z})$, каковые ожидания подтверждаются численными свидетельствами (см., например, [13]). Одно из главных препятствий в этом направлении — недостаток существенной информации о сингулярных кольцах Гекке–Шимуры и операторах Гекке на зигелевых модулярных формах (некоторые сингулярные операторы Гекке для групп $\Gamma_0^n(q)$ были использованы Шимурой в [16]). В настоящей работе мы начинаем заполнять этот пробел.

Мы развиваем теорию *сингулярных* (т. е. связанных с делителями ступеней) колец Гекке–Шимуры и операторов Гекке на зигелевых модулярных формах для конгруэнц-подгрупп группы Γ^n вида $\Gamma_0^n(q)$ (см. (2.1)). Доказано, в частности, что в случае $n = 2$ пространства новых касп-форм целых весов натягиваются на общие собственные функции всех регулярных операторов Гекке, операторов Гекке, соответствующих элементам сингулярных неразветвленных колец и всем сингулярным элементам Фробениуса.

Содержание. Гл. 1 содержит все необходимые определения и факты о зигелевых модулярных формах, общих кольцах Гекке–Шимуры и операторах Гекке. Гл. 2 посвящена регулярным приводимым кольцам и операторам для $\Gamma_0^n(q)$. Доказательства в гл. 1 и 2, как правило, опущены со ссылкой на наши книги [4] или [5]. Гл. 3 является ключевой. В ней рассматриваются сингулярные кольца Гекке–Шимуры для групп $\Gamma_0^n(q)$. Особенно важен §3.3, где для простых делителей p ступени q неделящих q/p (*неразветвленные простые*) построены и изучены канонические вложения регулярных приводимых p-колец групп $\Gamma_0^n(q/p)$ в (сингулярные) p-кольца группы $\Gamma_0^n(q)$. Эти вложения заменяют параболические вложения регулярных колец. Гл. 4 содержит определения старых и новых касп-форм и рассматривает вопросы их инвариантности относительно различных операторов Гекке и существования собственных форм. Изложение существенно опирается на свойства след-идемпотентов, рассмотренные в §4.1. Заключение содержит замечания о возможном обобщении результатов и их приложениях.

Благодарности. Прежде всего я хочу поблагодарить моих коллег из Института Фурье (Университет Жозефа Фурье, Гренобль, Франция) и Математического института Макса Планка (Бонн, Германия), где бо́льшая часть настоящего исследования была выполнена и доложена и была написана статья, за любезные приглашения, существенные обсуждения и разнообразную помощь. Особенно я хотел бы поблагодарить профессора Ролана Жиллара и профессора Алексея Панчишкина из Института Фурье и профессора Юрия Манина из Института Макса Планка, кто также научил меня технике подготовки amstex-файла английского текста этой статьи. Я благодарен Федору Андрианову, который прочитал файл как специалист и предложил многие улучшения.

Последние, но самые глубокие благодарности моей жене, как дань признательности за ее терпение и моральную поддержку.

Препринт настоящей статьи был опубликован на английском языке в Max-Plnck-Institut für Mathematic, Preprint series 1998 (118).

Обозначения. Мы фиксируем буквы $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$ для обозначения множества положительных целых рациональных чисел, кольца целых рациональных чисел, поля рациональных чисел, поля вещественных чисел и поля комплексных чисел соответственно. Мы полагаем

$$\mathbb{N}_{(q)} = \{n \in \mathbb{N}\,;\, \text{нод}(n,q) = 1\}$$

и

$$\mathbb{N}_q = \{n \in \mathbb{N}\,;\, n \mid q^\infty\},$$

где запись $n \mid q^\infty$ означает, что n делит некоторую степень числа q.

$\mathbb{A}_n^m$ обозначает множество всех матриц размеров $m \times n$ с элементами из множества $\mathbb{A}$. Мы обозначаем через

$$\mathbb{S}_n = \{M \in \mathbb{Z}_n^n\,;\, {}^tM = M\},$$

где ${}^tM$ всегда обозначает транспонированную матрицу, множество всех целочисленных симметрических матриц порядка n и через

$$\mathbb{E}_n = \{M = (m_{ij}) \in \mathbb{S}_n\,;\, m_{ii} \in 2\mathbb{Z}, i = 1, \ldots, n\}$$

— множество всех *четных матриц* порядка n. E_n будет обозначать единичную матрицу порядка n, и

$$J_n = \begin{pmatrix} 0 & -E_n \\ E_n & 0 \end{pmatrix},$$

где $0 = 0_n$ обозначает нулевую матрицу порядка n. Для краткости мы пишем $a(a+1)/2 = \langle a \rangle$.

Глава 1

Основные понятия

В этой главе мы кратко напомним основные определения и свойства симплектических матриц, зигелевых модулярных форм, колец Гекке–Шимуры и операторов Гекке для арифметических дискретных подгрупп вещественной симплектической группы $\mathrm{Sp}_n(\mathbb{R})$. Большинство доказательств можно найти в книгах [4, 5] или восстановить в качестве легких упражнений. Мы делаем исключение только для теоремы 1.9, поскольку затрудняемся указать точную ссылку.

§1.1. Симплектические матрицы, группы и операторы

Матрица $M \in \mathbb{C}_{2n}^{2n}$ называется *симплектической*, если она удовлетворяет соотношению

$$^tM \cdot J_n \cdot M = \mu J_n$$

с ненулевым скаляром $\mu = \mu(M)$, называемым *мультипликатором матрицы* M (см. Обозначения).

Лемма 1.1. *Пусть* $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$, *где* A, B, C, D *— комплексные матрицы размеров* $n \times n$, *и* μ *— ненулевое комплексное число. Тогда следующие условия эквивалентны*:

(1) *Матрица* M *является симплектической с мультипликатором* $\mu(M) = \mu$.
(2) *Матрица* ^tM *является симплектической с мультипликатором* $\mu(^tM) = \mu$.
(3) *Матрица* M *обратима и*

$$\mu M^{-1} = \begin{pmatrix} ^tD & -^tB \\ -^tC & ^tA \end{pmatrix}.$$

(4) $^tA \cdot C = {^tC} \cdot A, {^tB} \cdot D = {^tD} \cdot B, {^tA} \cdot D - {^tC} \cdot B = \mu E_n$.
(5) $A \cdot {^tB} = B \cdot {^tA}, C \cdot {^tD} = D \cdot {^tC}, A \cdot {^tD} - B \cdot {^tC} = \mu E_n$.

В наших арифметических построениях мы будем рассматривать дискретные подгруппы и подполугруппы общей вещественной положительной симплектической группы рода $n = 1, 2, \ldots$, состоящей из всех вещественных симплектических матриц порядка $2n$ с положительными мультипликаторами,

$$G^n = G\,\mathrm{Sp}_n^+(\mathbb{R}) = \{M \in \mathbb{R}_{2n}^{2n};\ {^tM} \cdot J_n \cdot M = \mu(M) J_n, \mu(M) > 0\}.$$

Группа G^n является вещественной группой Ли, действующей как группа аналитических автоморфизмов на $n(n+1)/2$-мерном комплексном многообразии

$$\mathbb{H}_n = \{Z = X + iY \in \mathbb{C}_n^n \, ; {}^tZ = Z, Y > 0\},$$

называемом *верхней полуплоскостью Зигеля рода* n, по правилу

$$G^m \ni M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} : Z \to M\langle Z\rangle = (AZ+B)(CZ+D)^{-1} \quad (Z \in \mathbb{H}_n).$$

Это действие удовлетворяет соотношениям

$$(M \cdot M')\langle Z\rangle = M\langle M'\langle Z\rangle\rangle \quad (M, M' \in G^n, \ Z \in \mathbb{H}_n).$$

Действуя на $\mathbb{H}_n$, группа G^n действует также и на функции $F : \mathbb{H}_n \to \mathbb{C}$ посредством *операторов Петерссона целочисленных весов* k,

$$G^n \ni M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} : F \to F|_k M = \det(CZ+D)^{-k} F(M\langle Z\rangle), \tag{1.1}$$

удовлетворяющих соотношениям

$$F|_k(M \cdot M') = F|_k M|_k M', \quad F|_k rM = r^{-nk} F|_k M \tag{1.2}$$

для любых $F : \mathbb{H}_n \to \mathbb{C}$, M, $M' \in G^n$ и $r \in \mathbb{R} - \{0\}$.

§1.2. Целочисленные матрицы и дискретные подгруппы

Рассмотрим полугруппу

$$\Sigma = \Sigma^n = G^n \cap \mathbb{Z}_{2n}^{2n}$$

целочисленных симплектических матриц порядка $2n$ с положительными мультипликаторами. Обратная матрица M^{-1} для матрицы M, содержащейся в Σ, не обязательно принадлежит Σ, но матрица

$$M^* = \mu(M)M^{-1} = J_n^{-1} \cdot {}^tM \cdot J_n \tag{1.3}$$

всегда содержится в Σ и отображение $M \to M^*$ является антиавтоморфизмом полугруппы Σ, сохраняющим мультипликаторы: $\mu(M^*) = \mu(M)$. Каждая подгруппа полугруппы Σ содержится в максимальной подгруппе

$$\Gamma = \Gamma^n = \mathrm{Sp}_n(\mathbb{Z}) = \{M \in \Sigma^n \, ; \mu(M) = 1\},$$

называемой *модулярной группой Зигеля рода* n.

Для построения матриц $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$, принадлежащих группе Γ, будет полезно описать „вторые строки" (C, D) таких матриц. Пара (C, D) квадратных матриц порядка n называется *симметричной*, если $C \cdot {}^tD = D \cdot {}^tC$; она называется *взаимно-простой*, если матрицы C и D целочисленны и произведения RC, RD на некоторую матрицу порядка n оба являются целочисленными, только если матрица R целочисленна.

Лемма 1.2. *Пусть (C, D) — пара целочисленных матриц порядка n. Тогда следующие условия эквивалентны:*

(1) *Существуют матрицы A, B такие, что $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma$.*

(2) *Пара (C, D) является симметричной и взаимно-простой.*

Модулярная группа $\Gamma = \Gamma^n$, очевидно, дискретна в G^n. Это также верно для любой подгруппы группы G^n, соизмеримой с Γ. Напомним, что две подгруппы $\mathcal{K}$, $\mathcal{K}'$ некоторой группы $\mathcal{G}$ называются *соизмеримыми*, если их пересечение $\mathcal{K} \cap \mathcal{K}'$ имеет конечный индекс в $\mathcal{K}$ и в $\mathcal{K}'$. Отношение соизмеримости является рефлексивным, симметричным и транзитивным, и поэтому множество всех подгрупп группы $\mathcal{G}$ является объединением непересекающихся *классов соизмеримых подгрупп. Главная конгруэнц-подгруппа ступени* q,

$$\Gamma(q) = \Gamma^n(q) = \{M \in \Gamma^n \; ; \; M \equiv E_{2n} \pmod{q}\},$$

и любая из промежуточных подгрупп K,

$$\Gamma(q) \subset K \subset \Gamma,$$

называемых *конгруэнц-подгруппами ступени* q, имеет конечный индекс в Γ и поэтому соизмерима с Γ. Кроме того, если K соизмерима с Γ, это же верно и для каждой из сопряженных подгрупп $M^{-1} \cdot K \cdot M$ с $M \in \Sigma$. Следующая легкая лемма, связывающая разложения двойных классов смежности с разложениями соответствующих групп, часто оказывается полезной в теории колец Гекке-Шимуры и операторов Гекке.

Лемма 1.3. *Пусть G — мультипликативная группа, K и K' — подгруппы группы G и $g \in G$. Тогда имеет место следующее разложение на непересекающиеся левые классы*

$$KgK' = \bigcup_{\gamma_i \in g^{-1}Kg \cap K' \backslash K'} Kg\gamma_i.$$

Из последней леммы следует

Лемма 1.4. *Если K соизмерима с Γ^n и $M \in \Sigma^n$, то двойной класс смежности KMK является объединением конечного числа левых классов смежности по модулю K.*

Аналогичные леммы справедливы также для правых классов смежности.

§1.3. Модулярные формы

Мы будем рассматривать комплекснозначные функции F на верхней полуплоскости $\mathbb{H}_n$. Такая функция называется *K-автоморфной веса k*, где K — подгруппа группы G^n и k — целое рациональное число, если она инвариантна относительно каждого оператора Петерссона $|_k\gamma$ веса k с $\gamma \in K$. Через $\mathcal{A}_k(K)$ мы обозначим $\mathbb{C}$-линейное пространство всех таких функций:

$$\mathcal{A}_k(K) = \{F : \mathbb{H}_n \to \mathbb{C} \; ; \; F|_k\gamma = F \text{ для всех } \gamma \in K\}. \tag{1.4}$$

Если $M \in G^n$, то из (1.4) следует, что условие $F|_k\gamma = F$ эквивалентно условию $(F|_kM)|_kM^{-1}\gamma M = F|_kM$. Откуда следует равенство

$$\mathcal{A}_k(M^{-1}KM) = \mathcal{A}_k(K)|_kM \quad (M \in G^n).$$

Если подгруппа $K \subset G^n$ соизмерима с модулярной группой $\Gamma = \Gamma^n$, то она содержит подгруппу конечного индекса группы Γ. Отсюда следует, что найдется число $r \in \mathbb{N}$, называемое *показателем* K, такое, что каждая из матриц вида

$$T(rB) = \begin{pmatrix} E_n & rB \\ 0 & E_n \end{pmatrix}, \quad \text{где } B \in \mathbb{S}_n,$$

содержится в K. Если $F \in \mathcal{A}_k(K)$, где K — группа показателя r, то, в частности,

$$F|_kT(rB) = F(Z + rB) = F(Z)$$

для каждой целочисленной симметрической матрицы B порядка n и, таким образом, функция $F = F((z_{ij}))$ является периодической периода r по каждой из переменных $z_{ij} = z_{ji}$.

Лемма 1.5. *Пусть $F = F((z_{ij}))$ — функция на $\mathbb{H}_n$ периодическая с периодом r по каждой из переменных z_{ij}. Предположим, что F голоморфна на $\mathbb{H}_n$. Тогда F имеет разложение вида*

$$F = \sum_{A \in r^{-1}\mathbb{E}_n} f(A)e(AZ) \quad (Z \in \mathbb{H}_n), \tag{1.5}$$

с постоянными коэффициентами $f(A)$, где для комплексной квадратной матрицы S мы используем обозначение

$$e(S) = \exp(\pi i \cdot \operatorname{Trace} S). \tag{1.6}$$

Ряд (1.5) сходится абсолютно на $\mathbb{H}_n$ и равномерно на каждом из подмножеств вида

$$\mathbb{H}_n(\varepsilon) = \{Z = X + iY \in \mathbb{H}_n \,;\, Y \geqslant \varepsilon E_n\}$$

с $\varepsilon > 0$.

Ряд (1.5) и его коэффициенты $f(A)$ называются *разложением Фурье и коэффициентами Фурье функции* F соответственно. Функция $F : \mathbb{H}_n \to \mathbb{C}$ называется *модулярной формой* (соответственно *касп-формой) для подгруппы* K группы G^n, соизмеримой с Γ^n, если она удовлетворяет следующим трем условиям:

(1) $F \in \mathcal{A}_k(K)$, т. е. $F|_k\gamma = F$ для всех $\gamma \in K$;

(2) F голоморфна на $\mathbb{H}_n$;

(3) для каждой матрицы $M \in \Sigma^n$ коэффициенты разложения Фурье

$$F|_kM = \sum_{A \in r^{-1}\mathbb{E}_n} f_M(A)e(AZ)$$

функции $F|_kM \in \mathcal{A}_k(M^{-1}KM)$, где r обозначает показатель группы $M^{-1}KM$, удовлетворяют соотношениям

$$f_M(A) = 0, \text{ если } A \text{ не удовлетворяет условию } A \geqslant 0, \text{ (соответственно } A > 0).$$

Если $n \geqslant 2$, то условие (3) определения модулярных форм является следствием условий (1) и (2) *(эффект Кёхера)*. Мы будем обозначать через $\mathfrak{M}_k(K)$ и $\mathfrak{N}_k(K)$ пространство всех модулярных форм и всех касп-форм веса k для группы K соответственно. Каждое пространство модулярных форм для группы K, соизмеримой с Γ, имеет конечную размерность над $\mathbb{C}$.

§1.4. Скалярное произведение Петерссона

Каждое пространство касп-форм может быть снабжено структурой гильбертова пространства при помощи скалярного произведения Петерссона, определение и свойства которого мы сейчас напомним. По определению K-автоморфных функций для подгрупп K группы G^n значения таких функций на $\mathbb{H}_n$ определяются их значениями на множестве представителей из орбит группы K на $\mathbb{H}_n$. Мы будем говорить, что подмножество $D = D(K)$ верхней полуплоскости $\mathbb{H}_n$ является *фундаментальной областью группы* K на $\mathbb{H}_n$, если оно замкнуто в $\mathbb{H}_n$, содержит представителя из каждой K-орбиты на $\mathbb{H}_n$ и не содержит внутренних точек, принадлежащих к той же K-орбите. В частности, вся верхняя полуплоскость является объединением образов фундаментальной области под действием различных преобразований из K:

$$\mathbb{H}_n = \bigcup_{\gamma' \in K'} \gamma'\langle D(K)\rangle,$$

где K' — соответствующая группе K группа преобразований $\mathbb{H}_n$, и образы $\gamma'\langle D(K)\rangle$ попарно не имеют общих внутренних точек. Фундаментальные области не всегда существуют, но если фундаментальная область $D(K)$ существует для некоторой группы K, то фундаментальные области существуют также для каждой группы вида $M^{-1}KM$ с $M \in G^n$ и для каждой подгруппы K_1 конечного индекса группы K, и можно взять

$$D(M^{-1}KM) = M^{-1}\langle D(K)\rangle \tag{1.7}$$

и

$$D(K_1) = \bigcup_{\gamma' \in K_1' \backslash K'} \gamma'\langle D(K)\rangle, \tag{1.8}$$

где K' и K_1' — соответствующие группы преобразований верхней полуплоскости.

Обратимся теперь к инвариантному интегрированию по фундаментальным областям. Напомним прежде всего, что мера на $\mathbb{H}_n$, задаваемая формулой

$$d^*Z = (\det Y)^{-(n+1)} \prod_{1 \le \alpha \le \beta \le n} dx_{\alpha\beta} dy_{\alpha\beta},$$

где $Z = X + iY = (x_{\alpha\beta}) + i(y_{\alpha\beta}) \in \mathbb{H}_n$ и $dx_{\alpha\beta}$, $dy_{\alpha\beta}$ — евклидовы меры на $\mathbb{R}$, является G^n-инвариантной, т. е. удовлетворяет условию

$$d^*M\langle Z\rangle = d^*Z \quad \text{для каждой } M \in G^n, \tag{1.9}$$

как следует рутинной проверкой из формулы

$$Y' = \mu(M)^t(C\overline{Z} + D)^{-1} Y (CZ + D)^{-1}, \tag{1.10}$$

где $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in G^n$, $Z = X + iY \in \mathbb{H}_n$, $M\langle Z\rangle = X' + iY'$ и где черта обозначает комплексное сопряжение. Из (1.9) и (1.10) следует, что каждая дифференциальная форма на $\mathbb{H}_n$ вида

$$w_k(F, F')(Z) = F(Z)\overline{F'(Z)}(\det Y)^k d^*Z \tag{1.11}$$

с произвольными функциями F и F' на $\mathbb{H}_n$ и любым целым числом k удовлетворяет соотношению

$$w_k(F, F')(M\langle Z\rangle) = \mu(M)^{nk} w_k(F|_k M, F'|_k M)(Z)$$

для каждой матрицы M из G^n, где $|_k$ обозначает оператор Петерссона (1.1).

Из инвариантности d^*Z следует, что объем

$$v(D(K)) = \int\limits_{D(K)} d^*Z \tag{1.12}$$

фундаментальной области для подгруппы K группы G^n не зависит от выбора фундаментальной области и может быть назван *объемом* $v(K)$ *группы* K. Более общо, если K — подгруппа группы G^n с фундаментальной областью $D(K)$ и F, F' — две K-автоморфные функции целого веса k, такие что интеграл

$$\int\limits_{D(K)} w_k(F, F')(Z)$$

абсолютно сходится, то интеграл не зависит от выбора фундаментальной области.

Возвращаясь к подгруппам группы G^n, соизмеримым с модулярной группой, напомним сначала следующую лемму, основанную на теории Минковского приведения квадратичных форм.

Лемма 1.6. *Модулярная группа* $\Gamma = \Gamma^n$ *имеет фундаментальную область* $D_n = D(\Gamma^n)$ *на* $\mathbb{H}_n$. *Инвариантный объем* $v(\Gamma^n) = v(D_n)$ *конечен.*

Из леммы и разложений (1.8) следует, что конечен объем каждой подгруппы группы G^n, соизмеримой с Γ^n.

Теорема 1.7. *Пусть* K *— подгруппа группы* $G = G^n$, *соизмеримая с модулярной группой* $\Gamma = \Gamma^n$, k *— целое число и* F, F' *— две модулярные формы веса* k *для группы* K. *Предположим, что по меньшей мере одна из этих форм является касп-формой. Тогда интеграл*

$$(F, F') = \nu(K_1')^{-1} \int\limits_{D(K_1)} w_k(F, F')(Z), \tag{1.13}$$

где K_1 *— подгруппа конечного индекса в* $K \cap \Gamma$, $K_1' = K_1 \cup (-E_n)K_1/(\pm E_n)$ *— соответствующая* K_1 *группа преобразований,* $\nu(K_1') = [\Gamma' : K_1']$ *— ее индекс в* $\Gamma' = \Gamma/(\pm E_n)$, $D(K_1)$ *— фундаментальная область группы* K_1 *на* $\mathbb{H}_n$ *и* w_k *— дифференциальная форма* (1.11) *имеет следующие свойства:*

(1) (F, F') *сходится абсолютно и не зависит от выбора фундаментальной области.*

(2) (F, F') *не зависит ни от выбора группы* K *в ее классе соизмеримых подгрупп группы* Γ *с* $F, F' \in \mathfrak{M}_k(K)$, *ни от выбора группы* K_1.

(3) (F, F') *линеен по* F *и сопряженно линеен по* F'.
(4) $\overline{(F, F')} = (F', F)$.
(5) $(F, F) \geq 0$ *и* $(F, F) = 0$, *только если* $F = 0$.
(6) *Если* M *— матрица из* G *с рациональными коэффициентами, то*

$$(F|_k M, F'|_k M) = \mu(M)^{-nk}(F, F'), \tag{1.14}$$

где $|_k$ *обозначает оператор Петерссона* (1.1), *и функции* $F|_k M$, $F'|_k M$ *рассматриваются как элементы пространства* $\mathfrak{M}_k(M^{-1}KM)$.

Число (F, F') называется *скалярным произведением* (*Петерссона*) *форм* F *и* F'. Первоначально произведение было введено Петерссоном в [12] для модулярных форм от одной переменной и было распространено затем на зигелевы модулярные формы Маассом в [10].

Пространство $\mathfrak{N}_k(K)$ касп-форм веса k для подгруппы K группы G, соизмеримой с Γ, является конечномерным гильбертовым пространством относительно скалярного произведения Петерссона.

§1.5. Кольца Гекке–Шимуры и операторы Гекке

Предположим, что даны мультипликативная группа G, ее подгруппа K и подполугруппа Δ, содержащая K. Мы будем говорить, что пара (K, Δ) является *конечной* (более точно, *лево-конечной*), если для каждого элемента $g \in \Delta$ двойной класс смежности KgK состоит из конечного числа левых классов смежности Kg'. Для такой пары (K, Δ) и коммутативного ассоциативного кольца $\mathbb{A}$ с единицей мы обозначим через

$$\mathcal{W} = \mathrm{Lin}_{\mathbb{A}}(K \setminus \Delta)$$

свободный $\mathbb{A}$-модуль, состоящий из всех конечных формальных линейных комбинаций

$$t = \sum_i a_i(Kg_i)$$

с коэффициентами $a_i \in \mathbb{A}$ символов (Kg_i) с $g_i \in \Delta$, находящихся во взаимнооднозначном соответствии с левыми классами Kg множества Δ по модулю группы K. Для краткости мы будем называть эти символы также *левыми классами полугруппы* Δ *по модулю* K.

Затем обозначим через

$$\mathcal{H} = HS_{\mathbb{A}}(K, \Delta)$$

подмодуль модуля $\mathcal{W}$, состоящий из всех элементов, инвариантных оносительно естественного (правого) действия группы K на $\mathcal{W}$:

$$K \ni \gamma : t \to t\gamma = \sum_i a_i(Kg_i\gamma),$$

т. е.

$$\mathcal{H} = \{t \in \mathcal{W} \,;\, t\gamma = t \text{ для всех } \gamma \in K\}.$$

Умножение элементов модуля $\mathcal{H}$, задаваемое формулой

$$\left(\sum_i a_i(Kg_i)\right) \cdot \left(\sum_j b_j(Kh_j)\right) = \sum_{i,j} a_i b_j(Kg_i h_j),$$

не зависит от выбора представителей $g_i \in Kg_i$ и $h_j \in Kh_j$ и превращает модуль $\mathcal{H}$ в ассоциативную $\mathbb{A}$-алгебру с единицей $(K) = (K \cdot 1_G)$, называемую *кольцом Гекке-Шимуры* (*HS-кольцом*) *пары* (K, Δ) *над* $\mathbb{A}$. Элементы

$$(g) = (g)_K = \sum_{g_i \in K \backslash KgK} (Kg_i), \tag{1.15}$$

взаимно-однозначно соответствующие двойным классам KgK полугруппы Δ относительно K, принадлежат кольцу $\mathcal{H}$ и образуют свободный $\mathbb{A}$-базис этого кольца. Для краткости мы будем называть эти элементы также *двойными классами* Δ *по модулю* K.

Предположим теперь, что полугруппа Δ действует (справа) на (левом) $\mathbb{A}$-модуле V линейными операторами

$$|g : v \to v|g \quad (v \in V,\ g \in \Delta),$$

удовлетворяющими условиям

$$v|g|g' = v|gg' \quad (v \in V,\ g, g' \in \Delta),$$

и обозначим через

$$\mathfrak{M} = \{v \in V\ ;\ v|\gamma = v \text{ для всех } \gamma \in K\}$$

подмодуль K-инвариантных элементов из V. Тогда для каждого $v \in \mathfrak{M}$ и каждого $t = \sum_i a_i(Kg_i)$ из $\mathcal{H} = HS_{\mathbb{A}}(K, \Delta)$ элемент

$$v|t = \sum_i a_i v|g_i$$

не зависит от выбора представителей $g_i \in Kg_i$, снова принадлежит подмодулю $\mathfrak{M}$ и для каждых $v \in \mathfrak{M}$, t, $t' \in \mathcal{H}$ выполняется соотношение

$$v|t|t' = v|tt'.$$

Таким образом, отображение $t \to |t$ является линейным представлением HS-кольца $\mathcal{H}$ на модуле $\mathfrak{M}$. Операторы $|t$ называются *операторами Гекке*.

Операторы Гекке были впервые изучены Гекке в [8] для пространств модулярных форм от одной переменной, хотя идея таких операторов была первоначально использована Морделлом в [11] для доказательства гипотез Рамануджана о мультипликативных свойствах функции $\tau(n)$ и других аналогичных функций. Общие кольца Гекке-Шимуры над $\mathbb{Z}$ были первоначально введены Шимурой в конце 50-х годов в формально отличной, но эквивалентной форме как абстракция колец операторов Гекке.

В ситуации, которая интересует нас в настоящей статье, — действие операторов Гекке на модулярные формы, — роль группы G играет общая вещественная положительная симплектическая группа рода n, $G^n = G\mathrm{Sp}_n^+(\mathbb{R})$, введенная в §1.1; роль полугруппы Δ играет полугруппа Σ^n целочисленных матриц из G^n; и роль группы K играет подгруппа группы G^n, соизмеримая с модулярной группой Γ^n рода n. Тогда, согласно лемме 1.4, пара (K, Σ) является конечной, и мы можем определить соответствующее HS-кольцо над любым коммутативным кольцом $\mathbb{A}$. В этой работе мы берем в качестве $\mathbb{A}$ поле $\mathbb{Q}$ рациональных чисел для всех HS-колец симплектической группы и потому основное кольцо, как правило, не указываем. В частности, HS-кольцо группы K,

$$\mathcal{H}(K) = HS(K, \Sigma), \tag{1.16}$$

— это HS-кольцо пары (K, Σ) над $\mathbb{Q}$. Чтобы определить операторы Гекке, мы рассмотрим действие полугруппы Σ на комплекснозначных функциях F на верхней полуплоскости $\mathbb{H} = \mathbb{H}_n$, задаваемое операторами Петерссона (1.1). Тогда по сказанному выше подпространство (1.4) всех K-инвариантных с весом k функций инвариантно относительно всех операторов Гекке веса k,

$$|_kT : F \to F|_kT = \sum_i a_i F|_k M_i \quad (T = \sum_i a_i(KM_i) \in \mathcal{H}(K), \ \ F \in \mathcal{A}_k(K)),$$

и линейные операторы

$$|_kT : \mathcal{A}_k(K) \to \mathcal{A}_k(K) \quad (T \in \mathcal{H}(K)) \tag{1.17}$$

удовлетворяют соотношениям

$$|_kT|_kT' = |_kTT'.$$

Предложение 1.8. *Подпространства $\mathfrak{M}_k(K)$ и $\mathfrak{N}_k(K)$ модулярных форм и каспформ, содержащихся в $\mathcal{A}_k(K)$, инвариантны относительно всех операторов Гекке* (1.17).

Все кольцо $\mathcal{H}(K)$, вообще говоря, некоммутативно. Оказывается, однако, что различные вопросы теории операторов Гекке часто могут быть сведены к рассмотрению подходящих коммутативных подколец. Существенную роль в таком сведении играет *отображение звездочка*

$$T \to T^* \quad (T \in \mathcal{H}(K)), \tag{1.18}$$

кольца $\mathcal{H}(K)$, определяемое на элементах вида (1.15) формулой

$$(M)_K^* = (M^*)_K \quad (M \in \Sigma),$$

где $M \to M^*$ обозначает антиавтоморфизм (1.3), и затем распространяемое по линейности на все кольцо $\mathcal{H}(K)$.

Теорема 1.9. (1) *Отображение звездочка является линейным антиавтоморфизмом второго порядка кольца $\mathcal{H}(K)$; в частности, оно удовлетворяет соотношениям*

$$(T^*)^* = T, \ (T \cdot T_1)^* = T_1^* \cdot T^* \quad (T, T_1 \in \mathcal{H}(K)).$$

(2) *Операторы Гекке $|_k T$ и $|_k T^*$ сопряжены относительно скалярного произведения Петерссона* (1.13). *Точнее, если F и F' — две модулярные формы веса k относительно K и по меньшей мере одна из форм является касп-формой, то выполняются соотношения*

$$(F|_k T, F') = (F, F'|_k T^*) \quad (T \in \mathcal{H}(K)).$$

Доказательство. (1) Линейное отображение

$$\mathcal{H}(K) \to HS(K, \Sigma^{-1}) = \mathcal{H}',$$

задаваемое на двойных классах формулой

$$(M)_K \to (M^{-1})_K \quad (M \in \Sigma),$$

является антиизоморфизмом $\mathbb{Q}$-алгебр (см., например, [4], предложение 3.1.7). С другой стороны, линейное отображение, задаваемое на двойных классах формулами

$$(M^{-1})_K \to (\mu(M)M^{-1})_K \quad (M \in \Sigma),$$

очевидно, является изоморфизмом алгебры $\mathcal{H}'$ на $\mathcal{H}(K)$. Это доказывает первое утверждение, поскольку отображение звездочка является композицией указанных отображений.

(2) Достаточно рассмотреть случай $T = (M)_K$ с $M \in \Sigma$. По лемме 1.3 число $\#(K \setminus KMK)$ левых классов по модулю K, содержащихся в двойном классе KMK, равно индексу $\nu = [K : K \cap M^{-1}KM]$. Число правых классов по модулю K в KMK, очевидно, равно числу левых классов в $KM^{-1}K$ и поэтому равно индексу $\nu' = [K : K \cap MKM^{-1}]$. Пусть D — некоторая фундаментальная область для группы $K \cap M^{-1}KM$ на $\mathbb{H}_n$. Поскольку

$$K \cap MKM^{-1} = M(K \cap M^{-1}KM)M^{-1},$$

то из (1.7) следует, что в качестве фундаментальной области для группы $K \cap MKM^{-1}$ можно взять множество $M\langle D \rangle$. Тогда на основании разложений (1.8) мы получаем следующие соотношения для инвариантных объемов (1.12):

$$v(D) = \nu v(D(K)), \quad v(M\langle D \rangle) = \nu' v(D(K)),$$

где $D(K)$ — некоторая фундаментальная область для группы K. Согласно (1.9), мы заключаем, что $v(D) = v(M\langle D \rangle)$, откуда $\nu = \nu'$. Отсюда следует, что количества левых и правых классов смежности по модулю K в двойном классе KMK равны

$$\#(K \setminus KMK) = \#(KMK/K) \quad (M \in \Sigma). \tag{1.19}$$

Поскольку каждый из этих левых классов, очевидно, пересекается с каждым из правых классов, то на основании (1.19) мы заключаем, что существует множество $M_1, \ldots, M_\nu$ общих представителей из левых и правых классов смежности двойного класса KMK по модулю K. Тогда множество $M_1^*, \ldots, M_\nu^*$ является системой представителей из левых и правых классов смежности двойного класса KM^*K по модулю K. Наконец, по (1.14) и (1.2) мы получаем

$$(F|_k(M), F') = \left(\sum_i F|_k M_i, F'\right) = \mu(M)^{-nk}\left(F, \sum_i F'|_k M_i^{-1}\right)$$
$$= \left(F, \sum_i F'|_k M_i^*\right) = (F, F'|_k(M)^*). \quad \bullet$$

В настоящей работе мы практически не касаемся, кроме §2.4, важного вопроса о действии операторов Гекке на коэффициенты Фурье модулярных форм, оставляя это до будущих работ о дзета-функциях. Для таких приложений оказывается удобным нормировать операторы Гекке на модулярных формах для групп K, соизмеримых с Γ^n, с помощью подходящих постоянных множителей. Для элемента $T = \sum_i a_i(KM_i) \in \mathcal{H}(K)$ мы определим *нормированный оператор Гекке* $\|_k T$ *на* $\mathfrak{M}_k(K)$, полагая

$$F\|_k T = \sum_i a_i \mu(M_i)^{nk-\langle n\rangle} F|_k M_i \quad (F \in \mathfrak{M}_k(K)). \tag{1.20}$$

Поскольку, очевидно,

$$F\|_k(M)_K = \mu(M)^{nk-\langle n\rangle} F|_k(M)_K \quad (F \in \mathfrak{M}_k(K),\ M \in \Sigma^n),$$

то нормированные операторы отображают пространства $\mathfrak{M}_k(K)$ и $\mathfrak{N}_k(K)$ в себя, отображение $T \to \|_k T$ является линейным представлением кольца $\mathcal{H}(K)$ и удовлетворяет соотношениям

$$(F\|_k T, F') = (F, F'\|_k T^*), \tag{1.21}$$

если $T \in \mathcal{H}(K)$ и $F, F' \in \mathfrak{N}_k(K)$. Отметим, что операторы Гекке, рассматривавшиеся в книгах [4] и [5], являются нормированными операторами.

§1.6. Приводимые, регулярные и сингулярные подкольца

Мы завершим эту главу несколькими простыми, но полезными определениями, относящимися к кольцам Гекке–Шимуры дискретных симплектических групп K, соизмеримых с модулярной группой Γ^n.

Стандартные приложения операторов Гекке обычно основаны на соотношениях между собственными числами операторов на пространствах модулярных форм и коэффициентами Фурье собственных функций. Для этого необходимо сначала вычислить коэффициенты Фурье образов под действием операторов Гекке в терминах коэффициентов Фурье оригиналов. Поскольку оператор Гекке $|_k T$ с $T \in \mathcal{H}(K)$ является линейной комбинацией операторов Петерссона

$|_k M$ с $M \in \Sigma$, то задача сводится к аналогичной задаче для операторов Петерссона. Если $F \in \mathfrak{M}_k(K)$, то единственная известная общая ситуация, когда коэффициенты Фурье функции $F|_k M$ могут быть прямо вычислены в терминах коэффициентов Фурье функции F, возникает, если оператор $|_k M$ сводится к *„треугольному оператору"* $|_k M'$ с матрицей M', принадлежащей полугруппе

$$\Sigma_0 = \Sigma_0^n = \left\{ \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} \in \Sigma \right\} \tag{1.22}$$

„треугольных" матриц из Σ. Это происходит, если, скажем, $M \in K\Sigma_0$, так как тогда

$$F|_k M = F|_k \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} = (\det D)^{-k} F(AZD^{-1} + BD^{-1})$$

и коэффициенты Фурье последней функции легко могут быть выражены через коэффициенты Фурье функции F. Эти соображения оправдывают следующее определение. Ненулевой элемент

$$T = \sum_i a_i(KM_i) \in \mathcal{H}(K), \tag{1.23}$$

где все коэффициенты отличны от нуля и все левые классы попарно различны (*кратчайшая запись*), называется ***приводимым***, если каждый из левых классов KM_i содержит „треугольного" представителя, т. е.

$$KM_i \cap \Sigma_0 \neq \varnothing.$$

Если T приводим, то можно считать, что все представители M_i содержатся в Σ_0. В этом случае мы будем говорить, что T записан ***в треугольной форме*** или является *треугольным*. Так как произведение двух треугольных элементов является, очевидно, треугольным, то множество

$$R(\mathcal{D}) = \{T \in \mathcal{D}\,;\, T \text{ — приводимый}\}$$

всех приводимых элементов, содержащихся в некотором подкольце $\mathcal{D}$ кольца $\mathcal{H}(K)$, является подкольцом, которое мы будем называть ***приводимым подкольцом кольца $\mathcal{D}$***.

Из определений следует, что элемент $(M)_K$ из $\mathcal{H}(K)$ вида (1.15) является приводимым в том и только в том случае, если $KMK \subset K\Sigma_0$. В этом случае мы будем говорить, что элемент M из Σ является ***K-приводимым***. Множество

$$R(K) = \{M \in \Sigma\,;\, KMK \subset K\Sigma_0\}$$

всех K-приводимых элементов из Σ является, очевидно, подполугруппой полугруппы Σ, называемой ***K-приводимой полугруппой***. Если

$$\mathcal{D} = HS(K, \Sigma') \subset \mathcal{H}(K)$$

является HS-кольцом полугруппы Σ', содержащейся в Σ, то приводимое подкольцо $R(\mathcal{D})$ кольца $\mathcal{D}$ является ни чем иным, как HS-кольцом пары $(K, \Sigma' \cap R(K))$.

В приложениях обычно бывает возможно ограничиться рассмотрением подходящих приводимых подколец или их простых расширений. В следующей главе мы увидим, как это выглядит в случае групп $K = \Gamma_0^n(q)$.

Свойства левых и двойных классов матриц M из $\Sigma = \Sigma^n$ относительно конгруэнц-подгрупп ступени $q > 1$ в большой мере зависят от общих делителей их мультипликаторов $\mu(M)$ и ступени. Два крайних случая: *регулярный случай*, когда

$$\text{нод}(\mu(M), q) = 1, \tag{1.24}$$

и *сингулярный случай*, когда

$$\mu(M) \mid q^\infty, \tag{1.25}$$

т. е. каждый из простых делителей числа $\mu(M)$ делит q, особенно важны, поскольку общий случай обычно сводим к этим частным случаям. Такое сведение основано на следующем следствии теории элементарных делителей для симплектических групп.

Лемма 1.10. *Пусть $M \in \Sigma = \Sigma^n$. Предположим, что мультипликатор $\mu(M)$ является произведением двух взаимно-простых множителей*: $\mu(M) = ab$, нод$(a, b) = 1$. *Тогда существуют матрицы M_1, $M_2 \in \Sigma$ такие, что $M = M_1M_2$ и $\mu(M_1) = a$, $\mu(M_2) = b$. Если $M = M_1'M_2'$ — другое такое разложение, то $M_1' = M_1\gamma$ и $M_2' = \gamma^{-1}M_2$ с $\gamma \in \Gamma^n$.*

Мы будем говорить, что матрица M из $\Sigma = \Sigma^n$ является *q-регулярной* (соответственно *q-сингулярной*), если она удовлетворяет условию (1.24) (соответственно (1.25)), и обозначать через

$$\Sigma_{(q)} = \Sigma_{(q)}^n \quad \text{и} \quad \Sigma_q = \Sigma_q^n \tag{1.26}$$

множества всех q-регулярных и q-сингулярных матриц из Σ соответственно. Элемент HS-кольца $\mathcal{H}(K)$ называется *q-регулярным* (соответственно *q-сингулярным*), если каждый из левых классов, входящих в кратчайшую запись (1.23) этого элемента, состоит из q-регулярных (соответственно q-сингулярных) матриц. Подкольца

$$\mathcal{H}_{(q)}(K) = HS(K, \Sigma_{(q)}) \quad \text{и} \quad \mathcal{H}_q(K) = HS(K, \Sigma_q) \tag{1.27}$$

всех q-регулярных и q-сингулярных элементов из $\mathcal{H}(K)$ называются *q-регулярным* и *q-сингулярным HS-кольцом группы K* соответственно. Подкольцо $\mathcal{D}$ кольца $\mathcal{H}(K)$ называется *q-регулярным* (соответственно q-сингулярным), если оно содержится в $\mathcal{H}_{(q)}(K)$ (соответственно в $\mathcal{H}_q(K)$). Если q фиксировано, указание на q будет, как правило, опускаться.

Глава 2

Регулярные приводимые кольца и операторы для $\Gamma_0^n(q)$

В этой главе мы напомним регулярную теорию для групп

$$K = \Gamma_0^n(q) = \left\{ \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma^n; C \equiv 0 \pmod q \right\} \tag{2.1}$$

с n, $q \in \mathbb{N}$. Числа n и q остаются фиксированными на протяжении всей главы и потому часто не указываются. По поводу деталей и опущенных доказательств см. [4] или [5]. Читатель может также найти там регулярную теорию для более общих конгруэнц-подгрупп.

§2.1. Глобальные кольца

Лемма 2.1. *Множество* $R^*(K)$ *всех* q*-регулярных и* K*-приводимых элементов из* Σ^n *для группы* (2.1) *имеет вид*

$$R^*(K) = \left\{ \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Sigma^n_{(q)}; C \equiv 0 \pmod{q} \right\}; \tag{2.2}$$

в частности, $R^*(\Gamma^n) = \Sigma^n$.

Доказательство. По поводу включения $\supset$ см., например, [4], лемма 3.3.4. Обратное включение следует из определения K-приводимых элементов. •

Из леммы следует, что (максимальным) регулярным приводимым подкольцом кольца $\mathcal{H}(K)$ является кольцо

$$\mathcal{H}_{\mathrm{rr}} = \mathcal{H}^n_{\mathrm{rr}}(q) = HS(K, R^*(K)). \tag{2.3}$$

Согласно общим свойствам HS-колец, элементы $(M)_K$ вида (1.15), ассоциированные с различными двойными классами множества $R^*(K)$ по модулю K, образуют свободный базис кольца $\mathcal{H}_{\mathrm{rr}}$ над $\mathbb{Q}$. Для описания этого базиса мы напомним следующую лемму об элементарных делителях для симплектической группы над $\mathbb{Z}$.

Лемма 2.2. *Каждый из двойных классов* KMK *с* $M \in R^*(K)$ *для группы* (2.1) *содержит представителя вида*

$$\mathrm{sd}(M) = \mathrm{diag}(d_1, \ldots, d_n; e_1, \ldots, e_n), \tag{2.4}$$

где числа d_i, $e_j \in \mathbb{N}$ *удовлетворяют условиям* $d_i | d_{i+1}, d_n | e_n, e_{i+1} | e_i, d_i e_i = \mu(M)$. *Если* M, $M' \in R^*(K)$ *и мультипликаторы* $\mu(M)$ *и* $\mu(M')$ *взаимно-просты, то*

$$\mathrm{sd}(MM') = \mathrm{sd}(M)\,\mathrm{sd}(M'). \tag{2.5}$$

Диагональная матрица $\mathrm{sd}(M)$ называется ***матрицей симплектических делителей матрицы*** M, а положительные целые рациональные числа $d_1 = d_1(M), \ldots, d_n = d_n(M)$, $e_1 = e_1(M), \ldots, e_n = e_n(M)$ называются ***симплектическими делителями матрицы*** M.

Теорема 2.3. *Отображение звездочка* (1.18) *тождественно на двойных классах* $(M)_K$, *содержащихся в регулярном приводимом кольце* $\mathcal{H}_{\mathrm{rr}}$ *группы* (2.1):

$$(M)_K^* = (\mu(M)M^{-1})_K = (M)_K \quad (M \in R^*(K)); \tag{2.6}$$

в частности, кольцо $\mathcal{H}_{\mathrm{rr}}$ *коммутативно.*

Проблема нахождения точных правил умножения для конкретных элементов кольца $\mathcal{H}_{\mathrm{rr}}$ может оказаться довольно сложной, кроме некоторых специальных случаев, которые, в частности, позволяют провести важную редукцию этой проблемы.

Отметим прежде всего, что для любых $M \in \Sigma$ и $r \in \mathbb{N}$ имеют место правила

$$[r](M)_K = (M)_K[r] = (rM)_K, \tag{2.7}$$

где

$$[r] = [r]_K = (rE_{2n})_K = (K(rE_{2n})); \tag{2.8}$$

в частности, элемент [1] является единичным элементом кольца $\mathcal{H}(K)$. Затем имеет место следующее

Предложение 2.4. *Предположим, что отношения делителей* $e_1(M)/d_1(M)$ *и* $e_1(M')/d_1(M')$ *двух матриц* M, $M' \in R^*(K)$ *взаимно-просты. Тогда имеет место следующее соотношение*:

$$(M)_K(M')_K = (MM')_K. \tag{2.9}$$

Если диагональная матрица $\mathrm{diag}(d_1, \dots, d_n; e_1, \dots e_n)$ является матрицей симплектических делителей некоторой матрицы $M \in R^*(K)$, то мы пишем

$$T(d_1, \dots d_n; e_1, \dots, e_n) = (\mathrm{sd}(M))_K = (M)_K, \tag{2.10}$$

и для числа $a \in \mathbb{N}$ взаимно-простого с q мы обозначаем через $T(a) = T_K(a)$ сумму всех различных двойных классов $(M)_K$ с $M \in R^*(K)$ и $\mu(M) = a$:

$$T(a) = \sum_{\substack{KMK \subset R^*(K), \\ \mu(M)=a}} (M)_K. \tag{2.11}$$

Тогда на основании (2.5), (2.7) и (2.9) мы получаем соотношения

$$T(d_1, \dots, e_n)T(d'_1, \dots, e'_n) = T(d_1d'_1, \dots, e_ne'_n) \tag{2.12}$$

при условии, что числа e_1/d_1 и e'_1/d'_1 взаимно-просты, и соотношения

$$T(a)T(b) = T(ab), \tag{2.13}$$

если числа a, b, q попарно взаимно-просты.

Для простого числа p не делящего q мы определим *матрицу симплектических p-делителей матрицы* M, полагая

$$\operatorname{sd}_p(M) = \operatorname{diag}(p^{\nu_p(d_1)}, \ldots, p^{\nu_p(e_n)}), \tag{2.14}$$

где $\nu_p(r)$ обозначает p-порядок числа r. Матрица (2.14) является, очевидно, матрицей симплектических делителей некоторой матрицы $M_p \in R^*(K)$ (например, $M_p = \operatorname{sd}_p(M)$):

$$\operatorname{sd}_p(M) = \operatorname{sd}(M_p) \quad (M, M_p \in R^*(K), \ \text{нод}(p, q) = 1). \tag{2.15}$$

Из соотношений (2.9) следует разложение

$$(M)_K = \prod_p (M_p)_K, \tag{2.16}$$

где p пробегает все простые делители мультипликатора $\mu(M)$.

Все p-компоненты $(M_p)_K$ двойных классов $(M)_K \in \mathcal{H}_{\mathrm{rr}}$ линейно порождают, очевидно, подкольцо $\mathcal{H}_p$, (*приводимое*) *p-кольцо*, которое само можно интерпретировать как HS-кольцо пары

$$(K, R_p(K) = \{M \in R(K) \ ; \mu \mid p^\infty\}) : \mathcal{H}_p = \mathcal{H}_p^n(q) = HS(K, R_p(K)). \tag{2.17}$$

Из разложений (2.16) вытекает следующая теорема.

Теорема 2.5. *Кольцо $\mathcal{H}_{\mathrm{rr}}$ порождается p-кольцами $\mathcal{H}_p$ для всех простых чисел p, которые не делят q.*

Разложение элементов из $\mathcal{H}_{\mathrm{rr}}$ на p-множители можно естественно переформулировать в терминах эйлеровых разложений формальных симплектических дзета-функций. Например, из (2.13) следуют разложения

$$T\Big(\prod_i p_i^{\nu_i}\Big) = \prod_i T(p_i^{\nu_i}),$$

если p_i пробегает конечное множество различных простых чисел, не делящих q, откуда следует (формальное) эйлерово разложение формального ряда Дирихле над $\mathcal{H}_{\mathrm{rr}}$ с коэффициентами $T(a)$ для a взаимно-простых с q:

$$\sum_{\substack{a \in \mathbb{N},\\ \text{нод}(a,q)=1}} \frac{T(a)}{a^s} = \prod_{\substack{p \ \text{простые}\\ p \nmid q}} \Big(\sum_{\delta=0}^{\infty} T(p^\delta) \cdot p^{-\delta s}\Big). \tag{2.18}$$

В следующем параграфе мы увидим, что каждый из формальных степенных рядов

$$Z_p(v) = Z_p^n(v) = \sum_{\delta=0}^{\infty} T(p^\delta) v^\delta \tag{2.19}$$

формально равен рациональной дроби над кольцом $\mathcal{H}_p$.

§2.2. Локальные кольца

Теорема 2.6. *Пусть p — простое число, не делящее q. Тогда имеют место следующие утверждения:*

(1) *если $T = \Sigma_i a_i(KM_i)$ — некоторый элемент из $\mathcal{H}_p^n(q)$ с треугольными представителями M_i, то отображение $T \to i(T) = \Sigma_i a_i(\Gamma^n M_i)$ является изоморфизмом кольца $\mathcal{H}_p^n(q)$ на $\mathcal{H}_p^n(1)$;*

(2) *кольцо $\mathcal{H}_p^n(q)$ над $\mathbb{Q}$ порождается $n+1$ элементами вида*

$$\begin{cases} T^n(p) = T(\underbrace{1,\ldots,1}_{n};\underbrace{p,\ldots,p}_{n}), \\ T_i^n(p^2) = T(\underbrace{1,\ldots,1}_{n-i},\underbrace{p,\ldots,p}_{i};\underbrace{p^2,\ldots,p^2}_{n-i},\underbrace{p,\ldots,p}_{i}) \quad (i=1,\ldots,n); \end{cases} \tag{2.20}$$

(3) *элементы (2.20) алгебраически независимы над $\mathbb{Q}$.*

Проблема выражения элементов кольца $\mathcal{H}_p = \mathcal{H}_p^n(q)$ через образующие (2.20) не является легкой. Однако она может быть значительно упрощена, если воспользоваться другой реализацией кольца, задаваемой сферическими полиномами.

Поскольку кольцо $\mathcal{H}_p$ приводимо, то каждый левый класс KM с $K = \Gamma_0^n(q)$ и $M \in R_p(K)$ содержит треугольный представитель

$$\begin{pmatrix} A & B \\ 0 & D \end{pmatrix}, \quad \text{где } {}^tAD = p^\delta E_n,\ p^\delta = \mu(M). \tag{2.21}$$

Так как группа K содержит подгруппу

$$V^n = \left\{ v(U) = \begin{pmatrix} {}^tU^{-1} & 0 \\ 0 & U \end{pmatrix}; U \in \mathrm{GL}_n(\mathbb{Z}) \right\}, \tag{2.22}$$

то матрицу D в (2.21) можно заменить любой матрицей UD с $U \in \mathrm{GL}_n(\mathbb{Z})$, и потому можно предполагать, что D является верхней треугольной матрицей вида

$$D = (d_{ij}), \text{ где } d_{ij} = 0, \text{ если } i > j, \text{ и } d_{ii} = p^{d_i}, \quad (i,j = 1,\ldots,n). \tag{2.23}$$

Мы положим тогда

$$\omega(KM) = x_0^\delta \prod_{i=1}^n (x_i p^{-i})^{d_i},$$

где $x_0, x_1, \ldots, x_n$ алгебраически независимы над $\mathbb{Q}$. Продолжая отображение ω по линейности на все кольцо $\mathcal{H}_p$, мы получаем линейное отображение

$$\omega = \omega_p : \mathcal{H}_p \to \mathbb{Q}[x_0,\ldots,x_n] \tag{2.24}$$

этого кольца в кольцо многочленов от $n+1$ независимых переменных над $\mathbb{Q}$, называемое *сферическим отображением*. Многочлены $\omega(T)$ с $T \in \mathcal{H}_p$ называются *сферическими многочленами*.

Теорема 2.7. *Сферическое отображение* ω_p *является изоморфизмом кольца* $\mathcal{H}_p = \mathcal{H}_p^n(q)$ *с подкольцом* $\mathbb{Q}^W[x_0,\dots,x_n]$ *кольца многочленов* $\mathbb{Q}[x_0,\dots,x_n]$, *состоящим из всех многочленов, инвариантных относительно группы* $W = W_n$ *всех* $\mathbb{Q}$*-автоморфизмов поля рациональных функций* $\mathbb{Q}(x_0,\dots,x_n)$, *порожденной всеми перестановками переменных* $x_1,\dots,x_n$ *и автоморфизмами* $\tau_1,\dots,\tau_n$, *удовлетворяющими условиям*

$$\tau_i(x_0) = x_0x_i, \quad \tau_i(x_i) = x_i^{-1} \quad \tau_i(x_j) = x_j, \quad (j \neq 0, i).$$

Кольцо $\mathbb{Q}^W[x_0,\dots,x_n]$ *над* $\mathbb{Q}$ *порождается* $n+1$ *многочленами*

$$t = t^n(x_0,\dots,x_n) = x_0\prod_{i=1}^{n}(1+x_i),$$

$$\rho_a = \rho_a^n(x_0,\dots,x_n) = x_0^2x_1\dots x_n r_a^n(x_1,\dots,x_n) \quad (a = 0,1,\dots,n-1),$$

где

$$\sum_{a=0}^{2n}(-1)^a r_a^n(x_1,\dots,x_n)v^a = \prod_{i=1}^{n}(1-x_iv)(1-x_i^{-1}v).$$

С помощью сферического отображения можно доказать следующие формулы для формальных степенных рядов (2.19):

$$Z_p^1(v) = Q_p^1(v)^{-1},$$

где

$$Q_p^1(v) = [1] - T^1(p)v + p[p]v^2; \tag{2.25}$$

также

$$Z_p^2(v) = Q_p^2(v)^{-1}([1] - p^2[p]v^2),$$

где

$$Q_p^2(v) = [1] - T^2(p)v + q_2(p)v^2 - p^3[p]T^2(p)v^3 + p^6[p^2]v^4 \tag{2.26}$$

с

$$q_2(p) = pT(1,p,p^2,p) + p(p^2+1)[p];$$

и для общего n

$$Z_p^n(v) = Q_p^n(v)^{-1}N_p^n(v),$$

где

$$Q_p^n(v) = \sum_{i=0}^{m}(-1)^i q_i^n(p)v^i \quad (m = 2^n), \tag{2.27}$$

является многочленом степени $m = 2^n$ над кольцом $\mathcal{H}_p^n(q)$, удовлетворяющим соотношению

$$\omega(Q_p^n)(v) = \sum_{i=0}^{m}(-1)^i\omega(q_i^n(p))v^i$$

$$= (1-x_0v)\prod_{r=1}^{n}\prod_{1\le i_1<\dots<i_r\le n}(1-x_0x_{i_1}\dots x_{i_r}v),$$

где $\omega = \omega_p$ обозначает сферическое отображение (2.24) и где $N_p^n(v)$ многочлен над кольцом $\mathcal{H}_p^n(q)$ степени не больше, чем $2^n - 2$. Коэффициенты $q_i^n(p)$ удовлетворяют соотношениям

$$q_{m-i}^n(p) = (p^{\langle n \rangle}[p])^{(m/2)-i} q_i^n(p), \quad (0 \le i \le m = 2^n),$$
$$q_0^n(p) = [1] \quad \text{и} \quad q_m^n(p) = (p^{\langle n \rangle}[p])^{m/2}.$$

Формула (2.25) восходит к Гекке и была формально доказана вместе с формулой для $Z_p^2(v)$ в [14] и [15]. Общий случай был рассмотрен в работах [1] и [2].

§2.3. Параболические вложения

Часто оказывается полезным расщеплять элементы симплектических HS-колец на подходящие элементарные компоненты. Однако, вообще говоря, эти компоненты не принадлежат первоначальному кольцу. Согласно нашему подходу, они содержатся в HS-кольце „треугольной“ подгруппы

$$\Gamma_0 = \Gamma_0^n = \left\{ \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} \in \Gamma^n \right\}$$

модулярной группы $\Gamma = \Gamma^n$.

Легко видеть, что пара (Γ_0, Σ_0), где Σ_0 определено равенством (1.22), является конечной, и поэтому можно ввести соответствующее кольцо Гекке–Шимуры над $\mathbb{Q}$

$$\mathcal{L} = \mathcal{L}^n = HS(\Gamma_0^n, \Sigma_0^n) \tag{2.28}$$

вместе с его q-регулярным и q-сингулярным подкольцами

$$\mathcal{L}_{(q)} = \mathcal{L}_{(q)}^n = HS(\Gamma_0^n, \Sigma_{0,(q)}^n), \quad \mathcal{L}_q = \mathcal{L}_q^n = HS(\Gamma_0^n, \Sigma_{0,q}^n) \tag{2.29}$$

для $q \in \mathbb{N}$, где

$$\Sigma_{0,(q)} = \Sigma_{0,(q)}^n = \Sigma_0^n \cap \Sigma_{(q)}^n, \quad \Sigma_{0,q} = \Sigma_{0,q}^n = \Sigma_0^n \cap \Sigma_q^n$$

(см. (1.22) и (1.26)).

Пусть $\mathcal{D}$ — приводимое подкольцо кольца $\mathcal{H}(K)$ для группы $K = \Gamma_0^n(q)$ и пусть $T = \Sigma_i a_i(KM_i)$ — некоторый элемент из $\mathcal{D}$, записанный в треугольной форме. Так как $K \cap \Sigma_0 = \Gamma_0$, то отображение

$$j : T \to j(T) = \widehat{T} = \sum_i a_i(\Gamma_0 M_i) \tag{2.30}$$

не зависит от выбора треугольных представителей $M_i \in KM_i$, образ $\widehat{T}$ принадлежит кольцу $\mathcal{L}$, и $\widehat{T} = 0$, только если $T = 0$. Из определения умножения в HS-кольцах следует, что отображение $T \to \widehat{T}$ является линейным гомоморфизмом колец. Таким образом, мы получаем гомоморфное включение

$$j : \mathcal{D} \hookrightarrow \widehat{\mathcal{D}} \subset \mathcal{L} \tag{2.31}$$

кольца $\mathcal{D}$ в $\mathcal{L}$, которое мы будем называть *параболическим вложением*.

Обратимся теперь к мультипликативным свойствам кольца $\mathcal{L}$. В отличие от приводимых колец, рассмотренных ранее, кольцо $\mathcal{L}$ некоммутативно и содержит делители нуля. Однако некоторые важные свойства сохраняются, и фактически нам понадобятся только определенные подкольца и подмодули кольца $\mathcal{L}$ с хорошими свойствами.

Отметим прежде всего, что *отображение звездочки*

$$X \to X^* \quad (X \in \mathcal{L}), \tag{2.32}$$

кольца $\mathcal{L}$, которое определяется на двойных классах формулой

$$(M)^*_{\Gamma_0} = (\mu(M)M^{-1})_{\Gamma_0} \tag{2.33}$$

и затем распространяется на все кольцо $\mathcal{L}$ по линейности, снова является линейным антиавтоморфизмом второго порядка кольца $\mathcal{L}$. То же, очевидно, справедливо и для подколец $\mathcal{L}_{(q)}$ и $\mathcal{L}_q$. Образы двойных классов $(M)_K \in \mathcal{H}^n_{\mathfrak{r}\mathfrak{r}}(q)$ относительно параболического вложения (2.31) инвариантны относительно отображения звездочка:

$$j((M)_K)^* = j((M)_K) \quad (M \in R^*(K)). \tag{2.34}$$

Отметим, что образ $j((M)_K)$ не обязательно является двойным классом по модулю Γ_0, но суммой таких классов.

Далее, по аналогии с (2.7) мы имеем соотношения

$$\widehat{[r]}(M)_{\Gamma_0} = (M)_{\Gamma_0}\widehat{[r]} = (rM)_{\Gamma_0} \quad (r \in \mathbb{N},\ M \in \Sigma_0), \tag{2.35}$$

где

$$\widehat{[r]} = [r]_{\Gamma_0} = (\Gamma_0(rE_{2n})); \tag{2.36}$$

в частности, элемент $\widehat{[1]}$ является единичным элементом кольца $\mathcal{L}$.

Оказывается, что кольцо $\mathcal{L}$ содержит не только HS-кольца симплектической группы, но также подкольца, естественно изоморфные определенным подкольцам HS-колец общей линейной группы. Это обстоятельство позволяет сводить некоторые вопросы теории колец Гекке-Шимуры и операторов Гекке для симплектической группы к аналогичным вопросам для общей линейной группы.

Рассмотрим элементы из $\mathcal{L} = \mathcal{L}^n$, определяемые формулой

$$\widehat{\Pi}(a) = \widehat{\Pi}^n(a) = \left(\begin{pmatrix} E_n & 0 \\ 0 & aE_n \end{pmatrix}\right)_{\Gamma_0}, \tag{2.37}$$

с $a \in \mathbb{N}$. Эти элементы имеют следующие разложения на левые классы по модулю Γ_0^n:

$$\widehat{\Pi}(a) = \sum_{B \in \mathbb{S}/a\mathbb{S}} \left(\Gamma_0\begin{pmatrix} E & B \\ 0 & aE \end{pmatrix}\right), \tag{2.38}$$

где $E = E_n$ и $\mathbb{S} = \mathbb{S}_n$ (см. Обозначения). Отсюда следуют соотношения

$$\widehat{\Pi}(a)\widehat{\Pi}(b) = \widehat{\Pi}(ab) \quad (a, b \in \mathbb{N}). \tag{2.39}$$

Элементы $\widehat{\Pi}(a)$ будут называться *элементами Фробениуса кольца* $\mathcal{L}$.

Рассмотрим теперь *централизаторы элементов Фробениуса в кольцах* $\mathcal{L}$, $\mathcal{L}_{(q)}$ и $\mathcal{L}_q$:

$$\begin{aligned} \widehat{C}^n &= \{X \in \mathcal{L} ; \widehat{\Pi}(a)X = X\widehat{\Pi}(a), a \in \mathbb{N}\}, \\ \widehat{C}^n_{(q)} &= \{X \in \mathcal{L}_{(q)} ; \widehat{\Pi}(a)X = X\widehat{\Pi}(a), a \in \mathbb{N}, \text{нод}(a, q) = 1\}, \\ \widehat{C}^n_q &= \{X \in \mathcal{L}_q ; \widehat{\Pi}(a)X = X\widehat{\Pi}(a), a \mid q^\infty\}. \end{aligned} \tag{2.40}$$

Следующая теорема доказана в [4] и [5] только для колец $\mathcal{L}_{(q)}$, но то же доказательство с очевидными изменениями проходит и для колец $\mathcal{L}$ и $\mathcal{L}_q$.

Теорема 2.8. *Кольцо* $\widehat{C}$ *(соответственно* $\widehat{C}_{(q)}, \widehat{C}_q$*) линейно порождается над* $\mathbb{Q}$ *всеми двойными классами по модулю* Γ_0 *матриц из* Σ_0 *(соответственно* $\Sigma_{0,(q)}$, $\Sigma_{0,q}$*) вида*

$$M = U(\mu, D) = \begin{pmatrix} \mu \cdot {}^tD^{-1} & 0 \\ 0 & D \end{pmatrix}, \tag{2.41}$$

удовлетворяющими условию

$$\mu \mid d(D)^2, \tag{2.42}$$

где $d(D)$ *обозначает наибольший общий делитель коэффициентов матрицы* D. *Двойной класс* $(M)_{\Gamma_0}$ *для каждой такой* M *имеет следующее разложение на левые классы:*

$$(M)_{\Gamma_0} = \sum_{D', B} \left(\Gamma_0 U(\mu, D') \begin{pmatrix} E & B \\ 0 & E \end{pmatrix}\right), \tag{2.43}$$

где D' *пробегает множество представителей из левых классов смежности по модулю группы*

$$\Lambda = \Lambda^n = \mathrm{GL}_n(\mathbb{Z}), \tag{2.44}$$

содержащихся в двойном классе $\Lambda D \Lambda$, *и* B *пробегает множество представителей аддитивной группы* $\mathbb{S} = \mathbb{S}_n$ *по модулю подгруппы* $\mu^{-1} \cdot {}^tD'\mathbb{S}D'$.

Пусть теперь

$$X = \sum_i a_i \left(\Gamma_0 \begin{pmatrix} \mu_i \cdot {}^tD_i^{-1} & B_i \\ 0 & D_i \end{pmatrix}\right)$$

— некоторый элемент кольца $\mathcal{L}$. Мы положим

$$\Omega(X) = \sum_i a_i\{\mu_i\}(\Lambda D_i), \tag{2.45}$$

где коэффициенты $a_i\{\mu_i\}$ рассматриваются как элементы полугруппового кольца $\mathbb{Q}[\mathbb{N}]$ полугруппы положительных целых чисел над полем $\mathbb{Q}$. Легко видеть, что фактически $\Omega(X)$ принадлежит HS-кольцу пары (Λ, Δ), где

$$\Delta = \Delta^n = \{D \in \mathbb{Z}^n_n ; \det D \neq 0\}, \tag{2.46}$$

над $\mathbb{Q}[\mathbb{N}]$, и отображение

$$\Omega : \mathcal{L} \to HS_{\mathbb{Q}[\mathbb{N}]}(\Lambda, \Delta) \tag{2.47}$$

является $\mathbb{Q}$-линейным гомоморфизмом колец.

Предложение 2.9. *Ограничение $\Omega|_{\widehat{C}}$ гомоморфизма Ω на централизатор $\widehat{C}$ элементов Фробениуса в $\mathcal{L}$ является мономорфизмом; в частности, $\widehat{C}$ является коммутативной областью целостности.*

Отметим, что HS-кольцо пары (Λ^n, Δ^n) над любым коммутативным кольцом без делителей нуля является коммутативным и не содержит делителей нуля.

Обратимся теперь к локальным треугольным кольцам. Локальное подкольцо $\mathcal{L}_p = \mathcal{L}_p^n$ кольца $\mathcal{L}$ для каждого простого числа p состоит из тех линейных комбинаций левых (или двойных) классов, содержащихся в $\mathcal{L}$, чьи мультипликаторы являются степенями числа p.

Согласно предложению 2.9, локальные централизаторы

$$\widehat{C}_p = \{X \in \mathcal{L}_p \; ; \; \widehat{\Pi}(p)X = X\widehat{\Pi}(p)\} = \widehat{C} \cap \mathcal{L}_p \tag{2.48}$$

являются коммутативными областями целостности.

Теорема 2.10. *Кольцо $\widehat{C}$ (соответственно $\widehat{C}_{(q)}, \widehat{C}_q$) порождается подкольцами $\widehat{C}_p$, где p пробегает все простые числа (соответственно все простые числа, не делящие число q, все простые числа, делящие q).*

Хотя кольцо $\mathcal{L}_p$ некоммутативно и содержит делители нуля, оказывается, что каждый элемент из $\mathcal{L}_p$ может быть „спроектирован" в коммутативную область целостности $\widehat{C}_p$ и, кроме того, каждый элемент из кольца $\widehat{\mathcal{H}}_p = \mathcal{H}_p(1)$ может быть восстановлен по его проекциям.

Предложение 2.11. *Пусть $X = \Sigma_i a_i(\Gamma_0 M_i)$ — элемент из $\mathcal{L}_p$ с $\mu(M_i) = p^{\nu_i}$ и пусть d — целое рациональное число, удовлетворяющее неравенствам $d \geqslant \nu_i$ для всех i. Тогда*

$$X\widehat{\Pi}(p)^d \in \widehat{C}_p. \tag{2.49}$$

Если, кроме того, $X \in \widehat{\mathcal{H}}_p$, то

$$\Pi_+^{-d} \cdot X\widehat{\Pi}(p)^d = X, \tag{2.50}$$

где $\Pi_+^{-d} = \widehat{\Pi}(p)^{(-d)}$ — независимые от X элементы из расширения $\widehat{C}'_p = \widehat{C}[[p]^{-1}]$ кольца $\widehat{C}_p$.

Элементы Π_+^{-d} — это так называемые „*отрицательные степени*" *элемента Фробениуса*. По поводу их определения и свойств см., например, [4], §3.5.1.

Из определений следует, что $\widehat{\mathcal{H}}_p(q)$, образ p-кольца группы $K = \Gamma_0^n(q)$, содержится в $\mathcal{L}_p$. Кроме того, из первой части теоремы 2.6 следует, что параболическое вложение кольца $\mathcal{H}_p(q)$ в кольцо $\mathcal{L}_p$ можно разложить в произведение изоморфизма кольца $\mathcal{H}_p^n(q)$ на $\mathcal{H}_p(1)$, определенного в теореме, и параболического вложения кольца $\mathcal{H}_p(1)$; в частности, образ

$$\widehat{\mathcal{H}}_p(q) = \widehat{\mathcal{H}}_p = \widehat{\mathcal{H}}_p(1) \tag{2.51}$$

не зависит от выбора q, не делящегося на p.

Что касается связей между введенными локальными кольцами для различных простых чисел, то имеет место следующее предложение.

Предложение 2.12. *Пусть p и p' — два различных простых числа. Тогда каждый элемент кольца $\widehat{\mathcal{H}}_p$ коммутирует с каждым элементом кольца $\widehat{\mathcal{C}}_{p'}$.*

Мы заключим этот параграф следующей теоремой, которая играет ключевую роль в наших предстоящих построениях.

Теорема 2.13. *Элемент Фробениуса $\widehat{\Pi}(p) = \widehat{\Pi}^n(p)$, где p — простое число, удовлетворяет уравнению*

$$\sum_{j=0}^{m}(-1)^j\widehat{q_j^n}(p)\widehat{\Pi}(p)^{m-j} = 0 \quad (m = 2^n), \tag{2.52}$$

где $\widehat{q_j^n}(p) \in \widehat{\mathcal{H}}_p$ обозначают образы коэффициентов многочлена (2.27) над кольцом $\mathcal{H}_p(q)$ при параболическом вложении и где q не делится на p.

§2.4. Регулярные приводимые операторы Гекке и треугольные операторы

Сначала мы рассмотрим представление регулярного приводимого кольца $\mathcal{H}_{\mathrm{rr}}(q) = \mathcal{H}^n_{\mathrm{rr}}(q)$ на пространстве $\mathfrak{N}_k(K)$ касп-форм веса k для группы $K = \Gamma^n_0(q)$, задаваемое операторами Гекке, как они были определены в §1.5.

Согласно теореме 2.3 и теореме 1.9(2), операторы Гекке на пространстве $\mathfrak{N}_k(K)$, соответствующие элементам кольца $\mathcal{H}_{\mathrm{rr}}(q)$, коммутируют друг с другом и являются самосопряженными относительно скалярного произведения Петерссона. Пространство касп-форм конечномерно, отсюда вытекает следующая теорема.

Теорема 2.14. *Существует ортогональный базис пространства $\mathfrak{N}_k(K)$, состоящий из общих собственных функций всех операторов Гекке $|_kT$ и $\|_kT$ с $T \in \mathcal{H}_{\mathrm{rr}}(q)$.*

Операторы Гекке для группы $\Gamma_0 = \Gamma^n_0$ не обязательно отображают в себя пространства $\mathfrak{M}_k(K)$. Поэтому чтобы применить соотношения между элементами HS-колец групп K и Γ_0, приведенные в §2.3, необходимо сначала расширить пространства модулярных форм.

Каждая функция F из $\mathfrak{M}_k(K)$ удовлетворяет, в частности, соотношениям

$$F|_kM = (\det D)^{-k}F(M\langle Z\rangle) = F \quad \text{для каждой } M = \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} \in \Gamma_0. \tag{2.53}$$

Кроме того, она разлагается в абсолютно сходящийся на $\mathbb{H}_n$ ряд Фурье вида

$$F(Z) = \sum_{A\in\mathbb{E}_n, A\geq 0} f(A)e(AZ) \tag{2.54}$$

(см. Обозначения и (1.6)) с постоянными коэффициентами Фурье $f(A)$. Эти замечания позволяют определить пространство $\mathcal{T}_k = \mathcal{T}^n_k$ *модулярных форм веса k для группы* Γ_0 как пространство всех абсолютно сходящихся на $\mathbb{H}_n$ рядов Фурье вида (2.54), удовлетворяющих соотношениям (2.53). Отметим, что пространство $\mathcal{T}_k$ зависит только от четности числа k. Ясно, что

$$\mathfrak{M}_k(K) \subset \mathcal{T}_k. \tag{2.55}$$

HS-кольцо $\mathcal{L}$ группы Γ_0, определенное формулой (2.28), естественно действует на $\mathcal{T}_k$ посредством, например, нормализованных операторов Гекке:

$$\mathcal{L} \ni T = \sum_i a_i(\Gamma_0 M_i) : F \to F\|_k T = \sum_i a_i \mu(M_i)^{nk-\langle n\rangle} F|_k M_i. \tag{2.56}$$

Отображение $T \to \|_k T$ является линейным представлением кольца $\mathcal{L}$ на пространстве $\mathcal{T}_k$, которое согласуется с параболическим вложением

$$H_{\mathrm{rr}}(q) \to \widehat{\mathcal{H}}_{\mathrm{rr}}(q) \subset \mathcal{L},$$

определенным формулой (2.30) в том смысле, что

$$F\|_k T = F\|_k \widehat{T} \quad (F \in \mathfrak{M}_k(K),\ T \in \mathcal{H}_{\mathrm{rr}}(q)). \tag{2.57}$$

Следующая лемма показывает, что нормализованные операторы Гекке, отвечающие элементам централизатора $\widehat{C}$ элементов Фробениуса $\widehat{\Pi}(a)$ (см. (2.38) и (2.40)), особенно просто действуют на коэффициенты Фурье функций из $\mathcal{T}_k$.

Лемма 2.15. *Пусть F — функция из $\mathcal{T}_k$ с коэффициентами Фурье $f(A)$ и пусть $M = U(\mu, D)$ — матрица из Σ_0 вида* (2.41), *удовлетворяющая условию* (2.42). *Тогда коэффициенты Фурье $(f\|_k(M)_{\Gamma_0})(A)$ функции $F\|_k(M)_{\Gamma_0}$ задаются формулой*

$$(f\|_k(M)_{\Gamma_0})(A) = \mu^{nk-n(n+1)}|\det D|^{n+1} \sum_{D' \in \Lambda\backslash\Lambda D\Lambda} (\det D)^{-k} f(\mu^{-1} D' A \cdot {}^t D'); \tag{2.58}$$

в частности,

$$(f\|_k \widehat{\Pi}(a))(A) = f(aA) \quad (a \in \mathbb{N},\ A \in \mathbb{E}_n). \tag{2.59}$$

В качестве иллюстрации техники параболических вложений мы докажем здесь теорему рациональности, первоначально доказанную Жарковской в [18] для группы Γ^n.

Теорема 2.16. *Пусть*

$$F = \sum_{A \in \mathbb{E}_n, A \geq 0} f(A) e(AZ) \in \mathfrak{M}_k(K)$$

— собственная функция всех операторов Гекке $\|_k T$ с $T \in \mathcal{H}_p^n(q)$, где p — простое число, не делящее q:

$$F\|_k T = \lambda(T) F \quad (T \in \mathcal{H}_p^n(q)).$$

Тогда каждый формальный степенной ряд вида

$$\sum_{\delta=0}^{\infty} f(p^\delta A) v^\delta \quad с\ A \in \mathbb{E}_n$$

формально равен рациональной дроби со знаменателем

$$(\lambda Q_p^n)(v) = \sum_{i=0}^{m} (-1)^i \lambda(q_i^n(p)) v^i \quad (m = 2^n),$$

где $Q_p^n(v)$ — многочлен (2.27), и с числителем степени не больше, чем $2^n - 1$.

Доказательство. Используя (2.57) и (2.59), получаем

$$\left(\sum_{i=0}^{m}(-1)^i\lambda(q_i^n(p))v^i\right)\left(\sum_{\delta=0}^{\infty}f(p^\delta A)v^\delta\right) = \sum_{i,\delta}(-1)^i(f\|_k q_i^n(p))(p^\delta A)v^{i+\delta}$$
$$= \sum_{i,\delta}(-1)^i(f\|_k\widehat{q_i^n}(p)\widehat{\Pi}(p)^\delta)(A)v^{i+\delta}.$$

Если $i+\delta = r \geqslant m$, то, согласно (2.52), имеем

$$\sum_{i+\delta=r}(-1)^i\widehat{q_i^n}(p)\widehat{\Pi}(p)^\delta = \sum_{i=0}^{m}((-1)^i\widehat{q_i^n}(p)\widehat{\Pi}(p)^{m-i})\widehat{\Pi}(p)^{r-m} = 0. \quad \bullet$$

Глава 3

Сингулярные кольца Гекке–Шимуры для $\Gamma_0^n(q)$

Наша теория сингулярных HS-колец для групп $\Gamma_0^n(q)$ основана на двух фундаментальных фактах: первый заключается в том, что централизатор элемента Фробениуса $\Pi(p)$ в приводимом p-кольце для $\Gamma_0^n(q)$, где p является простым делителем числа q, естественно изоморфен централизатору элемента $\widehat{\Pi}(p)$ в треугольном кольце $\mathcal{L}_p$, как следует из теорем 3.3 и 2.8; согласно второму, элемент $\Pi(p)$ для простых p, делящих q, но не делящих q/p, является обратимым, что основано на свойствах нейтральных HS-колец, рассмотренных в §3.2. Эти обстоятельства позволят нам построить в §3.3 естественное вложение регулярного приводимого p-кольца для группы $\Gamma_0^n(q/p)$ в p-подкольцо группы $\Gamma_0^n(q)$ при условии, что $p \mid q$ и $p^2 \nmid q$, которое заменяет параболическое вложение регулярного кольца, рассмотренное в §2.3.

§3.1. Централизаторы элементов Фробениуса

Обозначим через

$$\begin{aligned} S(q) &= S^n(q) \subset \mathcal{H}_q(K), \\ S_p(q) &= S_p^n(q) = \left\{\sum_i a_i(KM_i) \in S(q)\ ;\ \mu(M_i) \mid p^\infty\right\}, \end{aligned} \tag{3.1}$$

где p — простой делитель числа q (*максимальное*), *приводимое подкольцо* сингулярного HS-кольца $\mathcal{H}_q(K)$ группы $K = \Gamma_0^n(q)$ и *сингулярное приводимое p-кольцо* соответственно. В этом параграфе мы покажем, что *сингулярные элементы Фробениуса*

$$\Pi(a) = \Pi_K^n(a) = \left(\begin{pmatrix} E_n & 0 \\ 0 & aE_n \end{pmatrix}\right)_K, \quad \text{где } a \mid q^\infty, \tag{3.2}$$

принадлежат кольцу $S(q)$, и определим их централизатор в этом кольце.

Оказывается, что указанный централизатор естественно изоморфен централизатору $\widehat{C}_q^n$ соответствующих элементов $\widehat{\Pi}(a)$ в q-сингулярном подкольце $\mathcal{L}_q^n$ треугольного кольца $\mathcal{L}^n$ (см. теорему 3.3). Это обстоятельство является решающим для нашего подхода к сингулярным HS-кольцам и операторам для группы K.

Мы начнем с двух простых лемм о рациональных матрицах [17].

Лемма 3.1. *Пусть R — матрица порядка n с рациональными элементами. Тогда существует целочисленная матрица D порядка n с ненулевым определителем, удовлетворяющая следующим двум условиям:*

(1) *матрица DR целочисленна;*

(2) *если произведение $D'R$ является целочисленным, то $D' = TD$ с целочисленной матрицей T.*

Доказательство. Если $R = 0$, то можно взять $D = E_n$. Если же $R \neq 0$, то матрица R может быть приведена к диагональному виду посредством умножения справа и слева на матрицы из группы $\Lambda = \mathrm{GL}_n(\mathbb{Z})$:

$$URV = R' = \mathrm{diag}(a_1/b_1, \dots, a_r/b_r, 0, \dots, 0) \quad (U, V \in \Lambda),$$

где a_i, b_j — положительные целые числа, удовлетворяющие условиям нод$(a_i, b_i) = 1$, для $i = 1, \dots, r$. Заметим, что произведение SR', где $S = (s_i, \dots, s_n)$ — некоторая целочисленная матрица со столбцами s_i, снова является целочисленным в том и только в том случае, если столбцы s_i делятся на b_i для $i = 1, \dots, r$, что эквивалентно условию делимости S справа на матрицу $B = \mathrm{diag}(b_1, \dots, b_r, 1, \dots, 1)$. Положим $D = BU$. Тогда матрица $DR = BR'V^{-1}$ является целочисленной, и если произведение $D'R$ целочисленно, то матрица $D'U^{-1}R'$ является целочисленной, откуда следует, что $D'U^{-1} = TB$ с целочисленной матрицей T, т. е. $D' = TBU = TD$. •

Матрица D, удовлетворяющая условиям (1) и (2) леммы, называется (*левым*) *знаменателем матрицы R*. Из определения следует, что все знаменатели матрицы R образуют один левый класс смежности ΛD по модулю группы $\Lambda = \Lambda^n$, который также будет называться *знаменателем матрицы R*.

Лемма 3.2. *Если R — рациональная матрица порядка n со знаменателем D, то пара (DR, D) является взаимно-простой.*

Доказательство. Если $DR = SC_1$ и $D = SD_1$ с целочисленными матрицами S, C_1, D_1, то $R = D_1^{-1}C_1$ и, следовательно, матрица D_1R является целочисленной. Отсюда следует, что $D_1 = TD$ с целочисленной матрицей T. Поэтому $ST = E$, откуда $S \in \Lambda$. •

Теорема 3.3. *Пусть n, q — целые положительные числа и $q > 1$. Тогда справедливы следующие утверждения:*

(1) *Каждый двойной класс* $(M)_K$ *матрицы* $M = U(\mu, D)$ *вида* (2.41), *которая содержится в множестве* $\Sigma_{0,q}^n$ *и удовлетворяет условию* (2.42), *имеет следующее разложение на левые классы по модулю группы* $K = \Gamma_0^n(q)$:

$$(M)_K = \sum_{D', B} \left(KU(\mu, D') \begin{pmatrix} E & B \\ 0 & E \end{pmatrix} \right), \tag{3.3}$$

где D' *пробегает множество представителей из левых классов смежности по группе* $\Lambda = \Lambda^n$, *содержащихся в двойном классе* $\Lambda D \Lambda$, *а* B *пробегает множество представителей из классов смежности аддитивной группы* $\mathbb{S} = \mathbb{S}_n$ *по подгруппе* $\mu^{-1} \cdot {}^t D' \mathbb{S} D'$. *В частности, каждый сингулярный элемент Фробениуса* (3.2) *имеет разложение*

$$\Pi(a) = \Pi_K^n(a) = (U(a, aE))_K = \sum_{B \in \mathbb{S}/a\mathbb{S}} \left(K \begin{pmatrix} E & B \\ 0 & aE \end{pmatrix} \right). \tag{3.4}$$

(2) *Все двойные классы* $(M)_K$ *матриц* $M = U(\mu, D)$ *из* $\Sigma_{0,q}^n$, *удовлетворяющих* (2.42), *линейно порождают над* $\mathbb{Q}$ *подкольцо* $C_q = C_q^n$ *кольца* $S(q) = S^n(q)$.

(3) *Ограничение параболического вложения*

$$j : S(q) \to \mathcal{L}_q \tag{3.5}$$

на подкольцо C_q *является изоморфизмом кольца* C_q *на централизатор* $\widehat{C}_q$*-элементов Фробениуса, содержащихся в* $\mathcal{L}_q$. *В частности,* C_q *является коммутативной областью целостности, которая порождается локальными подкольцами*

$$C_p = \left\{ T = \sum_i a_i(KM_i) \in C_q \; ; \; \mu(M_i) \mid p^\infty \right\} \tag{3.6}$$

для всех простых чисел p, *делящих* q.

(4) *Кольцо* C_q *(соответственно* C_p*) можно охарактеризовать как централизатор в* $S(q)$ *(соответственно* $S_p(q)$*) элементов Фробениуса* (3.2) *(соответственно* $\Pi(p)$*).*

Докажем сначала две леммы.

Лемма 3.4. *Каждая матрица вида* $U(\mu, D) \in \Sigma_0^n$, *удовлетворяющая условию* (2.42), *является* K*-приводимой.*

Доказательство. По лемме 2.1 можно считать, что $q > 1$. Достаточно доказать, что для каждой матрицы $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in K$ найдется матрица $\gamma' = \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right) \in K$, такая что

$$\gamma' U(\mu, D) \gamma = \begin{pmatrix} * & * \\ c'Aa + d'DC & * \end{pmatrix} = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}, \tag{3.7}$$

где $A = \mu \cdot {}^t D^{-1}$. Так как $a \cdot {}^t d \equiv 1 \pmod q$, то $\det a$ взаимно-прост с q, и поэтому матрица a обратима. Положим

$$R = -Dca^{-1}A^{-1} = -\mu^{-1} Dca^{-1} \cdot {}^t D.$$

По лемме 1.1(4) матрица R симметрична. Так как $\mu \mid d(D)^2$, матрица $\det a \cdot R$ является целочисленной. Так как $\det a$ взаимно-прост с q и $c \equiv 0 \pmod q$, мы заключаем, что $\det a \cdot R \equiv 0 \pmod q$. Пусть d' обозначает знаменатель матрицы R и $c' = d'R$. Тогда $d' \mid \det a \cdot E$, откуда $\det d' \mid (\det a)^n$, и потому $\det d'$ взаимно-прост с q. Далее, так как $(\det a)c' = d' \cdot (\det a)R \equiv 0 \pmod q$, то $c' \equiv 0 \pmod q$. Пара (c', d') является взаимно-простой по лемме 3.2 и симметричной, поскольку R симметрична. По лемме 1.2 найдутся матрицы a', b', такие что матрица $\gamma' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \Gamma^n$. Тогда $\gamma' \in K$ и γ' удовлетворяет условию (3.7). •

Лемма 3.5. *Каждый из левых классов по модулю K, содержащийся в двойном классе KMK матрицы $M = U(\mu, D) \in \sum_{0,q}$ вида* (2.41), *удовлетворяющей условию* (2.42), *содержит представителя вида*

$$\begin{pmatrix} A' & B' \\ 0 & D' \end{pmatrix} \quad \text{с } D' \in \Lambda D \Lambda. \tag{3.8}$$

Доказательство. Возьмем представителя

$$\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} M \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in KM \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{вида} \begin{pmatrix} A' & B' \\ 0 & D' \end{pmatrix},$$

где $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in K$, который существует по предыдущей лемме. Тогда $c'Aa + d'Dc = 0$, где $A = \mu \cdot {}^tD^{-1}$, откуда $(d')^{-1}c' = -\mu^{-1}Dca^{-1} \cdot {}^tD$. С другой стороны, мы имеем

$$\begin{aligned} D' &= c'Ab + d'Dd = d'((d')^{-1}c'Ab + Dd) \\ &= d'(-\mu^{-1}Dca^{-1}\,{}^tDAb + Dd) = d'D(-ca^{-1}b + d) \\ &= d'D \cdot {}^ta^{-1}({}^tad - {}^ta \cdot {}^ta^{-1} \cdot {}^tcb) = d'D \cdot {}^ta^{-1}. \end{aligned}$$

Так как $\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in K$, то $\det d'$ и $\det a$ взаимно-просты с q и поэтому взаимно-просты с μ, поскольку $\mu \mid q^\infty$. С другой стороны, матрица $\mu \cdot {}^tD^{-1}$ целочисленна и поэтому $D \mid \mu^n \mid q^\infty$. Поскольку определители целочисленных матриц d' и D взаимно-просты, из теории элементарных делителей для полной линейной группы над $\mathbb{Z}$ (см., например, [4, гл. 3]) легко следует, что можно написать $d'D = D_1 d_1$, где D_1 и d_1 — целочисленные матрицы с теми же элементарными делителями, что D и d' соответственно. Тогда мы получаем соотношение

$$D' = d'D \cdot {}^ta^{-1} = D_1 d_1 \cdot {}^ta^{-1}.$$

Так как все элементарные делители матриц D' и D взаимно-просты с элементарными делителями матриц d_1 и a, из последнего соотношения следует, что все элементарные делители матрицы $d_1 \cdot {}^ta^{-1}$ равны 1. Отсюда следует, что матрицы D', D_1 и D имеют одинаковые элементарные делители, и, значит, $D' \in \Lambda D \Lambda$. •

Доказательство теоремы 3.3. (1) Возьмем представителя вида (3.8) в левом классе $KM\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, где $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in K$. Тогда мы получаем

$$\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} M \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} A' & B' \\ 0 & D' \end{pmatrix} = \begin{pmatrix} {}^t\eta^{-1} & 0 \\ 0 & \eta \end{pmatrix} \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} \begin{pmatrix} {}^t\nu^{-1} & 0 \\ 0 & \nu \end{pmatrix},$$

где $\left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right) \in K$, $\eta, \nu \in \Lambda$. Отсюда следует, что

$$M = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} * & a_1Ab_2 + a_1Bd_2 + b_1Dd_2 \\ * & * \end{pmatrix},$$

где матрицы

$$\begin{aligned} \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} &= \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}^{-1} \begin{pmatrix} {}^t\eta^{-1} & 0 \\ 0 & \eta \end{pmatrix}, \\ \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} &= \begin{pmatrix} {}^t\nu^{-1} & 0 \\ 0 & \nu \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \end{aligned} \tag{3.9}$$

принадлежат группе K. Отсюда мы получаем соотношение $a_1Ab_2 + a_1Bd_2 + b_1Dd_2 = 0$, которое можно переписать в виде

$$B = -(Ab_2d_2^{-1} + a_1^{-1}b_1D) = AS,$$

где $S = -(b_2d_2^{-1} + A^{-1}a_1^{-1}b_1D)$. Отметим, что поскольку матрицы (3.9) содержатся в K, то имеют место сравнения ${}^ta_1d_1 \equiv 1 \pmod q$ и ${}^ta_2d_2 \equiv 1 \pmod q$, откуда следует, что определители $\det a_1$ и $\det d_2$ взаимно-просты с q. В частности, поскольку $q > 1$, матрицы a_1 и d_2 обратимы. Кроме того, если p — простое число и $p \mid \det a_1 \det d_2$, то p не делит q и поэтому p не делит $\det A$. Отсюда следует, что матрица $A^{-1}B$ является p-целой, поскольку B — целочисленная матрица. Если же $p \mid \det A$, то $p \mid q$, откуда $p \nmid \det a_1 \det d_2$. Кроме того, матрица $S = -(b_2d_2^{-1} + \mu^{-1} \cdot {}^tDa_1^{-1}bD)$ является p-целой, согласно условию (2.42). На основании сказанного мы заключаем, что матрица S является целочисленной, и поэтому

$$B' = {}^t\eta^{-1}B\nu = {}^t\eta^{-1}AS\nu = A' \cdot {}^t\nu S\nu = A'S',$$

где S' — целочисленная симметрическая матрица.

Наконец, ясно, что две матрицы $\left(\begin{smallmatrix} A' & B' \\ 0 & D' \end{smallmatrix}\right)$ и $\left(\begin{smallmatrix} A_1 & B_1 \\ 0 & D_1 \end{smallmatrix}\right)$ вида (3.8), где $B' = A'S'$ и $B_1 = A_1S_1$ с $S, S_1 \in \mathbb{S}$, принадлежат к одному левому классу смежности по модулю K в том и только в том случае, если они принадлежат к одному левому классу по модулю группы Γ_0^n:

$$\begin{pmatrix} \alpha & \alpha\beta \\ 0 & \delta \end{pmatrix} \begin{pmatrix} A_1 & A_1S_1 \\ 0 & D_1 \end{pmatrix} = \begin{pmatrix} A' & A'S' \\ 0 & D' \end{pmatrix},$$

где $\alpha, \delta \in \Lambda$, ${}^t\alpha\delta = E$, $\beta \in \mathbb{S}$, что эквивалентно соотношениям

$$\delta D_1 = D' \quad \text{и} \quad \alpha A_1S_1 + \alpha\beta D_1 = A'S'.$$

Эти соотношения означают, что $\Lambda D_1 = \Lambda D'$, и поэтому можно считать, что $D_1 = D'$ и $\delta = E$. Тогда второе из соотношений превращается в равенство

$$A'S_1 + \beta D' = A'S', \quad \text{т.е. } S' - S_1 = (A')^{-1}\beta D' = \mu^{-1} \cdot {}^tD'\beta D'.$$

(2) Если $(M)_K = (U(\mu, D))_K$ и $(M_1)_K = (U(\mu_1, D_1))_K$ — два двойных класса из C_q, записанных в виде (3.3), то их произведение является суммой левых классов произведений

$$U(\mu, D')\begin{pmatrix} E & B \\ 0 & E \end{pmatrix} U(\mu_1, D_1')\begin{pmatrix} E & B_1 \\ 0 & E \end{pmatrix} = U(\mu\mu_1, D'D_1')\begin{pmatrix} E & \mu_1^{-1} \cdot {}^tD_1BD_1 + B_1 \\ 0 & E \end{pmatrix},$$

которые принадлежат двойному классу матрицы $U(\mu\mu_1, D'D_1')$, поскольку матрица $\mu^{-1} \cdot {}^tD_1BD_1$ является целочисленной по условию (2.42) для матрицы $U(\mu_1, D_1)$. Кроме того,

$$\mu\mu_1 | (\det D \det D_1)^2 = (\det D' \det D_1')^2 = (\det D'D_1')^2.$$

(3) Утверждение следует из частей (1) и (2), теоремы 2.8, предложения 2.9 и теоремы 2.10.

(4) Поскольку кольцо C_q коммутативно и содержит элементы (3.2), то достаточно доказать, что каждый элемент T из $S(q)$, коммутирующий с элементами (3.2), содержится в C_q. Образ $\widehat{T}$ в $\mathcal{L}_q$ элемента T при параболическом вложении коммутирует с каждым из элементов Фробениуса кольца $\mathcal{L}_q$ и поэтому содержится в подкольце $\widehat{C}_q$. Тогда по теореме 2.8 элемент $\widehat{T}$ является линейной комбинацией левых классов по модулю Γ_0 матриц вида

$$U(\mu, D')\begin{pmatrix} E & B \\ 0 & E \end{pmatrix}$$

с целочисленными симметрическими матрицами B и целочисленными D', удовлетворяющими условиям $\mu \mid (\det D')^2 \mid q^\infty$. По определению параболических вложений элемент T является линейной комбинацией левых классов тех же матриц по модулю группы K. Тогда T содержится в C_q по части (1). Случай колец C_p с простыми делителями числа q рассматривается аналогично. •

§3.2. Нейтральные кольца

Нейтральное кольцо

$$\mathcal{N}(q) = \mathcal{N}^n(q) = HS(K, \Gamma^n) \tag{3.10}$$

группы $K = \Gamma_0^n(q)$ содержится и в регулярном кольце $\mathcal{H}_{(q)}(K)$ и в сингулярном кольце $\mathcal{H}_q(K)$ (см. (1.27)), поскольку

$$\Gamma^n = \Sigma_{(q)}^n \cap \Sigma_q^n.$$

Хотя нейтральное кольцо не играет существенной роли в регулярной теории, оно важно в сингулярном случае. В этом параграфе мы докажем несколько свойств нейтрального кольца и его подколец вида

$$\mathcal{N}(q_1, q) = \mathcal{N}^n(q_1, q) = HS(K, \Gamma_0^n(q_1)), \tag{3.11}$$

где q_1 делит q.

Лемма 3.6. *Две матрицы* $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ *и* $M' = \begin{pmatrix} A' & B' \\ C' & D' \end{pmatrix}$ *из группы* $\Gamma = \Gamma^n$ *принадлежат одному левому классу смежности* $KM = KM'$ *по подгруппе* K *в том и только в том случае, если их „вторые строки" „пропорциональны" по модулю* q,

$$(C', D') \simeq (C, D) \pmod q, \tag{3.12}$$

в том смысле, что

$$(C', D') \equiv d(C, D) \pmod q \tag{3.13}$$

с некоторой целочисленной матрицей d *порядка* n, *обратимой по модулю* q.

Доказательство. Если $KM' = KM$, то $M' = \gamma M$ с $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in K$, откуда следует соотношение

$$(C', D') = (cA + dC, cB + dD) \equiv d(C, D) \pmod q.$$

Если же выполняется (3.13), то матрица

$$\gamma = \begin{pmatrix} A' & B' \\ C' & D' \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix}^{-1} = \begin{pmatrix} A' & B' \\ C' & D' \end{pmatrix} \begin{pmatrix} {}^tD & -{}^tB \\ -{}^tC & {}^tA \end{pmatrix} = \begin{pmatrix} * & * \\ C' \cdot {}^tD - D' \cdot {}^tC & * \end{pmatrix}$$

содержится в K, поскольку

$$C' \cdot {}^tD - D' \cdot {}^tC \equiv d(C \cdot {}^tD - D \cdot {}^tC) = 0 \pmod q. \quad \bullet$$

Лемма 3.7. *Индексы*

$$\nu(q) = \nu_n(q) = [\Gamma^n : \Gamma_0^n(q)] \tag{3.14}$$

удовлетворяют соотношениям

$$\nu(q_1 q_2) = \nu(q_1)\nu(q_2), \quad \text{если } \text{нод}(q_1, q_2) = 1. \tag{3.15}$$

Доказательство. Хорошо известно, что естественное отображение $\Gamma^n \to Sp_n(\mathbb{Z}/q\mathbb{Z})$ является эпиморфизмом (см., например, [4, лемма 3.3.2]). Отсюда следует, что индекс $\nu(q)$ может быть интерпретирован как индекс в группе $Sp_n(\mathbb{Z}/q\mathbb{Z})$ подгруппы

$$\left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} \in Sp_n(\mathbb{Z}/q\mathbb{Z}) \right\}. \tag{3.16}$$

Группа и подгруппа являются множествами решений конечных систем полиномиальных сравнений по модулю q, и соотношение (3.15) следует из китайской теоремы об остатках. $\bullet$

Чтобы сформулировать следующую лемму, нам потребуются некоторые обозначения. Мы положим

$$I_{r,n} = \{(i_1, \ldots, i_r) \in \mathbb{N}^r \; ; \; 1 \leqslant i_1 < \cdots < i_r \leqslant n\}. \tag{3.17}$$

Для $\mathbf{i} = (i_1, \ldots, i_r) \in I_{r,n}$ мы обозначим через $\widehat{\mathbf{i}}$ множество $(j_1, \ldots, j_{n-r}) \in I_{n-r,n}$, дополнительное к $(i_1, \ldots, i_r)$ в $(1, \ldots, n)$. Далее, каждому $\mathbf{i} = (i_1, \ldots, i_r) \in I_{r,n}$ мы сопоставим перестановку

$$\sigma(\mathbf{i}) : (i_1, \ldots, i_r, j_1, \ldots, j_{n-r}) \to (1, \ldots, r, r+1, \ldots, n) \tag{3.18}$$

множества $(1, \ldots, n)$, где $(j_1, \ldots, j_{n-1}) = \widehat{\mathbf{i}}$, и матрицу

$$M(\mathbf{i}) = M(\sigma(\mathbf{i})) \tag{3.19}$$

этой перестановки, где под матрицей перестановки σ множества $(1, \ldots, n)$ понимается матрица $M(\sigma) = (\delta_{\sigma^{-1}(i),j})$ с $\delta_{i,i} = 1$ и $\delta_{i,j} = 0$, если $i \neq j$, для $i, j = 1, \ldots, n$. Наконец, для $\mathbf{i} \in I_{r,n}$ и целого положительного числа p мы положим

$$V_p(\mathbf{i}) = \{V = (v_{\alpha\beta}) \in \mathbb{Z}_n^r \,;\, 0 \leqslant v_{\alpha\beta} < p, \text{ если } i_\alpha < j_\beta, \text{ и } v_{\alpha\beta} = 0, \text{ если } i_\alpha > j_\beta\}, \tag{3.20}$$

где $(j_1, \ldots, j_{n-r}) = \widehat{\mathbf{i}}$.

Лемма 3.8. *Пусть p — простой делитель числа q, который не делит частное q/p, и пусть a, b — два целых числа, удовлетворяющие соотношению $ap - bq_1 = 1$, где $q_1 = q/p$. Тогда множество*

$$\bigcup_{r=0}^{n} W_r(p,q), \tag{3.21}$$

где $W_0(p,q) = W_0^n(p,q) = \{E_{2n}\}$, и для $r > 1$

$$W_r(p,q) = W_r^n(p,q) = \{M_r \cdot U_{\mathbf{i}}(V,D) \,;\, \mathbf{i} \in I_{r,n}, V \in V_p(\mathbf{i}), D \in \mathbb{S}_{r/p}\mathbb{S}_r\} \tag{3.22}$$

с

$$M_r = \begin{pmatrix} aE_r & 0 & bE_r & 0 \\ 0 & E_{n-r} & 0 & 0 \\ q_1 E_r & 0 & pE_r & 0 \\ 0 & 0 & 0 & E_{n-r} \end{pmatrix}$$

и

$$U_{\mathbf{i}}(V,D) = \begin{pmatrix} E_r & V & D & 0 \\ 0 & E_{n-r} & 0 & 0 \\ 0 & 0 & E_r & 0 \\ 0 & 0 & -{}^tV & E_{n-r} \end{pmatrix} \begin{pmatrix} M(\mathbf{i}) & 0 \\ 0 & {}^tM(\mathbf{i})^{-1} \end{pmatrix}$$

являются полным множеством представителей из различных левых классов смежности $\Gamma_0^n(q) \setminus \Gamma_0^n(q_1)$.

Доказательство. Мы покажем сначала, что матрицы из множества (3.21) принадлежат к различным левым классам по модулю $K = \Gamma_0^n(q)$. Пусть $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ и $M' = \begin{pmatrix} A' & B' \\ C' & D' \end{pmatrix}$ — две такие матрицы. Предположим, что $KM = KM'$. Тогда по лемме 3.6 их вторые строки пропорциональны по модулю p, т.е.

$$C' \equiv dC \pmod{q}, \quad D' \equiv dD \pmod{q} \tag{3.23}$$

с целочисленной матрицей d порядка n, обратимой по модулю q. Отсюда следует, что матрицы C и C' имеют одинаковый ранг r по модулю p, и поэтому M и M' обе принадлежат к одному и тому же множеству $W_r^n(p,q)$. Если

$$C = \begin{pmatrix} q_1E_r & q_1V \\ 0 & 0 \end{pmatrix} M(\mathbf{i}), \quad C' = \begin{pmatrix} q_1E_r & q_1V' \\ 0 & 0 \end{pmatrix} M(\mathbf{i}') \quad \text{и} \quad d = \begin{pmatrix} d_1 & d_2 \\ d_3 & d_4 \end{pmatrix},$$

где d_1 обозначает блок размеров $r \times r$, то из приведенных сравнений следуют сравнения

$$(q_1E_r, q_1V')M(\mathbf{i}') \equiv d_1(q_1E_r, q_1V)M(\mathbf{i}) \pmod q. \tag{3.24}$$

Отсюда следует, что матрица d_1 обратима по модулю p. Если $q_1(E_r, V)M(\mathbf{i}) = (t_1, \dots, t_n)$, то

$$q_1(E_r, V) = (t_1, \dots, t_n)M(\mathbf{i})^{-1} = (t_{i_1}, \dots, t_{i_r}, t_{j_1}, \dots, t_{j_{n-r}}),$$

где $(i_1, \dots, i_r) = \mathbf{i}$ и $(j_1, \dots, j_{n-r}) = \widehat{\mathbf{i}}$, по определению матрицы $M(\mathbf{i})$, откуда по определению множества $V_p(\mathbf{i})$ (см. (3.20)) система $\mathbf{i} = (i_1, \dots, i_r)$ является наименьшей в смысле лексикографического упорядочивания системой номеров столбцов матрицы $(t_1, \dots, t_n)$, которые линейно-независимы по модулю p. Таким образом, из сравнения (3.24) следует, что $\mathbf{i}' = \mathbf{i}$, откуда $d_1 \equiv E_r \pmod p$ и $V' \equiv V \pmod p$. Согласно (3.30), последнее сравнение означает, что $V' = V$. Тогда из второго сравнения (3.23) следует сравнение

$$\begin{pmatrix} q_1D' & 0 \\ -{}^tV & E_{n-r} \end{pmatrix} {}^tM(\mathbf{i})^{-1} \equiv \begin{pmatrix} E_r & d_2 \\ d_3 & d_4 \end{pmatrix} \begin{pmatrix} q_1D & 0 \\ {}^tV & E_{n-r} \end{pmatrix} {}^tM(\mathbf{i})^{-1} \pmod p.$$

Сравнивая соответствующие блоки, мы заключаем, что $d_2 \equiv 0 \pmod p$ и $q_1D' \equiv q_1D - d_2{}^tV \equiv q_1D \pmod p$, откуда $D' = D$.

Для завершения доказательства леммы достаточно показать, что число элементов множества (3.21) равно индексу $[\Gamma_0^n(q_1) : \Gamma_0^n(q)]$. Отметим сначала, что число элементов множества (3.20) для $\mathbf{i} = (i_1, \dots, i_r) \in I_{r,n}$ равно $p^{j_1 + \dots + j_{n-r} - \langle n-r \rangle}$ (см. Обозначения), где $(j_1, \dots, j_{n-r}) = \widehat{\mathbf{i}}$, поскольку число индексов i_α, удовлетворяющих неравенству $i_\alpha < j_\beta$, с фиксированным β равно $j_\beta - \beta$. Отсюда следует, что число элементов множества (3.21) равно

$$\sum_{r=0}^{n} \Bigl(p^{-\langle n-r \rangle} \sum_{1 \leqslant j_1 < \dots < j_{n-r} \leqslant n} p^{j_1 + \dots + j_{n-r}}\Bigr) p^{\langle r \rangle} = \sum_{r=0}^{n} p^{\langle r \rangle} \frac{\varphi_n(p)}{\varphi_r(p)\varphi_{n-r}(p)} = \prod_{i=1}^{n} (1 + p^i), \tag{3.25}$$

где

$$\varphi_0(x) = 1, \quad \varphi_r(x) = (x-1)(x^2-1)\dots(x^r-1) \ (r \in \mathbb{N}) \tag{3.26}$$

и где мы использовали следующее тождество от двух переменных x, t:

$$\prod_{i=1}^{n} (1 + tx^i) = \sum_{r=0}^{n} t^r x^{\langle r \rangle} \frac{\varphi_n(x)}{\varphi_r(x)\varphi_{n-r}(x)}$$

и его следствия

$$\sum_{1\leqslant i_1<\cdots<i_r\leqslant n} x^{i_1+\cdots+i_r} = x^{\langle r\rangle}\frac{\varphi_n(x)}{\varphi_r(x)\varphi_{n-r}(x)} \quad (1\leqslant r\leqslant n). \tag{3.27}$$

С другой стороны, по лемме 3.7 мы можем написать

$$[\Gamma_0^n(q_1):\Gamma_0^n(q)] = \nu_n(q)/\nu(q_1) = \nu_n(p) \tag{3.28}$$

и

$$\begin{aligned}\nu_n(p) &= [\Gamma^n:\Gamma_0^n(p)] = \#(Sp_n(\mathbb{Z}/p\mathbb{Z}))/p^{\langle n\rangle}\#(GL_n(\mathbb{Z}/p\mathbb{Z}))\\ &= p^{n^2}\prod_{i=1}^n(p^{2i}-1)/p^{\langle n\rangle}p^{\langle n-1\rangle}\prod_{i=1}^n(p^i-1) = \prod_{i=1}^n(p^i+1)\end{aligned} \tag{3.29}$$

(см., например, [6, гл. 3, 4]). Сравнение формул (3.28) и (3.29) с (3.25) заканчивает доказательство леммы. •

Предложение 3.9. *Пусть p — простое число, делящее q, но не делящее $q_1 = q/p$. Тогда имеют место следующие утверждения:*

(1) *Кольцо*

$$\mathcal{N}_p(q) = \mathcal{N}_p^n(q) = \mathcal{N}^n(q_1,q) \tag{3.30}$$

состоит из линейных комбинаций $n+1$ различных двойных классов

$$\xi_r(p) = \xi_r^n(p) = (M_r)_K, \tag{3.31}$$

где $M_0 = E_{2n}$, а матрицы $M_1,\ldots,M_n$ были введены в лемме 3.8. Каждый двойной класс KM_rK может быть охарактеризован как множество всех матриц $M = \left(\begin{smallmatrix}A & B\\ C & D\end{smallmatrix}\right)$ из $\Gamma_0^n(q_1)$ с блоком C ранга r по модулю p.

(2) *Каждый двойной класс (3.31) имеет следующее разложение на левые классы:*

$$\xi_r(p) = \sum_{M\in W_r^n(p,q)}(KM), \tag{3.32}$$

где $W_r^n(p,q)$ — множество (3.22). В частности, число различных левых классов, входящих в $\xi_r(p)$, равно

$$\#(W_r^n(p,q)) = p^{\langle r\rangle}\frac{\varphi_n(p)}{\varphi_r(p)\varphi_{n-r}(p)}, \tag{3.33}$$

где $\varphi_r(x)$ — многочлены (3.26).

(3) *Двойные классы (3.31) инвариантны относительно антиавтоморфизма звездочка (1.18):*

$$\xi_r^*(p) = \xi_r(p) \quad (r = 0,1,\ldots,n). \tag{3.34}$$

В частности, кольцо $\mathcal{N}_p(q)$ коммутативно.

(4) *Если p и p' — два различных простых делителя числа q и p^2 не делят q, то каждый элемент кольца $\mathcal{N}_p(q)$ перестановочен с элементом Фробениуса $\Pi(p')$.*

Доказательство. Прежде всего поскольку $K \subset \Gamma_0^n(p)$, то функция

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \to r_p(C) \quad (M \in \Sigma^n), \tag{3.35}$$

где $r_p(C)$ обозначает ранг матрицы C по модулю p, принимает постоянное значение на каждом левом и двойном классе по группе K; в частности, ее значение на $W_r(p,q)$ и на KM_rK равно r. Таким образом, двойные классы ξ_r попарно различны. Так как

$$W_r(p,q) \subset M_r\Gamma_0^n \subset KM_rK,$$

то из леммы 3.8 следует, что каждый из классов ξ_r имеет разложение (3.32) и в $\mathcal{N}_p(q)$ нет других двойных классов, кроме $\xi_0, \xi_1, \ldots, \xi_n$.

Формула (3.33) следует из тождеств (3.27), поскольку число элементов множества $V_p(\mathrm{i})$ для $\mathrm{i} \in I_{r,n}$ равно, очевидно, $p^{j_1+\cdots+j_{n-r}-\langle n-r\rangle}$, где $(j_1,\ldots,j_{n-r}) = \widehat{\mathrm{i}}$.

Далее, по сказанному выше

$$M_r^* = M_r^{-1} = \begin{pmatrix} * & * & * & * \\ * & * & * & * \\ -q_1E_r & 0 & * & * \\ 0 & 0 & * & * \end{pmatrix} \in KM_rK,$$

откуда следует (3.34).

Наконец, если $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_0^n(q_1)$ и матрицы S, S' из $\mathbb{S}_n$ удовлетворяют сравнению $AS' \equiv B + SD \pmod{p'}$, то матрица

$$\begin{aligned} M' = \begin{pmatrix} A' & B' \\ C' & D' \end{pmatrix} &= \begin{pmatrix} E & S \\ 0 & p'E \end{pmatrix}\begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} E & S' \\ 0 & p'E \end{pmatrix}^{-1} \\ &= \begin{pmatrix} A+SC & (-(A+SC)S'+B+SD)/p \\ p'C & -CS'+D \end{pmatrix} \end{aligned}$$

содержится в группе $\Gamma_0^n(q_1)$, $r_p(C') = r_p(C)$, и она удовлетворяет соотношению

$$\begin{pmatrix} E & S \\ 0 & p'E \end{pmatrix} M = M' \begin{pmatrix} E & S' \\ 0 & p'E \end{pmatrix}.$$

Легко видеть, что для любых двух матриц $M, M_1 \in \Gamma_0^n(q_1)$ с различными левыми классами KM, KM_1 левые классы KM', KM_1' снова различны. Отсюда следует соотношение

$$\begin{aligned} \Pi(p')\xi_r(p) &= \sum_{\substack{M \in K\backslash\Gamma_0^n(q_1), r_p(C(M))=r, \\ S \in \mathbb{S}_n/p\mathbb{S}_n}} \left(K\begin{pmatrix} E & S \\ 0 & p'E \end{pmatrix} M\right) \\ &= \sum_{\substack{M' \in K\backslash\Gamma_0^n(q_1), r_p(C(M'))=r, \\ S' \in \mathbb{S}_n/p\mathbb{S}_n}} \left(KM'\begin{pmatrix} E & S' \\ 0 & p'E \end{pmatrix}\right) = \xi_r(p)\Pi(p'), \end{aligned}$$

где $C(M)$ и $C(M')$ обозначают левые нижние $n \times n$-блоки соответствующих матриц. •

Лемма 3.10. *В обозначениях и предположениях предложения* 2.9 *произведения элементов* (3.31) *кольца* $\mathcal{N}_p(q)$ *на элемент* $\xi_n(p)$ *задаются следующими формулами*

$$\xi_n(p)\xi_r(p) = \sum_{s=0}^{r} p^{\langle n-r\rangle+(r-s)(n-r+s)}\,\mathrm{sm}_p(s, n-r+s)\xi_{n-r+s}(p), \tag{3.36}$$

где $r = 0, 1, \ldots, n$ *и* $\mathrm{sm}_p(a, b)$ *обозначает число симметрических матриц порядка* b *и ранга* a *над полем из* p *элементов.*

Доказательство. По предложению 3.9 и определению умножения в HS-кольцах произведение $\xi_n(p)\xi_r(p)$ является суммой левых классов всех произведений вида

$$\begin{pmatrix} aE_n & aD+bE_n \\ q_1E_n & q_1D+pE_n \end{pmatrix} M_r \begin{pmatrix} E_r & V & D' & 0 \\ 0 & E_{n-r} & 0 & 0 \\ 0 & 0 & E_r & 0 \\ 0 & 0 & -{}^tV & E_{n-r} \end{pmatrix} \begin{pmatrix} M(\mathrm{i}) & 0 \\ 0 & {}^tM(\mathrm{i})^{-1} \end{pmatrix}$$
$$= \begin{pmatrix} * & * & * & * \\ * & * & * & * \\ \check{D}_1 & 0 & * & * \\ q_1^2D_3 & q_1E_{n-r} & * & * \end{pmatrix} \begin{pmatrix} E_r & V & D' & 0 \\ 0 & E_{n-r} & 0 & 0 \\ 0 & 0 & E_r & 0 \\ 0 & 0 & -{}^tV & E_{n-r} \end{pmatrix} \begin{pmatrix} M(\mathrm{i}) & 0 \\ 0 & {}^tM(\mathrm{i})^{-1} \end{pmatrix},$$

где $D = \left(\begin{smallmatrix} D_1 & D_2 \\ D_3 & D_4 \end{smallmatrix}\right)$, $D' \in \mathbb{S}_n/p\mathbb{S}_n$, $V \in V(\mathrm{i})$, $\mathrm{i} \in I_{r,n}$ и где $\check{D} = q_1^2D_1 + q_1(a+p)E_r$. Такое произведение принадлежит двойному классу $KM_{r'}K$ в том и только в том случае, если ранг матрицы

$$\begin{pmatrix} \check{D}_1 & 0 \\ q_1^2D_3 & q_1E_{n-r} \end{pmatrix}$$

по модулю p равен r' (см. (3.35) и далее). С другой стороны, этот ранг, очевидно, равен $n-r+s$, где s обозначает ранг $r_p(\check{D}_1)$. Поскольку матрица $\check{D}_1$ пробегает вместе с D_1 все симметрические матрицы порядка r по модулю p, мы заключаем, что число произведений, принадлежащих двойному классу $KM_{n-r+s}K$, равно

$$\mathrm{sm}_p(s, r)p^{\langle n-r\rangle+r(n-r)}\#(W_r(p,q)) = \mathrm{sm}_p(s, r)p^{\langle n\rangle}\frac{\varphi_n(p)}{\varphi_r(p)\varphi_{n-r}(p)}$$

(см. (3.33)). Деля это число на число $\#(W_{n-r+s}(p,q))$ левых классов, содержащихся в $\xi_{n-r+s}(p)$, мы видим, что коэффициент при $\xi_{n-r+s}(p)$ в произведении $\xi_n(p)\xi_r(p)$ равен

$$\mathrm{sm}_p(s, r)p^{\langle n\rangle-\langle n-r+s\rangle}\frac{\varphi_{n-r+s}(p)\varphi_{r-s}(p)}{\varphi_r(p)\varphi_{n-r}(p)}$$
$$= p^{\langle r-s\rangle+(r-s)(n-r+s)}\,\mathrm{sm}_p(s,s)\frac{\varphi_r(p)\varphi_{n-r+s}(p)\varphi_{r-s}(p)}{\varphi_s(p)\varphi_{r-s}(p)\varphi_r(p)\varphi_{n-r}(p)}$$
$$= p^{\langle r-s\rangle+(r-s)(n-r+s)}\,\mathrm{sm}_p(s, n-r+s),$$

где мы дважды воспользовались формулой

$$\mathrm{sm}_p(a,b) = \mathrm{sm}_p(a,a)\frac{\varphi_b(p)}{\varphi_a(p)\varphi_{b-a}(p)} \quad (0 \leqslant a \leqslant b) \tag{3.37}$$

(см., например, [4, лемма 3.5.20]) и очевидным соотношением $\langle a+b\rangle = \langle a\rangle + \langle b\rangle + ab$. •

Отметим, что числа $\mathrm{sm}_p(a,b)$ можно явно вычислить с помощью формул (3.37) и формулы

$$\mathrm{sm}_p(a,a) = \sum_{i=0}^{a}(-1)^i p^{\langle i-1\rangle+\langle a-i\rangle}\frac{\varphi_a(p)}{\varphi_i(p)\varphi_{a-i}(p)}, \tag{3.38}$$

которая эквивалентна первому тождеству леммы 3.5.21 из [4].

Лемма 3.11. *В обозначениях и предположениях предложения 2.9 элемент $\xi_n^n = \xi_n^n(p)$ обратим в кольце $\mathcal{N}_p^n(q)$. В частности, имеют место формулы*

$$(\xi_1^1)^{-1} = ((1-p)\xi_0^1 + \xi_1^1)/p; \tag{3.39}$$

$$(\xi_2^2)^{-1} = ((1-p)\xi_0^2 + (1-p)\xi_1^2 + \xi_2^2)/p^3. \tag{3.40}$$

Доказательство. Формулы (3.36) показывают, что матрицы оператора умножения на ξ_n^n в базисе $\xi_0^n, \xi_1^n, \dots, \xi_n^n$ пространства $\mathcal{N}_p^n(q)$ имеют нули над второй диагональю и ненулевые элементы $p^{\langle r\rangle+r(n-r)}\mathrm{sm}_p(0, n-r) = p^{\langle r\rangle+r(n-r)}$ для $r = 0, 1, \dots, n$ на этой диагонали. Например, для $n = 1$ и $n = 2$ мы получаем матрицы

$$\begin{pmatrix} 0 & 1 \\ p & p-1 \end{pmatrix} \quad \text{и} \quad \begin{pmatrix} 0 & 0 & 1 \\ 0 & p^2 & p^2-1 \\ p^3 & p^2(p-1) & p^2(p-1) \end{pmatrix}$$

соответственно. Такая матрица, очевидно, обратима, что доказывает обратимость элемента ξ_n^n. Формулы (3.39) и (3.40) получаются обращением соответствующих матриц. •

В отличие от леммы 3.8, где числа q/q_1 и q_1 взаимно-просты, в случае, когда число q и его делитель q_1 имеют одинаковые простые множители, левые классы $\Gamma_0^n(q) \setminus \Gamma_0^n(q_1)$ допускают очень простое описание, которое нам потребуется в случае, когда частное q/q_1 является простым числом.

Предложение 3.12. *Пусть p — простое число такое, что p^2 делит q. Тогда имеют место следующие утверждения:*

(1) *Множество*

$$\left\{\begin{pmatrix} E_n & 0 \\ q_1 C & E_n \end{pmatrix}; C \in \mathbb{S}_n/p\mathbb{S}_n\right\},$$

где $q_1 = q/p$, является полным множеством представителей из различных левых классов группы $K_1 = \Gamma_0^n(q_1)$ по подгруппе $K = \Gamma_0^n(q)$.

(2) *Элемент*

$$\begin{aligned}\tau(p) = \tau^n(p,q) &= p^{-\langle n\rangle} \sum_{M_i \in K\backslash K_1} (KM_i) \\ &= p^{-\langle n\rangle} \sum_{C\in \mathbb{S}_n/p\mathbb{S}_n} \left(K\begin{pmatrix} E_n & 0 \\ q_1C & E_n\end{pmatrix}\right) \in \mathcal{N}(q_1,q) \end{aligned} \tag{3.41}$$

удовлетворяет соотношению

$$\Pi(p)\tau(p) = \Pi(p),$$

где $\Pi(p)$ *— элемент Фробениуса мультипликатора* p.

(3) *Элемент* $\tau(p)$ *коммутирует с каждым элементом Фробениуса* $\Pi(p')$ *для простых* $p' \neq p$ *и делящих* q.

(4) *Элемент* $\tau(p)$ *удовлетворяет соотношению*

$$\tau^*(p) = \tau(p),$$

где звездочка обозначает антиавтоморфизм (1.18).

Доказательство. „Вторые строки" различных матриц из указанного множества, очевидно, не пропорциональны по модулю q в смысле (3.13), и, таким образом, по лемме 3.6 эти матрицы принадлежат различным левым классам по модулю K. Если $\begin{pmatrix} * & * \\ q_1C' & D\end{pmatrix} \in K_1$, то матрица D обратима по модулю q_1 и, поскольку $q \mid q_1^2$, она имеет также обратную матрицу D' по модулю q. Отсюда следует, что пара (q_1C', D) пропорциональна по модулю q паре

$$(q_1D'C', D'D) \equiv (q_1C, E_n) \pmod q,$$

что завершает доказательство части (1).

Так как все произведения

$$\begin{pmatrix} E & B \\ 0 & pE\end{pmatrix}\begin{pmatrix} E & 0 \\ q_1C & E\end{pmatrix}\begin{pmatrix} E & B \\ 0 & pE\end{pmatrix}^{-1} = \begin{pmatrix} E+q_1BC & -(q_1/p)BCB \\ qC & E-q_1CB\end{pmatrix},$$

где $E = E_n$ и $B, C \in \mathbb{S}_n$ принадлежат группе K, то

$$\begin{aligned}\Pi(p)\tau(p) &= p^{-\langle n\rangle} \sum_{B,C\in \mathbb{S}/p\mathbb{S}} \left(K\begin{pmatrix} E & B \\ 0 & pE\end{pmatrix}\begin{pmatrix} E & 0 \\ q_1C & E\end{pmatrix}\right) = \sum_{B\in \mathbb{S}/p\mathbb{S}} \left(K\begin{pmatrix} E & B \\ 0 & pE\end{pmatrix}\right) \\ &= \Pi(p),\end{aligned}$$

где $\mathbb{S} = \mathbb{S}_n$, что доказывает часть (2).

Можно считать, что все матрицы C в (3.41) делятся на p'. Тогда мы имеем

$$\begin{aligned} p^{\langle n\rangle}\Pi(p')\tau(p) &= \sum_{\substack{B\in \mathbb{S}/p'\mathbb{S},\\ C\in \mathbb{S}/p\mathbb{S}}} \left(K\begin{pmatrix} E & B \\ 0 & p'E\end{pmatrix}\begin{pmatrix} E & 0 \\ q_1p'C & E\end{pmatrix}\right) \\ &= \sum_{B,C} \left(K\begin{pmatrix} E+q_1p'BC & -q_1BCB \\ q_1(p')^2C & E-q_1p'CB\end{pmatrix}\begin{pmatrix} E & B \\ 0 & p'E\end{pmatrix}\right) \\ &= p^{\langle n\rangle}\tau(p)\Pi(p'),\end{aligned}$$

поскольку матрица

$$\begin{pmatrix} E & B \\ 0 & p'E \end{pmatrix}\begin{pmatrix} E & 0 \\ q_1p'C & E \end{pmatrix}\begin{pmatrix} E & B \\ 0 & p'E \end{pmatrix}^{-1} = \begin{pmatrix} E + q_1p'BC & -q_1BCB \\ q_1(p')^2C & E - q_1p'CB \end{pmatrix}$$

содержится в K_1 и пробегает полную систему представителей из $K \setminus K_1$, когда C пробегает множество $\mathbb{S}/p\mathbb{S}$.

Часть (4) легко следует из определений. •

В следующем параграфе мы увидим, как нейтральные кольца работают в сингулярной теории.

§3.3. Неразветвленные вложения локальных колец

Мы говорим, что q-сингулярное простое число p называется *неразветвленным*, если оно не делит частное $q_1 = q/p$, в противном случае оно называется *разветвленным*. В этом параграфе мы покажем, что элементы Фробениуса $\Pi(p)$ для неразветвленных простых чисел p обратимы в некотором расширении сингулярного HS-кольца $\mathcal{H}_q(K)$ группы $K = \Gamma_0^n(q)$. Это позволит нам определить естественное гомоморфное вложение (регулярного) p-кольца

$$\mathcal{H}_p(q_1) = \mathcal{H}_p^n(q_1) = HS(\Gamma_0^n(q_1), R_p(\Gamma_0^n(q_1))) \tag{3.42}$$

группы $\Gamma_0^n(q_1)$ в это расширение. Такие вложения заменяют параболические вложения регулярной теории и имеют многие аналогичные свойства.

Лемма 3.13. *Пусть p — неразветвленный простой делитель числа q. Тогда матрица*

$$H(p) = H^n(p,q) = \begin{pmatrix} apE_n & bE_n \\ qE_n & pE_n \end{pmatrix}, \tag{3.43}$$

где a и b — рациональные целые числа, удовлетворяющие соотношению $ap - bq_1 = 1$, является симплектической матрицей с мультипликатором $\mu(H(p)) = p$, удовлетворяющей следующим соотношениям

$$H(p)^2 = \gamma_p \cdot (pE_{2n}), \quad \text{где } \gamma_p \in K, \tag{3.44}$$

$$KH(p)K = H(p)K. \tag{3.45}$$

Доказательство является рутинным упражнением на умножение блочных матриц, которые мы оставляем читателю.

Лемма 3.14. *Пусть p — неразветвленный простой делитель числа q. Тогда двойной класс*

$$\Omega(p) = \Omega^n(p,q) = (H^n(p,q))_K \in \mathcal{H}_q(K) \tag{3.46}$$

имеет следующие свойства:

$$\Omega(p) = (KH(p)); \tag{3.47}$$

$$\Omega(p)^2 = [p], \tag{3.48}$$

где $[p]$ *элемент* (2.8);

$$\Omega(p)^* = \Omega(p), \tag{3.49}$$

где звездочка обозначает антиавтоморфизм (1.18);

$$\Pi(p) = \Omega(p)\xi_n(p), \tag{3.50}$$

где $\Pi(p)$ *и* $\xi_n(p) = \xi_n^n(p)$ *были определены соотношениями* (3.2) *и* (3.31) *соответственно*;

$$\Omega(p)\Omega(p') = \Omega(p')\Omega(p), \tag{3.51}$$

если p' *— другое неразветвленное простое число*;

$$\Omega(p)\Pi(p') = \Pi(p')\Omega(p), \tag{3.52}$$

если p' *— сингулярное простое число, отличное от* p.

Доказательство. Разложение (3.47) следует из (3.45). Соотношение (3.48) следует из (3.47) и (3.44). По определению отображения звездочка и (3.44) мы имеем

$$\Omega(p)^* = (pH(p)^{-1}) = (\gamma_p H(p)) = \Omega(p).$$

Согласно (3.47), (3.32) и (3.4), мы получаем

$$\begin{aligned}
\Omega(p)\xi_n(p) &= \sum_{B\in\mathbb{S}_n/p\mathbb{S}_n} \left(KH(p)M_n\begin{pmatrix} E_n & B \\ 0 & E_n \end{pmatrix}\right) \\
&= \sum_B \left(KH(p)M_n\begin{pmatrix} E & 0 \\ 0 & pE \end{pmatrix}^{-1}\begin{pmatrix} E & B \\ 0 & pE \end{pmatrix}\right) \\
&= \Pi(p),
\end{aligned}$$

так как матрица

$$H(p)M_n\begin{pmatrix} E & 0 \\ 0 & pE \end{pmatrix}^{-1} = \begin{pmatrix} (a^2p+bq_1)E & (ab+b)E \\ q(a+1)E & (q_1b+p)E \end{pmatrix},$$

где $E = E_n$ и $q_1 = q/p$ принадлежит группе K.

Далее, можно без труда проверить, что матрица $H(p)H(p')H(p)^{-1}H(p')^{-1}$ содержится в K, откуда следует (3.51).

Наконец, легко проверить, что произведение

$$H(p)\begin{pmatrix} E & B \\ 0 & p'E \end{pmatrix}H(p)^{-1}\begin{pmatrix} E & B' \\ 0 & p'E \end{pmatrix}^{-1}$$

с $B, B' \in \mathbb{S}_n$ принадлежит группе K, если выполняется сравнение

$$B' \equiv aB - p^{-1}bE \pmod{p'}.$$

Отсюда следует соотношение

$$\Omega(p)\Pi(p') = \sum_{B\in\mathbb{S}_n/p'\mathbb{S}_n} \left(KH(p)\begin{pmatrix} E & B \\ 0 & p'E\end{pmatrix}\right) = \sum_{B'\in\mathbb{S}_n/p'\mathbb{S}_n} \left(K\begin{pmatrix} E & B' \\ 0 & p'E\end{pmatrix}H(p)\right)$$
$$= \Pi(p')\Omega(p). \quad \bullet$$

Теперь мы сделаем небольшой перерыв для того, чтобы напомнить простую конструкцию, которая нам потребуется позднее. Если $\mathbb{A}$ — ассоциативное кольцо с единичным элементом и $a_1, \dots, a_r$ — неделители нуля, приндлежащие центру кольца $\mathbb{A}$, то можно построить наименьшее расширение кольца $\mathbb{A}$, где все элементы $a_1, \dots, a_r$ обратимы, используя стандартную процедуру локализации относительно мультипликативной системы

$$S = \{a_1^{n_1} \dots a_r^{n_r}\ ;\ n_1, \dots, n_r = 0, 1, \dots\}.$$

Мы будем обозначать это расширение через

$$\mathbb{A}[S^{-1}] = \mathbb{A}[a_1^{-1}, \dots, a_r^{-1}].$$

(Это обозначение уже было использовано ранее в предложении 2.11).

Предложение 3.15. *Пусть p — простой делитель числа q, не делящий отношение q/p, тогда элемент Фробениуса $\Pi(p) = \Pi_K^n(p)$ обратим в расширении*

$$\mathcal{H}'_p(K) = \mathcal{H}_p(K)[[p]^{-1}]$$

кольца $\mathcal{H}_p(K)$, и

$$\Pi(p)^{-1} = [p]^{-1} \cdot \xi_n(p)^{-1} \cdot \Omega(p). \tag{3.53}$$

Доказательство. Утверждение следует из (3.50), (3.48) и леммы 3.11. $\bullet$

Теперь при помощи обратного элемента Фробениуса (3.53) мы определим гомоморфизм локального p-подкольца $\mathcal{L}_p = \mathcal{L}_p^n$ треугольного кольца (2.28), где p — некоторое q-сингулярное неразветвленное простое число, в подходящее расширение локального p-кольца группы $K = \Gamma_p^n(q)$.

Пусть $X \in \mathcal{L}_p$. Согласно предложению 2.11, „проекции" $X \cdot \widehat{\Pi}(p)^d$ содержатся в централизаторе $\widehat{C}_p$ элемента $\widehat{\Pi}(p)$ в $\mathcal{L}_p$,

$$X \cdot \widehat{\Pi}(p)^d \in \widehat{C}_p, \tag{3.54}$$

если d достаточно велико. По теореме 3.3(3), (4) кольцо $\widehat{C}_p$ является изоморфным образом при параболическом вложении (2.30) централизатора C_p элемента $\Pi(p) = \Pi_K(p)$ в кольце $S_p(q)$,

$$j(C_p) = \widehat{C}_p,$$

и потому имеется единственный элемент

$$i(X \cdot \widehat{\Pi}(p)^d) \in C_p, \tag{3.55}$$

где i обозначает отображение кольца $\widehat{C}_p$, обратное к отображению j. Тогда мы положим

$$\widetilde{X} = \Pi(p)^{-d} \cdot i(X \cdot \widehat{\Pi}(p)^d) \in C'_p = C_p[\Pi(p)^{-1}] \in \mathcal{H}'_p(K), \tag{3.56}$$

где $\Pi(p)^{-d} = (\Pi(p)^{-1})^d$.

Теорема 3.16. *Пусть p — некоторое q-сингулярное неразветвленное простое число, т.е. $p \mid q$, но $p^2 \nmid q$. Тогда справедливы следующие утверждения:*

(1) *Для каждого $X \in \mathcal{L}_p = \mathcal{L}_p^n$ элемент X, определенный соотношением* (3.56), *не зависит от выбора числа $d \in \mathbb{N}$, удовлетворяющего условию* (3.54).

(2) *Отображение*

$$X \to \widetilde{X} \in C_p[\Pi(p)^{-1}] \quad (X \in \mathcal{L}_p) \tag{3.57}$$

является $\mathbb{Q}$-линейным гомоморфизмом колец.

(3) *Ограничение отображения* (3.57) *на образ $\widehat{\mathcal{H}}_p(q_1) \subset \mathcal{L}_p$ локального HS-кольца* (3.42) *группы $\Gamma_0^n(q_1)$, где $q_1 = q/p$, при параболическом вложении* (2.30) *является изоморфным вложением этого кольца в $C_p[\Pi(p)^{-1}]$.*

Доказательство. (1) Если d_1 — другой показатель, удовлетворяющий условию (3.54), и, скажем, $d_1 > d$, то

$$\begin{aligned}\Pi^{-d_1} \cdot i(X\widehat{\Pi}^{d_1}) &= \Pi^{-d_1} \cdot i(X\widehat{\Pi}^{d} \cdot \widehat{\Pi}^{d_1-d}) \\ &= \Pi^{-d_1} \cdot i(\widehat{\Pi}^{d_1-d} \cdot i(X\widehat{\Pi}^{d})) = \Pi^{-d_1}\Pi^{d_1-d} \cdot i(X\widehat{\Pi}^{d}) \\ &= \Pi^{-d} \cdot i(X\widehat{\Pi}^{d}),\end{aligned}$$

где $\Pi = \Pi(p)$.

(2) Если $X, X_1 \in \mathcal{L}_p$ и d удовлетворяют условию (3.54) и для X, и для X_1, то мы имеем

$$\begin{aligned}\widetilde{XX_1} &= \Pi^{-2d} \cdot i(XX_1\widehat{\Pi}^{2d}) = \Pi^{-2d} \cdot i(X(X_1\widehat{\Pi}^{d})\widehat{\Pi}^{d}) = \Pi^{-2d} \cdot i((X\widehat{\Pi}^{d}) \cdot (X_1\widehat{\Pi}^{d})) \\ &= \Pi^{-d} \cdot i(X\widehat{\Pi}^{d}) \cdot \Pi^{-d} \cdot i(X_1\widehat{\Pi}^{d}),\end{aligned}$$

поскольку элемент $i(X\widehat{\Pi}^{d})$ содержится в C_p, и потому коммутирует с Π и Π^{-1}.

(3) Если X — ненулевой элемент кольца $\widehat{\mathcal{H}}_p(q_1)$, то $X\widehat{\Pi}(p)^d \neq 0$ по предложению 2.11 и равенствам (2.51), откуда $\widetilde{X} \neq 0$, поскольку элемент $\Pi(p)^{-d}$ не является делителем нуля в кольце $\mathcal{H}'_p(K)$. •

Из определения параболических вложений и последней части теоремы 3.16 следует, что отображение

$$T \to \widehat{T} \to \widetilde{T} \in C_p[\Pi(p)^{-1}] \quad (T \in \mathcal{H}_p(q_1)) \tag{3.58}$$

является композицией двух изоморфных вложений и потому само является изоморфным вложением. Мы будем говорить, что отображение (3.58) является *неразветвленным вложением кольца $\mathcal{H}_p^n(q_1)$*, и называть его образ

$$\mathcal{H}_p(q) = \mathcal{H}_p^n(q) = \widetilde{\mathcal{H}_p^n}(q_1) \tag{3.59}$$

неразветвленным (сингулярным) p-кольцом группы $K = \Gamma_0^n(q)$.

Теорема 3.17. *Пусть p — некоторое q-сингулярное неразветвленное простое число. Тогда справедливы следующие утверждения:*

(1) *Каждый элемент p-кольца (3.59) коммутирует с каждым элементом регулярного приводимого кольца (2.3).*

(2) *Каждый элемент p-кольца (3.59) коммутирует с каждым элементом любого другого неразветвленного p'-кольца $\mathcal{H}_{p'}(q)$ и с каждым из сингулярных элементов Фробениуса $\Pi(a)$ с $a \mid q^\infty$.*

(3) *Элемент $\Pi(p)$ удовлетворяет уравнению*

$$\sum_{j=0}^{m} \widetilde{q_j^n}(p)\Pi(p)^{m-j} = 0 \quad (m = 2^n), \tag{3.60}$$

коэффициенты которого $\widetilde{q_j^n}(p) \in \mathcal{H}_p(q)$ являются образами при отображении (3.58) соответствующих коэффициентов $q_j^n(p) \in \mathcal{H}_p(q_1)$ многочлена (2.27) с $q_1 = q/p$ вместо q; коэффициенты $\tilde{q}_j^n(p)$ удовлетворяют соотношениям

$$\begin{aligned} \widetilde{q_{m-i}^n}(p) &= (p^{\langle n\rangle}[p]K)^{(m/2)-i}\widetilde{q_i^n}(p) \quad (0 \leqslant i \leqslant m), \\ \widetilde{q_0^n}(p) &= [1]_K, \\ \widetilde{q_m^n}(p) &= (p^{\langle n\rangle}[p]_K)^{m/2}. \end{aligned} \tag{3.61}$$

Доказательство. По теореме 2.3 и 2.5, утверждение (1) достаточно доказать для локального регулярного приводимого кольца $\mathcal{D}$ вместо кольца $\mathcal{H}_{\text{rr}}(q)$. В этом случае из предложения 2.12 следует, что каждый элемент из $\mathcal{D}$ перестановочен с каждым элементом из C_p. В частности, он коммутирует с $\Pi(p)$ и, стало быть, с $\Pi(p)^{-1}$. Отсюда следует, что каждый элемент из $\mathcal{D}$ коммутирует с каждым элементом кольца $C_p[\Pi(p)^{-1}]$, которое содержит p-кольцо $\mathcal{H}_p(q)$. Утверждение (1) доказано.

Поскольку кольца $\mathcal{H}_p(q)$, $\mathcal{H}_{p'}(q)$ и элементы $\Pi(a)$ для неразветвленных простых p, p' и $a \mid q^\infty$ содержатся в коммутативном расширении кольца C_q, утверждение (2) выполняется.

Соотношение (3.60) следует из (2.52), если применить к левой и правой частям гомоморфизм (3.57). Аналогично соотношения (3.61) следуют из соответствующих соотношений для коэффициентов многочлена (2.27) и очевидных соотношений

$$\widetilde{[p^\delta]_{K_1}} = [\widetilde{p^\delta}]_{\Gamma_0} = [p^\delta]_K, \tag{3.62}$$

где

$$K_1 = \Gamma_0^n(q_1) \quad \text{и} \quad \delta = 0, 1, \ldots \quad \bullet$$

Неразветвленные вложения (3.58) и гомоморфизмы (3.57) позволяют преобразовать все разложения многочленов над локальными HS-кольцами группы $\Gamma = \Gamma^n$ с множителями над HS-кольцами $\mathcal{L}_p$ треугольных подгрупп, полученные, например, в [4, §3.5], в соответствующие разложения многочленов над p-кольцами $\mathcal{H}_p(q)$ с множителями над кольцами $C'_p = C_p[\Pi(p)^{-1}]$, если p —

неразветвленное простое число. Интересно отметить, что хотя порядок множителей над кольцами $\mathcal{L}_p$ строго фиксирован, порядок их образов не имеет значения, поскольку коэффициенты образов принадлежат коммутативному кольцу C'_p.

Пусть p — неразветвленное простое число и пусть

$$\widetilde{Q}_p(v) = \widetilde{Q}_p^n(v) = \sum_{i=0}^{m}(-1)^i\widetilde{q_i^n}(p)v^i \quad (m = 2^n) \tag{3.63}$$

— многочлен над p-кольцом $\mathcal{H}_p(q)$, коэффициенты которого являются образами соответствующих коэффициентов многочлена (2.27) над кольцом $\mathcal{H}_p(q_1)$ при неразветвленном вложении. Тогда из предложения 3.5.11 книги [4] следует разложение

$$\widetilde{Q}_p(v) = Q'(v)([1] - \Pi(p)v),$$

где $Q'(v)$ — многочлен степени $2^n - 1$ над C'_p, что следует также из равенства (3.60). Для небольших n можно получить более точные результаты.

Предложение 3.18. *Пусть p — некоторое q-сингулярное неразветвленное простое число и пусть $n = 1$. Тогда многочлен $\widetilde{Q}_p^1$ имеет следующее разложение над кольцом $(C_p^1)'$:*

$$\widetilde{Q}_p^1(v) = [1] - \widetilde{T}^1(p)v + p[p]v^2 = ([1] - p[p]\Pi(p)^{-1}v)([1] - \Pi(p)v), \tag{3.64}$$

где $[1] = [1]_K$, $[p] = [p]_K$ с $K = \Gamma_0^1(q)$ и где $T^1(p) \in \mathcal{H}_p^1(q_1)$ имеет вид (2.20). *В частности, средний коэффициент $\widetilde{T}^1(p)$ можно записать в виде*

$$\widetilde{T}^1(p) = p[p]\Pi(p)^{-1} + \Pi(p) = (1-p)\Omega(p) + \Pi(p)^* + \Pi(p), \tag{3.65}$$

где $\Omega(p) = \Omega^1(p, q)$ — элемент (3.46) *и где звездочка обозначает антиавтоморфизм* (1.18).

Доказательство. Применяя покоэффициентно отображение (3.57) к разложению многочлена $\widehat{Q}_p^1(v)$, полученному в [4, предложение 3.5.13], мы получаем разложение

$$\widetilde{Q}_p = ([1] - \widetilde{\Pi}_0^1(p)v)([1] - \Pi(p)v),$$

что доказывает равенство (3.64), так как

$$\widetilde{\Pi}_0^1(p) = \Pi(p)^{-1} \cdot i(\Pi_0^1(p)\widehat{\Pi}(p)) = \Pi(p)^{-1} \cdot p[p],$$

согласно (3.62) и соотношению (3.4.13) из [4]. Формулы (3.65) следуют из (3.64), (3.53) и (3.39), так как

$$\xi_1(p)\Omega(p) = \xi_1(p)^*\Omega(p)^* = (\Omega(p)\xi_1(p))^* = \Pi(p)^*$$

по (3.34) и (3.49). •

В случае $n = 2$ формулы сложнее.

Предложение 3.19. *Пусть p — некоторое q-сингулярное неразветвленное простое число и пусть $n = 2$. Тогда многочлен $\widetilde{Q}_p^2(v)$ имеет следующее разложение над кольцом $C_p[\Pi(p)^{-1}]$:*

$$\begin{aligned}\widetilde{Q}_p^2(v) &= [1] - \widetilde{T}^2(p)v + \widetilde{q}_2(p)v^2 - p^3[p]\widetilde{T}^2(p)v^3 + p^6[p^2]v^4 \\ &= ([1] - p^3[p]\Pi(p)^{-1}v)([1] - p\Pi(p)^{-1}\Pi_1(p^2)v + p^3[p]v^2)([1] - \Pi(p)v),\end{aligned} \tag{3.66}$$

где $[p^\delta] = [p^\delta]_K$, $K = \Gamma_0^2(q)$, $T^2(p)$ *и* $q_2(p)$ *были определены в* (2.20) *и* (2.26) *и где*

$$\Pi_1(p^2) = (\mathrm{diag}(p, 1, p, p^2))_K \in C_p. \tag{3.67}$$

Доказательство. Из разложения многочлена $\widehat{Q}_p^2(v)$, приведенного в [4], предложение 3.5.14, где элемент $\Pi_{2,0}^{(2)}$ (опечатка!) должен быть заменен на $\Pi_{2,0}^{(0)}$, следует разложение

$$\widetilde{Q}_p^2(v) = ([1] - \widetilde{\Pi}_-v)([1] - \widetilde{\Pi}v + p(\widetilde{\Pi}_{2,0}^{(1)} + \widetilde{\Pi}_{2,0}^{(0)})v^2)([1] - \widetilde{\Pi}_+v),$$

где мы использовали обозначения указанного предложения. Используя (3.56) и соотношения (3.4.14), (3.5.23) и (3.5.25) из [4], мы получаем равенства

$$\begin{aligned}\widetilde{\Pi}_- &= \Pi(p)^{-1} \cdot i(\Pi_-\Pi_+) = p^3[p]\Pi(p)^{-1}, \\ \widetilde{\Pi} &= \Pi(p)^{-1} \cdot i(\Pi\Pi_+) = \Pi(p)^{-1} \cdot i(p\Pi_{1,1}^{(0)}) = p\Pi(p)^{-1} \cdot \Pi_1(p^2), \\ \widetilde{\Pi}_{2,0}^{(1)} + \widetilde{\Pi}_{2,0}^{(0)} &= \Pi(p)^{-2} \cdot i(\Pi_{2,0}^{(1)}\Pi_+^2 + \Pi_{2,0}^{(0)}\Pi_+^2) = \Pi(p)^{-2} \cdot i(p^2[p]\Pi_+^2) = p^2[p]\end{aligned}$$

и

$$\widetilde{\Pi}_+ = \Pi(p)^{-1} \cdot i(\Pi_+\Pi_+) = \Pi(p). \quad \bullet$$

Мы будем говорить, что элемент T некоторого HS-кольца группы $K = \Gamma_0^n(q)$ является *симметричным*, если он инвариантен относительно отображения звездочка (1.18):

$$T^* = T. \tag{3.68}$$

Выглядит правдоподобно, что локальные p-кольца $\mathcal{H}_p(q)$ в неразветвленных случаях состоят из симметричных элементов, как это было в регулярных случаях, согласно теореме 2.3. Поскольку кольца $\mathcal{H}_p(q)$ вместе с кольцами $\mathcal{H}_p(q/p)$ являются коммутативными полиномиальными кольцами, то было бы достаточно проверить справедливость (3.68) для некоторого множества образующих, скажем, для элементов

$$\widetilde{T}(p) = \Pi(p)^{-1} \cdot i(\widehat{T}^n(p)\widehat{\Pi}(p)), \quad \widetilde{T}_j^n(p^2) = \Pi(p)^{-2} \cdot i(\widehat{T}_j^n(p^2)\Pi(p)^2), \tag{3.69}$$

где $j = 1, \ldots, n$ (см. теорему 2.6 для кольца $\mathcal{H}_p^n(q/p)$). Однако такая проверка оказывается весьма неформальной, требует детальной информации о произведениях двойных классов в соответствующих HS-кольцах и объем необходимых вычислений растет экспоненциально с ростом n. Поэтому мы ограничимся только случаями $n = 1$ и $n = 2$.

Предложение 3.20. *Пусть p — q-сингулярное неразветвленное простое число. Тогда p-кольца $\mathcal{H}_p^1(q)$ и $\mathcal{H}_p^2(q)$ состоят из симметричных элементов.*

Доказательство. По (2.20) и (3.62) мы имеем равенства

$$\widetilde{T}_1^1(p^2) = [p]_{\Gamma_0^1(q)} \quad \text{и} \quad \widetilde{T}_2^2(p^2) = [p]_{\Gamma_0^2(q)},$$

и, стало быть, эти элементы, очевидно, симметричны. Элемент $\widetilde{T}^1(p)$ симметричен на основании формул (3.65) и (3.49), что заканчивает доказательство в случае $n = 1$. Если $n = 2$, то, как мы видели, достаточно показать, что элементы

$$\widetilde{T}(p) = \widetilde{T}^2(p) \quad \text{и} \quad \tilde{q}_2(p) = p\widetilde{T}_1^2(p^2) + p(p^2+1)[p]_{\Gamma_0^2(q)} \tag{3.70}$$

являются симметричными (см. (2.26)), что оказывается совсем непросто и требует дополнительной информации об умножении некоторых двойных классов в кольце

$$\mathcal{H}_p^2(q_1, q) = HS(K, \Sigma_p^2(q_1)), \tag{3.71}$$

где $K = \Gamma_0^2(q)$, $q_1 = q/p$, и

$$\Sigma_p^2(q_1) = \left\{ M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Sigma_p^2; C \equiv 0 \pmod{q_1} \right\}. \tag{3.72}$$

Конкретнее, нам потребуются формулы для произведений двойных классов мультипликатора 1 на двойные классы мультипликаторов 1 и p.

Что касается произведений двойных классов мультипликатора 1, то они принадлежат нейтральному подкольцу $\mathcal{N}^2(q_1, q)$ кольца (3.71), и по лемме 3.10 мы имеем формулы

$$\begin{aligned} \xi \cdot \xi_1 = \xi_1 \cdot \xi &= p^2\xi_1 + (p^2-1)\xi, \\ \xi^2 &= p^3[1] + p^2(p-1)\xi_1 + p^2(p-1)\xi, \end{aligned} \tag{3.73}$$

где $\xi_1 = \xi_1^2(p)$, $\xi = \xi_2^2(p)$ — элементы вида (3.31), из которых следует соотношение

$$\xi^{-1}\xi_1 = ((1-p^2)[1] + \xi_1)/p^2, \tag{3.74}$$

так как

$$\xi((1-p^2)[1] + \xi_1)/p^2 = ((1-p^2)\xi + p^2\xi_1 + (p^2-1)\xi)/p^2 = \xi_1.$$

Для рассмотрения двойных классов мультипликатора p мы сначала должны представить в удобной форме представителей из всех левых классов KM, где $M \in \Sigma_p^2(q_1)$ и $\mu(M) = p$. Для этого можно умножить систему представителей из классов смежности $K \backslash \Gamma_0^2(q_1)$ на систему представителей из классов смежности

$$\Gamma_0^2(q_1) \setminus \{M \in \Sigma_p^2(q_1)\,;\, \mu(M) = p\}. \tag{3.75}$$

Что касается первой системы, мы возьмем систему, описанную в лемме 3.8, т.е. объединение трех множеств $W_0 = \{E_n\}$,

$$W_1 = M_1\left\{ \begin{pmatrix} \varepsilon & \delta \cdot {}^t\varepsilon^{-1} \\ 0 & {}^t\varepsilon^{-1} \end{pmatrix}; \varepsilon = \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \delta = \begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix}, c, d \bmod p \right\}$$

и

$$W_2 = M_2\left\{\begin{pmatrix} E & B \\ 0 & E \end{pmatrix} ; B \in \mathbb{S}_2/p\mathbb{S}_2\right\} = M_2 \cdot R_2,$$

где $E = E_2$,

$$M_1 = \begin{pmatrix} a & 0 & b & 0 \\ 0 & 1 & 0 & 0 \\ q_1 & 0 & p & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{и} \quad M_2 = \begin{pmatrix} aE & bE \\ q_1E & pE \end{pmatrix} \tag{3.76}$$

с целыми числами a и b, удовлетворяющими соотношению $ap - bq_1 = 1$.

Поскольку p не делит q_1, то по лемме 2.1 в качестве представителей из классов (3.75) мы можем взять множество треугольных представителей из классов

$$\Gamma_0^2 \setminus \{M \in \Sigma_{0,p}^2 \ ; \mu(M) = p\},$$

которое с помощью леммы 3.3.32 и 3.2.7 из [4] может быть описано как объединение трех множеств

$$\{D_0\}, \quad D_1 \cdot R_1 \quad \text{и} \quad D_2 \cdot R_2,$$

где

$$D_0 = \mathrm{diag}(p, p, 1, 1), \quad D_1 = \mathrm{diag}(1, p, p, 1), \quad D_2 = \mathrm{diag}(1, 1, p, p).$$

Однако для последующих вычислений будет удобнее изменить представителей, заменяя матрицы D_0 и D_1 матрицами $D_0' = M_2D_0$ и

$$D_1' = \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix} M_1 \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix} D_1 = M_1'D_1 \quad \text{с } I = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

соответственно, где M_1 и M_2 — матрицы (3.76). Отметим, что

$$D_0' = H(p) \quad \text{и} \quad D_1' = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & pa & 0 & b \\ 0 & 0 & p & 0 \\ 0 & q & 0 & p \end{pmatrix}, \tag{3.77}$$

где $H(p) = H^2(p, q)$ является матрицей (3.43) для $n = 2$.

Если мы умножим каждое из трех множеств выбранной системы представителей из классов $K \setminus \Gamma_0^2(q_1)$ на каждое из трех множеств измененной системы представителей из классов (3.75) и примем во внимание формулы (3.77), мы получим полную систему представителей из различных левых классов смежности множества

$$\{M \in \Sigma_p^2(q_1) \ ; \mu(M) = p\}$$

по группе K в виде объединения следующих девяти множеств:

$$\begin{aligned} &S_1 = \{H\}, && S_2 = \{D_1'R_1\}, && S_3 = \{D_2R_2\}, \\ &S_4 = \{M_1R_1H\}, && S_5 = \{M_1R_1D_1'R_1\}, && S_6 = \{M_1R_1D_2R_2\}, \\ &S_7 = \{M_2R_2H\}, && S_8 = \{M_2R_2D_1'R_1\}, && S_9 = \{M_2R_2D_2R_2\}. \end{aligned}$$

Пусть матрица $\begin{pmatrix} A & B \\ 0 & D \end{pmatrix}$ принадлежит группе Γ_0^n, тогда матрицы

$$H^{-1}\begin{pmatrix} A & B \\ 0 & D \end{pmatrix}H = \begin{pmatrix} apA + qB - bq_1D & bA + pB - bD \\ -aqA - q_1qB + aqD & -q_1bA - qB + apD \end{pmatrix}$$

и

$$D_2^{-1}\begin{pmatrix} A & B \\ 0 & D \end{pmatrix}D_2 = \begin{pmatrix} A & pB \\ 0 & D \end{pmatrix}$$

содержатся в группе K. Что же касается матрицы $(D_1')^{-1}\begin{pmatrix} A & B \\ 0 & D \end{pmatrix}D_1'$, то нетрудно проверить, перемножив соответствующие матрицы, что она принадлежит группе K, если $\begin{pmatrix} A & B \\ 0 & D \end{pmatrix} \in R_2$ или

$$\begin{pmatrix} A & B \\ 0 & D \end{pmatrix} \in R_1' = \left\{\begin{pmatrix} \varepsilon & \delta \cdot {}^t\varepsilon^{-1} \\ 0 & {}^t\varepsilon^{-1} \end{pmatrix};\ \varepsilon = \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}, \delta = \begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix}, c, d \bmod p\right\}.$$

Поэтому мы получаем включения

$$\begin{aligned}
&S_1 \subset KHK,\\
&S_2 \subset KD_1'K,\\
&S_3 \subset KD_2K,\\
&S_4 = \{M_1HH^{-1}R_1H\} \subset KM_1HK,\\
&S_6 = \{M_1D_2D_2^{-1}R_1D_2R_2\} \subset KM_1D_2K,\\
&S_7 = \{M_2HH^{-1}R_2H\} \subset KM_2HK,\\
&S_8 = \{M_2D_1'(D_1')^{-1}R_2D_1'R_1\} \subset KM_2D_1'K,\\
&S_9 = \{M_2D_2D_2^{-1}R_2D_2R_2\} \subset KM_2D_2K.
\end{aligned} \tag{3.78}$$

Что же касается множества S_5, мы разделим множество R_1 на определенное выше подмножество R_1' и дополнительное подмножество

$$R_1'' = \left\{\begin{pmatrix} I & \delta I \\ 0 & I \end{pmatrix} = \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix}\begin{pmatrix} E & \delta' \\ 0 & E \end{pmatrix};\ \delta' = I\delta I = \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}, d \bmod p\right\}.$$

Тогда мы получаем следующее разбиение:

$$\begin{aligned}
S_5 &= \{M_1R_1'D_1'R_1\} \cup \{M_1R_1''D_1'R_1\}\\
&= \{M_1D_1'(D_1')^{-1}R_1'D_1'R_1\} \cup \left\{M_1\begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix}D_1'(D_1')^{-1}\begin{pmatrix} E & \delta' \\ 0 & E \end{pmatrix}D_1'R_1\right\}\\
&= S_5' \cup S_5''\\
&\subset KM_1D_1'K \cup KM_1\begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix}D_1'K.
\end{aligned} \tag{3.79}$$

С другой стороны, если мы перемножим двойные классы, используя разложения (3.47), (3.32), (3.4), (3.50) и соотношение

$$D_1' = HQM_1 \quad \text{с} \quad Q = H^{-1}D_1'M_1^{-1} = \begin{pmatrix} * & * \\ Q_{2,1} & * \end{pmatrix} \in K,$$

поскольку $Q_{2,1} = \begin{pmatrix} -q(a+1) & 0 \\ 0 & 0 \end{pmatrix}$, мы получим следующие разложения:

$$\begin{aligned} \Omega &= (KH), & \Omega\xi_1 &= \sum_{M\in S_2}(KM), & \Omega\xi &= \sum_{M\in S_3}(KM), \\ \xi_1\Omega &= \sum_{M\in S_4}(KM), & \xi_1\Omega\xi_1 &= \sum_{M\in S_5}(KM), & \xi_1\Omega\xi &= \sum_{M\in S_6}(KM), \\ \xi\Omega &= \sum_{M\in S_7}(KM), & \xi_1\Omega\xi_1 &= \sum_{M\in S_8}(KM), & \xi\Omega\xi &= \sum_{M\in S_9}(KM), \end{aligned} \tag{3.80}$$

где $\Omega = \Omega^2(p,q)$ обозначает двойной класс (3.46), а $\xi_1 = \xi_1^2(p)$ и $\xi = \xi_2^2(p)$ — двойные классы (3.31). Сравнивая разложения (3.80) с включениями (3.78) и (3.79), мы получаем соотношения

$$\begin{gathered} \Omega\xi_1 = (D_1')_K, \quad \Omega\xi = (D_2)_K, \quad \xi_1\Omega = (M_1H)_K, \quad \xi_1\Omega\xi = (M_1D_2)_K, \\ \xi\Omega = (M_2H)_K, \quad \xi\Omega\xi_1 = (M_2D_1')_K, \quad \xi\Omega\xi = (M_2D_2)_K \end{gathered}$$

и

$$\xi_1\Omega\xi_1 = \Phi + \Psi, \tag{3.81}$$

где

$$\Phi = \sum_{M\in S_5'}(KM) = (P)_K \quad \text{и} \quad \Psi = \sum_{M\in S_5''}(KM) = (P')_K, \tag{3.82}$$

при этом

$$P = M_1D_1' = \begin{pmatrix} * & * \\ P_{2,1} & * \end{pmatrix} \quad \text{и} \quad P' = M_1\begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix}D_1' = \begin{pmatrix} * & * \\ P_{2,1}' & * \end{pmatrix},$$

где

$$P_{2,1} = \begin{pmatrix} q_1 & 0 \\ 0 & q \end{pmatrix}, \quad P_{2,1}' = \begin{pmatrix} 0 & q(a+p) \\ 0 & 0 \end{pmatrix}.$$

Отметим, что двойные классы Φ и Ψ различны, поскольку блоки $P_{2,1}$ и $P_{2,1}'$ имеют разные ранги по модулю p.

Зная все десять двойных классов мультипликатора p кольца (3.71) и их разложения на левые классы, мы можем вывести все необходимые свойства этих двойных классов. Прежде всего, используя (3.34) и (3.49), мы получаем соотношения

$$\Phi^* + \Psi^* = \xi_1^*\Omega^*\xi_1^* = \xi_1\Omega\xi_1 = \Phi + \Psi,$$

откуда

$$\Phi^* = \Phi \quad \text{и} \quad \Psi^* = \Psi, \tag{3.83}$$

поскольку $\Phi^* \neq \Psi$ по той же причине, что была использована для доказательства неравенства $\Phi \neq \Psi$. Проверка следующих трех соотношений не содержит ничего, кроме стандартных, но утомительных вычислений по умножению двойных классов HS-колец, которые мы оставляем читателю:

$$\xi\Psi = p\Phi + (p-1)\xi\Omega\xi_1; \tag{3.84}$$

$$\Omega\Psi = \Psi\Omega; \tag{3.85}$$

$$\Pi_1(p^2) = \Omega\Phi, \tag{3.86}$$

где $\Pi_1(p^2)$ — элемент (3.67). Из (3.84) следует соотношение

$$\xi^{-1}\Phi = (\Psi + (1-p)\Omega\xi_1)/p, \tag{3.87}$$

так как

$$\xi(\Psi + (1-p)\Omega\xi_1)/p = (p\Phi + (p-1)\xi\Omega\xi_1 + (1-p)\xi\Omega\xi_1)/p = \Phi.$$

Наконец, на основании (3.74), (3.87) и (3.81) мы получаем

$$\begin{aligned}\xi^{-1}\Psi = \xi^{-1}(\xi_1\Omega\xi_1 - \Phi) &= ((1-p^2)[1] + \xi_1)\Omega\xi_1/p^2 - (\Psi + (1-p)\Omega\xi_1)/p \\ &= (\Phi + (1-p)\Psi + (1-p)\Omega\xi_1)/p^2.\end{aligned} \tag{3.88}$$

Возвращаясь к элементам (3.70), мы можем теперь представить их в симметричной форме. Используя (3.66), мы имеем

$$\widetilde{T}^2(p) = p^3[p]\Pi^{-1} + p\Pi^{-1}\Pi_1(p^2) + \Pi = p^3\xi^{-1}\Omega + p\xi^{-1}\Omega^{-1}\Omega\Phi + \Omega\xi,$$

где были использованы также соотношения (3.53), (3.86) и (3.50). По (3.40) и (3.87) последнее выражение можно переписать в виде

$$\begin{aligned}\widetilde{T}^2(p) &= (\xi + (1-p)\xi_1 + (1-p)[1])\Omega + (\Psi + (1-p)\Omega\xi_1) + \Omega\xi \\ &= \xi\Omega + \Omega\xi + (1-p)(\xi_1\Omega + \Omega\xi_1) + \Psi + (1-p)\Omega,\end{aligned} \tag{3.89}$$

что, согласно (3.34), (3.49) и (3.83), доказывает симметричность рассматриваемого элемента. Используя снова разложение (3.66), мы получаем

$$\begin{aligned}\tilde{q}_2(p) &= p^4[p]\Pi^{-1}\Pi^{-1}\Pi_1(p^2) + p\Pi^{-1}\Pi_1(p^2)\Pi + 2p^3[p] \\ &= p^4\xi^{-1}\Omega\xi^{-1}\Omega^{-1}\Omega\Phi + p\Omega\Phi + 2p^3[p],\end{aligned}$$

где мы также использовали соотношения (3.53), (3.48), (3.86) и теорему 3.3(4). На основании соотношений (3.87), (3.85) и (3.88) последнее выражение может быть переписано в виде

$$\begin{aligned}\tilde{q}_2(p) &= p^3\xi^{-1}\Omega(\psi + (1-p)\Omega\xi_1) + p\Omega\Phi + 2p^3[p] \\ &= p^3\xi^{-1}\Psi\Omega + p^3(1-p)[p]\xi^{-1}\xi_1 + p\Omega\Phi + 2p^3[p] \\ &= p(\Phi + (1-p)\Psi + (1-p)\Omega\xi_1)\Omega + p(1-p)[p]((1-p^2)[1] + \xi_1) \\ &\quad + p\Omega\Phi + 2p^3[p] \\ &= p(\Phi\Omega + \Omega\Phi) + p(1-p)(\Psi\Omega + \Omega\xi_1\Omega + [p]\xi_1) \\ &\quad + p(p^3 + p^2 - p + 1)[p],\end{aligned} \tag{3.90}$$

что, согласно (3.49), (3.83), (3.85) и (3.34), доказывает его симметричность. •

Глава 4

Старые формы, новые формы, собственные формы

В этой главе мы определим старые и новые касп-формы для группы $\Gamma_0^n(q)$ и докажем, в частности, что пространства новых форм рода $n \leqslant 2$ линейно порождаются собственными функциями всех операторов Гекке, соответствующих элементам регулярного приводимого кольца $\mathcal{H}_{\mathrm{rr}}^n(q)$, элементам *сингулярного неразветвленного кольца*

$$\mathcal{H}_{\mathrm{su}}^n(q) = \prod_{p|q,p^2\nmid q} \mathcal{H}_p^n(q), \tag{4.1}$$

порожденного всеми сингулярными неразветвленными p-кольцами, и всем сингулярным элементам Фробениуса $\Pi(a)$ (см. теорему 4.15). В случае $n = 1$ этот результат для регулярных операторов принадлежит Петерссону [12], а действие сингулярных элементов Фробениуса было рассмотрено Аткиным и Ленером в [7].

Мы ограничиваемся здесь только случаем касп-форм. Можно также рассматривать старые и новые ряды Эйзенштейна–Клингена, но это другая история.

§4.1. След-идемпотенты

Мы введем здесь простую, но полезную абстрактную конструкцию.

Пусть G — мультипликативная группа и $\Gamma \subset G$ — подгруппа конечного индекса $\nu = [G:\Gamma]$. Рассмотрим элемент HS-кольца $\mathcal{H} = HS_{\mathbb{Q}}(\Gamma, G)$, задаваемый формулой

$$\tau = \tau(\Gamma \setminus G) = \nu^{-1} \sum_{g_i \in \Gamma\setminus G} (\Gamma g_i). \tag{4.2}$$

Лемма 4.1. *Элемент* (4.2) *удовлетворяет следующим соотношениям*:

$$\tau g = \nu^{-1} \sum_{g_i \in \Gamma\setminus G} (\Gamma g_i g) = \tau \quad (g \in G), \tag{4.3}$$

$$\tau \cdot (g)_\Gamma = \tau \cdot \sum_{g_j \in \Gamma\setminus\Gamma g\Gamma} (\Gamma g_j) = \#(\Gamma \setminus \Gamma g \Gamma) \cdot \tau \tag{4.4}$$

и $\tau^2 = \tau$.

Доказательство. Поскольку множество $\{g_i g\}$ снова является системой представителей из классов смежности $\Gamma \setminus G$, соотношение (4.3) выполнено. Соотношение (4.4) является следствием соотношения (4.3). Последнее соотношение следует из (4.3) и определения умножения в HS-кольцах. •

Мы будем называть элемент $\tau = \tau(\Gamma \setminus G)$ *след-идемпотентом пары* (Γ, G).

Предположим теперь, что группа G действует на векторном пространстве V над $\mathbb{C}$ посредством линейных операторов

$$|g : v \to v|g \quad (v \in V,\ g \in G),$$

удовлетворяющих условиям

$$v|g|g' = v|gg' \quad (v \in V,\ g, g' \in G).$$

Обозначим через $V(\Gamma)$ и $V(G)$ подпространства Γ-инвариантных и G-инвариантных элементов из V соответственно. Тогда $V(G) \subset V(\Gamma)$, и HS-кольцо $\mathcal{H}$ действует на пространстве $V(\Gamma)$ посредством операторов Гекке. Поскольку элемент (4.2) является идемпотентом, то пространство $V(\Gamma)$ разлагается в прямую сумму подпространств

$$V_1(\Gamma) = V(\Gamma)|\tau, \quad V_2(\Gamma) = \{v \in V(\Gamma)\ ;\ v|\tau = 0\};$$
$$V(\Gamma) = V_1(\Gamma) + V_2(\Gamma), \quad V_1(\Gamma) \cap V_2(\Gamma) = \{0\}.$$

Лемма 4.2. $V_1(\Gamma) = V(G)$.

Доказательство. Включение $\subset$ следует из (4.3). Обратное включение очевидно. •

Предположим, наконец, что пространство V снабжено невырожденным эрмитовым скалярным произведением (v, v'), удовлетворяющим условиям

$$(v|g, v') = (v, v'|g^{-1}) \quad (v, v' \in V,\ g \in G).$$

Тогда подпространство $V_2(\Gamma)$ может быть охарактеризовано как ортогональное дополнение подпространства $V(G)$ в $V(\Gamma)$.

Лемма 4.3. $V_2(\Gamma) = V(G)^{\perp} = \{v \in V(\Gamma);\ (v, V(G)) = 0\}$.

Доказательство. Пусть $v \in V_2(\Gamma)$ и $v' = v'|\tau \in V(G) = V_1(\Gamma)$. Тогда мы имеем

$$\begin{aligned}(v, v') = (v, v'|\tau) &= \nu^{-1} \sum_{g_i \in \Gamma\backslash G} (v, v'|\tau g_i^{-1}) \\ &= \nu^{-1} \sum_{g_i \in \Gamma\backslash G} (v|g_i, v'|\tau) = (v|\tau, v') = 0,\end{aligned}$$

и поэтому $v \in V(G)^{\perp}$. Обратно, если $v \in V(G)^{\perp}$, то мы получаем

$$\begin{aligned}(v|\tau, v|\tau) &= \nu^{-1} \sum_{g_i \in \Gamma\backslash G} (v|\tau, v|g_i) \\ &= \nu^{-1} \sum_{g_i \in \Gamma\backslash G} (v|\tau g_i^{-1}, v) = (v|\tau, v) = 0,\end{aligned}$$

откуда $v|\tau = 0$. •

Суммируя полученные результаты, мы приходим к следующей теореме.

Теорема 4.4. *В приведенных выше обозначениях и предположениях подпространство $V(G) \subset V(\Gamma)$ и его ортогональное дополнение $V(G)^{\perp}$ можно охарактеризовать следующим образом:*

$$V(G) = V(\Gamma)|\tau(\Gamma \setminus G), \quad V(G)^{\perp} = \{v \in V(\Gamma), v|\tau(\Gamma \setminus G) = 0\}. \tag{4.5}$$

§4.2. Определение старых и новых форм

Мы рассматриваем представление HS-кольца $\mathcal{H}(K) = HS_{\mathbb{Q}}(K, \Sigma^n)$ группы $K = \Gamma_0^n(q)$ на пространстве

$$\mathfrak{N} = \mathfrak{N}(q) = \mathfrak{N}_k^n(q) = \mathfrak{N}_k(K)$$

касп-форм фиксированного целого веса k для группы K, задаваемое операторами Гекке (1.17) или нормированными операторами Гекке (1.20). Для определенности мы будем говорить об операторах (1.17), хотя все определения, результаты и доказательства (с заменой теоремы 1.9(2) на соотношения (1.21)) остаются справедливыми также и для нормированных операторов. Пространство $\mathfrak{N}$ снабжено скалярным произведением Петерссона (1.13), которое является эрмитовым, невырожденным и удовлетворяет соотношениям (1.14).

Пусть p — простой делитель числа q и пусть $\Pi(p)$ и $\Pi^*(p)$ — отвечающие ему элемент Фробениуса (3.2) и двойственный ему элемент относительно антиавтоморфизма (1.18). Мы определим *подпространство p-старых форм* пространства $\mathfrak{N}$, полагая

$$\mathbf{O}_p = \mathbf{O}_k^n(q)_p = \sum_{i=0}^{m-1} \mathfrak{N}(q/p)|\Pi^*(p)^i \quad (m = 2^n), \tag{4.6}$$

если p не разветвлено (т.е. $p^2 \nmid q$), и

$$\mathbf{O}_p = \mathbf{O}_k^n(q)_p = \mathfrak{N}(q/p) + \mathfrak{N}(q/p)|\Pi^*(p), \tag{4.7}$$

если p разветвлено (т.е. $p^2 \mid q$), где

$$\mathfrak{N}(q/p) = \mathfrak{N}_k(\Gamma_0^n(q/p)) \tag{4.8}$$

и $|$ обозначает оператор Гекке (1.17).

Пусть

$$\tau(p) = \tau^n(p,q) = [K' : K]^{-1} \sum_{M_i \in K \backslash K'} (KM_i), \tag{4.9}$$

где $K' = \Gamma_0^n(q/p)$, обозначает след-идемпотент пары (K, K'). Тогда по теореме 4.4 мы можем написать, что

$$\mathbf{O}_p = \sum_{i=0}^{m-1} \mathfrak{N}|\tau(p) \cdot \Pi^*(p)^i \quad (m = 2^n), \tag{4.10}$$

если p^2 не делит q, и

$$\mathbf{O}_p = \mathfrak{N}|\tau(p) + \mathfrak{N}|\tau(p)\Pi^*(p), \tag{4.11}$$

если p^2 делит q.

Пространство

$$\mathbf{O} = \mathbf{O}_k^n(q) = \sum_{p|q} \mathbf{O}_p \tag{4.12}$$

мы будем называть (*глобальным*) *подпространством старых форм* пространства $\mathfrak{N}$.

Мы определим N_p, подпространство *p-новых форм*, и N, *подпространство(глобально) новых форм*, как ортогональное дополнение относительно скалярного произведения Петерссона подпространства p-старых форм и подпространства старых форм соответственно:

$$\mathrm{N}_p = \mathrm{N}_k^n(q)_p = \{F \in \mathfrak{N}\,;\,(F, \mathbf{O}_p) = 0\}, \tag{4.13}$$

$$\mathrm{N} = \mathrm{N}_k^n(q) = \{F \in \mathfrak{N}\,;\,(F, \mathbf{O}) = 0\}. \tag{4.14}$$

Тогда мы имеем

$$\mathrm{N} = \bigcap_{p|q} \mathrm{N}_p, \tag{4.15}$$

и по теоремам 4.4 и 1.9(2) каждое из подпространств N_p может быть представлено в виде

$$\mathrm{N}_p = \{F \in \mathfrak{N}\,;\,F|\Pi(p)^i\tau(p) = 0, i = 0, 1, \ldots, 2^n - 1\}, \tag{4.16}$$

если p^2 не делит q, или в виде

$$\mathrm{N}_p = \{F \in \mathfrak{N}\,;\,F|\tau(p) = 0, F|\Pi(p)\tau(p) = 0\}, \tag{4.17}$$

если p^2 делит q.

§4.3. Инвариантные подпространства и собственные формы

Здесь мы рассмотрим вопросы инвариантности подпространств старых и новых форм относительно операторов Гекке и покажем, что при определенных условиях подпространства новых форм линейно порождаются общими собственными функциями этих операторов. Мы сохраняем обозначения, введенные в §4.2.

Лемма 4.5. *Пусть p и p' — два простых числа, причем p делит q, а p' не делит q. Тогда имеют место следующие утверждения*:

(1) *Подпространство $\mathfrak{N}(q/p) \subset \mathfrak{N}$ инвариантно относительно каждого из операторов Гекке $|T$ для $T \in \mathcal{H}_{p'}(q)$.*

(2) *Каждый элемент кольца $\mathcal{H}_{p'}(q)$ перестановочен с элементом Фробениуса $\Pi(p)$ и двойственным ему элементом $\Pi^*(p)$.*

Доказательство. По теореме 2.6 кольца $\mathcal{H}_{p'}(q)$, $\mathcal{H}_{p'}(q/p)$ изоморфны, и если $T \in \mathcal{H}_{p'}(q)$, $T' \in \mathcal{H}_{p'}(q/p)$ — некоторая пара элементов, соответствующих при этом изоморфизме, то их образы $\widehat{T}$ и $\widehat{T}'$ при параболическом вложении (2.30) совпадают. Отсюда следует, что

$$\mathfrak{N}(q/p)|T = \mathfrak{N}(q/p)|\widehat{T} = \mathfrak{N}(q/p)\widehat{T}' = \mathfrak{N}(q/p)|T' \subset \mathfrak{N}(q/p),$$

что доказывает первое утверждение.

Что же касается второго утверждения, то по предложению 2.12(1) мы получаем

$$\widehat{\Pi T} = \widehat{\Pi}\widehat{T} = \widehat{T}\widehat{\Pi} = \widehat{T\Pi}, \quad (\Pi = \Pi(p))$$

для каждого $T \in \mathcal{H}_{p'}(q)$, откуда $\Pi T = T\Pi$. Из этого равенства следуют соотношения

$$T^*\Pi^* = (\Pi T)^* = (T\Pi)^* = \Pi^* T^*,$$

которые вместе с теоремой 2.3 заканчивают доказательство леммы. •

Теорема 4.6. (1) *Каждое из локальных подпространств* $\mathbf{O}_p$ *и* $\mathbf{N}_p$, *где* $p|q$, *а также и глобальные подпространства* $\mathbf{O}$ *и* $\mathbf{N}$ *инвариантны относительно всех операторов Гекке, отвечающих элементам регулярного приводимого кольца* $\mathcal{H}^n_{\mathrm{rr}}(q)$, *определенного равенством* (2.3).

(2) *Каждое из перечисленных подпространств линейно порождается общими собственными функциями всех операторов части* (1).

Доказательство. По теореме 2.5 теорему достаточно доказать для некоторого локального кольца $\mathcal{H}_{p'}(q)$, где $p' \nmid q$, вместо кольца $\mathcal{H}^n_{\mathrm{rr}}(q)$. Из леммы 4.5 и определений (4.6), (4.7) подпространств старых форм следует, что каждое из подпространств $\mathbf{O}_p$, а с ними и вся сумма (4.12) инвариантны относительно операторов $|T$ с $T \in \mathcal{H}_{p'}(q)$. Инвариантность подпространств $\mathbf{N}_p$ и $\mathbf{N}$ следует тогда из (4.13), (4.14), (2.6) и теоремы 1.9(2). Утверждение (1) доказано.

По теореме 2.3 и 1.9(2) операторы $|T$ для $T \in \mathcal{H}^n_{\mathrm{rr}}(q)$ коммутируют друг с другом и являются самосопряженными. Поскольку пространство $\mathfrak{N}$ конечномерно, то второе утверждение следует из первого по хорошо известной теореме линейной алгебры. •

Обратимся теперь к сингулярным операторам Гекке.

Предложение 4.7. *Пусть* p — *неразветвленный простой делитель числа* q. *Тогда для каждой функции* $F \in \mathfrak{N}(q/p)$ *и каждого элемента* $T \in \mathcal{H}_p(q/p)$ *имеет место соотношение*

$$F|\widetilde{T} = F|T, \tag{4.18}$$

где $T \to \widetilde{T}$ *отображение* (3.58). *В частности, пространство* $\mathfrak{N}(q/p)$ *инвариантно относительно всех операторов Гекке, отвечающих элементам неразветвленного* p-*кольца* $\mathcal{H}_p(q)$.

Доказательство. Достаточно проверить соотношение (4.18) для образующих (3.69) кольца $\mathcal{H}_p(q)$. По определению элементов $T^n(p)$ и $T^n_j(p^2)$ (см. (2.20)) и предложению 2.11 имеют место включения

$$\widehat{T}^n(p)\widehat{\Pi}(p), \quad \widehat{T}^n_j(p^2)\widehat{\Pi}(p)^2 \in \widehat{C}_p,$$

откуда, согласно (3.56), получаем формулы

$$\widetilde{T}^n(p) = \Pi(p)^{-1} \cdot i(\widehat{T}^n(p)\widehat{\Pi}(p)), \quad \widetilde{T}^n_j(p^2) = \Pi(p)^{-2} \cdot (\widehat{T}^n_j(p^2)\widehat{\Pi}(p)^2).$$

Так как операторы Гекке на пространстве $\mathfrak{N}$, отвечающие элементам $\widehat{T} \in \widehat{C}_p$ и $i(\widehat{T}) \in C_p$, очевидно, совпадают, то соотношение (4.18) для образующих будет следовать из соотношений (2.49) и (2.50), если мы сможем доказать формулы

$$F|\Pi(p)^{-1} = F|\Pi_+^{-1} \tag{4.19}$$

и

$$F|\Pi(p)^{-2} = F|\Pi_+^{-2} \tag{4.20}$$

для каждой $F \in \mathfrak{N}(q/p)$, где

$$\Pi_+^{-1}, \Pi_+^{-2} \in \mathcal{L}'_p = \mathcal{L}_p[[p]^{-1}]$$

— первые „отрицательные степени“ элемента Фробениуса $\Pi_+ = \widehat{\Pi}(p)$.

По предложению 3.9 мы получаем соотношения

$$F|\xi_n(p) = p^{\langle n\rangle}F \quad (F \in \mathfrak{N}(q/p)),$$

откуда следуют соотношения

$$F|\xi_n(p)^{-1} = p^{-\langle n\rangle}F \quad (F \in \mathfrak{N}(q/p)). \tag{4.21}$$

Тогда на основании (3.53) и (3.43) мы получаем

$$\begin{aligned} F|\Pi(p)^{-1} &= F|[p]^{-1}\xi_n(p)^{-1}\Omega(p) \\ &= F|(p^{\langle n\rangle}[p])^{-1}\begin{pmatrix} aE_n & bE_n \\ (q/p)E_n & pE_n \end{pmatrix}\begin{pmatrix} pE_n & 0 \\ 0 & E_n \end{pmatrix} \\ &= F|(p^{\langle n\rangle}[p])^{-1}\begin{pmatrix} pE_n & 0 \\ 0 & E_n \end{pmatrix}, \end{aligned}$$

что равно $F|\Pi_+^{-1}$ (см., например, [4, упражнение 3.5.7(3)]). Мы доказали соотношения (4.19), откуда, в частности, следует включение

$$\mathfrak{N}(q/p)|\Pi_+^{-1} \subset \mathfrak{N}.$$

Докажем включение

$$\mathfrak{N}(q/p)|\Pi_+^{-2} \subset \mathfrak{N}. \tag{4.22}$$

По определению „отрицательных степеней“ (см. [4, §3.5]) мы имеем

$$\Pi_+^{-2} = -\widehat{q_m}^{-1}\left(\sum_{i=1}^{m}(-1)^i\widehat{q_{m-i}^n}(p)\Pi_+^{i-2}\right),$$

где $m = 2^n$ и где $\widehat{q_j^n}(p)$ — образы при параболическом вложении соответствующих коэффициентов многочлена (2.27) над кольцом $\mathcal{H}_p(q/p)$. Отсюда следуют включения

$$\begin{aligned} \mathfrak{N}(q/p)|\Pi_+^{-2} &\subset \sum_{i=1}^{m}\mathfrak{N}(q/p)|\widehat{q_m^n}(p)^{-1}\widehat{q_{m-i}^n}(p)\Pi_+^{i-2} \\ &\subset \mathfrak{N}(q/p)|\Pi_+^{-1} + \mathfrak{N}(q/p) + \sum_{i=3}^{m}\mathfrak{N}(q/p)|\Pi_+^{i-2} \\ &\subset \mathfrak{N}, \end{aligned}$$

так как по определению и теореме 3.3

$$\mathfrak{N}(q/p)|\Pi_+^d = \mathfrak{N}(q/p)|\Pi(p)^d \subset \mathfrak{N},$$

если $d \geqslant 1$. Теперь мы можем доказать соотношения (4.20). Пусть $F \in \mathfrak{N}(q/p)$;

$$F_1 = F|\Pi(p)^{-2}, \quad F_2 = F|\Pi_+^{-2}.$$

Так как оператор $|\Pi(p)^{-2}$ отображает пространство $\mathfrak{N}$ в себя, то $F_1 \in \mathfrak{N}$. Согласно (4.22), имеет место включение $F_2 \in \mathfrak{N}$. Кроме того,

$$F_1|\Pi(p)^2 = F|\Pi(p)^{-2}\Pi(p)^2 = F$$

и

$$F_2|\Pi(p)^2 = F|\Pi_+^{-2}|\Pi_+^2 = F|\Pi_+^{-2}\Pi_+^2 = F$$

по (2.38), (3.4), определению операторов Гекке и соотношению (2.50) с $d = 2$ и $X = [1]$. Поскольку оператор $|\Pi(p)^2$ обратим на $\mathfrak{N}$, мы заключаем, что $F_1 = F_2$. •

Теперь мы можем доказать следующую теорему.

Теорема 4.8. *Предположим, что $n = 1$ или $n = 2$. Тогда справедливы следующие утверждения:*

(1) *Каждое из локальных подпространств $\mathbf{O}_p$ и N_p для простых p, делящих q вместе с глобальными подпространствами $\mathbf{O}$ и N, инвариантно относительно всех операторов Гекке, отвечающих элементам сингулярного неразветвленного кольца $\mathcal{H}_{\mathrm{su}}^n(q)$, определенного равенством* (4.1).

(2) *Каждое из перечисленных пространств линейно порождается общими собственными функциями указанных операторов.*

Доказательство. Согласно теореме 3.17(2) и (4.1), теорему достаточно доказать для некоторого локального сингулярного неразветвленного кольца $\mathcal{H}_{p'}(q)$ вместо $\mathcal{H}_{\mathrm{su}}(q)$.

Пусть p — сингулярное простое число и пусть $T \in \mathcal{H}_{p'}(q)$. Тогда $T^* = T$ по предложению 3.20, откуда по теореме 3.17(2) мы получаем соотношение $\Pi(p)T = T\Pi(p)$ и соотношения

$$T \cdot \Pi^*(p) = T^* \cdot \Pi^*(p) = (\Pi(p) \cdot T)^* = (T \cdot \Pi(p))^* = \Pi^*(p) \cdot T. \tag{4.23}$$

Из (4.23) и (4.6) или (4.7) следует, что подпространство $\mathbf{O}_p$ инвариантно относительно оператора $|T$, если справедливо включение

$$\mathfrak{N}(q/p)|T \subset \mathfrak{N}(q/p) \quad (T \in \mathcal{H}_{p'}(q)). \tag{4.24}$$

По предложению 4.7 включение справедливо, если $p' = p$. Таким образом, можно предполагать, что $p' \neq p$. По теореме 4.4 для каждого сингулярного простого числа p можно написать равенство

$$\mathfrak{N}(q/p) = \mathfrak{N}|\tau(p), \tag{4.25}$$

где $\tau(p)$ обозначает след-идемпотент (4.9). С другой стороны, каждый элемент $T \in \mathcal{H}_{p'}(q)$ имеет вид $T = \Pi(p')^{-d}T_1$ с $d \in \mathbb{N}$ и $T_1 \in C_{p'}$. По предложению 3.9(4), если p^2 не делит q, и по предложению 3.12(3), если p^2 делит q, мы имеем равенство

$$\tau(p)\Pi(p') = \Pi(p')\tau(p), \tag{4.26}$$

откуда

$$\tau(p)\Pi(p')^{-1} = \Pi(p')^{-1}\tau(p). \tag{4.27}$$

Из (4.27) и (4.25) получаем

$$\mathfrak{N}(q/p)|\Pi(p')^{-d} = \mathfrak{N}|\tau(p)\Pi(p')^{-d} = (\mathfrak{N}|\Pi(p')^{-d})|\tau(p) \subset \mathfrak{N}(q/p).$$

Так как p' делит q/p, то из теоремы 3.3 следует, что каждый оператор $|T_1$ с $T_1 \in C_{p'}$ отображает пространство $\mathfrak{N}(q/p)$ в себя. Отсюда следуют включение (4.24) и инвариантность каждого подпространства $\mathbf{O}_p$, а значит, и пространства $\mathbf{O}$. Инвариантность подпространств N_p и N следует из (4.13), (4.15), теоремы 1.9(2) и предложения 3.20. Утверждение (1) доказано.

По теореме 3.17(2) кольцо $\mathcal{H}^n_{\mathrm{su}}$ коммутативно. Тогда из предложения 3.20 следует, что оно состоит из симметричных элементов. Утверждение (2) следует из теоремы 1.9(2) на основании тех же аргументов, что были использованы в конце доказательства теоремы 4.6. •

Замечание 4.9. То же доказательство проходит без каких-либо изменений для данного n, если известно, что все неразветвленные локальные кольца $\mathcal{H}^n_p(q)$ для этого n состоят из симметричных элементов.

Обратимся теперь к операторам Гекке, отвечающим сингулярным элементам Фробениуса (3.2).

Лемма 4.10. *Пусть p — неразветвленный простой делитель q и $n = 1$ или $n = 2$. Тогда оба подпространства $\mathbf{O}_p$ и N_p инвариантны относительно операторов Гекке, отвечающих элементам $\Pi(p)^{\pm 1}$, $\Pi^*(p)^{\pm 1}$, $\xi_n(p)$ и $\Omega(p)$.*

Доказательство. По теореме 1.9(2) достаточно рассмотреть только случай подпространства $\mathbf{O}_p$. По (4.6) мы имеем

$$\mathbf{O}_p|\Pi^*(p) = \sum_{i=1}^{m} \mathfrak{N}(q/p)|\Pi^*(p)^i \subset \mathbf{O}_p + \mathfrak{N}(q/p)|\Pi^*(p)^m. \tag{4.28}$$

По теореме 3.17(2), (3) и предложению 3.20 мы получаем соотношение

$$\begin{aligned}
&\left(\sum_{j=0}^{m}(-1)^j\widetilde{q^n_j}(p)\Pi(p)^{m-j}\right)^* \\
&= \left(\sum_{j=0}^{m}(-1)^j\Pi(p)^{m-j}\widetilde{q^n_j}(p)^*\right)^* = \sum_{j=0}^{m}\widetilde{q^n_j}(p)\Pi^*(p)^{m-j} \\
&= 0,
\end{aligned} \tag{4.29}$$

где коэффициенты $\tilde{q}_j^m(p)$ принадлежат кольцу $\mathcal{H}_p(q)$. Тогда на основании (3.61) можно написать соотношение

$$\Pi^*(p)^m = -\sum_{j=1}^{m}(-1)^j\widetilde{q_j^n}(p)\Pi^*(p)^{m-j},$$

откуда по предлсжению 4.7 мы получаем

$$\begin{aligned}\mathfrak{N}(q/p)|\Pi^*(p)^m &\subset \sum_{j=1}^{m}\mathfrak{N}(q/p)|\widetilde{q_j^n}(p)\Pi^*(p)^{m-j}\\ &\subset \sum_{j=1}^{m}\mathfrak{N}(q/p)|\Pi^*(p)^{m-j} = \mathbf{O}_p,\end{aligned}$$

что вместе с (4.28) доказывает инвариантность пространства $\mathbf{O}_p$ относительно оператора, отвечающего элементу $\Pi^*(p)$. Поскольку на основании (3.50), (3.49) и (3.34) имеет место соотношение

$$\Pi^*(p) = (\Omega(p)\xi_n(p))^* = \xi_n(p)\Omega(p), \tag{4.30}$$

то из леммы 3.11 и (3.48) следует, что элемент $\Pi^*(p)$ является обратимым и

$$\Pi^*(p)^{-1} = [p]^{-1}\Omega(p)\xi_n(p)^{-1}. \tag{4.31}$$

В частности, из включения $\mathbf{O}_p|\Pi^*(p) \subset \mathbf{O}_p$ следуют равенства

$$\mathbf{O}_p|\Pi^*(p) = \mathbf{O}_p, \quad \mathbf{O}_p|\Pi^*(p)^{-1} = \mathbf{O}_p, \tag{4.32}$$

поскольку мы имеем дело только с конечномерными пространствами.

На основании (3.53), (3.39) и (3.40) мы получаем соотношение

$$p[p]\Pi(p)^{-1} = ((1-p)(\xi_0(p)+\xi_1(p)) + p\xi_1(p))\Omega(p), \tag{4.33}$$

если $n=1$, и соотношение

$$p^3[p]\Pi(p)^{-1} = ((1-p)(\xi_0(p)+\xi_1(p)+\xi_2(p)) + p\xi_2(p))\Omega(p), \tag{4.34}$$

если $n=2$. По предложению 3.9 имеет место соотношение

$$\xi_0(p)+\xi_1(p)+\dots+\xi_n(p) = \nu(p)\tau(p), \tag{4.35}$$

где $\nu(p) = [\Gamma_0^n(q/p) : \Gamma_0^n(q)]$ и $\tau(p)$ — след-идемпотент (4.9). Затем, используя (4.33), (4.34), (4.35), (4.30) и (4.4), мы получаем соотношение

$$\begin{aligned}p^{\langle n\rangle}[p]\Pi(p)^{-1} &= (1-p)\nu(p)\tau(p)\Omega(p) + p\Pi^*(p)\\ &= c(p)\tau(p)\xi_n(p)\Omega(p) + p\Pi^*(p)\\ &= c(p)\tau(p)\Pi^*(p) + p\Pi^*(p),\end{aligned} \tag{4.36}$$

где $c(p)$ — ненулевая константа, справедливое для $n = 1$ и $n = 2$. (К сожалению, оно не верно, если $n \geqslant 3$). Из (4.36), (4.32) и (4.25) следуют включения

$$\mathbf{O}_p|\Pi(p)^{-1} \subset \mathbf{O}|\tau(p)\Pi^*(p) + \mathbf{O}_p|\Pi^*(p) \subset \mathfrak{N}(q/p)|\Pi^*(p) + \mathbf{O}_p \subset \mathbf{O}_p,$$

откуда

$$\mathbf{O}_p|\Pi(p)^{-1} = \mathbf{O}_p, \quad \mathbf{O}_p|\Pi(p) = \mathbf{O}_p. \tag{4.37}$$

По (4.6) и (4.5) мы получаем

$$\mathbf{O}_p = \sum_{i=0}^{m-1} \mathfrak{N}(q/p)|(\Pi^*)^i = \sum_{i=0}^{m-1} \mathfrak{N}|\tau(\Pi^*)^i,$$

где $\tau = \tau(p)$ и $\Pi^* = \Pi^*(p)$, откуда на основании (4.32) имеем

$$\begin{aligned}\mathbf{O}_p &= \mathfrak{N}|\tau(\Pi^*)^{-1} + \sum_{i=1}^{m-1} \mathfrak{N}|\tau(\Pi^*)^{i-1} = \mathfrak{N}|\tau\Omega\xi^{-1} + \mathfrak{N}|\tau\\ &= \mathfrak{N}|\tau\xi\Omega\xi^{-1} + \mathfrak{N}|\tau,\end{aligned}$$

если $n = 1$, и

$$\begin{aligned}\mathbf{O}_p &= \mathfrak{N}|\tau\Omega\xi^{-1} + \mathfrak{N}|\tau + \mathfrak{N}|\tau\xi\Omega + \mathfrak{N}|\tau\Omega\xi\Omega\\ &= \mathfrak{N}|\tau\xi\Omega\xi^{-1} + \mathfrak{N}|\tau + \mathfrak{N}|\tau\Omega + \mathfrak{N}|\tau\Omega\xi\Omega,\end{aligned}$$

если $n = 2$, где $\xi = \xi_n(p)$, $\Omega = \Omega(p)$ и где мы несколько раз использовали соотношение (4.4). Используя (4.25), (4.31) и (3.50), получаем

$$\mathbf{O}_p|\xi = \mathfrak{N}|\tau\xi\Omega + \mathfrak{N}|\tau\xi = \mathfrak{N}(q/p)|\Pi^* + \mathfrak{N}(q/p),$$

если $n = 1$, и

$$\begin{aligned}\mathbf{O}_p|\xi &= \mathfrak{N}|\tau\xi\Omega + \mathfrak{N}|\tau\xi + \mathfrak{N}|\tau\Omega\xi + \mathfrak{N}|\tau\Omega\xi\Omega\xi\\ &= \mathfrak{N}(q/p)|\Pi^* + \mathfrak{N}(q/p) + \mathfrak{N}(q/p)|\Pi + \mathfrak{N}(q/p)|\Pi^2,\end{aligned}$$

если $n = 2$, где $\Pi = \Pi(p)$. В обоих случаях эти соотношения вместе с соотношениями (4.32) и (4.37) доказывают включение $\mathbf{O}_p|\xi \subset \mathbf{O}_p$, а значит, и соотношения

$$\mathbf{O}_p|\xi = \mathbf{O}_p|\xi_n(p) = \mathbf{O}_p|\xi_n(p)^{-1} = \mathbf{O}_p, \tag{4.38}$$

поскольку элемент $\xi = \xi_n(p)$ обратим. Наконец, на основании (4.32) и (4.38) мы получаем

$$\mathbf{O}_p|\Omega(p) = \mathbf{O}_p|\xi_n(p)^{-1}\xi_n(p)\Omega = \mathbf{O}_p|\Pi^*(p) = \mathbf{O}_p. \tag{4.39}$$

Соответствующие равенства для подпространства $\mathbf{N}_p$ следуют тогда из теоремы 1.9(2). •

Лемма 4.11. *Пусть p — неразветвленный простой делитель q и пусть $n = 1$ или $n = 2$. Тогда операторы Гекке $|\Pi(p)$ и $|\Pi^*(p)$ на N_p, пространстве p-новых форм, удовлетворяют следующим соотношениям:*

$$F|\Pi(p) = F|\Pi^*(p) = -F|\Omega(p) \quad (F \in \mathrm{N}_p), \tag{4.40}$$

если $n = 1$, и

$$F|\Pi(p)\Pi^*(p) = F|\Pi^*(p)\Pi(p) = p^2 F|[p] \quad (F \in \mathrm{N}_p), \tag{4.41}$$

если $n = 2$.

Доказательство. Если $n = 1$ и $F \in \mathrm{N}_p$, то по (4.16), (4.35) и (3.50) мы получаем соотношения

$$F|\tau(p) = \nu(p)^{-1} F|(\xi_0(p) + \xi_1(p)) = 0$$

и

$$F|\Pi(p)\tau(p) = F|\Omega(p)\xi_1\tau(p) = F|\Omega(p)p(\xi_0(p) + \xi_1(p)) = 0,$$

откуда

$$F|\xi_1(p) = -F \quad \text{и} \quad F|\Pi(p) = -F|\Omega(p).$$

С другой стороны, на основании (4.30) мы имеем

$$F|\Pi^*(p) = F|\xi_1(p)\Omega(p) = -F|\Omega(p).$$

Если же $n = 2$, то по (3.36) и (4.35) мы можем написать

$$\xi_2(p)^2 = p^2(p-1)(\xi_0(p) + \xi_1(p) + \xi_2(p)) + p^2\xi_0(p) = p^2(p-1)\nu(p)\tau(p) + p^2\xi_0(p),$$

откуда на основании (3.50), (4.30) и (3.38) мы получаем

$$\begin{aligned} F|\Pi(p)\Pi^*(p) &= F|\Omega(p)\xi_2(p)^2\Omega(p) \\ &= F_1|\xi_2(p)^2\Omega(p) \\ &= p^2 F_1|\Omega(p) = p^2 F|\Omega(p)^2 = p^2 F|[p], \end{aligned}$$

поскольку по предыдущей лемме $F_1 = F|\Omega(p) \in \mathrm{N}_p$. Аналогично

$$F|\Pi^*(p)\Pi(p) = F|\xi_2(p)\Omega(p)^2\xi_2(p) = F|\xi_2(p)^2[p] = p^2 F|[p]. \quad \bullet$$

Лемма 4.12. *Пусть $n \in \mathbb{N}$ и пусть p, p' — два различных простых делителя числа q, причем p^2 не делит q. Тогда справедливы следующие утверждения:*

(1) Элемент Фробениуса $\Pi(p)$ и двойственный ему элемент $\Pi^*(p)$ коммутируют с $\Pi(p')$ и с $\Pi^*(p')$.

(2) Подпространства $\mathbf{O}_{p'}$ и $\mathbf{N}_{p'}$ инвариантны относительно операторов $|\Pi(p)$ и $|\Pi^*(p)$.

Доказательство. Элементы $\Pi(p)$ и $\Pi(p')$ содержатся оба в коммутативном кольце C_q и потому коммутируют. Отсюда по двойственности элемент $\Pi^*(p)$ коммутирует с $\Pi^*(p')$. По (3.50) и (3.52) получаем

$$\Omega(p)\xi_n(p)\Pi(p') = \Pi(p')\Omega(p)\xi_n(p) = \Omega(p)\Pi(p')\xi_n(p).$$

Так как элемент $\Omega(p)$ обратим, то отсюда следует соотношение

$$\xi_n(p)\Pi(p') = \Pi(p')\xi_n(p),$$

откуда на основании (4.30) получаем

$$\Pi^*(p)\Pi(p') = \xi_n(p)\Omega(p)\Pi(p') = \xi_n(p)\Pi(p')\Omega(p) = \Pi(p')\Pi^*(p).$$

Элемент $\Pi(p)$ коммутирует с $\Pi^*(p')$ по двойственности. Утверждение (1) доказано.

Для доказательства второго утверждения достаточно, согласно сказанному выше и соотношениям (4.16), (4.17), проверить, что оба элемента $\Pi(p)$ и $\Pi(p^*)$ коммутируют со след-идемпотентом $\tau(p')$. По предложению 3.9(4) это верно, если p^2 не делит q, а по предложению 3.12(3), если p^2 делит q. •

Лемма 4.13. *Пусть p, p' — два простых делителя числа q, причем p^2 делит q. Тогда для каждого рода n подпространства $\mathbf{N}_{p'}$ и $\mathbf{N}$ инвариантны относительно оператора $|\Pi(p)$ и*

$$\mathbf{N}_p|\Pi(p) = \mathbf{N}|\Pi(p) = \{0\}. \tag{4.42}$$

Доказательство. Предположим сначала, что $p' \neq p$. Тогда, поскольку $\Pi(p)$ и $\Pi(p')$ коммутируют, инвариантность подпространства $\mathbf{N}_{p'}$ следует в случае неразветвленного p' из (4.16) и предложения 3.9(4), а в случае разветвленного p' — из (4.17) и предложения 3.12(3).

Остается доказать равенства (4.42). Если $F \in \mathbf{N}_p$, то $F|\Pi(p)\tau(p) = 0$, согласно (4.17). С другой стороны, по предложению 3.12(2) мы имеем $\Pi(p)\tau(p) = \Pi(p)$. Соотношение (4.42) следует из этих равенств. •

Теорема 4.14. *Пусть p — простой делитель числа q. Предположим, что $n = 1$ или $n = 2$. Тогда справедливы следующие утверждения:*

(1) Каждое из локальных подпространств $\mathbf{N}_p$, ра́вно, как и глобальное подпространство $\mathbf{N}$, инвариантно относительно всех операторов Гекке вида $|\Pi(p')$ для простых делителей p' числа q и вида $|\Pi^*(p')$ для простых делителей p' числа q, не

делящих частное q/p'. Указанные операторы на пространстве N *коммутируют друг с другом.*

(2) *Операторы* $|\Pi(p)$ *на* N *являются самосопряженными, если* $n = 1$, *нормальными, если* $p^2 \nmid q$ *и* $n = 2$, *и равны нулевому оператору, если* $p^2 \mid q$.

(3) *Подпространство* N *имеет базис, состоящий из общих собственных функций всех операторов Фробениуса* $|\Pi(p)$ *для простых* p, *делящих* q, *и всех двойственных операторов* $|\Pi^*(p)$ *для простых делителей* p *числа* q, *не делящих отношение* q/p.

Доказательство. Инвариантность пространств N_p относительно операторов $|\Pi(p')$ и $|\Pi^*(p')$ для неразветвленных p' была доказана в леммах 4.10 и 4.12. Инвариантность N_p относительно $|\Pi(p')$ для разветвленных p' была доказана в лемме 4.13. Так как все элементы Фробениуса $\Pi(p')$ коммутируют друг с другом, то остальные утверждения части (1) следуют из лемм 4.11 и 4.12(1).

Утверждения части (2) следуют из лемм 4.11 и 4.13.

Часть (3) следует из частей (1) и (2) и хорошо известных теорем линейной алгебры. •

Теперь мы можем объединить вместе все группы операторов, рассмотренные в теоремах 4.6, 4.8 и 4.14, и доказать следующую окончательную теорему о собственных функциях операторов Гекке на подпространстве N новых форм из $\mathfrak{N}$.

Теорема 4.15. *Подпространство*

$$\mathrm{N} = \mathrm{N}_k^n(q) \subset \mathfrak{N} = \mathfrak{N}_k(K)$$

всех новых касп-форм целого веса k *для группы* $K = \Gamma_0^n(q)$, *где* $n = 1$ *или* $n = 2$, *инвариантно относительно всех операторов Гекке, отвечающих элементам регулярного приводимого кольца* $\mathcal{H}_{\mathrm{rr}}^n(q)$, *элементам сингулярного неразветвленного кольца* $\mathcal{H}_{\mathrm{su}}^n(q)$, *всем сингулярным элементам Фробениуса* $\Pi(p)$ *для простых* p, *делящих* q, *и всем двойственным элементам* $\Pi^*(p)$ *для простых делителей* p *числа* q, *не делящих* q/p.

Существует базис указанного подпространства, состоящий из общих собственных функций всех перечисленных операторов.

Доказательство. Все перечисленные в теореме операторы порождаются локальными операторами, которые можно разделить на четыре группы операторов, отвечающих соответственно элементам:

(i) $T \in \mathcal{H}_p(q)$ для простых p, не делящих q;
(ii) $T \in \mathcal{H}_p(q)$ для простых p, делящих q, но не делящих q/p;
(iii) $\Pi(p)$ для простых p, делящих q;
(iv) $\Pi^*(p)$ для простых p, делящих q, но не делящих q/p.

Инвариантность пространства N и существование базисов из общих собственных функций для каждой из этих четырех групп операторов были установлены в теоремах 4.6, 4.8, 4.15. Таким образом, согласно линейной алгебре, единственное, что требуется проверить для завершения доказательства, это перестановочность операторов из различных групп. Мы имеем: элементы из групп (i) и (ii) коммутируют по теореме 3.17(1); элементы из групп (i) и (iii) коммутируют по предложению 2.12, теоремам 2.8 и 3.3; отсюда следует по двойственности и теореме 2.3, что коммутируют элементы групп (i) и (iv); элементы групп (ii) и (iii) коммутируют по теореме 3.17(2); отсюда по двойственности и предложению 3.20 следует, что коммутируют элементы группы (ii) и (iv); наконец, по теореме 4.14(1) операторы на N, отвечающие элементам групп (iii) и (iv), коммутируют. •

Заключение

Говоря о возможном обобщении приведенных результатов о собственных функциях, я хотел бы отметить, что для доказательства теоремы 4.8 для некоторого рода $n > 2$ было бы достаточно доказать, что кольцо $\mathcal{H}_p^n(q)$ состоит из симметрических элементов для всех q-сингулярных неразветвленных простых чисел p. С другой стороны, сомнительно, что часть теоремы 4.14, относящаяся к неразветвленным простым, может быть обобщена на любой род $n > 2$. Причина заключается в том, что соотношения (4.36) и (4.41) перестают быть верными, если $n \geqslant 3$.

Вероятно, рассматривая не только элементы Фробениуса, можно сказать больше о разветвленных простых, чем сказано в этой статье. Это было бы интересно для рассмотрения стандартных дзета-функций групп $\Gamma_0^n(q)$ в разветвленных случаях.

Первое и основное приложение результатов о собственных функциях операторов Фробениуса будет заключаться в расширении моих результатов, полученных почти 25 лет назад в [3] о спинорных дзета-функциях группы $\Gamma^2 = \mathrm{Sp}_2(\mathbb{Z})$ на случай групп $\Gamma_0^n(q)$, что является нашей следующей задачей.

Список литературы

[1] Андрианов А. Н., *Теоремы рациональности для рядов Гекке и дзета-функций групп* GL_n *и* Sp_n *над локальными полями*, Изв. АН СССР. Сер. мат. **33** (1969), № 3, 466–505.

[2] Андрианов А. Н., *Сферические функции для* GL_n *над локальными полями и суммирование рядов Гекке*, Мат. сб. **83(125)** (1970), № 3, 429–451.

[3] Андрианов А. Н., *Эйлеровы произведения, отвечающие модулярным формам Зигеля рода 2*, Успехи мат. наук **29** (1974), № 3, 43–110.

[4] Andrianov A. N., *Quadratic forms and Hecke operators*, Grundlehren Math. Wiss., Bd. 286, Springer-Verlag, Berlin–New York, 1987.

[5] Андрианов А. Н., Журавлев В. Г., *Модулярные формы и операторы Гекке*, Наука, М., 1990.

[6] Artin E., *Geometric algebra*, Interscience Tracts Pure Appl. Math., No. 3, Interscience Publishers, Inc., New York–London, 1957; Пер. на рус. яз., Наука, М., 1969.

[7] Atkin A. O. L., Lehner J., *Hecke operators on* $\Gamma_0(m)$, Math. Ann. **185** (1970), 134–160.

[8] Hecke E., *Über Modulfunktionen und die Dirichletschen Reihen mit Eulerscher Produktentwicklung*. I, II, Math. Ann. **114** (1937), 1–28, 316–351.

[9] Li Wen-Ch'ing Winnie, *Newforms and functional equations*, Math. Ann. **212** (1975), 285–315.

[10] Maass H., *Die Primzahlen in der Theorie der Siegelschen Modulfunktionen*, Math. Ann. **124** (1951), 87–122.

[11] Mordell L. J., *On Mr Ramanujan's empirical expansions of modular functions*, Proc. Cambridge Philos. Soc. **19** (1917), 117–124.

[12] Petersson H., *Konstruktion der sämtlichen Lösungen einer Riemannschen Funktionalgleichung durch Dirichlet-Reihen mit Eulerscher Produktentwicklung.* I, II III, Math. Ann. **116** (1939), 401–412; **117** (1939), 39–64, 277–300.

[13] Salvati-Manni R., Top J., *Cusp forms of weight* 2 *for the group* $\Gamma_2(4,8)$, Amer. J. Math. **115** (1993), no. 2, 455–486.

[14] Satake I., *Theory of spherical functions on reductive algebraic groups over* $\mathfrak{p}$*-adic fields*, Inst. Hautes Études Sci. Publ. Math. No. 18 (1963), 5–69.

[15] Shimura G., *On modular correspondences for* $\mathrm{Sp}(n,\mathbb{Z})$ *and their congruence relations*, Proc. Nat. Acad. Sci. U.S.A. **49** (1963), no. 6, 824–828.

[16] Shimura G., *Euler products and Fourier coefficients of automorphic forms on symplectic groups*, Invent. Math. **116** (1994), 531–576.

[17] Siegel C. L., *Lectures on the analytical theory of quadratic forms*, Buchhandlung Robert Peppmüller, Göttingen, 1963.

[18] Жарковская Н. А., *О связи собственнх чисел операторов Гекке и коэффициентов Фурье собственных функций для зигелевых модулярных форм рода* n, Мат. сб. **96(138)** (1975), № 4, 584–593.

С.-Петербургское отделение
Математического института
им. В. А. Стеклова РАН
191011, Санкт-Петербург
наб. р. Фонтанки, 27
Россия

Mux-Planck-Institut für Mathematic
Vivatgasse 7
53111, Bonn, Germany

Universite J. Fourier, Institut Fourier
UFR de Mathématiques, BP 74
38402 St. Martin D'Heres, France

Поступило 11 февраля 1999 г.