Math-Net.Ru

Общероссийский математический портал

В. М. Бухштабер, А. В. Устинов, Кольца коэффициентов формальных групп, *Матем. сб.*, 2015, том 206, номер 11, 19–60

DOI: <https://doi.org/10.4213/sm8523>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением <http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 18.234.156.22

26 апреля 2023 г., 17:39:54

УДК 512.741+517.583

В. М. Бухштабер, А. В. Устинов

Кольца коэффициентов формальных групп

Описаны кольца коэффициентов универсальных формальных групповых законов, которые играют важную роль в алгебраической геометрии, алгебраической топологии и их приложениях в математической физике. Построены гомоморфизмы этих колец, соответствующие редукциям одного вида группового закона к другому. Доказательства опираются на теоретико-числовые свойства биномиальных коэффициентов.

Библиография: 37 названий.

Ключевые слова: формальные группы, теоремы сложения, биномиальные коэффициенты, роды Хирцебруха.

DOI: 10.4213/sm8523

§ 1. Введение

Мы будем использовать следующие стандартные обозначения: $\mathbb{Z}$ – кольцо целых чисел, $\mathbb{Q}$ – поле рациональных чисел, $\mathbb{Z}_p$ – кольцо целых p -адических чисел, $\mathbb{F}_p$ – поле вычетов из p элементов.

В своей первой публикации [1] Н. Абель рассмотрел задачу: найти функции $\varphi(x)$, $f(x)$ и $\psi(x)$ такие, что выполняется тождество

$$\psi(\alpha(x, y)) = F(x, y, \varphi(x), f(y), \varphi'(x), f'(y), \dots),$$

где $\alpha(x, y)$ и $F(x, y, \dots)$ – заданные функции.

Предложенный им метод сводит поставленную задачу к решению дифференциальных уравнений. Этот метод широко используется до сих пор, когда речь идет о построении решения в рядах с коэффициентами в кольцах при условии, что в кольцах допустимо умножение на рациональные числа. В качестве примера в [1] решено функциональное уравнение

$$\psi(x + y) = \varphi(x)f'(y) + f(y)\varphi'(x), \quad (1.1)$$

которое благодаря работе Ф. Хирцебруха [2] нашло важные приложения в алгебраической геометрии и алгебраической топологии.

В работе [3] Н. Абель рассмотрел задачу: найти функцию $F(x, y)$ такую, что

$$F(F(x, y), z) = F(x, F(y, z)), \quad F(x, y) = F(y, x).$$

Метод Абеля из [1] позволяет найти решение этой задачи в рядах, которое на современном языке формулируется так: пусть одномерный формальный групповой закон задан над кольцом, в котором можно умножать на рациональные

Работа выполнена при поддержке Российского фонда фундаментальных исследований (первый автор – грант № 14-01-00537а; второй автор – грант № 14-01-00203а).

числа; тогда существует замена переменных, которая приводит этот закон к линейному виду. Этот результат заложил основы теории групп Ли и, в частности, теории формальных групп.

Центральное место в докладе Ж. Дьедонне “Дифференциальное исчисление в полях характеристики $p > 0$ ” на Математическом конгрессе в Стокгольме (1954 г.; см. [4]) по существу занимала задача решения уравнения ассоциативности $F(F(x, y), z) = F(x, F(y, z))$ в полях характеристики $p > 0$. Этот доклад положил начало современной теории формальных групп над произвольными кольцами.

Задача описания всех формальных групповых законов над произвольным коммутативным кольцом R несложно сводится к задаче описания всех кольцевых гомоморфизмов $\mathcal{R} \rightarrow R$, где $\mathcal{R}$ – кольцо коэффициентов универсального формального группового закона. Важнейшим результатом теории формальных групп явилась теорема М. Лазара (см. [5]), согласно которой кольцо $\mathcal{R}$ является кольцом полиномов с целыми коэффициентами от бесконечного набора мультипликативных образующих. Таким образом, задача эффективного описания формальных групповых законов над произвольным коммутативным кольцом R была сведена к задаче построения мультипликативных образующих кольца $\mathcal{R}$. Другой важной задачей теории формальных групп является следующая: классифицировать формальные группы над данным кольцом с точностью до изоморфизма, т.е. с точностью до замены переменных над данным кольцом. Эта задача для (одномерных) формальных групп над кольцом целых чисел была решена в работе Т. Хонды [6] с помощью методов и глубоких результатов из аналитической теории чисел.

Большое внимание к теории формальных групп было привлечено благодаря открытию А. С. Мищенко и С. П. Новиковым формальной группы в теории комплексных кобордизмов (см. [7]). Остановимся на этом более подробно. В 1966 г. на Математическом конгрессе в Москве С. П. Новиков представил программу перестройки методов алгебраической топологии на базе комплексных кобордизмов. В его предисловии к монографии [8] отмечено, что он “в 1967 г. представил развитие этой программы, совершая визит в США. В частности, на докладе в Гарварде, где присутствовал и Квиллен, были представлены приложения формальной группы”. В 1969 г. была опубликована работа Д. Квиллена [9], в которой показано, что из теоремы М. Лазара и теоремы Милнора–Новикова о кольце комплексных кобордизмов следует, что кольцо коэффициентов $\mathcal{R}$ можно отождествить с кольцом комплексных кобордизмов. Важнейшим следствием этого результата явилось утверждение: каждая формальная группа над кольцом R без кручения однозначно задает род Хирцебруха стабильно комплексных многообразий, принимающий значения в кольце R . Это открыло дорогу для приложений теории формальных групп в алгебраической топологии. Д. Квиллен в [9] применил классификацию с точностью до изоморфизма формальных групп над кольцом $\mathcal{R} \otimes \mathbb{Z}_p$. В результате он получил канонические аналоги когомологических операций Ландвебера–Новикова в незадолго до того построенной теории Брауна–Петерсона, которые ранее уже были использованы С. П. Новиковым в [7]. Операции Квиллена заняли видное место в аппарате гомотопической топологии. Одним из первых важнейших развитий результата работы [9] было построение Дж. Моравой так называемых

K -теорий Моравы. Благодаря этим теориям когомологий получены фундаментальные результаты. Универсальная формальная группа явилась основой для построения теории алгебраических кобордизмов в алгебраической геометрии, включающей аналоги операций Ландвебера–Новикова (см. обзор [10]). В известной проблеме построения эллиптических когомологий существенно используются результаты Дж. Тейта [11] об арифметической униформизации общей модели эллиптической кривой (см. [12]).

Анализ результатов теории формальных групп с точки зрения теории кобордизмов был проведен в работе В. М. Бухштабера и С. П. Новикова [13], в которой, в частности, был предложен метод доказательства теоремы Лазара на основе выбора мультипликативных образующих кольца коэффициентов универсального закона в терминах коэффициентов этого закона. Развитие этого метода было дано М. Хазевинкелем в фундаментальной монографии по теории формальных групп [14]. Метод работы [13] был использован в [15] для вычисления кольца коэффициентов универсального группового закона

$$F(u, v) = uA(v) + vA(u) - a_1 uv, \quad a_1 = A'(0), \quad (1.2)$$

соответствующего уравнению (1.1). Несмотря на простой вид этого формального группового закона задача вычисления структуры кольца его коэффициентов оказалась более трудной, чем вычисление структуры универсального кольца $\mathcal{R}_U$ (сравните доказательства из § 4 и § 5). Решение этой задачи нашло нетривиальные приложения. На основе этого результата построена $\mathbb{C}$ -ориентированная теория когомологий, в которой реализуется эта формальная группа; см. [16]. Формальную группу вида (1.2) естественно рассматривать как деформацию мультипликативной формальной группы $F(u, v) = u + v - \mu uv$, которая реализуется в комплексной K -теории. Связь формальной группы (1.2) с мультипликативной формальной группой описана в [17]. Свойства кольца коэффициентов формальной группы (1.2) в настоящей работе использованы при изучении формальной группы более общего вида

$$F(u, v) = \frac{u^2 A(v) - v^2 A(u)}{uB(v) - vB(u)}, \quad (1.3)$$

введенной в [18].

Важным шагом в развитии теории родов Хирцебруха явилось открытие рода, задаваемого эллиптическим синусом Якоби $\operatorname{sn}(x; k)$. Это открытие было сделано С. Опаниным в ходе доказательства гипотезы П. Ландвебера и Р. Стонга о характеристических числах Spin -многообразий с действием окружности (см. [19]). Вскоре последовала знаменитая работа Э. Виттена “Эллиптические роды и квантовая теория поля” (см. [20]) со ссылкой на препринт работы С. Опанина [19]. В связи с этим большое внимание было привлечено к классическим теоремам сложения для эллиптической функции $\operatorname{sn}(x; k)$. В [19] и последующих многочисленных работах, связанных с так называемым родом Опанина–Виттена, использовалась формула Эйлера. С развитием теории соответствующей формальной группы стала использоваться форма теоремы сложения, предложенная А. Кэли (см. [21]),

$$\psi(x + y) = \frac{\psi(x)^2 - \psi(y)^2}{\psi(x)\psi'(y) - \psi(y)\psi'(x)}.$$

Этой теореме сложения соответствует формальная группа вида

$$F(u, v) = \frac{u^2 - v^2}{uB(v) - vB(u)}. \quad (1.4)$$

Имеется много работ с теоретико-числовыми результатами, посвященных кольцу коэффициентов формальной группы, экспонентой которой является функция $\text{sn}(x; k)$.

Новые результаты в алгебраической топологии и новые связи с физикой стали возможными благодаря роду Хирцебруха, введенному И. М. Кричевером (см. [22]). Этот род задается функцией Бейкера–Ахиезера $\Phi_s(x)$ эллиптической кривой. Эта функция играет фундаментальную роль в теории интегрируемых систем (см. [23]). В работе [18] было показано, что экспонентой формальной группы вида (1.3) является функция $\psi_s(x) = e^{\alpha x} / \Phi_s(x)$. Кольцу коэффициентов этой формальной группы посвящено несколько работ, в которых были получены важные, но частные результаты (см. [12], [24]).

В настоящей работе вычислены кольца коэффициентов универсальных формальных групп, вид которых описан выше. Доказательства используют предложенный общий метод, опирающийся на теоретико-числовые результаты о свойствах биномиальных коэффициентов. Этот метод продемонстрирован при доказательстве теоремы Лазара, которое, в частности, упрощает доказательство из [14]. Приведено более простое вычисление кольца коэффициентов универсальной формальной группы вида (1.2), названной в [15] формальной группой Абеля. Основными результатами работы являются вычисления колец коэффициентов универсальных формальных групп вида (1.3) и (1.4). В §9 приведены доказательства необходимых свойств биномиальных коэффициентов.

Авторы благодарят Федора Владимировича Петрова за ценные предложения и замечания по тексту статьи, в том числе за замечания, позволившие упростить некоторые доказательства из §9.

§ 2. Формальные группы

2.1. Основные понятия и первые результаты. Все кольца, рассматриваемые в настоящей работе, будут предполагаться коммутативными. Для формального степенного ряда $f(t)$ такого, что $f(0) = 0$ и $f'(0) = 1$, через $\bar{f}(t)$ будем обозначать ряд, обратный к $f(t)$ по отношению к операции композиции:

$$\bar{f}(f(t)) = f(\bar{f}(t)) = t.$$

Одномерным формальным групповым законом (или формальной группой) над кольцом R называется формальный ряд

$$F(u, v) = u + v + \sum_{i, j \geq 1} a_{i, j} u^i v^j \in R[[u, v]], \quad (2.1)$$

удовлетворяющий условиям ассоциативности

$$F(u, F(v, w)) = F(F(u, v), w) \quad (2.2)$$

и коммутативности

$$F(u, v) = F(v, u).$$

Общую теорию формальных групп см. в [14].

Пусть $F_1(u, v)$, $F_2(u, v)$ – формальные группы над R . Гомоморфизмом формальных групп $b: F_1 \rightarrow F_2$ над кольцом R называется формальный ряд $b(u) \in R[[u]]$, где $b(0) = 0$, такой, что $b(F_1(u, v)) = F_2(b(u), b(v))$. Гомоморфизм b называется *изоморфизмом*, если $b'(0)$ – обратимый элемент в кольце R , и *сильным изоморфизмом*, если $b'(0) = 1$.

Следующая лемма демонстрирует общий метод Абеля, представленный в [1], и одновременно, при определенных начальных данных, решение задачи, поставленной им в [3].

ЛЕММА 2.1. Пусть $F(u, v) \in R[[u, v]]$, где R – кольцо без кручения. Введем ряд $b(u) \in R[[u]]$ такой, что $b(0) = 0$ и $b'(0) = 1$. Тогда соотношение

$$b(F(u, v)) = b(u) + b(v) \quad (2.3)$$

имеет место тогда и только тогда, когда $F(u, v)$ является формальной группой и

$$b'(u)\omega(u) = 1, \quad (2.4)$$

где

$$\omega(u) = \left. \frac{\partial}{\partial v} F(u, v) \right|_{v=0}. \quad (2.5)$$

ДОКАЗАТЕЛЬСТВО. Пусть выполняется соотношение (2.3). Так как в условиях леммы $b(0) = 0$ и $b'(0) = 1$, то существует ряд $\bar{b}(u) \in R[[u]]$ и, значит, $F(u, v) = \bar{b}(b(u) + b(v))$; следовательно, $F(u, v)$ является формальной группой над кольцом R . Дифференцируя (2.3) по v , полагая $v = 0$ и используя условие леммы, получаем соотношение (2.4).

Обратно, пусть ряд $F(u, v)$ задает групповой закон над кольцом R и существует ряд $b(u) \in R[[u]]$ такой, что выполняется соотношение (2.4), где ряд $\omega(u)$ задается формулой (2.5). Докажем, что в этом случае выполняется соотношение (2.3). Положим

$$C(u, v) = b(F(u, v)) - b(u) - b(v). \quad (2.6)$$

Тогда $C(u, v) = C(v, u)$, $C(u, 0) = 0$. Покажем, что

$$\frac{\partial C(u, v)}{\partial u} \equiv 0.$$

Используя формулы (2.4) и (2.5), получаем, что

$$\frac{\partial C(u, v)}{\partial u} = b'(F(u, v)) \frac{\partial F(u, v)}{\partial u} - b'(u) = \frac{1}{\omega(F(u, v))} \frac{\partial F(u, v)}{\partial u} - \frac{1}{\omega(u)}.$$

Дифференцируя соотношение ассоциативности

$$F(F(u, v), s) = F(F(u, s), v)$$

по s и полагая $s = 0$, приходим к соотношению

$$\omega(F(u, v)) = \omega(u) \frac{\partial F(u, v)}{\partial u}. \quad (2.7)$$

Следовательно,

$$\frac{\partial C(u, v)}{\partial u} \equiv 0.$$

Так как кольцо R не имеет кручения, то из последней формулы и начального условия $C(0, v) = 0$ следует, что $C(u, v) \equiv 0$. Таким образом, соотношение (2.6) превращается в (2.3).

СЛЕДСТВИЕ 2.2. Пусть $F(u, v)$ – формальный ряд над кольцом R и

$$b(u) = \int_0^u \frac{ds}{\omega(s)}$$

– ряд над кольцом $R \otimes \mathbb{Q}$, где $\omega(u) \in R[[u]]$ задается формулой (2.5). Тогда над кольцом $R \otimes \mathbb{Q}$ имеет место соотношение

$$b(F(u, v)) = b(u) + b(v).$$

Таким образом, над кольцом $R \otimes \mathbb{Q}$ всегда существует сильный изоморфизм формальной группы $F(u, v)$ и аддитивной группы $F_a(u, v) = u + v$. Ряд $b(u)$ в этом случае обозначается как $g(u)$ и называется логарифмом формальной группы $F(u, v)$. Ряд $f(t) = \bar{g}(t) \in R \otimes \mathbb{Q}[[t]]$ называется экспонентой формальной группы $F(u, v)$. Для него выполняется соотношение

$$f(t_1 + t_2) = F(f(t_1), f(t_2)), \quad (2.8)$$

причем $f(0) = 0$, $f'(0) = 1$. Таким образом, ряд $f(t)$ задает сильный изоморфизм $f: F_a \rightarrow F$.

СЛЕДСТВИЕ 2.3. Экспонента $f(t)$ формальной группы $F(u, v)$ однозначно определяется как решение дифференциального уравнения

$$f'(t) = \omega(f(t)) \quad (2.9)$$

с начальным условием $f(0) = 0$, где $\omega(u)$ задается формулой (2.5).

Обратим внимание на то, что $g'(u) \in R[[u]]$. Формальная группа над кольцом R называется *линеаризуемой*, если $g(u) \in R[[u]]$, и поэтому $f(u) \in R[[u]]$. Простейшим примером нелинеаризуемой группы над кольцом целых чисел является формальная группа $F(u, v) = u + v - uv$. В этом случае $\omega(u) = 1 - u$ и $g(u) = -\log(1 - u)$, $f(u) = 1 - e^{-u}$ – ряды с рациональными коэффициентами.

2.2. Универсальная формальная группа. Важным фактом из теории формальных групп является существование *универсального кольца* $\mathcal{R}_U$ и *универсального формального группового закона*

$$\mathcal{F}_U(u, v) = u + v + \sum_{i,j=1}^{\infty} \alpha_{i,j} u^i v^j \in \mathcal{R}_U[[u, v]], \quad (2.10)$$

для которых справедливо следующее свойство: для любого кольца R и любой формальной группы $F(u, v)$ над R существует канонический кольцевой гомоморфизм $H_F: \mathcal{R}_U \rightarrow R$ такой, что

$$F(u, v) = u + v + \sum_{i,j=1}^{\infty} H_F(\alpha_{i,j}) u^i v^j.$$

Гомоморфизм H_F называется *классифицирующим*.

Для формального группового закона (2.1) через I^2 будем обозначать идеал в кольце R , порожденный всевозможными элементами вида $a_{i_1, j_1} a_{i_2, j_2}$, где $i_1, i_2, j_1, j_2 \geq 1$. В случае, когда кольцо R порождается элементами $a_{i, j}$, идеал I^2 совпадает с идеалом разложимых элементов.

ЛЕММА 2.4. *Универсальная формальная группа существует.*

ДОКАЗАТЕЛЬСТВО. Рассмотрим множество алгебраически независимых элементов $\{\tilde{a}_{i, j} : 1 \leq i, j < \infty\}$ с условием $\tilde{a}_{i, j} = \tilde{a}_{j, i}$, кольцо $\mathcal{R} = \mathbb{Z}[\tilde{a}_{1, 1}, \dots, \tilde{a}_{i, j}, \dots]$ и ряд

$$\mathcal{F}(u, v) = u + v + \sum_{i, j=1}^{\infty} \tilde{a}_{i, j} u^i v^j \in \mathcal{R}[[u, v]].$$

Рассмотрим ряд, возникающий из уравнения ассоциативности,

$$\mathcal{F}(u, \mathcal{F}(v, w)) - \mathcal{F}(\mathcal{F}(u, v), w) = \sum_{i, j, k} P_{i, j, k} u^i v^j w^k \in \mathcal{R}[[u, v, w]].$$

Обозначим через I_{ass} идеал в кольце $\mathcal{R}$, порожденный полиномами $P_{i, j, k}$ от коэффициентов закона $\mathcal{F}(u, v)$, положим $\mathcal{R}_U = \mathcal{R}/I_{\text{ass}}$ и обозначим через π каноническую проекцию $\mathcal{R} \rightarrow \mathcal{R}_U$. Тогда ряд

$$\mathcal{F}_U(u, v) = u + v + \sum_{i, j=1}^{\infty} \alpha_{i, j} u^i v^j \in \mathcal{R}_U[[u, v]],$$

где $\alpha_{i, j} = \pi(\tilde{a}_{i, j})$, задает формальный групповой закон. Лемма доказана.

Канонический гомоморфизм $H_F: \mathcal{R}_U \rightarrow R$, о котором шла речь выше, однозначно определяется следующим образом: по групповому закону (2.1) над кольцом R однозначно определен гомоморфизм $H: \mathcal{R} \rightarrow R$ такой, что $H(\tilde{a}_{i, j}) = a_{i, j}$. Из условия ассоциативности (2.2) следует, что гомоморфизм H раскладывается в композицию $H = H_F \circ \pi$.

2.3. Формальные группы фиксированного вида. Если на коэффициенты формального группового закона (2.1) или на закон $F(u, v)$ в целом наложены дополнительные фиксированные ограничения (наличие таких ограничений будем обозначать знаком $\#$), то можно говорить о формальных группах заданного вида. При этом возникает следующая задача: построить *универсальный формальный групповой закон заданного вида*, т.е. найти кольцо $\mathcal{R}_{\#}$ и ряд $\mathcal{F}_{\#}(u, v)$, удовлетворяющие наложенным условиям, такие, что для любого кольца R и любой формальной группы $F(u, v)$, удовлетворяющих тем же условиям, существует канонический гомоморфизм $H_{\#, F}: \mathcal{R}_{\#} \rightarrow R$ такой, что

$$F(u, v) = u + v + \sum_{i, j=1}^{\infty} H_{\#, F}(\alpha_{i, j}) u^i v^j \in R[[u, v]].$$

ОПРЕДЕЛЕНИЕ 2.5. Формальный групповой закон (2.1) назовем *порождающим*, если кольцо R мультипликативно порождается элементами $a_{i, j}$, $i, j \geq 1$.

По построению универсальный формальный групповой закон $\mathcal{F}_U$ является порождающим. Очевидно, что порождающими также являются универсальные аддитивный и мультипликативный групповые законы

$$\begin{aligned}\mathcal{F}_0(u, v) &= u + v, & \mathcal{R}_0 &= \mathbb{Z}, \\ \mathcal{F}_1(u, v) &= u + v - \mu uv, & \mathcal{R}_1 &= \mathbb{Z}[\mu].\end{aligned}$$

Формальный групповой закон $\mathcal{F}_0$ соответствует роду Хирцебруха, который на точке принимает значение единица, а на всех многообразиях положительной размерности – значение нуль. Формальная группа $\mathcal{F}_1$ соответствует роду Тодда, который однозначно определяется тем, что на n -мерном комплексном проективном пространстве $\mathbb{C}P^n$ он принимает значения μ^n .

Порождающим, очевидно, является также формальный групповой закон

$$\mathcal{F}_2(u, v) = \frac{u + v + \sigma_1 uv}{1 - \sigma_2 uv}, \quad \mathcal{R}_2 = \mathbb{Z}[\sigma_1, \sigma_2].$$

Эта формальная группа соответствует двухпараметрическому роду Тодда.

Настоящая работа посвящена решению задачи об описании колец коэффициентов для следующих универсальных формальных групповых законов:

$$\mathcal{F}_3(u, v) = \frac{u^2 - v^2}{uB(v) - vB(u)}, \quad \mathcal{R}_3 = \mathbb{Z}[\beta_2, \beta_3, \dots]/I_{\text{ass}}, \quad (2.11)$$

$$\mathcal{F}_4(u, v) = uA(v) + vA(u) - \alpha_1 uv, \quad \mathcal{R}_4 = \mathbb{Z}[\alpha_1, \alpha_2, \dots]/I_{\text{ass}}, \quad (2.12)$$

$$\mathcal{F}_5(u, v) = \frac{u^2 A(v) - v^2 A(u)}{uB(v) - vB(u)}, \quad \mathcal{R}_5 = \mathbb{Z}[\alpha_1, \alpha_3, \dots, \beta_2, \beta_3, \dots]/I_{\text{ass}}, \quad (2.13)$$

$$\mathcal{F}_6(u, v) = \frac{u^2 B(v) - v^2 B(u)}{uB(v) - vB(u)}, \quad \mathcal{R}_6 = \mathbb{Z}[\beta_1, \beta_2, \beta_3, \dots]/I_{\text{ass}}, \quad (2.14)$$

где

$$A(x) = 1 + \sum_{i=1}^{\infty} \alpha_i x^i, \quad B(x) = 1 + \sum_{i=1}^{\infty} \beta_i x^i.$$

Всегда будем предполагать, что неопределенности, возникающие при $u = v$, разрешаются с помощью предельного перехода. Как отмечено выше, формальные групповые законы (2.11)–(2.13) над $R \otimes \mathbb{Q}$ полностью задаются своими экспонентами. Вид этих законов определяется формулами сложения для экспонент. В случае формальной группы вида $\mathcal{F}_3$ экспонента является эллиптическим синусом Якоби (см. [21]), в случае группы $\mathcal{F}_4$ – линейной комбинацией двух экспонент, в частности тригонометрическим синусом (см. [1], [15]), и, наконец, вид закона $\mathcal{F}_5$ определяется формулой сложения для функции Бейкера–Ахизера эллиптической кривой (см. [23], [18]). Формальная группа $\mathcal{F}_3$ соответствует роду Ошанина, а формальная группа $\mathcal{F}_5$ – комплексному роду Кричевера (детали см. в [10] и [25; приложение E]).

ЗАМЕЧАНИЕ 2.6. В формальной группе $\mathcal{F}_3(u, v)$ коэффициент β_1 не дает вклад в кольцо $\mathcal{R}_3$.

В формальной группе $\mathcal{F}_5(u, v)$ вклад в кольцо $\mathcal{R}_5$ не дают коэффициенты α_2 и β_1 .

Коэффициенты β_1 (в случае группы $\mathcal{F}_3$) и α_2, β_1 (в случае группы $\mathcal{F}_5$) играют роль начальных данных в задаче о редукции одного формального группового закона к другому.

ЛЕММА 2.7. *Формальные групповые законы $\mathcal{F}_0$ – $\mathcal{F}_4$, $\mathcal{F}_6$ являются частными случаями закона $\mathcal{F}_5$.*

ДОКАЗАТЕЛЬСТВО. Для каждого из законов $\mathcal{F}_i$, $i = 0, 1, 2, 3, 4$, укажем явно функции $A(x)$ и $B(x)$, для которых закон $\mathcal{F}_5$ превращается в $\mathcal{F}_i$:

$$\begin{aligned} A_0(x) &= B_0(x) = 1; \\ A_1(x) &= 1 - \mu x, & B_1(x) &= 1; \\ A_2(x) &= B_2(x) = 1 + \sigma_1 x + \sigma_2 x^2; \\ A_3(x) &= 1, & B_3(x) &= B(x); \\ A_4(x) &= A(x)^2 - a_1 x A(x), & B_4(x) &= A(x); \\ A_6(x) &= B_6(x) = B(x). \end{aligned}$$

ЗАМЕЧАНИЕ 2.8. Формальная группа $\mathcal{F}_2$ является специализацией формальной группы $\mathcal{F}_6$. В частности, в кольце $\mathcal{R}_6$ можно выбрать такой набор мультипликативных образующих, что гомоморфизм $\mathcal{R}_U \rightarrow \mathcal{R}_2$, классифицирующий формальную группу $\mathcal{F}_2$, раскладывается в композицию $\mathcal{R}_U \rightarrow \mathcal{R}_6 \rightarrow \mathcal{R}_2$, где первое отображение – это гомоморфизм, классифицирующий формальную группу $\mathcal{F}_6$.

ЛЕММА 2.9. *Формальные групповые законы $\mathcal{F}_3$ – $\mathcal{F}_6$ являются порождающими.*

ДОКАЗАТЕЛЬСТВО. Для закона $\mathcal{F}_4$ утверждение леммы тривиально. Доказательство остается провести для закона $\mathcal{F}_5$, поскольку законы $\mathcal{F}_3$, $\mathcal{F}_6$ являются его частными случаями. Сокращая числитель и знаменатель группового закона (2.13) на $u - v$, получаем, что

$$\begin{aligned} \mathcal{F}_5(u, v) &= \frac{u + v + \alpha_1 uv - u^2 v^2 (\alpha_3 + \alpha_4 h_1 + \alpha_5 h_2 + \cdots)}{1 - uv(\beta_2 + \beta_3 h_1 + \beta_4 h_2 + \cdots)} \\ &\equiv (u + v + \alpha_1 uv - u^2 v^2 (\alpha_3 + \alpha_4 h_1 + \alpha_5 h_2 + \cdots)) \\ &\quad \times (1 + uv(\beta_2 + \beta_3 h_1 + \beta_4 h_2 + \cdots)) \\ &\equiv u + v + \alpha_1 uv - u^2 v^2 (\alpha_3 + \alpha_4 h_1 + \cdots) \\ &\quad + uv(u + v)(\beta_2 + \beta_3 h_1 + \cdots) \pmod{I^2}, \end{aligned}$$

где

$$h_n = h_n(u, v) = \frac{u^{n+1} - v^{n+1}}{u - v}.$$

Приравнивая коэффициенты при мономах $u^i v^j$ к $\alpha_{i,j}$, приходим к равенствам

$$\begin{aligned} \alpha_{1,1} &\equiv \alpha_1, \\ \alpha_{i,1} &\equiv \alpha_{1,i} \equiv \beta_i \pmod{I^2}, & i > 1, \\ \alpha_{i,j} &\equiv \alpha_{j,i} \equiv 2\beta_{i+j-1} - \alpha_{i+j-1} \pmod{I^2}, & i, j > 1. \end{aligned} \tag{2.15}$$

Отсюда следует, что коэффициенты рядов $A(x)$ и $B(x)$ выражаются через коэффициенты ряда $\mathcal{F}_5(u, v)$.

СЛЕДСТВИЕ 2.10. *Гомоморфизмы $H_i: \mathcal{R}_U \rightarrow \mathcal{R}_i$, $i = 1, \dots, 6$, классифицирующие формальные группы $\mathcal{F}_i$, являются эпиморфизмами. Для каждого i в кольце $\mathcal{R}_U$ можно выбрать такой набор мультипликативных образующих $\{e_1, \dots, e_n, \dots\}$, что множество ненулевых элементов $H_i(e_n)$ представляет собой минимальный набор мультипликативных образующих кольца $\mathcal{R}_i$.*

Для натуральных $m_1, \dots, m_k$ обозначим через $(m_1, \dots, m_k)$ наибольший общий делитель чисел $m_1, \dots, m_k$. С помощью алгоритма Евклида всегда можно найти целые $\lambda_1, \dots, \lambda_k$, для которых выполняется равенство

$$\lambda_1 m_1 + \dots + \lambda_k m_k = (m_1, \dots, m_k).$$

Для натуральных $n \geq 2$ определим числа

$$d(n) = \left(\binom{n}{1}, \binom{n}{2}, \dots, \binom{n}{n-1} \right). \quad (2.16)$$

Из теоремы Куммера 9.2 (см. п. 9.2) следует, что

$$d(n) = \begin{cases} p, & \text{если } n = p^k, \text{ где } p - \text{простое число,} \\ 1 & \text{в остальных случаях.} \end{cases} \quad (2.17)$$

В явном виде этот результат впервые был опубликован в статье [26]. Для каждого $n \geq 1$ зафиксируем набор чисел $(\lambda_1, \dots, \lambda_n) = (\lambda_1^{(n+1)}, \dots, \lambda_n^{(n+1)})$, для которых выполняется равенство

$$\lambda_1 \binom{n+1}{1} + \lambda_2 \binom{n+1}{2} + \dots + \lambda_n \binom{n+1}{n} = d(n+1)$$

(явное описание одного из таких наборов см. в § 9). Для формальной группы (2.1) над кольцом R введем элемент $e_n \in R$ по формуле

$$e_n = \lambda_1 a_{1,n} + \lambda_2 a_{2,n-1} + \dots + \lambda_n a_{n,1}. \quad (2.18)$$

Для $a \in R$ через $\hat{a}$ будем обозначать соответствующий элемент $\hat{a} \in \hat{R} = R/I^2$.

ОПРЕДЕЛЕНИЕ 2.11. Для каждой формальной группы $F(u, v)$ над кольцом R введем функцию $\rho: \mathbb{N} \rightarrow \{\mathbb{N} \cup \infty\}$ такую, что $\rho(n)$ есть порядок элемента $\hat{e}_n$ в кольце $\hat{R} = R/I^2$.

§ 3. Экспоненты и логарифмы формальных групп

Экспоненты и логарифмы формальных групп $\mathcal{F}_0$ – $\mathcal{F}_2$ над полем $\mathbb{Q}$ хорошо известны:

$$\begin{aligned} f_0(t) &= t, & g_0(u) &= u; \\ f_1(t) &= \frac{1 - e^{-\mu t}}{\mu}, & g_1(u) &= -\frac{\log(1 - \mu u)}{\mu}; \\ f_2(t) &= \frac{e^{at} - e^{bt}}{ae^{bt} - be^{at}}, & g_2(u) &= \frac{\log(1 + au) - \log(1 + bu)}{a - b}, \end{aligned}$$

где $a + b = \sigma_1$, $ab = \sigma_2$.

Формальная группа $\mathcal{F}_6$ над полем $\mathbb{Q}$ оказывается изоморфна $\mathcal{F}_2$ и, как следствие, имеет те же экспоненту и логарифм.

3.1. Формальная группа $\mathcal{F}_3$.

ПРЕДЛОЖЕНИЕ 3.1. *Имеет место изоморфизм $\mathcal{R}_3 \otimes \mathbb{Q} \cong \mathbb{Q}[\beta_2, \beta_4]$, где β_2 и β_4 – коэффициенты ряда $B(x)$ из формулы (2.11). Сильный изоморфизм аддитивной формальной группы $\mathcal{F}_0$ в формальную группу $\mathcal{F}_3$ реализуется над кольцом $\mathbb{Q}[\delta, \varepsilon]$ и задается экспонентой, которая однозначно определяется как регулярное в нуле решение дифференциального уравнения*

$$(f'(t))^2 = 1 - 2\delta f^2(t) + \varepsilon f^4(t) \quad (3.1)$$

с начальными данными $f(0) = 0$ и $f'(0) = 1$. При вложении

$$\mathcal{R}_3 \otimes \mathbb{Q} \subset \mathbb{Q}[\delta, \varepsilon] : \quad \beta_2 \rightarrow -\delta, \quad \beta_4 \rightarrow \frac{\varepsilon - \delta^2}{2}, \quad (3.2)$$

ряд $B(u)$ переходит в производящую функцию полиномов от ε и δ , которая задается формулой

$$B(u) = \sqrt{1 - 2\delta u^2 + \varepsilon u^4}.$$

Экспонента $f(x)$, определяемая уравнением (3.1), реализуется разложением в ряд при $t = 0$ функции

$$f(t) = \sqrt{\xi} \operatorname{sn} \left(\frac{t}{\sqrt{\xi}}, k \right), \quad (3.3)$$

где

$$\xi = \frac{\delta \pm \sqrt{\delta^2 - \varepsilon}}{\varepsilon}, \quad k = \frac{\delta \pm \sqrt{\delta^2 - \varepsilon}}{\sqrt{\varepsilon}}.$$

ДОКАЗАТЕЛЬСТВО. Эллиптический синус Якоби $y(z) = \operatorname{sn}(z, k)$ однозначно определяется как решение дифференциального уравнения

$$(y'(z))^2 = (1 - y^2)(1 - k^2 y^2) \quad (3.4)$$

с начальными данными $y(0) = 0$, $y'(0) = 1$. Таким образом, экспонента $f(t)$ имеет вид (3.3). Из закона сложения для эллиптического синуса Якоби следует, что

$$F(u, v) = f(t_1 + t_2) = \frac{u\sqrt{1 - 2\delta v^2 + \varepsilon v^4} + v\sqrt{1 - 2\delta u^2 + \varepsilon u^4}}{1 - \varepsilon u^2 v^2},$$

где $u = f(t_1)$, $v = f(t_2)$. Этот закон можно преобразовать к виду

$$F(u, v) = \frac{u^2 - v^2}{u\tilde{B}(v) - v\tilde{B}(u)},$$

где

$$\tilde{B}(u) = \sqrt{1 - 2\delta u^2 + \varepsilon u^4} = 1 - \delta t^2 + \frac{1}{2}t^4(\varepsilon - \delta^2) + \frac{1}{2}t^6(\delta\varepsilon - \delta^3) + \dots \in \mathbb{Z}\left[\frac{1}{2}, \delta, \varepsilon\right].$$

Вложение $\mathcal{R}_3 \otimes \mathbb{Q} \subset \mathbb{Q}[\delta, \varepsilon]$ позволяет отождествить ряд $B(u)$ с рядом $\tilde{B}(u)$.

3.2. Формальная группа $\mathcal{F}_4$. Обозначим через $[F^k]_{m,n}$ коэффициент при $u^m v^n$ у ряда $F^k(u, v)$.

ЛЕММА 3.2. *Гомоморфизм $H_4: \mathcal{R}_U \rightarrow \mathcal{R}_4$, классифицирующий формальную группу $\mathcal{F}_4$, является эпиморфизмом таким, что идеал $\ker H_4$ порожден следующими соотношениями:*

$$n\alpha_n + \sum_{k=2}^{n-1} k\alpha_k \alpha_{n-k} = 0, \quad n \geq 3, \quad (3.5)$$

$$\alpha_m \alpha_n = \binom{m+n}{m} \alpha_{m+n} + \sum_{k=2}^{m+n-1} [F^k]_{m,n} \alpha_k, \quad m, n \geq 2. \quad (3.6)$$

ДОКАЗАТЕЛЬСТВО. Приравнивая к нулю коэффициент при uvw^n , $n \geq 2$, в уравнении ассоциативности (2.2), получаем соотношение (3.5). Для монома $uv^m w^n$, $m, n \geq 2$, соответственно получаем равенство

$$\alpha_m \alpha_n = \sum_{k \geq 2} [F^k]_{m,n} \alpha_k, \quad m, n \geq 2, \quad (3.7)$$

равносильное (3.6). Непосредственная проверка показывает, что при рассмотрении остальных мономов новых соотношений не возникает.

ПРЕДЛОЖЕНИЕ 3.3. *Имеет место изоморфизм $\mathcal{R}_4 \otimes \mathbb{Q} \cong \mathbb{Q}[\alpha_1, \alpha_2]$. Экспонента формальной группы $\mathcal{F}_4$ задается формулой*

$$f(u) = \frac{e^{\alpha u}}{\sqrt{\beta}} \operatorname{sh}(\sqrt{\beta}u), \quad (3.8)$$

где $\alpha = \alpha_1/2$, $\beta = 2\alpha_2 + \alpha_1^2/4$.

ДОКАЗАТЕЛЬСТВО. Из соотношения (3.5) следует, что кольцо $\mathcal{R}_4 \otimes \mathbb{Q}$ имеет не более двух образующих α_1 и α_2 . Проверим непосредственно, что функция (3.8), зависящая от свободных параметров α_1 и α_2 , является экспонентой формальной группы вида $\mathcal{F}_4$ над кольцом $\mathbb{Q}[\alpha, \beta]$. Используя теорему сложения для гиперболического синуса, получаем, что

$$f(t_1 + t_2) = f(t_1) \cdot e^{at_2} \operatorname{ch}(\sqrt{\beta}t_2) + f(t_2) \cdot e^{at_1} \operatorname{ch}(\sqrt{\beta}t_1).$$

Следовательно,

$$F(u, v) = f(g(u) + g(v)) = uA(v) + vA(u) - auv,$$

где $g = \bar{f}$ (логарифм формальной группы) и

$$A(u) = e^{ag(u)} \operatorname{ch}(\sqrt{\beta}g(u)) + \frac{au}{2}.$$

Как отмечалось выше, в алгебраической геометрии и алгебраической топологии каждой формальной группе ставится в соответствие род Хирцебруха (см. [27]).

Опишем важные роды Хирцебруха, определяемые формальной группой Абеля:

1) A -род: $\alpha = 0$,

$$f(t) = \frac{\operatorname{sh}(\sqrt{\beta}t)}{\sqrt{\beta}}, \quad g(u) = \frac{\operatorname{Arsh}(\sqrt{\beta}u)}{\sqrt{\beta}}, \quad F(u, v) = u\sqrt{1 + \beta v^2} + v\sqrt{1 + \beta u^2};$$

2) род Тодда: $\alpha = -\sqrt{\beta}$,

$$f(t) = \frac{e^{at} - 1}{a}, \quad g(u) = \frac{\log(1 + au)}{a}, \quad F(u, v) = u + v + auv;$$

3) $\beta = 0$:

$$f(t) = te^{\alpha t}, \quad g(u) = \frac{W(\alpha u)}{\alpha} = \log \mathcal{E}_{-\alpha}(u),$$

$$F(u, v) = ue^{W(\alpha v)} + ve^{W(\alpha u)} = u\mathcal{E}_{-\alpha}^\alpha(v) + v\mathcal{E}_{-\alpha}^\alpha(u),$$

где

$$\mathcal{E}_t(u) = \sum_{k=0}^{\infty} (tk + 1)^{k-1} \frac{z^k}{k!}$$

– обобщенный экспоненциальный ряд (см. [28; п. 5.4]) и

$$W(u) = \sum_{n=1}^{\infty} \frac{(-n)^{n-1}}{n!} u^n = \log \mathcal{E}_{-1}(u) \quad (3.9)$$

– функция Ламберта, которая в анализе определяется как решение функционального уравнения $z = W(z)e^{W(z)}$ (см. [29]).

Для универсальной группы $\mathcal{F}_4$ ряд $A(u)$ и логарифм g ниже будут в явном виде выражены через обобщенный биномиальный ряд Ламберта

$$\mathcal{B}_t(z) = \sum_{k=0}^{\infty} \binom{tk + 1}{k} \frac{1}{tk + 1} z^k. \quad (3.10)$$

Известно, что обобщенный биномиальный ряд $\mathcal{B}_t(z)$ и его степени $\mathcal{B}_t^r(z)$ связаны следующими замечательными соотношениями:

$$\mathcal{B}_t^{1-t}(z) - \mathcal{B}_t^{-t}(z) = z, \quad (3.11)$$

$$\mathcal{B}_t^r(z) = \sum_{k=0}^{\infty} \binom{tk + r}{k} \frac{r}{tk + r} z^k, \quad (3.12)$$

$$\frac{\mathcal{B}_t^r(z)}{1 - t + t\mathcal{B}_t^{-1}(z)} = \sum_{k=0}^{\infty} \binom{tk + r}{k} z^k, \quad (3.13)$$

$$\log \mathcal{B}_t(z) = \sum_{k=1}^{\infty} \binom{tk}{k} \frac{z^k}{tk}, \quad (3.14)$$

где r – произвольное действительное число. (Равенства (3.11)–(3.13) – это формулы (5.59)–(5.61) из [28], равенство (3.14) следует из результатов работы [30], оно также может быть получено дифференцированием по r функции $(\mathcal{B}_t^r(z) - 1)/r$ в точке $r = 0$.) В дальнейшем параметр r будет также

рассматриваться как формальная переменная. Нам потребуются следующие частные случаи формулы (3.12):

$$\begin{aligned}\mathcal{B}_\lambda^{-\lambda}(z) &= \sum_{k=0}^{\infty} \binom{\lambda k + \lambda}{k} \frac{\lambda}{\lambda k + \lambda} z^k, \\ \mathcal{B}_\lambda^{\lambda}(z) &= \sum_{k=0}^{\infty} \binom{\lambda k - \lambda}{k} \frac{-\lambda}{\lambda k - \lambda} z^k.\end{aligned}\quad (3.15)$$

ЛЕММА 3.4. Пусть параметры α_1, α_2 фиксированы, $\alpha = \alpha_1/2$, $\beta = 2\alpha_2 + \alpha_1^2/4$, $a = -2\sqrt{\beta}$ и $\lambda = (\alpha + \sqrt{\beta})/(2\sqrt{\beta})$. Тогда решением рекуррентного соотношения (3.5) является последовательность

$$\alpha_{n+1} = -\frac{1}{n} \binom{\lambda n}{n+1} (-2\sqrt{\beta})^{n+1} \in \mathbb{Q}[\alpha_1, \alpha_2], \quad n \geq 1. \quad (3.16)$$

Производящая функция $A(z) = 1 + \alpha_1 z + \alpha_2 z^2 + \dots$ последовательности коэффициентов $\{\alpha_n\}_{n=0}^{\infty}$ формальной группы $\mathcal{F}_4$ имеет вид

$$A(z) = (\alpha - \sqrt{\beta})z + \mathcal{B}_\lambda^{-\lambda}(-2\sqrt{\beta}z) = a(1 - \lambda)z + \mathcal{B}_\lambda^{-\lambda}(az). \quad (3.17)$$

ДОКАЗАТЕЛЬСТВО. Предположим, что числа α_n при $n \geq 2$ определены равенством (3.16). Формула (3.17) является прямым следствием определения обобщенного биномиального ряда, и для доказательства леммы достаточно проверить равенство (3.5).

Из (3.12) и (3.13) следует, что

$$(\mathcal{B}_t^{-t}(z))' = -t \sum_{k=0}^{\infty} \binom{tk-1}{k} z^k = \frac{-t}{(1-t)\mathcal{B}_t(z) + t}.$$

Поэтому

$$A'(z) = \alpha - \sqrt{\beta} - \frac{a\lambda}{(1-\lambda)\mathcal{B}_\lambda(az) + \lambda}. \quad (3.18)$$

Кроме того, согласно (3.11)

$$A(z) = (\alpha - \sqrt{\beta})z + \frac{az}{\mathcal{B}_\lambda(az) - 1}. \quad (3.19)$$

Из (3.18), (3.19) следует, что функция $A(z)$ является решением дифференциального уравнения

$$A'(z)A(z) = 2\alpha_2 z + \alpha_1 A(z), \quad (3.20)$$

равносильного рекуррентному соотношению (3.5).

ЗАМЕЧАНИЕ 3.5. Равенство (3.16) означает, что при $n \geq 1$

$$\alpha_{2n} = \frac{\alpha_2}{n \cdot (2n-2)!} \prod_{i=1}^{n-1} ((2n-1)^2 \alpha^2 - (2i-1)^2 \beta), \quad (3.21)$$

$$\alpha_{2n+1} = -\frac{4\alpha_1 \alpha_2 n^2}{(2n+1)!} \prod_{i=1}^{n-1} ((2n)^2 \alpha^2 - (2i)^2 \beta). \quad (3.22)$$

ЗАМЕЧАНИЕ 3.6. Если $2n - 2 < p$, то значение коэффициента α_{2n} по модулю p можно находить по формуле (3.21).

Перейдем теперь к явному описанию сильных изоморфизмов группы $\mathcal{F}_4$ с аддитивной и мультипликативной формальными группами над соответствующими кольцами.

ТЕОРЕМА 3.7. 1. *Сильный изоморфизм аддитивной формальной группы $\mathcal{F}_0(u, v)$ в формальную группу $\mathcal{F}_4(u, v)$ реализуется над кольцом $\mathbb{Q}[\alpha, \beta]$ и задается экспонентой (3.8). Обратный изоморфизм задается логарифмом*

$$g(z) = \frac{\log \mathcal{B}_\lambda(az)}{a} = -\frac{1}{2\sqrt{\beta}} \sum_{n=1}^{\infty} \binom{\lambda n}{n} \frac{(-2\sqrt{\beta}z)^n}{\lambda n} \in \mathbb{Q}[\alpha_1, \alpha_2]. \quad (3.23)$$

Имеет место изоморфизм $\mathcal{R}_4 \otimes \mathbb{Q} \cong \mathbb{Q}[\alpha, \beta]$, при котором $\alpha_1 = \alpha$, $\alpha_2 = -2\alpha^2 + \beta/2$ и α_n при $n > 2$ задаются формулами (3.21), (3.22). При таком вложении производящая функция $A(z)$ коэффициентов формального группового закона переходит в производящую функцию (3.17) полиномов (3.21), (3.22) от α и β .

2. *Сильный изоморфизм формальной группы $\mathcal{F}_4(u, v)$ в мультипликативную формальную группу $\mathcal{F}_1(u, v)$ реализуется над кольцом $\mathbb{Q}[a, \eta]$ рядом*

$$b(u) = u\mathcal{B}_\lambda^\lambda(au),$$

где $\lambda = \eta/a$. Обратный изоморфизм задается рядом

$$\bar{b}(u) = u(1 + au)^{-\lambda}. \quad (3.24)$$

Имеет место изоморфизм $\mathcal{R}_4 \otimes \mathbb{Q} \cong \mathbb{Q}[a, \eta]$, при котором производящая функция $A(u)$ коэффициентов формального группового закона переходит в ряд

$$(a - \eta)u + \mathcal{B}_\lambda^{-\lambda}(au) = 1 + (a - 2\eta)u + \sum_{k=2}^{\infty} \binom{\lambda k - \lambda}{k} \frac{(au)^k}{1 - k} = \sum_{k=0}^{\infty} \frac{p_k(a, \eta)}{k!} u^k,$$

являющийся экспоненциальной производящей функцией полиномов

$$p_k(a, \eta) = -\eta((k-1)\eta - a)((k-1)\eta - 2a) \cdots ((k-1)\eta - (k-1)a), \quad k \geq 2.$$

ДОКАЗАТЕЛЬСТВО. 1. Полагая $\mathcal{B}_t(z) = e^y$, перепишем равенство (3.11) в виде

$$2e^{y(1/2-t)} \operatorname{sh} \frac{y}{2} = z.$$

Отсюда следует, что

$$\mathcal{B}_t \left(2e^{y(1/2-t)} \operatorname{sh} \frac{y}{2} \right) = \mathcal{B}_t(z) = e^y.$$

Подставляя в последнюю формулу $t = \lambda$ и $y = au$, получаем

$$\log \mathcal{B}_\lambda \left(2e^{\alpha u} \operatorname{sh} \frac{au}{2} \right) = au.$$

Это равенство означает, что обратной к функции f является функция $g(z) = a^{-1} \log \mathcal{B}_\lambda(az)$. Представление для функции g в виде ряда следует из равенства (3.14). Разложение в ряд функции $A(u)$ вычислено в лемме 3.4.

2. Согласно формуле (3.11) обратной к функции $b(u) = u\mathcal{B}_\lambda^\lambda(au)$ является функция (3.24). Проверим непосредственно, что функция $\bar{b}(t) = t(1+at)^{-\lambda}$, зависящая от свободных параметров a и λ , задает сильный изоморфизм мультипликативной формальной группы с формальной группой вида $\mathcal{F}_4$ над кольцом $\mathbb{Q}[a, \eta]$. Действительно,

$$\bar{b}(t_1 + t_2 + at_1t_2) = \bar{b}(t_1) \cdot \frac{\bar{b}(t_2)}{t_2} + \bar{b}(t_2) \cdot \frac{\bar{b}(t_1)}{t_1} + a\bar{b}(t_1)\bar{b}(t_2).$$

Следовательно,

$$F(u, v) = \bar{b}(b(u) + b(v) + ab(u)b(v)) = uH(v) + vH(u) + auv,$$

где

$$H(x) = (1 + ab(x))^{-\lambda} = \frac{x}{b(x)} = \mathcal{B}_\lambda^{-\lambda}(ax).$$

Вид полиномов $p_k(a, \eta)$ следует из формулы (3.15).

Теорема доказана.

ЗАМЕЧАНИЕ 3.8. Другой способ нахождения полиномов α_n , основанный на использовании многочленов Гульда, см. в [31]. Формулы для вычисления коэффициентов рядов (3.17) и (3.23) получены также в работе М. Бакурадзе [24] без использования обобщенных биномиальных рядов Ламберта.

ЗАМЕЧАНИЕ 3.9. В случае, когда $\alpha = 0$,

$$b(u) = u(\sqrt{1 + \beta u^2} - \sqrt{\beta}u), \quad \bar{b}(u) = u(1 - 2\sqrt{\beta}u)^{-1/2},$$

$$F(u, v) = uv \left(\frac{1}{b(u)} + \frac{1}{b(v)} - 2\sqrt{\beta} \right).$$

Если $\eta = 0$, то $b(u) = \bar{b}(u) = u$; если $\beta = 0$, то, как и в случае аддитивного закона, приходим к функциям

$$\bar{b}(u) = ue^{\alpha u}, \quad b(u) = \frac{W(\alpha u)}{\alpha},$$

$$F(u, v) = ue^{W(\alpha v)} + ve^{W(\alpha u)} = \alpha uv \left(\frac{1}{W(\alpha u)} + \frac{1}{W(\alpha v)} \right),$$

где $W(z)$ – функция Ламберта (3.9).

3.3. Формальная группа $\mathcal{F}_5$. Рассмотрим эллиптическую кривую в стандартной модели Вейерштрасса

$$\{(x, y) \in \mathbb{C}^2 : y^2 = 4x^3 - g_2x - g_3\}. \quad (3.25)$$

По этой кривой строится σ -функция Вейерштрасса $\sigma(z)$ и функции Вейерштрасса

$$\zeta(z) = \frac{d}{dz} \log \sigma(z), \quad \wp(z) = -\frac{d}{dz} \zeta(z).$$

По построению $\zeta(z) - 1/z$ – регулярная функция при $z = 0$. Обозначим через $\Phi_s(t)$ функцию Бейкера–Ахиезера

$$\Phi_s(t) = \frac{\sigma(s-t)}{\sigma(t)\sigma(s)} e^{\zeta(s)t} \quad (3.26)$$

эллиптической кривой (3.25). В окрестности точки $t = 0$ имеет место разложение

$$\begin{aligned} \Phi_s(t) = & \frac{1}{t} - \frac{1}{2}\wp(s)t - \frac{1}{6}\wp'(s)t^2 + \left(\frac{1}{40}g_2 - \frac{1}{8}\wp(s)^2 \right)t^3 + \frac{1}{60}\wp(s)\wp'(s)t^4 \\ & + \frac{1}{7!}(6g_3 - 21g_2\wp(s) + 21\wp(s)^3 - 14\wp'(s)^2)t^5 + \dots \end{aligned}$$

ЛЕММА 3.10 (см. [23]). *Справедливо тождество*

$$\Phi(t_1 + t_2) = \frac{\Phi(t_1)\Phi'(t_2) - \Phi'(t_1)\Phi(t_2)}{\wp(t_1) - \wp(t_2)}.$$

ПРЕДЛОЖЕНИЕ 3.11. *Имеет место изоморфизм $\mathcal{R}_5 \otimes \mathbb{Q} \cong \mathbb{Q}[\alpha_1, \beta_2, \alpha_3, \beta_4]$, где $\alpha_1, \beta_2, \beta_3, \beta_4$ – коэффициенты рядов $A(x)$ и $B(x)$ из формулы (2.13). Сильный изоморфизм аддитивной формальной группы $\mathcal{F}_0$ в формальную группу $\mathcal{F}_5$ реализуется над кольцом $\mathbb{Q}[\gamma_1, \gamma_2, \gamma_3, \gamma_4]$ и задается экспонентой*

$$f_s(t) = \frac{e^{\alpha t}}{\Phi_s(t)} \in \mathbb{Q}[\gamma_1, \gamma_2, \gamma_3, \gamma_4], \quad (3.27)$$

где $\Phi_s(t)$ – функция Бейкера–Ахиезера (3.26),

$$\gamma_1 = \alpha, \quad \gamma_2 = \wp(s), \quad \gamma_3 = \wp'(s), \quad \gamma_4 = \frac{g_2}{2}. \quad (3.28)$$

Вложение $\widehat{\mathcal{R}}_5 \subset \mathbb{Q}[\gamma_1, \gamma_2, \gamma_3, \gamma_4]$, где $\widehat{\mathcal{R}}_5 = \mathcal{R}_5/(2\text{-torsion})$, задается выражениями для коэффициентов рядов

$$A(u) = u^2\wp(g(u)), \quad B(u) = -u^2\Phi'(g(u))e^{-\alpha g(u)} \quad (3.29)$$

в виде полиномов от $\gamma_1, \gamma_2, \gamma_3, \gamma_4$.

ДОКАЗАТЕЛЬСТВО. Покажем, что коэффициенты ряда

$$\omega(u) = \frac{\partial \mathcal{F}_5(u, v)}{\partial v} \Big|_{v=0}$$

принадлежат кольцу $\mathbb{Q}[\gamma_1, \gamma_2, \gamma_3, \gamma_4]$; см. (3.28). Введем ряд $\varphi_s(t)$ при помощи формулы

$$\frac{1}{\Phi_s(t)} = \sigma(t)e^{\varphi_s(t)}.$$

Тогда

$$\varphi_s(t) = \log \sigma(s) - \log \sigma(s-t) - t\zeta(s).$$

Раскладывая функцию $\log \sigma(s-t)$ в ряд Тэйлора по t , получаем

$$\varphi_s(t) = \sum_{k=2}^{\infty} (-1)^k \left(-\frac{d^k}{ds^k} \log \sigma(s) \right) \frac{t^k}{k!} = \sum_{k=1}^{\infty} (-1)^{k-1} \wp^{(k-1)}(s) \frac{t^{k+1}}{(k+1)!}.$$

Покажем, что для каждого $k \geq 2$ функция $\wp^{(k)}(s)$ является полиномом от γ_2 , γ_3 , γ_4 . Воспользуемся теоремой Вейерштрасса об униформизации эллиптической кривой (3.25)

$$(\wp'(s))^2 = 4\wp^3(s) - g_2\wp(s) - g_3. \quad (3.30)$$

Дифференцируя (3.30) и сокращая общий множитель, получаем

$$\wp''(s) = 6\wp^2(s) - \frac{g_2}{2}. \quad (3.31)$$

Покажем, что $\wp^{(k)}(s) = \wp_k(\gamma_2, \gamma_3, \gamma_4)$, где $\wp_k$ – полиномы с целыми коэффициентами. При сделанных предположениях $\wp_0 = \gamma_2$, $\wp_1 = \gamma_3$, $\wp_2 = 6\gamma_2^2 - \gamma_4$. Остальные полиномы $\wp_k(\gamma_2, \gamma_3, \gamma_4)$ однозначно определяются рекурсией:

$$\wp_{k+1} = \gamma_3 \frac{\partial}{\partial \gamma_2} \wp_k + (6\gamma_2^2 - \gamma_4) \frac{\partial}{\partial \gamma_3} \wp_k, \quad k \geq 0. \quad (3.32)$$

Таким образом,

$$\varphi_s(t) \in \mathbb{Q}[\gamma_2, \gamma_3, \gamma_4][[t]].$$

Имеется классическая формула, задающая функцию $\sigma(t)$ в виде ряда:

$$\sigma(t) = t \sum_{i,j \geq 0} \frac{n_{i,j}}{(4i + 6j + 1)!} \left(\frac{g_2 t^4}{2} \right)^i (2g_3 t^6)^j,$$

где $n_{i,j}$ – целые числа. Из (3.30) следует, что $g_3 = 4\gamma_2^3 - 2\gamma_2\gamma_4 - \gamma_3^2$. Следовательно,

$$\sigma(t) \in \mathbb{Q}[\gamma_2, \gamma_3, \gamma_4][[t]].$$

Таким образом, мы показали, что

$$f_s(t) \in \mathbb{Q}[\gamma_1, \gamma_2, \gamma_3, \gamma_4][[t]].$$

По формуле сложения для функции Бейкера–Ахиезера (см. лемму 3.10)

$$f(t_1 + t_2) = \frac{\wp(t_1) - \wp(t_2)}{\Phi'(t_2)/(f(t_1)e^{\alpha t_2}) - \Phi'(t_1)/(f(t_2)e^{\alpha t_1})}. \quad (3.33)$$

Подставляя в это равенство $t_1 = g(u)$, $t_2 = g(v)$, где $g(u) = \bar{f}(u)$, находим, что

$$F(u, v) = \frac{u^2 \tilde{A}(v) - v^2 \tilde{A}(u)}{u \tilde{B}(v) - v \tilde{B}(u)}, \quad (3.34)$$

где $\tilde{A}(u) = u^2 \wp(g(u))$ и $\tilde{B}(u) = -u^2 \Phi'(g(u))e^{-\alpha g(u)}$ – регулярные в точке $u = 0$ функции, причем $\tilde{A}(0) = \tilde{B}(0) = 1$. Из этих равенств следует, что коэффициенты рядов (3.29) являются полиномами от γ_1 , γ_2 , γ_3 , γ_4 .

Рассмотрим гомоморфизм H из $\mathcal{R}_5$ в кольцо $\mathbb{Q}[\gamma_1, \gamma_2, \gamma_3, \gamma_4]$, классифицирующий формальную группу (3.34). Этот гомоморфизм переводит ряды $A(u)$ и $B(u)$ в ряды $\tilde{A}(u)$ и $\tilde{B}(u)$ и тем самым позволяет выразить коэффициенты рядов $A(u)$ и $B(u)$ в виде полиномов от γ_1 , γ_2 , γ_3 , γ_4 .

3.4. Формальная группа $\mathcal{F}_6$. Для произвольного ряда вида (2.1) через $N(x, y, z)$ будем обозначать формальный степенной ряд

$$N(x, y, z) = F(F(x, y), z) - F(x, F(y, z)), \quad (3.35)$$

который для формального группового закона должен быть тождественным нулем.

ПРЕДЛОЖЕНИЕ 3.12. *Имеет место изоморфизм $\mathcal{R}_6 \otimes \mathbb{Q} \cong \mathbb{Q}[\beta_1, \beta_2]$, где β_1, β_2 – коэффициенты ряда $B(x)$ из формулы (2.14).*

ДОКАЗАТЕЛЬСТВО. Из равенства

$$0 = [yz]N(x, y, z) = \frac{B(x)}{x}(x(B'(x) + \beta_1) + 2 - 2B(x))$$

следует, что ряд $B(x)$ удовлетворяет дифференциальному уравнению

$$x(B'(x) + \beta_1) + 2 - B(x) = 0.$$

Общее решение этого уравнения имеет вид

$$B(x) = 1 + \beta_1 x + \beta_2 x^2,$$

т.е. $\mathcal{R}_6 \otimes \mathbb{Q} \cong \mathbb{Q}[\beta_1, \beta_2]$, и над полем $\mathbb{Q}$ группа $\mathcal{F}_6$ изоморфна группе $\mathcal{F}_2$.

§ 4. Кольцо коэффициентов $\mathcal{R}_U$

Фундаментальным является следующий результат из теории формальных групп.

ТЕОРЕМА 4.1 (М. Лазар). *Кольцо $\mathcal{R}_U$ изоморфно кольцу $\mathbb{Z}[y_1, y_2, \dots]$.*

Доказательство теоремы Лазара можно найти как в его оригинальной статье [5], так и во многих монографиях и курсах лекций по теории формальных групп и ее приложениям (см. [13], [14], [32]–[34]). Ниже будет приведено доказательство теоремы Лазара методом, который дальше будет неоднократно использоваться при вычислении колец коэффициентов универсальных формальных групп.

Пусть $n \geq 2$ и целые числа $\lambda_1, \dots, \lambda_{n-1}$ выбраны так, что

$$\frac{\lambda_1}{d(n)} \binom{n}{1} + \dots + \frac{\lambda_{n-1}}{d(n)} \binom{n}{n-1} = 1. \quad (4.1)$$

Рассмотрим в $\mathbb{R}^{n-1}$ подпространство размерности $[(n+1)/2]$, состоящее из векторов $(x_1, \dots, x_{n-1})$, у которых $x_i = x_{n-i}$, $1 \leq i \leq n-1$. В двойственном пространстве рассмотрим решетку Λ , порожденную линейной формой

$$\lambda(\mathbf{x}) = \lambda_1 x_1 + \dots + \lambda_{n-1} x_{n-1} \quad (4.2)$$

и всевозможными формами вида

$$P_{i,j}(\mathbf{x}) = \binom{n-i}{j} x_i - \binom{n-j}{i} x_j, \quad i, j \geq 1, \quad i+j < n. \quad (4.3)$$

Доказательство теоремы Лазара будет существенно опираться на следующее утверждение.

ЛЕММА 4.2. *Решетка Λ совпадает с решеткой Γ всех целочисленных линейных форм. Другими словами, каждая переменная x_i может быть представлена в виде линейной комбинации с целыми коэффициентами линейных форм (4.2), (4.3).*

Лемма 4.2 впервые была сформулирована и использована без доказательства в [13]. Ее доказательство появилось в книге [14]. В п. 9.2 изложено видоизмененное доказательство из [14]. Отличие от доказательства из [14] заключается в отсутствии индукции по параметру $\text{ord}_p(n)$. Ввиду важности этой леммы в задаче вычисления колец коэффициентов формальных групп мы приводим также и доказательство, предложенное Ф. В. Петровым (см. п. 9.2).

СЛЕДСТВИЕ 4.3. *Через линейные формы (4.3) можно выразить любую линейную комбинацию $c_1x_1 + \dots + c_{n-1}x_{n-1}$ такую, что*

$$\frac{c_1}{d(n)} \binom{n}{1} + \dots + \frac{c_{n-1}}{d(n)} \binom{n}{n-1} = 0.$$

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 4.1. Рассмотрим кольцевой гомоморфизм $i: \mathbb{Z}[y_1, \dots, y_n, \dots] \rightarrow \mathcal{R}_U$ такой, что $y_n \rightarrow e_n$, где e_n задается формулой (2.18). Приравнявая к нулю коэффициент при $u^i v^j w^k$ в уравнении ассоциативности (2.2), получаем, что в кольце $\mathcal{R}_U$ выполняются соотношения

$$\binom{i+j}{j} \alpha_{i+j,k} \equiv \binom{j+k}{j} \alpha_{i,j+k} \pmod{I^2}, \quad i+j+k = n+1. \quad (4.4)$$

Согласно следствию 4.3

$$\alpha_{i,j} - \binom{n+1}{i} \frac{e_n}{d(n+1)} \equiv 0 \pmod{I^2}, \quad i+j = n+1. \quad (4.5)$$

Из формулы (4.5) получаем, что гомоморфизм i является эпиморфизмом. Для завершения доказательства остается проверить, что i является мономорфизмом.

Рассмотрим кольцевой гомоморфизм $i_1: \mathbb{Z}[x_1, \dots, x_n, \dots] \rightarrow \mathcal{R}_U$ такой, что $x_n \rightarrow \alpha_{n,1}$. Как отмечалось выше, над кольцом $\mathcal{R}_U \otimes \mathbb{Q}$ формальный ряд $\mathcal{F}_U(u, v)$ можно записать в виде

$$\mathcal{F}_U(u, v) = \bar{g}(g(u) + g(v)) \in \mathbb{Q}[g_1, \dots, g_n, \dots][[u, v]], \quad (4.6)$$

где

$$g(u) = u + g_1 u^2 + \dots + g_n u^{n+1} + \dots$$

– логарифм формальной группы $\mathcal{F}_U(u, v)$. Согласно равенству (2.8)

$$\alpha_{n,1} \equiv -(n+1)g_n \pmod{I^2}.$$

Поэтому при композиции

$$\mathbb{Z}[x_1, \dots, x_n, \dots] \rightarrow \mathcal{R}_U \rightarrow \mathcal{R}_U \otimes \mathbb{Q},$$

где $\mathcal{R}_U \rightarrow \mathcal{R}_U \otimes \mathbb{Q}$ – канонический гомоморфизм ($a \rightarrow a \otimes 1$), элементы x_n переходят в мультипликативные образующие кольца $\mathbb{Q}[g_1, \dots, g_n, \dots]$ и, следовательно, гомоморфизм i_1 является мономорфизмом.

С другой стороны, можно построить гомоморфизм

$$i_2: \mathbb{Z}[x_1, \dots, x_n, \dots] \rightarrow \mathbb{Z}[y_1, \dots, y_n, \dots]$$

такой, что композиция $i \circ i_2$ совпадает с i_1 . Так как i – эпиморфизм, то можно положить $i_2(x_n) = P_n(y_1, \dots, y_n)$, где $P_n(y_1, \dots, y_n)$ – такой полином, что $\alpha_{n,1} = P_n(e_1, \dots, e_n) = i(P_n(y_1, \dots, y_n))$. Поскольку $i_2 \otimes \mathbb{Q}$, $i_1 \otimes \mathbb{Q}$ являются изоморфизмами и $i \circ i_2 = i_1$, получаем, что i – мономорфизм.

Теорема 4.1 доказана.

ЗАМЕЧАНИЕ 4.4. Из доказательства теоремы 4.1 следует, что в качестве мультипликативного образующего элемента e_n кольца $\mathcal{R}_U$ можно брать любой элемент вида (2.18), или, что то же самое (см. следствие 4.3), любой элемент e_n , удовлетворяющий соотношениям (4.5). В частности, это означает, что для порождающих групповых законов определение функции ρ не зависит от выбора коэффициентов в разложении (2.18). В качестве мультипликативных образующих выступают в точности те элементы e_n , для которых $\rho(n) > 1$.

Теорема 4.1 позволяет усилить лемму 2.1. Так как согласно теореме 4.1 кольцо $\mathcal{R}_U$ не имеет кручения, то каноническое отображение $\mathcal{R}_U \rightarrow \mathcal{R}_U \otimes \mathbb{Q}$ является вложением. Это вложение разлагается в композицию $\mathcal{R}_U \subset \mathcal{B}_U = \mathbb{Z}[g_1, g_2, \dots] \subset \mathcal{R}_U \otimes \mathbb{Q}$. По построению над кольцом $\mathcal{B}_U$ формальная группа $\mathcal{F}_U(u, v)$ линейаризуется.

СЛЕДСТВИЕ 4.5. *Формальная группа $F(u, v) \in R[[u, v]]$ линейаризуется над кольцом R тогда и только тогда, когда классифицирующий ее гомоморфизм $\mathcal{R}_U \rightarrow R$ продолжается до гомоморфизма $\mathcal{B}_U \rightarrow R$.*

Приложения этого следствия используют выбор мультипликативных образующих e_n , $n = 1, 2, \dots$, кольца $\mathcal{R}_U$ и выражение их в виде однородных полиномов с целыми коэффициентами от $g_1, g_2, \dots, g_n, \dots$.

Приведем выражения для мультипликативных образующих e_n , $n = 1, \dots, 7$, построенных по формуле

$$e_n = \sum_{i=1}^n \lambda_i \alpha_{i,j},$$

где $\alpha_{i,j} = \alpha_{i,j}(g_1, \dots, g_{i+j-1})$ – коэффициенты ряда (4.6), а числа λ_i выбраны в соответствии с алгоритмом из предложения 9.4 (см. п. 9.2):

$$\begin{aligned} e_1 &= -2g_1; & e_2 &= 4g_1^2 - 3g_2; & e_3 &= -2(6g_1^3 - 6g_1g_2 + g_3); \\ e_4 &= 16g_1^4 - 36g_1^2g_2 + 16g_1g_3 + 9g_2^2 - 5g_4; \\ e_5 &= 144g_1^5 - 284g_1^3g_2 + 72g_1^2g_3 + 99g_1g_2^2 - 10g_1g_4 - 18g_2g_3 - g_5; \\ e_6 &= 64g_1^6 - 240g_1^4g_2 + 128g_1^3g_3 + 216g_1^2g_2^2 - 60g_1^2g_4 \\ &\quad - 144g_1g_2g_3 + 24g_1g_5 - 27g_2^3 + 16g_2^2g_3 + 30g_2g_4 - 7g_6; \\ e_7 &= 2(4584g_1^7 - 15528g_1^5g_2 + 6032g_1^4g_3 + 14100g_1^3g_2^2 - 1980g_1^3g_4 \\ &\quad - 7380g_1^2g_2g_3 + 516g_1^2g_5 - 2943g_1g_2^3 + 706g_1g_2^2g_3 \\ &\quad + 1350g_1g_2g_4 - 84g_1g_6 + 882g_2^2g_3 - 130g_3g_4 - 123g_2g_5 - g_7). \end{aligned}$$

ЗАМЕЧАНИЕ 4.6. В алгебраической топологии коэффициенты полиномов $e_n = P(g_1, \dots, g_n)$ представляют собой числа Чженя комплексных многообразий, класс кобордизмов которых равен e_n в реализации универсальной формальной группы как формальной группы геометрических кобордизмов.

§ 5. Кольцо коэффициентов $\mathcal{R}_4$

В статье [15] формальные группы вида (2.12) были названы *формальными группами Абеля*, чтобы подчеркнуть значение работы [1].

ТЕОРЕМА 5.1 (В. М. Бухштабер, А. Н. Холодов). *Кольцо $\mathcal{R}_4$ мультипликативно порождено элементами $\alpha_{p^r} = H_4(e_{p^r})$, где p пробегает множество всех простых чисел и $r \geq 0$. При этом*

$$\rho_4(n) = \begin{cases} \infty, & \text{если } n = 1, 2, \\ p, & \text{если } n = p^r \quad (r \geq 2, \text{ если } p = 2, \text{ и } r \geq 1, \text{ если иначе}), \\ 1 & \text{в остальных случаях.} \end{cases}$$

Кольцо $\mathcal{R}_4$ не содержит элементов конечного порядка.

Докажем утверждения из теоремы 5.1 по схеме, которая в дальнейшем будет использоваться при исследовании колец коэффициентов формальных групп $\mathcal{F}_3$, $\mathcal{F}_5$ и $\mathcal{F}_6$.

ПРЕДЛОЖЕНИЕ 5.2. *Кольцо $\mathcal{R}_4$ мультипликативно порождено элементами $\alpha_{p^r} = H_4(e_{p^r})$, где p пробегает множество всех простых чисел и $r \geq 0$.*

ДОКАЗАТЕЛЬСТВО. Кольцо $\mathcal{R}_4$ мультипликативно порождается элементами $H_4(e_n)$ (см. следствие 2.10). При этом

$$H_4(\alpha_{n,1}) = \alpha_n, \quad H_4(\alpha_{i,j}) = 0, \quad \min \{i, j\} > 1.$$

Если $n \neq p^r$, то коэффициент α_n можно выразить через коэффициенты с меньшими номерами, поскольку из формулы (4.5) и следствия 9.8 (см. п. 9.3) вытекает, что $H_4(e_n) \equiv 0 \pmod{I^2}$. Значит, в качестве образующих достаточно брать лишь коэффициенты вида α_{p^r} .

ЛЕММА 5.3. *Пусть $p > 2$ – простое число. Тогда в кольце $\mathcal{R}_4$ имеет место соотношение*

$$\gamma_3 \alpha_1 \alpha_2^{(p-1)/2} = Q_1(\alpha_1, \alpha_2) + p Q_2(\alpha_1, \dots, \alpha_p), \quad (5.1)$$

где γ_3 взаимно просто с p и степень полинома Q_1 по переменной α_2 не превосходит $(p-3)/2$.

ДОКАЗАТЕЛЬСТВО. Полагая $n = p$ в формуле (3.5), приходим к сравнению $\alpha_1 \alpha_{p-1} \equiv 0 \pmod{p}$. Подставим в него выражение для α_{p-1} , полученное по формуле (3.21), и воспользуемся замечанием 3.6:

$$\frac{2\alpha_1 \alpha_2}{(p-1) \cdot (p-3)!} \prod_{i=1}^{(p-3)/2} \left(\frac{(2n-1)^2 - (2i-1)^2}{4} \alpha_1^2 + 2(2i-1)^2 \alpha_2 \right) \equiv 0 \pmod{p}.$$

Утверждение леммы следует из того, что в полученном выражении коэффициент при $\alpha_1 \alpha_2^{(p-1)/2}$ не сравним с нулем по модулю p .

ЛЕММА 5.4. Пусть $p \geq 2$ – простое число. Тогда в кольце $\mathcal{A}_4$ мультипликативные образующие α_{p^r} связаны соотношением

$$\gamma_2(r) \alpha_{p^r}^p = \gamma_1(r) p \alpha_{p^{r+1}} + P_{p,r}(\alpha_1, \alpha_2, \alpha_p, \dots, \alpha_{p^r}), \quad (5.2)$$

где $r \geq 1$, $\gamma_1(r)$, $\gamma_2(r)$ – целые числа, $(\gamma_2(p), p) = 1$ и степень полинома $P_{p,r}$ по переменной α_{p^r} меньше p .

ДОКАЗАТЕЛЬСТВО. Пусть $p = 2$. Тогда согласно (3.6)

$$\alpha_{2^r}^2 = \binom{2^{r+1}}{2^r} \alpha_{2^{r+1}} + \sum_{2 \leq k < 2^{r+1}} \alpha_k [F^k]_{2^r, 2^r}. \quad (5.3)$$

В этом случае необходимо проверить, что коэффициенты при $\alpha_{2^{r+1}}$ и $\alpha_{2^r}^2$ в правой части равенства (5.3) сравнимы с нулем по модулю 2. Действительно, по теореме Куммера 9.2 (см. п. 9.1) выполняется сравнение $\binom{2^{r+1}}{2^r} \equiv 0 \pmod{2}$. Коэффициент при $\alpha_{2^r}^2$ равен коэффициенту при α_{2^r} в выражении $[F^{2^r}]_{2^r, 2^r}$. Проверим, что он сравним с нулем по модулю 2:

$$\begin{aligned} [(u + v + \alpha_{2^r} uv^{2^r} + vu^{2^r})^{2^r}]_{2^r, 2^r} &\equiv [(u + \alpha_{2^r} uv^{2^r})^{2^r} + (v + \alpha_{2^r} vu^{2^r})^{2^r}]_{2^r, 2^r} \\ &= 2[(u + \alpha_{2^r} uv^{2^r})^{2^r}]_{2^r, 2^r} \equiv 0 \pmod{2}. \end{aligned}$$

Пусть $p > 2$. Применяя $p-1$ раз формулу (3.7), находим, что

$$\alpha_{p^r}^p = \sum_{k_1, \dots, k_{p-1} \geq 2} [F^{k_1}]_{p^r, p^r} [F^{k_2}]_{k_1, p^r} \dots [F^{k_{p-1}}]_{k_{p-2}, p^r} \alpha_{k_{p-1}}. \quad (5.4)$$

Слагаемое $\alpha_{p^{r+1}}$ в формуле (5.4) возникает при $k_{p-1} = p^{r+1}$. Коэффициент при этом слагаемом имеет вид

$$\sum_{k_1, \dots, k_{p-1} \geq 2} [(u + v)^{k_1}]_{p^r, p^r} [(u + v)^{k_2}]_{k_1, p^r} \dots [(u + v)^{k_{p-1}}]_{k_{p-2}, p^r}.$$

Значения параметров $k_{p-2}, \dots, k_1$ и соответствующие сомножители вычисляются последовательно:

$$\begin{aligned} [(u + v)^{k_{p-1}}]_{k_{p-2}, p^r} &= [(u + v)^{p^{r+1}}]_{p^{r+1}-p^r, p^r} = \binom{p^{r+1}}{p^r}, \\ [(u + v)^{k_{p-2}}]_{k_{p-3}, p^r} &= [(u + v)^{p^{r+1}}]_{p^{r+1}-2p^r, p^r} = \binom{p^{r+1}-p^r}{p^r}, \\ &\dots \dots \dots \\ [(u + v)^{k_2}]_{k_1, p^r} &= [(u + v)^{p^{r+1}}]_{p^{r+1}-(p-2)p^r, p^r} = \binom{2p^r}{p^r}. \end{aligned}$$

Таким образом, коэффициент при $\alpha_{p^{r+1}}$ равен

$$\binom{p^{r+1}}{p^r} \binom{p^{r+1}-p^r}{p^r} \dots \binom{2p^r}{p^r}.$$

Согласно лемме 9.1 и теореме 9.2 этот коэффициент делится на p , но не делится на p^2 .

Коэффициент при $\alpha_{p^r}^p$ в правой части равенства (5.4) равен коэффициенту при $\alpha_{p^r}^{p-1}$ в выражении

$$\sum_{k_1, \dots, k_{p-1} \geq 2} [F^{k_1}]_{p^r, p^r} [F^{k_2}]_{k_1, p^r} \cdots [F^{p^r}]_{k_{p-2}, p^r}.$$

Для его вычисления можно предположить, что все элементы α_n , отличные от α_{p^r} , равны нулю. Тогда для завершения доказательства леммы остается проверить, что $[F^{p^r}]_{k_{p-2}, p^r} \equiv 0 \pmod{p, \alpha_{p^r}^p}$:

$$\begin{aligned} [(u + v + \alpha_{p^r}(uv^{p^r} + vu^{p^r}))^{p^r}]_{k_{p-2}, p^r} &\equiv [(u + \alpha_{p^r}uv^{p^r})^{p^r} + (v + \alpha_{p^r}vu^{p^r})^{p^r}]_{k_{p-2}, p^r} \\ &= [v^{p^r}(1 + \alpha_{p^r}u)^{p^r}]_{k_{p-2}, p^r} \equiv 0 \pmod{p, \alpha_{p^r}^p}. \end{aligned}$$

ПРЕДЛОЖЕНИЕ 5.5. *Кольцо $\mathcal{R}_4$ не имеет кручения.*

ДОКАЗАТЕЛЬСТВО. Согласно лемме 5.4 кольцо $\mathcal{R}_4 \otimes \mathbb{F}_2$ аддитивно порождено мономами

$$\alpha_1^n \alpha_2^{i_1} \cdots \alpha_2^{i_k}, \quad 0 < i_1 < \cdots < i_k. \quad (5.5)$$

Из леммы 3.4 следует, что группа $\mathcal{R}_4^{-2m} \otimes \mathbb{Q}$ порождена мономами

$$\alpha_1^m, \alpha_1^{m-2} \alpha_2, \alpha_1^{m-4} \alpha_2^2, \dots$$

и поэтому ее ранг равен $[m/2] + 1$. Значит, в группе $\mathcal{R}_4^{-2m} \otimes \mathbb{F}_2$ число образующих не меньше, чем $[m/2] + 1$. С другой стороны, число различных мономов вида (5.5), через которые выражаются все элементы группы $\mathcal{R}_4^{-2m} \otimes \mathbb{F}_2$, такое же. Таким образом, векторное пространство $\mathcal{R}_4^{-2m} \otimes \mathbb{Q}$ над полем $\mathbb{Q}$ и векторное пространство $\mathcal{R}_4^{-2m} \otimes \mathbb{F}_2$ над полем $\mathbb{F}_2$ имеют одинаковые размерности. Поэтому $\mathcal{R}_4$ не может иметь 2-кручения, так как подгруппа $\mathcal{R}_4^{(2\text{-torsion})}$ (подгруппа элементов второго порядка) дает вклад в $\mathcal{R}_4^{-2m} \otimes \mathbb{F}_2$ и не дает вклада в $\mathcal{R}_4^{-2m} \otimes \mathbb{Q}$.

Пусть $p > 2$ – простое число. Тогда по леммам 5.3 и 5.4 кольцо $\mathcal{R}_4 \otimes \mathbb{F}_p$ аддитивно порождено мономами

$$\begin{aligned} \alpha_1^n \alpha_{p^{i_1}}^{j_1} \cdots \alpha_{p^{i_k}}^{j_k}, \quad \alpha_1^n \alpha_2 \alpha_{p^{i_1}}^{j_1} \cdots \alpha_{p^{i_k}}^{j_k}, \quad \dots, \\ \alpha_1^n \alpha_2^{(p-3)/2} \alpha_{p^{i_1}}^{j_1} \cdots \alpha_{p^{i_k}}^{j_k}, \quad \alpha_2^n \alpha_{p^{i_1}}^{j_1} \cdots \alpha_{p^{i_k}}^{j_k}, \end{aligned} \quad (5.6)$$

где $n \geq 0$, $0 < i_1 < \cdots < i_k$, $0 \leq j_1, \dots, j_k < p$ (всевозможные мономы, не делящиеся на $\alpha_1 \alpha_2^{(p-1)/2}$). Как отмечалось выше, ранг группы $\mathcal{R}_4^{-2m} \otimes \mathbb{Q}$ равен $[m/2] + 1$. Число различных мономов вида (5.6), принадлежащих группе $\mathcal{R}_4^{-2m} \otimes \mathbb{F}_p$, такое же, что следует из равенства соответствующих производящих функций:

$$\frac{1}{(1-x)(1-x^2)} = \frac{1}{(1-x)(1-x^2)(1-x^p)} - \frac{x^{1+2(p-1)/2}}{(1-x)(1-x^2)(1-x^p)}.$$

Следовательно, кольцо $\mathcal{R}_4$ не может иметь p -кручения.

Таким образом, теорема 5.1, разбитая на предложения 5.2 и 5.5, полностью доказана.

Следующая теорема дает описание идеала $\ker H_4$ в терминах образующих кольца $\mathcal{R}_4$, завершая тем самым описание этого кольца.

ТЕОРЕМА 5.6. *Для кольца коэффициентов $\mathcal{R}_4$ универсальной формальной группы $\mathcal{F}_4$ имеет место изоморфизм градуированных колец $\mathcal{R}_4 \cong \mathbb{Z}[\alpha_{p^r}]/I_4$, где p пробегает множество всех простых чисел, $r \geq 0$ ($r \geq 1$ при $p = 2$), а идеал I_4 порожден однородными соотношениями (5.1) и (5.2).*

ДОКАЗАТЕЛЬСТВО. Обозначим через $\widehat{\mathcal{R}}_4$ кольцо $\mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_{p^r}, \dots]/I$, где I – идеал, порожденный однородными соотношениями (5.1) и (5.2). По построению имеет место эпиморфизм $j: \widehat{\mathcal{R}}_4 \rightarrow \mathcal{R}_4$. Согласно предложению 5.5 кольцо $\mathcal{R}_4$ не имеет кручения. При этом доказательство отсутствия кручения использует только соотношения (5.1) и (5.2). Поэтому кольцо $\widehat{\mathcal{R}}_4$ тоже не имеет кручения и гомоморфизм j является изоморфизмом. Это следует из того, что эпиморфизм j колец без кручения является изоморфизмом тогда и только тогда, когда изоморфизмом является гомоморфизм $j \otimes \mathbb{Q}$.

§ 6. Структура кольца $\mathcal{R}_5$

Формальная группа $\mathcal{F}_5(u, v)$ (см. (2.13)) в статье [24] была названа формальной группой Бухштабера, так как впервые она была введена в работе [15]. Частные нетривиальные результаты о кольце $\mathcal{R}_5$ были получены в работах [15], [12], [24]: в [15] было вычислено кольцо $\mathcal{R}_5 \otimes \mathbb{Q}$ и найдена экспонента группы $\mathcal{F}_5$; в [12] показано, что в кольце $\mathcal{R}_5$ имеются элементы порядка 2 и первый такой элемент имеет размерность 12; в [24] дано выражение начального отрезка ряда $\mathcal{F}_5(u, v)$ в виде полиномов от коэффициентов логарифма этой группы.

ТЕОРЕМА 6.1. *Кольцо $\mathcal{R}_5$ мультипликативно порождено элементами $H_5(e_n)$, где $n = 1, 2, 3, 4$ и $n = p^r$ ($r \geq 1$, p пробегает все простые числа), а также $n = 2^k - 2$ и $k > 2$. При этом*

$$\rho_5(n) = \begin{cases} \infty, & \text{если } n = 1, 2, 3, 4, \\ p, & \text{если } n = p^r, \quad n \neq 2, 3, 4, \quad r \geq 1, \\ 2, & \text{если } n = 2^k - 2, \quad k \geq 3, \\ 1 & \text{в остальных случаях.} \end{cases} \quad (6.1)$$

Кольцо $\mathcal{R}_5$ имеет кручение только второго порядка. В кольце $\mathcal{R}_U$ существуют мультипликативные образующие e_{2^k-2} , $k > 2$, такие, что $H_5(e_{2^k-2})$ порождают в $\mathcal{R}_5$ идеал элементов порядка 2.

ЛЕММА 6.2. *Пусть $p \geq 2$ – простое число. Тогда в кольце $\mathcal{R}_5$ мультипликативные образующие β_{p^r} связаны соотношением*

$$\gamma_2(r)\beta_{p^r}^p = \gamma_1(r)p\beta_{p^{r+1}} + P_{p,r}(\alpha_1, \beta_2, \alpha_3, \beta_4, \beta_p, \dots, \beta_{p^r}), \quad (6.2)$$

где $r \geq 1$ ($r \geq 2$ при $p = 2$), $\gamma_1(r)$ и $\gamma_2(r)$ – целые числа, $(\gamma_2(r), p) = 1$ и степень полинома $P_{p,r}$ по переменной β_{p^r} меньше p .

ДОКАЗАТЕЛЬСТВО. Рассмотрим сначала случай, когда $p > 2$. Обозначим через J идеал в кольце $\mathcal{R}_5 \otimes \mathbb{Z}_p$, порожденный всеми элементами, номера которых не превосходят p^r :

$$J = \mathbb{Z}_p[\alpha_1, \beta_2, \alpha_3, \beta_4, \beta_p, \dots, \beta_{p^{r-1}}]. \quad (6.3)$$

Для проверки утверждения леммы достаточно найти соотношение, которое приводится к виду

$$\gamma_2(r)\beta_{p^r}^p \equiv \gamma_1(r)p\beta_{p^{r+1}} \pmod{J, p^2}. \quad (6.4)$$

Из формулы (6.14) следует, что в кольце $\mathbb{Z}[1/2]$ выполняется равенство

$$A(x) = B(x)^2 + \alpha_1 x B(x) - \beta_2 x^2 - \frac{x B'(x)}{2} (B(x) + \alpha_1 x).$$

Поэтому

$$A(x) \equiv B(x)^2 - \frac{x}{2} B(x) B'(x) \pmod{J}. \quad (6.5)$$

Проверим, что для ряда

$$B(x) = 1 + \beta_{p^r} x^{p^r} + \beta_{2p^r} x^{2p^r} + \dots \quad (6.6)$$

всегда выполняется сравнение

$$B'(x) \equiv 0 \pmod{J, p^2}. \quad (6.7)$$

Оно очевидно при $r \geq 2$. Если же $r = 1$, то начальные коэффициенты ряда

$$B(x) = 1 + \beta_p x^p + \beta_{2p} x^{2p} + \dots$$

являются степенями образующего элемента β_p : $\beta_{kp} \equiv \lambda_k \beta_p^k \pmod{J}$, $1 \leq k \leq p-1$. Значит,

$$\begin{aligned} B'(x) &\equiv p\lambda_1 \beta_p x^{p-1} + 2p\lambda_2 \beta_{2p} x^{2p-1} + \dots \\ &\quad + (p-1)p\lambda_{p-1} \beta_{(p-1)p} x^{(p-1)p-1} \pmod{J, p^2}. \end{aligned}$$

Таким образом, соотношение (6.7) следует из того, что $p\beta_p \equiv 0 \pmod{J}$. Из (6.5) и (6.7) получаем, что $A(x) \equiv B(x)^2 \pmod{J, p^2}$ и

$$\mathcal{F}_5(u, v) \equiv \frac{u^2 B(v)^2 - v^2 B(u)^2}{uB(v) - vB(u)} = uB(v) + vB(u) \equiv \mathcal{F}_4(u, v) \pmod{J, p^2}.$$

Поэтому соотношения (6.2) следуют из аналогичных соотношений (5.2), выполняющихся в группе Абеля.

Рассмотрим теперь случай, когда $p = 2$. Также будем доказывать, что при $q \geq 2$ выполняется сравнение (6.4), где идеал J определен равенством (6.3). Для ряда (6.6) при $q \geq 2$, очевидно, выполняется сравнение $B'(x) \equiv 0 \pmod{4}$. Из него следует, что

$$[y^2 z] N(x, y, z) \equiv \frac{B(x)}{x^2} \left(A(x) - B(x)^2 + x^2 B(x) \frac{B''(x)}{2} \right) \pmod{J, 4}, \quad (6.8)$$

где $N(x, y, z)$ определяется равенством (3.35). Проверим, что для ряда (6.6) выполняется сравнение

$$\frac{B''(x)}{2} \equiv 0 \pmod{J, 4}.$$

Действительно, при $q \geq 3$ выполняется сравнение $B''(x)/2 \equiv 0 \pmod{4}$, а при $q = 2$ нужное сравнение следует из того, что $B''(x)/2 \equiv 2\beta_4 x^2 \pmod{4}$ и $2\beta_4 \equiv 0 \pmod{J}$. Значит, приравнявая к нулю выражение (6.8), получаем, что $A(x) \equiv B(x)^2 \pmod{J, p^2}$. Следовательно, как и в случае $p > 2$, соотношение (6.2) следует из аналогичного соотношения (5.2), выполняющегося в группе Абеля.

ПРЕДЛОЖЕНИЕ 6.3. *Кольцо $\mathcal{R}_5$ мультипликативно порождено элементами $H_5(e_n)$, где $n = 1, 2, 3, 4$ и $n = p^r$ ($r > 0$, p пробегает все простые числа), а также $n = 2^k - 2$ и $k > 2$. При этом выполняется формула (6.1).*

ДОКАЗАТЕЛЬСТВО. Подставляя (2.15) в (4.5), находим, что

$$H_5(e_1) = \alpha_1, \quad (6.9)$$

$$\frac{n+1}{d(n+1)} H_5(e_n) \equiv \beta_n \pmod{I^2}, \quad n \geq 2, \quad (6.10)$$

$$\binom{n+1}{i} \frac{H_5(e_n)}{d(n+1)} \equiv 2\beta_n - \alpha_n \pmod{I^2}, \quad n \geq 3, \quad 2 \leq i \leq n-1. \quad (6.11)$$

Вычитая друг из друга уравнения системы (6.11), получаем, что

$$\begin{aligned} & \left(\binom{n+1}{3} - \binom{n+1}{2} \right) \frac{H_5(e_n)}{d(n+1)} \equiv \dots \\ & \equiv \left(\binom{n+1}{n-2} - \binom{n+1}{n-3} \right) \frac{H_5(e_n)}{d(n+1)} \equiv 0 \pmod{I^2}, \end{aligned}$$

значит,

$$\frac{D(n)}{d(n+1)} H_5(e_n) \equiv 0 \pmod{I^2}, \quad n \geq 5, \quad (6.12)$$

где

$$D(n) = \left(\binom{n}{3} - \binom{n}{1}, \binom{n}{4} - \binom{n}{2}, \dots, \binom{n}{n-1} - \binom{n}{n-3} \right), \quad n \geq 5. \quad (6.13)$$

Отсюда, в частности, следует, что кольцо $\mathcal{R}_5 \otimes \mathbb{Q}$ мультипликативно порождается элементами $H_5(e_1)$, $H_5(e_2)$, $H_5(e_3)$, $H_5(e_4)$ и, следовательно (см. (6.9), (6.10)), — элементами α_1 , β_2 , α_3 , β_4 . Если $n \neq p^r, 2^k - 2$ ($r \geq 1, k \geq 3$), то из (6.12) и теоремы 9.9 (см. п. 9.5) следует, что $H_5(e_n) \equiv 0 \pmod{I^2}$.

ПРЕДЛОЖЕНИЕ 6.4. *При $n = 2^r - 2$ ($r \geq 3$) существуют образующие e_n такие, что $2H_5(e_n) = 0$.*

ДОКАЗАТЕЛЬСТВО. При $n = 2^r - 2$ ($r \geq 3$) система (6.10), (6.11) принимает вид

$$\begin{aligned} 2H_5(e_n) &\equiv 0 \pmod{I^2}, & H_5(e_n) &\equiv \beta_n \pmod{I^2}, \\ \binom{n+1}{2} \frac{H_5(e_n)}{d(n+1)} &\equiv 2\beta_n - \alpha_n \pmod{I^2}, \end{aligned}$$

т.е.

$$\begin{aligned} 2H_5(e_n) &\equiv 0 \pmod{I^2}, & H_5(e_n) &\equiv \beta_n \pmod{I^2}, \\ H_5(e_n) &\equiv \alpha_n \pmod{I^2}. \end{aligned}$$

Следовательно, в качестве образующей $H_5(e_n)$ (см. замечание 4.4) можно брать любую комбинацию вида $\lambda_1 \alpha_n + \lambda_2 \beta_n$, где $\lambda_1 + \lambda_2 \equiv 1 \pmod{2}$.

Для формального степенного ряда $G(x, y, \dots)$ через $[x^\alpha y^\beta \dots]G(x, y, \dots)$ будем обозначать коэффициент ряда G , стоящий перед $x^\alpha y^\beta \dots$. Из равенства

$$[xy]N(x, y, z) = \frac{2}{z} (B(z)^2 - A(z)) + 2\alpha_1 B(z) - 2\beta_2 z - B'(z)(B(z) + \alpha_1 z) \quad (6.14)$$

следует, что $[xy]N(x, y, z) \equiv B'(z)(B(z) + \alpha_1 z) \pmod{2}$. Так как $B(z) + \alpha_1 z$ — обратимый ряд, то

$$B'(z) \equiv 0 \pmod{2} \quad (6.15)$$

и $\beta_3 \equiv \beta_5 \equiv \beta_7 \equiv \dots \equiv 0 \pmod{2}$. С одной стороны, из этих соотношений и равенства

$$\begin{aligned} [x^2 y]N(x, y, z) &= \frac{a_1(A(z) + zA'(z)) + B(z)A'(z)}{z} + \alpha_1 B'(z)(B(z) + \alpha_1 z) \\ &\quad + z(\alpha_1 \beta_2 + \alpha_3 + \beta_3) \end{aligned}$$

следует, что для четных n

$$[x^2 y z^n]N(x, y, z) \equiv 0 \pmod{2}.$$

С другой стороны, при $n = 2^r - 2$ по модулю разложимых элементов

$$[x^2 y z^{n-2}]N(x, y, z) = \binom{3}{1} a_{3,n-2} - \binom{n-1}{1} a_{2,n-1} = (2^r - 6)(\alpha_n - 2\beta_n).$$

Таким образом, в качестве образующего элемента можно выбрать

$$H_5(e_n) = \frac{1}{2} [x^2 y z^{n-2}]N(x, y, z) = (2^{r-1} - 3)(\alpha_n - 2\beta_n) + \dots,$$

и при этом будет выполняться равенство $2H_5(e_n) = 0$.

ПРЕДЛОЖЕНИЕ 6.5. Пусть J — идеал в кольце $\mathcal{R}_5$, порожденный элементами второго порядка $H_5(e_{2^r-2})$, где $r \geq 3$. Тогда в кольце $\mathcal{R}_5/J$ нет кручения.

ДОКАЗАТЕЛЬСТВО. Сначала проверим, что в кольце $\mathcal{R}_5/J$ нет элементов второго и третьего порядков. Группа $\mathcal{R}_5^{-2m} \otimes \mathbb{Q}$ согласно предложению 3.11 порождена мономами $\alpha_1^{m_1} \beta_2^{m_2} \alpha_3^{m_3} \beta_4^{m_4}$, где

$$m_1 + 2m_2 + 3m_3 + 4m_4 = m, \quad (6.16)$$

и поэтому ее ранг равен числу решений уравнения (6.16) в целых неотрицательных числах. Значит, в группах $\mathcal{R}_5^{-2m} \otimes \mathbb{F}_3$ и $\mathcal{R}_5^{-2m} \otimes \mathbb{F}_2$ число образующих не меньше этого количества. С другой стороны, по лемме 6.2 все элементы группы $\mathcal{R}_5^{-2m} \otimes \mathbb{F}_2$ выражаются через мономы вида

$$\alpha_1^{m_1} \beta_2^{m_2} \alpha_3^{m_3} \beta_2^{j_2} \beta_3^{j_3} \beta_4^{j_4} \dots, \quad j_2, j_3, j_4, \dots = 0, 1, \quad (6.17)$$

где $m_1 + 2m_2 + 3m_3 + j_2 2^2 + j_3 2^3 + j_4 2^4 + \dots = m$, а элементы группы $\mathcal{R}_5^{-2m} \otimes \mathbb{F}_3$ выражаются через мономы вида

$$\alpha_1^{m_1} \beta_2^{m_2} \beta_4^{m_4} \alpha_3^{j_1} \alpha_3^{j_2} \alpha_3^{j_3} \dots, \quad j_1, j_2, j_3, \dots = 0, 1, 2, \quad (6.18)$$

где $m_1 + 2m_2 + 3m_3 + j_1 3^1 + j_2 3^2 + j_3 3^3 + \dots = m$. Вводя параметры m_4 (в первом случае) и m_3 (во втором) такие, что $4m_4 = j_2 2^2 + j_3 2^3 + j_4 2^4 + \dots$ или соответственно $3m_3 = j_1 3^1 + j_2 3^2 + j_3 3^3 + \dots$, получаем взаимно однозначное соответствие между мономами (6.17), (6.18) и решениями уравнения (6.16). Поэтому кольцо $\mathcal{R}_5/J$ не может иметь 2- и 3-крючения.

Теперь докажем, что в кольце $\mathcal{R}_5$ нет элементов порядка p , где p – простое число и $p > 3$. Поскольку $p\beta_p \equiv 0 \pmod{I^2}$, то

$$p\beta_p = \sum_{m_1+2m_2+3m_3+4m_4=p} \lambda_{m_1,m_2,m_3,m_4} \alpha_1^{m_1} \beta_2^{m_2} \alpha_3^{m_3} \beta_4^{m_4}. \quad (6.19)$$

Как отмечалось выше, согласно лемме 2.7 существует эпиморфизм $\mathcal{R}_5 \rightarrow \mathcal{R}_4$. Так как в кольце $\mathcal{R}_4$ нет p -крючения, то и в кольце $\mathcal{R}_5$ для элемента β_p выполняется условие $p\beta_p \not\equiv 0 \pmod{p}$. Пусть (j_1, j_2, j_3, j_4) – старший в лексикографическом порядке набор переменных суммирования в сумме (6.19), для которого выполняется условие $\lambda_{j_1,j_2,j_3,j_4} \not\equiv 0 \pmod{p}$.

Пользуясь соотношением (6.19) и леммой 6.2, получаем, что кольцо $\mathcal{R}_5 \otimes \mathbb{F}_p$ аддитивно порождено мономами

$$\alpha_1^{m_1} \beta_2^{m_2} \alpha_3^{m_3} \beta_4^{m_4} \beta_p^{k_1} \beta_{p^2}^{k_2} \beta_{p^3}^{k_3} \dots, \quad 0 \leq k_1, k_2, k_3, \dots \leq p-1, \quad (6.20)$$

не делящимися на $\alpha_1^{j_1} \beta_2^{j_2} \alpha_3^{j_3} \beta_4^{j_4}$.

Ранг группы $\mathcal{R}_5^{-2m} \otimes \mathbb{Q}$ равен числу решений уравнения $m_1 + 2m_2 + 3m_3 + 4m_4 = m$ (последовательность A001400; см. [35]). Общее число мономов вида (6.20) степени m равно числу решений уравнения

$$m_1 + 2m_2 + 3m_3 + 4m_4 + pm_p = m,$$

где m_1, m_2, m_3, m_4, m_p – целые неотрицательные числа и m_p ищется в виде $pm_p = k_1 p + k_2 p^2 + k_3 p^3 + \dots$. Количество тех мономов, которые делятся на $\alpha_1^{j_1} \beta_2^{j_2} \alpha_3^{j_3} \beta_4^{j_4}$, равно числу решений уравнения

$$m_1 + 2m_2 + 3m_3 + 4m_4 + pm_p = m - p.$$

Поэтому в группе $\mathcal{R}_5^{-2m} \otimes \mathbb{F}_p$ число различных мономов вида (6.20) равно числу решений уравнения (6.16), что следует из следующего равенства соответствующих производящих функций:

$$\frac{1}{(1-x)(1-x^2)(1-x^3)(1-x^4)} = \frac{1}{(1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^p)} - \frac{1}{(1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^p)}.$$

Следовательно, $\mathcal{R}_5$ не может иметь p -крючения.

Предложение доказано.

Теорема 6.1 является следствием предложений 6.3–6.5.

ЗАМЕЧАНИЕ 6.6. Подкольцо $\mathcal{R}_5^{(2\text{-torsion})} \subset \mathcal{R}_5$, порожденное элементами $H_5(e_{2^k-2})$, можно получить из формального группового закона (2.13), рассматривая его над полем $\mathbb{F}_2$ и предполагая равенство нулю образующих $\alpha_1, \alpha_3, \beta_{p^r}$ ($r \geq 2$ при $p = 3$ и $r \geq 1$ в остальных случаях). Тогда формула (справедливая при $\alpha_1 = \alpha_2 = \alpha_3 = \beta_1 = \beta_2 = \beta_3 = 0$)

$$\begin{aligned} 0 &= [y^2 z]N(x, y, z) \\ &= \frac{1}{x^2} \left(B(x)^2 \left(3B(x) - xB'(x) - x^2 \frac{B''(x)}{2} \right) - A(x)(3B(x) - xB'(x)) \right) \end{aligned}$$

с учетом того, что $B'(x) \equiv 0 \pmod{2}$, принимает вид

$$\frac{B(x)}{x^2} \left(B(x) \left(B(x) + x^2 \frac{B''(x)}{2} \right) + A(x) \right) \equiv 0 \pmod{2}.$$

Обратим внимание на то, что у ряда $B''(x)/2$ есть однозначно определенный представитель над полем $\mathbb{F}_2$. Поэтому $\mathcal{R}_5^{(2\text{-torsion})}$ – это кольцо формального группового закона (2.13) над полем $\mathbb{F}_2$ с дополнительным условием

$$A(x) = B(x)^2 + x^2 B(x) \frac{B''(x)}{2}.$$

Компьютерные вычисления приводят к следующей гипотезе:

$$\beta_{4k} \equiv 0 \pmod{2}, \quad k \geq 1.$$

Она равносильна тому, что $B(x) + x^2 B''(x)/2 = 1$, т.е. $A(x) = B(x)$ и кольцо $\mathcal{R}_5^{(2\text{-torsion})}$ является подкольцом кольца коэффициентов формального группового закона $\mathcal{F}_6$.

§ 7. Структура кольца $\mathcal{R}_6$

ТЕОРЕМА 7.1. Кольцо $\mathcal{R}_6$ мультипликативно порождено элементами $H_3(e_n)$, где $n = 1$ и $n = 2^r - 2$ ($r \geq 2$). При этом

$$\rho_6(n) = \begin{cases} \infty, & \text{если } n = 1, 2, \\ 2, & \text{если } n = 2^r - 2, \quad r \geq 3, \\ 1 & \text{в остальных случаях.} \end{cases}$$

При $n = 2^r - 2$ ($r \geq 3$) существуют образующие e_n такие, что $2H_6(e_n) = 0$.

ДОКАЗАТЕЛЬСТВО. Полагая в формулах (6.9)–(6.11) $\alpha_n = \beta_n$, получаем систему

$$\begin{aligned} H_6(e_1) &= \alpha_1, \\ \binom{n+1}{i} \frac{H_6(e_n)}{d(n+1)} &\equiv \beta_n \pmod{I^2}, \quad n \geq 2, \quad 1 \leq i \leq n. \end{aligned}$$

Значит, при $n \geq 3$

$$\frac{\Delta(n+1)}{d(n+1)} H_6(e_n) \equiv 0 \pmod{I^2},$$

где величина $\Delta(n)$ определяется равенством

$$\Delta(n) = \left(\binom{n}{2} - \binom{n}{1}, \binom{n}{3} - \binom{n}{2}, \dots, \binom{n}{n-2} - \binom{n}{n-1} \right), \quad n \geq 3. \quad (7.1)$$

По лемме 9.10 (см. п. 9.5) $\Delta(n) = 1$ при $n > 2$, $n \neq 2^r - 2$. Таким образом, кольцо $\mathcal{R}_6$ мультипликативно порождено элементами e_n , где $n = 1, 2, 2^r - 2$, $r \geq 3$.

В размерностях $n = 2^r - 2$, $r \geq 3$, образующие e_n такие, что $2H_6(e_n) = 0$, строятся так же, как в предложении 6.5.

§ 8. Структура кольца $\mathcal{R}_3$

Пусть $\pi = \{p_1, \dots, p_k, \dots\}$ – конечный или бесконечный набор простых чисел. Обозначим через $\mathbb{Z}_\pi$ кольцо целых чисел, локализованное по $p_k \in \pi$, т.е. $\mathbb{Z}_\pi = \mathbb{Z}[1/p_1, \dots, 1/p_k, \dots]$, если $\pi \neq \emptyset$, и положим $\mathbb{Z}_\emptyset = \mathbb{Z}$. Для данного конечного или бесконечного множества формальных переменных $Y = (y_1, \dots, y_n, \dots)$ обозначим через $\mathbb{Z}[Y]$ кольцо $\mathbb{Z}[y_1, \dots, y_n, \dots]$.

ЛЕММА 8.1. Пусть $F(u, v)$ – порождающий формальный групповой закон над кольцом A . Допустим, что существует конечное или бесконечное множество элементов $(a_1, \dots, a_n, \dots)$ кольца A такое, что для равномоного множества формальных переменных $Y = (y_1, \dots, y_n, \dots)$:

1) гомоморфизм

$$\lambda: \mathbb{Z}_\pi[Y] \longrightarrow A \otimes \mathbb{Z}_\pi: \lambda(y_i) = a_i$$

является эпиморфизмом;

2) композиция кольцевых гомоморфизмов

$$\mathbb{Z}_\pi[Y] \xrightarrow{\lambda} A \otimes \mathbb{Z}_\pi \xrightarrow{1 \otimes j} A \otimes \mathbb{Q},$$

где $j: \mathbb{Z}_\pi \rightarrow \mathbb{Q}$ – каноническое вложение, является мономорфизмом.

Тогда для любого простого числа p , не принадлежащего набору π , кольцо A не имеет элементов порядка p .

ДОКАЗАТЕЛЬСТВО. Пусть простое число p не принадлежит π . Тогда для любого $a \in A \otimes \mathbb{Z}_\pi$ существует элемент $y \in \mathbb{Z}_\pi[Y]$ такой, что $\lambda(y) = a$, и поэтому $(1 \otimes j)\lambda(y) = (1 \otimes j)(a)$. Следовательно, элемент a имеет бесконечный порядок.

ТЕОРЕМА 8.2. Кольцо $\mathcal{R}_3$ мультипликативно порождено элементами $H_3(e_n)$, где $n = 2^k$, $k \geq 1$. При этом

$$\rho_3(n) = \begin{cases} \infty, & \text{если } n = 2, 4, \\ 2, & \text{если } n = 2^k, \quad k \geq 3, \\ 1 & \text{в остальных случаях.} \end{cases}$$

Кольцо $\mathcal{R}_3$ не имеет кручения.

ДОКАЗАТЕЛЬСТВО. Для группы $\mathcal{F}_3$ система (6.10), (6.11) принимает вид

$$\frac{n+1}{d(n+1)} H_3(e_n) \equiv \beta_n \pmod{I^2}, \quad (8.1)$$

$$\binom{n+1}{i} \frac{H_3(e_n)}{d(n+1)} \equiv 2\beta_n \pmod{I^2}, \quad 2 \leq i \leq n-1. \quad (8.2)$$

Отсюда следует, что

$$\begin{aligned} \frac{D(n)}{d(n+1)} H_3(e_n) &\equiv 0 \pmod{I^2}, \\ \frac{1}{d(n+1)} \left(\binom{n+1}{2} - 2\binom{n+1}{1} \right) H_3(e_n) &\equiv 0 \pmod{I^2}. \end{aligned}$$

Согласно теореме 9.9 (см. п. 9.4) наибольший общий делитель

$$\begin{aligned} &\left(\frac{D(n)}{d(n+1)}, \frac{1}{d(n+1)} \left(\binom{n+1}{2} - 2\binom{n+1}{1} \right) \right) \\ &= \left(n, D(n), \frac{1}{d(n+1)} \left(\binom{n+1}{2} - 2\binom{n+1}{1} \right) \right) \\ &= \left(n, D(n), \frac{n(n+1)}{2} - 2(n+1) \right) \end{aligned}$$

отличен от единицы, только если $n = 2^k$. Значит, $H_3(e_n) = 0$ при $n \neq 2^k$.

При $n = 2^k$ система (8.1), (8.2) принимает вид

$$H_3(e_n) \equiv \beta_n \pmod{I^2}, \quad 2H_3(e_n) \equiv 0 \pmod{I^2},$$

т.е. образующие имеют вид $H_3(e_{2^k}) = \beta_{2^k}$ и по модулю разложимых элементов являются элементами порядка 2.

Проверим, что в кольце $\mathcal{R}_3$ нет кручения. Для этого, как и в лемме 5.4, покажем, что для любого $r \geq 2$ найдется многочлен Q_r с целыми коэффициентами такой, что

$$\beta_{2^r}^2 \equiv Q_r(\beta_2, \beta_4, \dots, \beta_{2^{r-1}}) \pmod{2}.$$

Поскольку $B'(z) \equiv 0 \pmod{2}$ (см. доказательство теоремы 6.1), то

$$[xy^2]N(x, y, z) \equiv \frac{B^3(z)}{z^2} + \frac{B(z)}{z^2} + \beta_2 B(z) + \frac{B^2(z)B''(z)}{2} \pmod{2}.$$

Значит, при $n = 2^{r+1} - 2$ коэффициент при $\beta_{2^r}^2$ у многочлена $[xy^2 z^n]N(x, y, z)$ является нечетным, а коэффициент при $\beta_{2^{r+1}}$ — четным. Поэтому группа $\mathcal{R}_3^{-4m} \otimes \mathbb{Q}$ порождена мономы $\beta_2^m, \beta_2^{m-2}\beta_4, \dots$, и ее ранг равен $[m/2] + 1$. Но число различных мономов вида $\beta_2^k \beta_{2^{i_1}} \beta_{2^{i_2}} \dots$, принадлежащих группе $\mathcal{R}_3^{-4m} \otimes \mathbb{Q}$, такое же, поэтому $\mathcal{R}_3$ не имеет 2-кручения.

Для простых $p \neq 2$ отсутствие p -кручения следует из леммы 8.1. Действительно, поскольку кольцо $\mathcal{R}_3$ мультипликативно порождено элементами $H_e(e_n)$, где $n = 2^k$, то для выполнения условия 1) из леммы 8.1 можно взять $\pi = \{2\}$. Условие 2) выполняется, поскольку экспонента формальной группы является рядом над кольцом $\mathbb{Z}[\delta, \varepsilon]$.

ЗАМЕЧАНИЕ 8.3. Группа $\mathcal{F}_3$ является частным случаем формальной группы $\mathcal{F}_5$. Так как формальный групповой закон $\mathcal{F}_3$ является порождающим, то определен эпиморфизм из $\mathcal{R}_5$ в $\mathcal{R}_3$, которому соответствует эпиморфизм $\mathbb{Q}[\gamma_1, \gamma_2, \gamma_3, \gamma_4] \rightarrow \mathbb{Q}[\delta, \varepsilon]$ такой, что

$$\gamma_1 \rightarrow 0, \quad \gamma_2 \rightarrow -\frac{2}{3}\delta, \quad \gamma_3 \rightarrow 0, \quad \gamma_4 \rightarrow \frac{16}{3}\delta^2 - 4\varepsilon.$$

Это следует из формул

$$g(u) = \int_0^u \frac{dt}{\sqrt{1 - 2\delta t^2 + t^4\varepsilon}} = u + \frac{\delta}{3}u^3 + \frac{1}{10}(3\delta^2 - \varepsilon)u^5 + O(u^7).$$

Обратная функция имеет вид

$$f(u) = u - \frac{\delta}{3}u^3 + \frac{1}{30}(\delta^2 + 3\varepsilon)u^5 + O(u^7).$$

Условие $\gamma_3 \rightarrow 0$ означает, что $\wp'(s) = 0$, т.е. s является одним из трех полупериодов эллиптической кривой. Это соответствует классическому результату о том, что при s , равном одному из трех полупериодов, функция Бейкера–Ахиезера переходит в эллиптический синус Якоби.

Классические полиномы Лежандра $P_n(x)$ определяются своей производящей функцией

$$\frac{1}{\sqrt{1 - 2tx + t^2}} = \sum_{n=0}^{\infty} P_n(x)t^n.$$

Из теоремы 8.2 непосредственно вытекает следующий результат.

СЛЕДСТВИЕ 8.4. *Кольцо полиномов Лежандра над кольцом целых чисел мультипликативно порождается полиномами Лежандра $P_{2^q}(x)$, $q \geq 0$.*

Например,

$$\begin{aligned} P_1 &= x, & P_2 &= \frac{1}{2}(3x^2 - 1), & 2P_2 &= 3P_1^2 - 1, \\ P_3 &= \frac{1}{2}(5x^3 - 3x) = P_1(3P_2 - 2P_1^2), \\ P_4 &= \frac{1}{8}(35x^4 - 30x^2 + 3), & 2P_4 &= 3P_2^2 + 6P_1P_2 - 7P_1^4, \\ P_5 &= \frac{x}{8}(63x^4 - 70x^2 + 15) = P_1(5P_4 + 4P_1^2(P_2^2 - 5P_2)). \end{aligned}$$

§ 9. Приложения: арифметические свойства биномиальных коэффициентов

9.1. Базовые свойства биномиальных коэффициентов.

ЛЕММА 9.1. *Пусть p – простое число. Тогда*

$$\binom{p^{n+i}}{p^i} \equiv p^n \pmod{p^{n+1}}, \quad n, i \geq 0, \quad (9.1)$$

$$\binom{pm}{pk} \equiv \binom{m}{k} \pmod{p}, \quad m, k \geq 0. \quad (9.2)$$

ДОКАЗАТЕЛЬСТВО. При $i = 0$ первое сравнение очевидно. При $i > 0$ оно следует из равенств

$$\binom{p^{n+i}}{p^i} = p^n \binom{p^{n+i} - 1}{p^i - 1} = p^n \prod_{k=1}^{p^i - 1} \frac{p^{n+i} - k}{p^i - k}$$

(в последнем произведении каждый сомножитель сравним с единицей по модулю p).

Для доказательства второго сравнения достаточно воспользоваться равенством

$$\binom{pm}{pk} = \binom{m}{k} \prod_{j=1}^{p-1} \prod_{i=1}^k \frac{p(m - k + i) - j}{pi - j}.$$

ТЕОРЕМА 9.2 (Э. Куммер, [36]). *Порядок вхождения простого числа p в разложение на простые множители числа $\binom{n}{m}$ равен количеству переносов в следящий разряд, возникающих при сложении чисел m и $n - m$ в p -ичной системе счисления.*

ПРЕДЛОЖЕНИЕ 9.3. *Справедливо равенство (2.17).*

ДОКАЗАТЕЛЬСТВО. Отметим, что для любого натурального n из равенства $\binom{n}{1} = n$ следует, что $d(n)$ может делиться только на простые числа, входящие в разложение n . Если $n = p^k$, то, с одной стороны, по теореме 9.2 $d(n) \equiv 0 \pmod{p}$. С другой стороны, по лемме 9.1

$$\binom{p^n}{p^{n-1}} \equiv p \pmod{p^2}.$$

Значит, $d(n) = p$.

Пусть число n не является степенью простого числа, $p^k \mid n$ и $p^{k+1} \nmid n$. Тогда по теореме 9.2

$$\binom{n}{p^k} \not\equiv 0 \pmod{p},$$

т.е. $(d(n), p) = 1$. Поскольку аналогичное равенство будет выполняться для любого простого числа p , делящего n , то $d(n) = 1$.

Доказательство предложения 9.3 позволяет дать явное описание коэффициентов $\lambda_1, \lambda_2, \dots, \lambda_{n-1}$, для которых выполняется равенство

$$\lambda_1 \binom{n}{1} + \lambda_2 \binom{n}{2} + \dots + \lambda_{n-1} \binom{n}{n-1} = d(n). \quad (9.3)$$

Следующий результат играет важную роль в задаче классификации формальных групп, кольца коэффициентов которых являются модулями над кольцом целых p -адических чисел.

ПРЕДЛОЖЕНИЕ 9.4. *Если $n = p^k$, то число $d(n) = p$ можно представить в виде линейной комбинации (9.3), в которой ненулевыми являются только коэффициенты λ_i с номерами $i = 1, p^{k-1}$.*

Если $n = p_1^{k_1} \cdots p_s^{k_s}$, $s > 1$, то число $d(n) = 1$ можно представить в виде линейной комбинации (9.3), в которой ненулевыми являются только коэффициенты λ_i с номерами $i = 1, p_1^{k_1}, \dots, p_s^{k_s}$.

ДОКАЗАТЕЛЬСТВО. Пусть $n = p^k$. Тогда согласно лемме 9.1

$$\binom{p^k}{p^{k-1}} / p \equiv 1 \pmod{p}$$

и при

$$\lambda_{p^{k-1}} \equiv \left(\binom{p^k}{p^{k-1}} / p \right)^{-1} \pmod{p^{k-1}}$$

выполняется сравнение

$$\lambda_{p^{k-1}} \binom{p^k}{p^{k-1}} \equiv p \pmod{p^k}.$$

Поэтому можно выбрать λ_1 так, что будет выполняться равенство

$$\lambda_{p^{k-1}} \binom{p^k}{p^{k-1}} + \lambda_1 \binom{p^k}{1} = p.$$

Пусть теперь $n = p_1^{k_1} \cdots p_s^{k_s}$, где $s > 1$. Тогда по теореме 9.2

$$\text{ord}_{p_i} \binom{n}{p_i^{k_i}} = 0, \quad \text{ord}_{p_j} \binom{n}{p_i^{k_i}} \geq k_j, \quad j \neq i.$$

Полагая

$$\lambda_{p_i^{k_i}} \equiv \binom{n}{p_i^{k_i}}^{-1} \pmod{p_i^{k_i}},$$

получаем

$$\lambda_{p_1^{k_1}} \binom{n}{p_1^{k_1}} + \cdots + \lambda_{p_s^{k_s}} \binom{n}{p_s^{k_s}} \equiv 1 \pmod{n}.$$

Поэтому при подходящем выборе λ_1 будет выполняться равенство

$$\lambda_{p_1^{k_1}} \binom{n}{p_1^{k_1}} + \cdots + \lambda_{p_s^{k_s}} \binom{n}{p_s^{k_s}} + \lambda_1 \binom{n}{1} = 1.$$

9.2. Приложение к § 4.

ЗАМЕЧАНИЕ 9.5. Из следствия 4.3 вытекает, что лемму 4.2 достаточно доказать хотя бы для одного набора $(\lambda_1, \dots, \lambda_{n-1})$.

Доказательству леммы 4.2 предпошлем несколько вспомогательных утверждений.

ПРЕДЛОЖЕНИЕ 9.6. Для доказательства леммы 4.2 достаточно проверить выполнение любого из следующих условий.

1. Для любого простого числа p каждая переменная x_i по модулю p может быть представлена в виде линейной комбинации форм (4.2), (4.3) с целыми коэффициентами.
2. Для любого простого числа p не существует ненулевого вектора остатков по модулю p $(c_1, \dots, c_{n-1})$, $c_i = c_{n-i}$, обнуляющего формы (4.2), (4.3).

ДОКАЗАТЕЛЬСТВО. Если определитель решетки Λ (как подрешетки Γ) отличен от ± 1 , то он кратен некоторому простому числу p . Тогда базисные формы решетки Λ линейно зависимы по модулю p , что противоречит каждому из условий 1, 2.

ДОКАЗАТЕЛЬСТВО ЛЕММЫ 4.2. Проведем доказательство, пользуясь достаточным условием 1 из предложения 9.6. Если предположить, что условие выполнено для одного набора $(\lambda_1, \dots, \lambda_{n-1})$, то из этого будет следовать, что через линейные формы (4.3) можно выразить любую линейную комбинацию $c_1x_1 + \dots + c_{n-1}x_{n-1}$, для которой

$$\frac{c_1}{d(n)} \binom{n}{1} + \dots + \frac{c_{n-1}}{d(n)} \binom{n}{n-1} \equiv 0 \pmod{p}.$$

Значит, условие 1 предложения 9.6 будет выполняться и для любых наборов $(\lambda_1, \dots, \lambda_{n-1})$, удовлетворяющих (9.3).

Из соотношений

$$\begin{aligned} \binom{p^s}{p^{s-1}} &\equiv p \pmod{p^2}, & s \geq 1, \\ \binom{mp^s}{p^s} &\not\equiv 0 \pmod{p}, & s \geq 0, \quad (m, p) = 1, \end{aligned}$$

следует, что в качестве чисел $\lambda_1, \dots, \lambda_{n-1}$ при $n = p^s$ можно выбрать

$$\lambda_i = \begin{cases} 1, & \text{если } i = p^{s-1}, \\ 0, & \text{если } i \neq p^{s-1}, \end{cases}$$

а при $n = p^s m$, где $m > 1$ и $(m, p) = 1$, выбрать

$$\lambda_i = \begin{cases} \binom{n}{p^s}^{-1} \pmod{p}, & \text{если } i = p^s, \\ 0, & \text{если } i \neq p^s. \end{cases}$$

Проверим, что если $n = p^\alpha m$, где $m > 1$, то по модулю p через формы (4.3) можно выразить переменные x_i с номерами $i = p^\beta(lp + r)$, где $0 \leq \beta < \alpha$, $0 < r < p$, l целое, $0 < p^\beta(lp + r) < n$.

Действительно, полагая в (4.3) $j = p^\beta$, $i = p^\beta i_1$, $k = p^\beta k_1$, пользуясь предположением $x_{k+j} = x_i$ и сравнением (9.2), находим, что

$$P_{p^\beta k_1, p^\beta i_1}(x) \equiv (i_1 + 1)x_{p^\beta(i_1+1)} + i_1 x_{p^\beta i_1} \pmod{p}. \quad (9.4)$$

Отсюда при $i_1 = lp$, $l > 0$, получаем переменные $x_{p^\beta(lp+1)}$, при $i_1 = lp + 1$, $l > 0$, – переменные $x_{p^\beta(lp+2)}$ и т.д. При $l = 0$ переменные $x_{p^\beta(lp+r)}$ получаются из (9.4) при $i_1 = p - 1, p - 2, \dots, 1$.

Из доказанного следует, что при $n = p^s$ через формы (4.3) можно выразить переменные x_i с номерами $i = p^\beta(lp + r)$, где $0 \leq \beta \leq s - 2$, $0 \leq l \leq p - 1$, $1 \leq r \leq p - 1$. Согласно выбору чисел λ_i можно считать, что $\lambda(\mathbf{x}) = x_{p^{s-1}}$. Кроме того, согласно (9.2)

$$P_{p^{s-1}k_1, p^{s-1}i_1}(x) \equiv (i_1 + 1)x_{p^{s-1}(i_1+1)} + i_1 x_{p^{s-1}i_1} \pmod{p}.$$

Подставляя сюда $i_1 = 1, \dots, p - 2$, находим оставшиеся переменные $x_{2p^{s-1}}, \dots, x_{(p-1)p^{s-1}}$.

Если $n = p^s m$, $m > 1$, $(m, p) = 1$, то из выражений (4.3) можно выразить переменные x_i с номерами $i = p^\beta(lp + r)$, где $0 \leq \beta \leq s - 1$, $l \geq 0$, $1 \leq r \leq p - 1$.

Согласно выбору чисел λ_i можно считать, что $\lambda(\mathbf{x}) = x_{p^s}$. Пусть при $2 \leq t \leq N$ числа $a(t) \in \{t, m-t\}$ выбираются так, что выполняется условие $(a(t), p) = 1$. Тогда, выбирая в (4.3)

$$\begin{aligned} i &= p^s, & j &= (a(2) - 1)p^s, \dots, (a(N) - 1)p^s, \\ k &= (m - a(2))p^s, \dots, (m - a(N))p^s, \end{aligned}$$

получим выражения

$$\binom{a(t)}{1} x_{p^s a(t)} - \binom{m-1}{a(t)} x_{p^s},$$

из которых находятся оставшиеся переменные $x_{2p^s}, \dots, x_{(m-1)p^s}$.

ВТОРОЕ ДОКАЗАТЕЛЬСТВО¹ ЛЕММЫ 4.2. Проведем доказательство, пользуясь достаточным условием 2 из предложения 9.6. Далее все сравнения выполняются по модулю p . Положим

$$t_k = \binom{n}{k} / d(n), \quad 1 \leq k \leq n-1.$$

В качестве s будем выбирать такой номер, что $t_s \not\equiv 0$. Приведем два условия, достаточных для того, чтобы вектор $\mathbf{c} = (c_1, \dots, c_{n-1})$ был нулевым.

(i) Для всех $k = 1, \dots, n-1$ выполняется сравнение $c_k \equiv t_k c_s t_s^{-1}$, которое в дальнейшем будем обозначать $C(k)$.

(ii) Для любого $k = 1, \dots, n-1$ по крайней мере одно из чисел $\binom{n-k}{s}$, $\binom{k}{s}$ не кратно p .

Действительно, из условия (i) следует, что

$$0 \equiv \lambda(\mathbf{c}) = \sum_{k=1}^{n-1} \lambda_k c_k = c_s t_s^{-1} \sum_{k=1}^{n-1} \lambda_k t_k = c_s t_s^{-1}.$$

Поэтому $c_s \equiv 0$ и $c_k \equiv 0$ для всех $k = 1, \dots, n-1$.

Если $\binom{n-k}{s} \not\equiv 0$, то сравнение $C(k)$ выполняется, так как

$$0 \equiv P_{s,k}(\mathbf{c}) = \binom{n-k}{s} c_k - \binom{n-s}{k} c_s = \binom{n-k}{s} (c_k - t_k t_s^{-1} c_s).$$

Кроме того, сравнения $C(k)$ и $C(n-k)$ априори равносильны, так что они имеют место и в случае, если $\binom{k}{s} \not\equiv 0$. Таким образом, условие (i) является следствием условия (ii).

Рассмотрим теперь три случая.

1) n не кратно p . Тогда при $s = 1$ выполняется условие (ii), поскольку для любого $k = 1, \dots, n-1$ по крайней мере одно из чисел $n-k$, k не кратно p .

2) $n = p^m$. Тогда при $s = p^{m-1}$ число $t_s = \binom{n}{s} p^{-1}$ не кратно p . В этом случае также проверим справедливость условия (ii). Для любого $k = 1, \dots, n-1$ по крайней мере одно из чисел $n-k$, k не меньше s . Например, если $n-k \geq s$, то $\binom{n-k}{s}$ не кратно p по теореме Куммера.

3) $n = p^k w$, где $w > 1$ и $(w, p) = 1$. Положим $s = p^m$. По теореме Куммера $t_s = \binom{n}{s} \not\equiv 0$. Предположим, что условие (i) не выполнено. Тогда не выполнено

¹Предложено Ф. В. Петровым.

и условие (ii), т.е. для некоторого k оба биномиальных коэффициента $\binom{n-k}{s}$ и $\binom{k}{s}$ кратны p . Отсюда следует, что $k \geq s$ (а в силу симметрии и $n-k \geq s$), так как в противном случае по теореме Куммера $\binom{n-k}{s} \not\equiv 0$. В частности, при $k < s$ справедливость сравнения $C(k)$ можно считать установленной; при этом $c_k \equiv 0$, поскольку $t_k = \binom{n}{k} \equiv 0$. Значит, к обоим биномиальным коэффициентам $\binom{n-k}{s}$ и $\binom{k}{s}$ применима теорема Куммера, из которой следует, что числа k и $n-k$ при записи в p -ичной системе счисления имеют нуль в m -м разряде. Таким образом, $k = i_1 + p^{m+1}x_1$, $n-k = i_2 + p^{m+1}x_2$, где $0 \leq i_1, i_2 < p^m$, $x_1, x_2 > 0$. Так как n не делится на p^{m+1} , то одно из чисел i_1, i_2 отлично от нуля. Пусть, например, $n-k = i + p^{m+1}x$, где $0 < i < p^m$, $x > 0$. Желаемое сравнение $C(k)$ равносильно тому, что $c_k \equiv 0$. Это следует из сравнения

$$0 \equiv P_{i,k} = \binom{n-k}{i} c_k - \binom{n-i}{k} c_i,$$

поскольку $\binom{n-k}{i}$ не кратно p и справедливость сравнения $c_i \equiv 0$ уже установлена.

9.3. Приложение к § 5. Пусть

$$d_2(n) = \left(\binom{n}{2}, \binom{n}{3}, \dots, \binom{n}{n-2} \right), \quad n \geq 4.$$

ЛЕММА 9.7. Пусть $n \geq 3$. Тогда $d_2(n+1) = d(n)d(n+1)$.

ДОКАЗАТЕЛЬСТВО. Поскольку $d_2(n+1) \mid \binom{n+1}{2}$, то

$$d_2(n+1) = (d_2(n+1), n)(d_2(n+1), n+1).$$

Остается заметить, что $(d_2(n+1), n+1) = d(n+1)$ и

$$(d_2(n+1), n) = \left(\binom{n}{1}, \binom{n}{1} + \binom{n}{2}, \dots, \binom{n}{n-2} + \binom{n}{n-1} \right) = d(n).$$

СЛЕДСТВИЕ 9.8. Если $n \geq 3$ и $d_2(n+1) \neq d(n+1)$, то $n = p^\alpha$.

9.4. Приложение к § 6.

ТЕОРЕМА 9.9. Пусть $n \geq 5$. Тогда для величины $D(n)$, определенной равенством (6.13), справедлива формула

$$\frac{D(n)}{d(n+1)} = \begin{cases} d(n), & \text{если } n \neq 2^k - 2, \\ 2 & \text{если } n = 2^k - 2. \end{cases}$$

Для нечетных n эта теорема была независимо получена в недавней работе [37] в связи с известной задачей о торических образующих кольца кобордизмов SU -многообразий.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 9.9. По определению $D(n) = (h_2, \dots, h_{n-2})$, где

$$h_i = \binom{n}{i+1} - \binom{n}{i-1} = \binom{n+1}{i+1} - \binom{n+1}{i}.$$

С одной стороны, для любого $j = 2, \dots, n-2$ выполняется равенство

$$d_2(n+1) = \left(\binom{n+1}{j}, D(n) \right).$$

С другой стороны,

$$D(n) \mid (n-1)h_2 - 4h_3 = 2 \binom{n+1}{3}.$$

Следовательно, либо $D(n) = d_2(n+1)$, либо $D(n) = 2d_2(n+1)$.

Число $4D(n)$ делит как число $A = 8 \binom{n+1}{3}$, так и число $B = 4h_3 = (n-6) \binom{n+1}{3}$. Поэтому

$$4D(n) \mid (A, B) = \binom{n+1}{3} (8, n-6).$$

Значит, если $n-6$ не кратно 8, то

$$D(n) \mid \binom{n+1}{3}, \quad d_2(n+1) = \left(\binom{n+1}{3}, D(n) \right) = D(n).$$

Если же $n = 8k + 6$, то $d_2(n+1)$ нечетно (так как $\binom{n+1}{2}$ нечетно) и $D(n) = 2d_2(n+1)$ тогда и только тогда, когда все числа $h_2, \dots, h_{n-2}$ четны. По модулю 2 имеем

$$h_i = \binom{n+1}{i+1} - \binom{n+1}{i} \equiv \binom{n+1}{i+1} + \binom{n+1}{i} = \binom{n+2}{i+1}.$$

Таким образом, четность $D(n)$ оказывается равносильна четности всех биномиальных коэффициентов $\binom{n+2}{3}, \dots, \binom{n+2}{n}$. Поскольку при $n = 8k + 6$ числа $\binom{n+2}{1}, \binom{n+2}{2}, \binom{n+2}{n+1}$ также заведомо четные, это равносильно четности числа $d(n+2)$. Согласно (2.17) это в свою очередь равносильно тому, что $n+2$ есть степень 2.

9.5. Приложение к § 7.

ЛЕММА 9.10. Пусть $n \geq 3$. Тогда для величины $\Delta(n)$, определенной равенством (7.1), выполняется равенство

$$\frac{\Delta(n)}{d(n)} = \begin{cases} 2, & \text{если } n = 2^k - 1, \quad k \geq 3, \\ 1 & \text{в остальных случаях.} \end{cases}$$

ДОКАЗАТЕЛЬСТВО. Согласно теореме 9.9

$$\frac{\Delta(n+1)}{d(n+1)} = 1$$

за исключением случаев, когда $n = p^k$, $k \geq 1$, и $n = 2^r - 2$, $r \geq 3$. В этих случаях утверждение леммы следует из теоремы 9.9 и того, что при $n = p^k$, $k \geq 1$, число

$$\binom{n+1}{2} - \binom{n+1}{1} = \frac{(n+1)(n-2)}{2}$$

является взаимно простым с p , а при $n = 2^r - 2$, $r \geq 3$, все биномиальные коэффициенты $\binom{n+1}{i}$, $1 \leq i \leq n$, суть нечетные числа.

Список литературы

- [1] N. H. Abel, “Méthode générale pour trouver des fonctions d’une seule quantité variable, lorsqu’une propriété de ces fonctions est exprimée par une équation entre deux variables”, *Oeuvres complètes*, v. 1, Grondahl et Son, Christiania, 1881, 1–10.
- [2] Ф. Хирцебрух, *Топологические методы в алгебраической геометрии*, Мир, М., 1973, 280 с.; пер. с нем.: F. Hirzebruch, *Neue topologische Methoden in der algebraischen Geometrie*, *Ergeb. Math. Grenzgeb. (N.F.)*, **9**, Springer-Verlag, Berlin–Göttingen–Heidelberg, 1956, viii+165 pp.
- [3] N. H. Abel, “Untersuchung der Functionen zweier unabhängig veränderlichen Größen x und y , wie $f(x, y)$, welche die Eigenschaft haben, daß $f(z, f(x, y))$ eine symmetrische Function von z, x und y ist”, *J. Reine Angew. Math.*, **1826**:1 (1826), 11–15; “Recherche des fonctions de deux quantités variables independantes x et y , telles que $f(x, y)$, qui ont la propriete que $f(z, f(x, y))$ est une fonction symetrique de z, x et y ”, *Oeuvres completes de N. H. Abel*, 1826.
- [4] Ж. Дьёдонне, “Дифференциальное исчисление в полях характеристики $p > 0$ ”, *Международный математический конгресс в Амстердаме* (1954), Физматгиз, М., 1961, 134–150; пер. с фр.: J. Dieudonné, “Le calcul différentiel dans les corps de caractéristique $P > 0$ ”, *Proceedings of the International Congress of Mathematicians*, v. 1 (Amsterdam, 1954), Erven P. Noordhoff N.V., Groningen, 1957, 240–252.
- [5] M. Lazard, “Sur les groupes de Lie formels à un paramètre”, *Bull. Soc. Math. France*, **83** (1955), 251–274.
- [6] Т. Хонда, “Формальные группы и дзета-функции”, *Математика*. Сб. пер., **13**, № 6, Мир, М., 1969, 3–17; пер. с англ.: T. Honda, “Formal groups and zeta-functions”, *Osaka J. Math.*, **5**:2 (1968), 199–213.
- [7] С. П. Новиков, “Методы алгебраической топологии с точки зрения теории кобордизмов”, *Изв. АН СССР. Сер. матем.*, **31**:4 (1967), 855–951; англ. пер.: S. P. Novikov, “The methods of algebraic topology from the viewpoint of cobordism theory”, *Math. USSR-Izv.*, **1**:4 (1967), 827–913.
- [8] *Кобордизмы в Советском Союзе*, 1967–1979, Топологическая библиотека, **4**, ред. С. П. Новиков, И. А. Тайманов, М.–Ижевск, Институт компьютерных исследований, 2011, 584 с.
- [9] D. Quillen, “On the formal group laws of unoriented and complex cobordism theory”, *Bull. Amer. Math. Soc.*, **75**:6 (1969), 1293–1298.
- [10] В. М. Бухштабер, “Комплексные кобордизмы и формальные группы”, *УМН*, **67**:5(407) (2012), 111–174; англ. пер.: V. M. Buchstaber, “Complex cobordism and formal groups”, *Russian Math. Surveys*, **67**:5 (2012), 891–950.
- [11] J. T. Tate, “The arithmetic of elliptic curves”, *Invent. Math.*, **23**:3 (1974), 179–206.
- [12] В. М. Бухштабер, Е. Ю. Бунькова, “Формальные группы Кричевера”, *Функц. анализ и его прил.*, **45**:2 (2011), 23–44; англ. пер.: V. M. Buchstaber, E. Yu. Bunkova, “Krichever formal groups”, *Funct. Anal. Appl.*, **45**:2 (2011), 99–116.
- [13] В. М. Бухштабер, С. П. Новиков, “Формальные группы, степенные системы и операторы Адамса”, *Матем. сб.*, **84**(126):1 (1971), 81–118; англ. пер.: V. M. Buchstaber, S. P. Novikov, “Formal groups, power systems and Adams operators”, *Math. USSR-Sb.*, **13**:1 (1971), 80–116.
- [14] M. Hazewinkel, *Formal groups and applications*, Pure Appl. Math., **78**, Academic Press, New York–London, 1978, xxii+573 pp.
- [15] В. М. Бухштабер, А. Н. Холодов, “Формальные группы, функциональные уравнения и обобщенные теории когомологий”, *Матем. сб.*, **181**:1 (1990), 75–94; англ. пер.: V. M. Bukhshtaber, A. N. Kholodov, “Formal groups, functional equations, and generalized cohomology theories”, *Math. USSR-Sb.*, **69**:1 (1991), 77–97.

- [16] P. Busato, “Realization of Abel’s universal formal group law”, *Math. Z.*, **239**:3 (2002), 527–561.
- [17] F. Clarke, K. Johnson, “On the classifying ring for Abel formal group laws”, *J. Pure Appl. Algebra*, **213**:7 (2009), 1290–1298.
- [18] В. М. Бухштабер, “Функциональные уравнения, ассоциированные с теоремами сложения для эллиптических функций, и двузначные алгебраические группы”, *УМН*, **45**:3(273) (1990), 185–186; англ. пер.: V. M. Bukhshtaber, “Functional equations associated with addition theorems for elliptic functions and two-valued algebraic groups”, *Russian Math. Surveys*, **45**:3 (1990), 213–215.
- [19] S. Ochanine, “Sur les genres multiplicatifs definis par des integrales elliptiques”, *Topology*, **26**:2 (1987), 143–151.
- [20] E. Witten, “Elliptic genera and quantum field theory”, *Comm. Math. Phys.*, **109**:4 (1987), 525–536.
- [21] Э. Т. Уиттекер, Д. Н. Ватсон, *Курс современного анализа*, т. 2: *Трансцендентные функции*, Физматлит, М., 1963, 515 с.; пер. с англ.: E. T. Whittaker, G. N. Watson, *A course of modern analysis. An introduction to the general theory of infinite processes and of analytic functions; with an account of the principal transcendental functions*, 4th ed., Cambridge Univ. Press, Cambridge, 1927, vi+608 pp.
- [22] И. М. Кричевер, “Обобщенные эллиптические роды и функции Бейкера–Ахиезера”, *Матем. заметки*, **47**:2 (1990), 34–45; англ. пер.: I. M. Krichever, “Generalized elliptic genera and Baker–Akhiezer functions”, *Math. Notes*, **47**:2 (1990), 132–142.
- [23] И. М. Кричевер, “Эллиптические решения уравнения Кадомцева–Петвиашвили и интегрируемые системы частиц”, *Функц. анализ и его прил.*, **14**:4 (1980), 45–54; англ. пер.: I. M. Krichever, “Elliptic solutions of the Kadomtsev–Petviashvili equation and integrable systems of particles”, *Funct. Anal. Appl.*, **14**:4 (1980), 282–290.
- [24] М. Бакурадзе, “О формальной группе Бухштабера и связанных с ней родах”, *Алгебраическая топология, выпуклые многогранники и смежные вопросы*, Сборник статей. К 70-летию со дня рождения члена-корреспондента РАН Виктора Матвеевича Бухштабера, Тр. МИАН, **286**, МАИК, М., 2014, 7–21; англ. пер.: M. Bakuradze, “On the Buchstaber formal group law and some related genera”, *Proc. Steklov Inst. Math.*, **286** (2014), 1–15.
- [25] V. M. Buchstaber, T. E. Panov, *Toric topology*, Math. Surveys Monogr., **204**, Amer. Math. Soc., Providence, RI, 2015.
- [26] B. Ram, “Common factors of $\frac{n!}{m!(n-m)!}$ ($m = 1, 2, \dots, n-1$)”, *J. Indian Math. Club*, **1** (1909), 39–43.
- [27] Ф. Хирцебрух, *Топологические методы в алгебраической геометрии*, Мир, М., 1973, 280 с.; пер. с нем.: F. Hirzebruch, *Neue topologische Methoden in der algebraischen Geometrie*, Ergeb. Math. Grenzgeb. (N.F.), **9**, Springer-Verlag, Berlin–Göttingen–Heidelberg, 1956, viii+165 pp.; англ. пер. с нем.: *Topological methods in algebraic geometry*, Grundlehren Math. Wiss., **131**, Springer Verlag, New York, 1966, x+232 pp.
- [28] Р. Л. Грэхем, Д. Э. Кнут, О. Паташник, *Конкретная математика. Основание информатики*, Мир, М., 1998, 703 с.; пер. с англ.: R. L. Graham, D. E. Knuth, O. Patashnik, *Concrete mathematics. A foundation for computer science*, 2nd ed., Addison-Wesley Publ. Co., Reading, MA, 1994, xiv+657 pp.
- [29] R. M. Corless, G. H. Gonnet, D. E. G. Hare, D. J. Jeffrey, D. E. Knuth, “On the Lambert W function”, *Adv. Comput. Math.*, **5** (1996), 329–359.
- [30] M. Bizley, “Derivation of a new formula for the number of minimal lattice paths from $(0, 0)$ to (km, kn) having just t contacts with the line $my = nx$ and having no points above this line; and a proof of Grossman’s formula for the number of paths which may touch but do not rise above this line”, *J. Inst. Actuar.*, **80** (1954), 55–62.

- [31] В. М. Бухштабер, “Кольцо простых многогранников и дифференциальные уравнения”, *Геометрия, топология и математическая физика*. I, Сборник статей. К 70-летию со дня рождения академика Сергея Петровича Новикова, Тр. МИАН, **263**, МАИК, М., 2008, 18–43; англ. пер.: V. M. Buchstaber, “Ring of simple polytopes and differential equations”, *Proc. Steklov Inst. Math.*, **263** (2008), 13–37.
- [32] A. Fröhlich, *Formal groups*, Lecture Notes in Math., **74**, Springer-Verlag, Berlin–New York, 1968, iii+140 pp.
- [33] В. М. Бухштабер, “Новые методы в теории кобордизмов”, Добавление к кн.: Р. Стонг, *Заметки по теории кобордизмов*, Мир, М., 1973, 185–186.
- [34] J. Lurie, *Chromatic homotopy theory*, Lecture course given at Harvard University, <http://www.math.harvard.edu/~lurie/252x.html>.
- [35] N. J. A. Sloane, *The on-line encyclopedia of integer sequences*, the sequence A001400, <http://www.oeis.org/A001400>.
- [36] E. E. Kummer, “Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen”, *J. Reine Angew. Math.*, **1852**:44 (1852), 93–146.
- [37] Zhi Lu, T. Panov, *On toric generators in the unitary and special unitary bordism rings*, arXiv: 1412.5084.

Виктор Матвеевич Бухштабер
(Victor M. Buchstaber)

Математический институт им. В.А. Стеклова
Российской академии наук, г. Москва;
Институт проблем передачи информации
им. А.А. Харкевича
Российской академии наук, г. Москва
E-mail: buchstab@mi.ras.ru

Поступила в редакцию
26.03.2015 и 14.09.2015

Алексей Владимирович Устинов
(Alexey V. Ustinov)

Хабаровское отделение
Института прикладной математики
Дальневосточного отделения
Российской академии наук
E-mail: ustinov@iam.khv.ru