Записки научных
семинаров ПОМИ
Том 470, 2018 г.

**М. А. Антипов, К. И. Пименов**

# О НЕКОТОРЫХ МУЛЬТИПЛИКАТИВНЫХ СТРУКТУРАХ НА КУБИЧЕСКИХ РАСШИРЕНИЯХ

## §1

**1.1. Введение.** Пусть $L$ – циклическое кубическое расширения поля $\mathbb{Q}$ с зафиксированной образующей $\sigma$ группы Галуа. В дальнейшем тексте термин "норма" без дополнительных эпитетов применяется для обозначения абсолютной нормы $\mathrm{Nm} : L^* \to \mathbb{Q}^*$. Пусть $a \in L^*$ – элемент, не являющийся кубом. В работе [1] показано, как элементу $a$ можно сопоставить чисто кубическое расширение $\mathbb{Q}\left[\sqrt[3]{d_{L,a}}\right]$ и элемент $m_{L,a} \in \mathbb{Q}\left[\sqrt[3]{d_{L,a}}\right]$, норма которого является кубом.

В случае, когда $\mathrm{Nm}(a) = 1$, но элемент $a$ не представим в виде $a = \frac{x}{\sigma(x)}$ мы определяем *соответствие Рамануджана* как сопоставление элементу $a$ выражения $m_{L,a} = \left(\sqrt[3]{a} + \sqrt[3]{\sigma(a)} + \sqrt[3]{\sigma^2(a)}\right)^3$, где результат является элементом, лежащим в некотором чисто кубическом расширении $\mathbb{Q}\left[\sqrt[3]{d_{L,a}}\right]$, см. [1].

Терминология обусловлена тем, что для $a = 2\cos\frac{2\pi}{7}$ и $L = \mathbb{Q}\left[\cos\frac{2\pi}{7}\right]$ явное вычисление приводит к формуле, приведенной в записных книжках Рамануджана [3, p.22–24]:

$$\sqrt[3]{2\cos\frac{2\pi}{7}} + \sqrt[3]{2\cos\frac{4\pi}{7}} + \sqrt[3]{2\cos\frac{8\pi}{7}} = \sqrt[3]{5 - 3\sqrt[3]{7}}.$$

В этом случае в качестве $d_{L,a}$ можно взять число 7. В том же источнике приводится общая формула Рамануджана для так называемого *шенксова* [2] циклического кубического полинома

$$X^3 - uX^2 - (u+3)X - 1.$$

---

*Ключевые слова*: циклическое кубическое расширение, радикалы, записные книжки Рамануджана, эллиптическая кривая Ферма.

Работа второго автора поддержана грантом РФФИ 16-01-00750 "Мотивные и классические методы в теории алгебраических групп, алгебраической геометрии и теории чисел".

В случае, когда при $u \in \mathbb{Q}$ данный полином не имеет рациональных корней, его корню $a_u$ отвечает по Рамануджану иррациональность $m_u = u + 6 - 3\sqrt[3]{u^2+3u+9}$.

В данной заметке мы обсуждаем свойства мультипликативности соответствия Рамануджана и его вариантов, для чего нам приходится модифицировать и уточнять область определения и область значения. Приведем мотивирующий численный пример, взяв два элемента $a = a' = 2\cos\frac{2\pi}{7}$, так что $m_a = m_{a'} = 5 - 3\sqrt[3]{7}$. Тогда их произведение $aa'$ является корнем циклического кубического полинома $X^3-5X^2-6X-1$ с отвечающей по Рамануджану иррациональностью $11+9\sqrt[3]{7}+3\sqrt[3]{49}$. Заметим, что

$$11+9\sqrt[3]{7}+3\sqrt[3]{49} = (5-3\sqrt[3]{7})^2 \cdot \left[\frac{1}{8}\left(11+5\sqrt[3]{7}+3\sqrt[3]{49}\right)\right]^3,$$

таким образом, $m_{aa'}$ отличается от $m_a \cdot m_{a'}$ домножением на куб элемента из $\mathbb{Q}\left[\sqrt[3]{7}\right]^*$. В разделе 1.2 мы определяем мультипликативный гомоморфизм, иллюстрацией которого является только что приведенный численный пример.

В разделе 2 мы уже не считаем циклическое кубическое поле $L$ фиксированным, но фиксируем параметр $d = d_{a,L}$ в правой части соответствия Рамануджана и задаемся вопросом, какая операция на входных данных $(L, a)$ отвечает умножению кубических иррациональностей в $\mathbb{Q}\left[\sqrt[3]{d}\right]^*$.

Раздел 3 содержит основной результат данной заметки – теорему 3.2.1. Гипотетически операция умножения кубических иррациональностей в $\mathbb{Q}[\sqrt[3]{d}]$, норма которых является кубом рационального числа, должна быть связанной с частично определенной операцией на точках кубической поверхности в $\mathbf{P}^3(\mathbb{Q})$, заданной уравнением $X^3 + dY^3+d^2Z^3-3dXYZ-T^3 = 0$. Нам удалось установить частный случай гипотетического результата, касающийся сложения точек на эллиптической кривой $X^3+dY^3-T^3 = 0$ и умножения двучленных кубических иррациональностей, рассматриваемых с точностью до умножения на куб.

**1.2. Мультипликативный гомоморфизм.** Через $L_1$ мы будем обозначать ядро норменного отображения $\mathrm{Nm} : L^* \to \mathbb{Q}^*$, а через $L_d$ для $d \in \mathbb{Q}^*$ мы будем обозначать подгруппу в $L^*$, которая является прообразом при норменном отображении для циклической подгруппы $\langle d\rangle \subset \mathbb{Q}^*$.

**Теорема 1.2.1.** *Зафиксируем циклическое кубическое расширения $L/\mathbb{Q}$ с образующей группы Галуа $\sigma$, а также рациональное число $d$, не являющееся кубом. Обозначим через $A_L$ аддитивно записанное коядро отображения $1-\sigma : L_1 \to L_1$ и образ элемента $a \in L_1$ при канонической проекции будем обозначать через $\overline{a}$. Через $A_{d,L}$ обозначим подгруппу в $A_L$, которая является образом композиции гомоморфизмов $L_d \xrightarrow{1-\sigma} L_1 \to A_L$, иначе говоря, состоит из элементов вида $\overline{\left(\frac{x}{\sigma(x)}\right)}$, где $x \in L_d$. Рассмотрим также группу $B_d = \mathbb{Q}\left[\sqrt[3]{d}\right]^* / \mathbb{Q}^* \cdot \left(\mathbb{Q}\left[\sqrt[3]{d}\right]^*\right)^3$. Иначе говоря, $B_d$ – это группа по умножению кубических иррациональностей, рассматриваемых по модулю кубов и с точностью до домножения на рациональное число.*

*Тогда сопоставление элементу $\overline{a} \in A_{d,L}$ выражения*

$$m_a = \left(\sqrt[3]{a} + \sqrt[3]{\sigma(a)} + \sqrt[3]{\sigma^2(a)}\right)^3$$

*задает корректно определенный гомоморфизм из $A_{d,L}$ в $B_d$.*

**Доказательство.** Фактически доказательство почти целиком было написано в работе [1, предложение 3] и является прямолинейным использованием теоремы Гильберта 90. Сохраним обозначения оттуда, т.е. для $a \in L_1$ положим $b = \sigma(a); c = \sigma(b)$, и введем элементы $\alpha \in L^*, \beta = \sigma(\alpha)$ и $\gamma = \sigma(\beta)$ для которых выполняются соотношения $\frac{\alpha}{\beta} = a$; $\frac{\beta}{\gamma} = b$; $\frac{\gamma}{\alpha} = c$. Например, мы можем положить $\alpha = 1 + a + ab$, если это выражение не равно нулю. Ясно, что элементы $\alpha, \beta, \gamma$ определены однозначно с точностью до домножения на рациональное число. По предположению теоремы $\alpha \in L_d$, так что произведение $\alpha\beta\gamma$ равно 1, $d$ или $d^2$ с точностью до умножения на куб рационального числа. Будем для простоты считать, что $\alpha\beta\gamma = d$. По теореме Гильберта 90 мы можем ввести в рассмотрение элементы $\varphi, \psi, \theta \in L\left[\sqrt[3]{d}\right]$, с тем, чтобы выполнялись соотношения $\frac{\varphi}{\psi} = \alpha$; $\frac{\psi}{\theta} = \beta$; $\frac{\theta}{\varphi} = \gamma$.

Тогда $\left(\sqrt[3]{a}+\sqrt[3]{b}+\sqrt[3]{c}\right)^3 = \varphi\psi\theta\cdot\left(\frac{1}{\psi}+\frac{1}{\theta}+\frac{1}{\varphi}\right)^3$, другими словами класс элемента $m_a$ в группе $B_d$ совпадает с классом $\varphi\psi\theta$.

Проверим корректность задания нами отображения из $A_{d,L}$ в $B_d$ формулой $\overline{a}\mapsto\overline{m_a}$. Пускай класс элемента $a'$ совпадает с классом элемента $a$ в $A_{d,L}$. Это значит, что $a' = a\cdot\frac{x}{\sigma(x)}$ при некотором $x\in L_1$. Введем обозначения $y=\sigma(x)$ и $z=\sigma(y)$. В качестве элементов $\alpha',\beta',\gamma'$, отвечающих элементу $a'$ можно взять $\alpha'=\alpha\cdot x$; $\beta'=\beta\cdot y$; $\gamma'=\gamma\cdot z$. Но $xyz=1$, поэтому по теореме Гильберта 90 имеется набор $u,v,w\in L^*$ такой, что $v=\sigma(u)$; $w=\sigma(v)$ и $x=\frac{u}{v}$; $y=\frac{v}{w}$; $z=\frac{w}{u}$. Тогда в качестве $\varphi',\psi',\theta'$ можно взять элементы $\varphi'=\varphi\cdot u$; $\psi=\psi'\cdot v$; $\theta'=\theta\cdot w$. Класс элемента $m_{a'}$ совпадает с классом $\varphi'\psi'\theta'$. Но произведение $\varphi'\psi'\theta'$ равно $\varphi\psi\theta\cdot uvw$, т.е. его класс совпадает с классом $\varphi\psi\theta$, который равен классу $m_a$.

Проверяем гомоморфность. Вводим обозначения для $\widetilde{\alpha}=1+aa'+aba'b'$; $\widetilde{\beta}=1=bb'+bcb'c'$; $\widetilde{\gamma}=1+cc'+cac'a'$. Тогда элемент $\frac{\widetilde{\alpha}}{\alpha\alpha'}$ неподвижен относительно действия группы Галуа $L$ над $\mathbb{Q}$, и после деления $\widetilde{\alpha},\widetilde{\beta},\widetilde{\gamma}$ на константу из $\mathbb{Q}^*$ мы можем считать, что $\widetilde{\alpha}=\alpha\alpha'$ и так далее. После произведенной нормировки вводим $\widetilde{\varphi}=1+\frac{\alpha\alpha'}{\sqrt[3]{d^2}}+\frac{\alpha\beta\alpha'\beta'}{\sqrt[3]{d^4}}$ и так далее. То же самое рассуждение, что двумя строчками выше показывает, что $\frac{\widetilde{\varphi}}{\varphi\varphi'}$ неподвижен под действием $\sigma\in\mathrm{Gal}\left(L\left[\sqrt[3]{d}\right]/\mathbb{Q}\left[\sqrt[3]{d}\right]\right)$. Так что $\widetilde{\varphi}\widetilde{\psi}\widetilde{\theta}$ отличается от $\varphi\psi\theta\varphi'\psi'\theta'$ умножением на куб элемента из $\mathbb{Q}\left[\sqrt[3]{d}\right]$.

Нам известно, что $m_a=\left(\sqrt[3]{a}+\sqrt[3]{b}+\sqrt[3]{c}\right)^3=\varphi\psi\theta\cdot\left(\frac{1}{\psi}+\frac{1}{\theta}+\frac{1}{\varphi}\right)^3$.

Аналогичным образом обстоит дело с $m_{a'}$ и элементом

$$m_{aa'}=\widetilde{\varphi}\widetilde{\psi}\widetilde{\theta}\cdot\left(\frac{1}{\widetilde{\varphi}}+\frac{1}{\widetilde{\psi}}+\frac{1}{\widetilde{\theta}}\right)^3.$$

Поэтому $m_{aa'}$ отличается от $m_a\cdot m_{a'}$ домножением на куб элемента из $\mathbb{Q}\left[\sqrt[3]{d}\right]$ $\square$

**Замечание 1.2.2.** Иллюстрацией к построенному гомоморфизму служит случай $a' = \dfrac{1}{a}$. В этой ситуации $m_a \cdot m_{\frac{1}{a}}$ окажется кубом в $\mathbb{Q}\left[\sqrt[3]{d}\right]$. А именно, кубом элемента

$$3 + \left(\sqrt[3]{\frac{b}{a}} + \sqrt[3]{\frac{c}{b}} + \sqrt[3]{\frac{a}{c}}\right) + \left(\sqrt[3]{\frac{a}{b}} + \sqrt[3]{\frac{b}{c}} + \sqrt[3]{\frac{c}{a}}\right),$$

который лежит в $\mathbb{Q}\left[\sqrt[3]{d}\right]$. Численный пример дается классической формулой Рамануджана: $(5 - \sqrt[3]{7})(4 - \sqrt[3]{7}) = (3 - \sqrt[3]{7})^3$. К другой интерпретации данного соотношения мы вернемся в разделе 3.

Отметим, что циклическое кубическое поле $L$ можно менять, так что для фиксированного $d$ мы получаем серию различных отображений с образами в $B_d$. Можем ли мы каким-либо образом объединить области определения построенных гомоморфизов в одну общую группу? Возможный ответ на этот вопрос дается в следующем разделе.

## §2. Умножение циклических кубических расширений

**2.1. Теория Куммера без корней из единицы.** Следующий результат из классических учебников по теории Галуа (см. [4]) связан с так называемой теорией Куммера без корней из единицы. Рассмотрим поле $F$ характеристики, отличной от 2 и 3, не содержащее нетривиального кубического корня из единицы $\omega$. Тогда циклические кубические расширения $L/F$ с выбранной ориентацией, т.е. образующей группы Галуа $\mathrm{Gal}(L/F)$ классифицируются элементами мультипликативной группы

$$\mathrm{Nm}^{-1}((F^*)^3)/(K^*)^3 \cdot F^*, \text{ где } K = F[\omega], \tag{1}$$

а $\mathrm{Nm} : K^* \to F^*$ – норменное отображение.

Умножение в этой факторгруппе отвечает некоторой операции над циклическими кубическими расширениями, явное описание которой мы напомним ниже. Называть эту операцию мы будем умножением по Куммеру циклических кубических расширений. Следует учитывать, что тривиальному элементу группы $\mathrm{Nm}^{-1}((F^*)^3)/(K^*)^3 \cdot F^*$ отвечает не поле $L$, а расщепленная алгебра Галуа третьей степени над $F$. Мы не будем использовать аппарат алгебр Галуа и потому избегаем полных определений. Тем не менее, множество циклических кубических расширений вместе с добавленным элементом, отвечающим расщепимой алгебре Галуа, образует группу.

Хорошо известно, как эта операция описывается в терминах корней полиномов, полем разложения которых данные циклические кубические расширения являются. Пусть $a$, $b = \sigma(a)$, $c = \sigma(b)$ – это корни полинома с коэффициентами из $F$, порождающие циклическое кубическое расширение $L/F$ с образующей группы Галуа $\sigma$, а $x$, $y = \tau(x)$, $z = \tau(y)$ – это корни полинома с коэффициентами из $F$, порождающие циклическое кубическое расширение $L'/F$ с образующей группы Галуа $\tau$. Тогда группа Галуа композита $LL'$ над $F$ равна либо $C_3 \times C_3 = \langle\sigma\rangle \times \langle\tau\rangle$, либо $C_3$ в том случае, когда $L = L'$.

Нетрудно видеть, что действия автоморфизмов $\sigma$ и $\tau$ на элементах

$$u = ax + bz + cy, \quad v = cz + ay + bx, \quad w = by + cx + az \tag{2}$$

совпадают: $\sigma(u) = \tau(u) = v$, $\sigma(v) = \tau(v) = w$ и $\sigma(w) = \tau(w) = u$. Если исходный выбор минимальных полиномов был удачен, $u, v, w$ не совпадают и являются корнями полинома с коэффициентами из $F$. В получившемся циклическом кубическом расширении в качестве образующей группы Галуа выбираем перестановку $(uvw)$ в цикленной записи. Если же $u, v, w$ попали в $F$, это означает, что $L = L'$ и $\sigma = \tau^2$.

В качестве илюстрации приведем результат вычисления описанной только что операции в применении к шенксовым полиномам.

Для шенксова полинома $X^3 - uX^2 - (u+3)X - 1$ упорядочим корни $a = \frac{x}{y}$; $b = \frac{y}{z}$; $c = \frac{z}{x}$, где $x = 1 + a + ab$, таким образом, что $x + y + z = 0$. В этом случае $x, y, z$ удовлетворяют соотношению $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 1$ и являются корнями полинома

$Y^3 - (u^2+3u+9)Y + (u^2+3u+9)$ с дискриминантом $(2u+3)^2(u^2+3u+9)^2$.

Уравнение такого вида мы будем называть *ассоциированным* с исходным шенксовым полиномом.

Оказывается, что при помощи формул (2) по двум шенксовым уравнениям с параметрами $u$ и $v$ нетрудно найти параметр некоторого шенксова уравнения, поле разложения которого является произведением по Куммеру полей разложения исходных шенксовых полиномов.

Пусть $p, q, r$ – корни полинома $X^3 - (v^2 + 3v + 9)X + (v^2 + 3v + 9)$. Тогда тройка $\varphi = xp + yr + zq$; $\psi = yq + xr + zp$; $\theta = zr + xq + yr$ пропорциональна набору корней кубического уравнения, ассоциированного с искомым шенксовым. Прямой подсчет показывает, что:

$$\varphi\psi + \psi\theta + \theta\varphi = -3(u^2 + 3u + 9)(v^2 + 3v + 9)$$
$$\varphi\psi\theta = (u^2 + 3u + 9)(v^2 + 3v + 9)(9 - 3(u + v) - 2uv).$$

В частности, дискриминант циклического кубического полинома с корнями $\varphi, \psi, \theta$ будет равен $\left[27(u^2 + 3u + 9)(v^2 + 3v + 9)(u + v + 3)\right]^2$.

Для шенксова уравнения с параметром $u$ через $s_u$ обозначим $2u + 3$. В терминах $s$-параметра формула для умножения по Куммеру шенксовых полиномов окажется более привлекательной.

Рассмотрим два полинома, ассоциированных с шенксовыми с параметрами $u$ и $v$ соответственно: $X^3 - AX + A$ и $X^3 - BX + B$. Тогда $4A = s_1^2 + 27$, где $s_1 = s_u$ для параметра $u$, задающего первое шенксово уравнение и $4B = s_2^2 + 27$, где $s_2 = s_v$ для параметра $v$, задающего второе шенксово уравнение.

Тогда третье уравнение, ассоциированное с шенксовым, построенное по данным двум полиномам окажется следующим:

$$X^3 - \frac{108AB}{(s_1s_2 - 27)^2}X + \frac{108AB}{(s_1s_2 - 27)^2} = 0.$$

Совсем простая формула получается получается для $s$-параметра $s_3$, отвечающего новому шенксовому полиному.

В самом деле,

$$s_3^2 = a \cdot \frac{108AB}{(s_1s_2 - 27)^2} - 27 = 27 \cdot \frac{(s_1^2 + 27)(s_2^2 + 27) - (s_1s_2 - 27)^2}{(s_1s_2 - 27)^2}$$
$$= 729 \cdot \frac{(s_1 + s_2)^2}{(s_1s_2 - 27)^2},$$

так что в терминах $s$-параметров мы имеем формулу, аналогичную формуле тангенса суммы.

**Замечание 2.1.1.** Умножение по Куммеру шенксовых полиномов, как и циклических кубических полиномов общего вида никак не согласовано с соответствием Рамануджана и приведено нами для того, чтобы подчеркнуть как различие, так и сходство с операцией, приведенной в следующем разделе.

**2.2. Операция на циклических кубических полиномах.** Рассмотрим циклический кубический полином с корнями $a, b, c$, такими, что $abc = 1$. Такие циклические кубические полиномы в последующем будем называть *унимодулярными*.

**Определение 2.2.1.** *Ориентацией циклического кубического полинома мы будем называть выбор циклического порядка на его корнях или, что то же самое, выбор образующей группы Галуа его поля разложения.*

Далее мы будем толковать понятие циклического кубического полинома расширительно, называя так произвольные (а не только неприводимые) полиномы с коэффициентами из $\mathbb{Q}$, дискриминант которых является квадратом рационального числа. В том случае, когда такой полином имеет рациональный корень, и тем самым он раскладывается на линейные множители над $\mathbb{Q}$, мы (с тем, чтобы не привлекать аппарат алгебр Галуа) используем лишь первый вариант определения (порядок на корнях).

По теореме Гильберта 90 для ориентированного унимодулярного циклического кубического полинома с корнями $a, b, c$ найдутся $x, y, z \in \mathbb{Q}[a, b, c]$ такие, что $\dfrac{x}{y} = a$; $\dfrac{y}{z} = b$ и $\dfrac{z}{x} = c$. Для рациональных $a, b, c$ сослаться непосредственно на теорему Гильберта 90 не удается и следует воспользоваться выкладкой из ее доказательства, взяв $x = 1 + a + ab$; $y = 1 + b + bc$; $z = 1 + c + ca$. В случае, если $1 + a + ab = 0$, мы полагаем $y = (1 + a + ac)^{-1}$; $z = (1 + b + ba)^{-1}$; $x = (1 + c + cb)^{-1}$. Ясно, что равенства $1 + a + ab = 1 + a + ac = 0$ не могут случиться одновременно.

Обозначим через $D = xyz$ рациональное число, которое определено однозначно с точностью до умножения на куб. При изменении ориентации исходного полинома на противоположную $D$ заменяется на взаимно обратный элемент в группе $\mathbb{Q}^* / (\mathbb{Q}^*)^3$. Далее мы будем считать, что $D$ представляет нееденичный элемент в группе $\mathbb{Q}^* / (\mathbb{Q}^*)^3$, хотя этот вырожденный случай также интересен.

**Определение 2.2.2.** *В описанной ситуации будем называть исходный ориентированный унимодулярный циклический кубический полином подчиненным данному рациональному числу $D$ или же его классу в группе $\mathbb{Q}^* / (\mathbb{Q}^*)^3$.*

Напомним, что соответствие Рамануджана сопоставляло исходному унимодулярному циклическому кубическому полиному кубическую иррациональность $\left(\sqrt[3]{a} + \sqrt[3]{b} + \sqrt[3]{c}\right)^3 \in \mathbb{Q}\left[\sqrt[3]{D}\right]$. В этом разделе мы будем рассматривать *ориентированное соответствие Рамануджана.*

Считаем, что в поле $\mathbb{C}$ зафиксирован нетривиальный кубический корень из единицы $\omega = -\dfrac{1}{2} + i\dfrac{\sqrt{3}}{2}$. Ориентированному унимодулярному циклическому кубическому полиному с корнями $a, b, c$ мы сопоставляем упорядоченную тройку кубических иррациональностей, сопряженных друг с другом над $\mathbb{Q}$:

$$m_0 = \left(\sqrt[3]{a} + \sqrt[3]{b} + \sqrt[3]{c}\right)^3; m_1 = \left(\sqrt[3]{a} + \sqrt[3]{b}\omega^2 + \sqrt[3]{c}\omega\right)^3;$$
$$m_2 = \left(\sqrt[3]{a} + \sqrt[3]{b}\omega + \sqrt[3]{c}\omega^2\right)^3.$$

Кубические корни, как и ранее, предполагаются вещественными. Тогда замена ориентации в циклическом кубическом полиноме отвечает транспозиции $m_1 \leftrightarrow m_2$. Непосредственное раскрытие скобок показывает, что

$$m_0 = a + b + c + 6 + 3 \cdot \frac{x+y+z}{\sqrt[3]{xyz}} + 3\sqrt[3]{xyz} \cdot \left(\frac{1}{x} + \frac{1}{y} + \frac{1}{z}\right);$$
$$m_1 = a + b + c + 6 + 3 \cdot \frac{x+y+z}{\sqrt[3]{xyz}} \cdot \omega^2 + 3\sqrt[3]{xyz} \cdot \left(\frac{1}{x} + \frac{1}{y} + \frac{1}{z}\right)\omega;$$
$$m_2 = a + b + c + 6 + 3 \cdot \frac{x+y+z}{\sqrt[3]{xyz}} \cdot \omega + 3\sqrt[3]{xyz} \cdot \left(\frac{1}{x} + \frac{1}{y} + \frac{1}{z}\right)\omega^2.$$

Понятие подчиненности можно переформулировать в терминах $m_0$, $m_1$, $m_2$ следующим образом. Пусть для унимодулярного ориентированного циклического кубического полинома $m_0$ лежит в чисто кубическом расширении $\mathbb{Q}\left[\sqrt[3]{D}\right]$. Тогда данный ориентированный полином подчинен классу $D$ в $\mathbb{Q}^*/(\mathbb{Q}^*)^3$ (а не обратному классу), если образующая группы Галуа $\mathrm{Gal}\left(\mathbb{Q}\left[\sqrt[3]{D}, \omega\right]/\mathbb{Q}[\omega]\right)$, переводящая $\sqrt[3]{D}$ в $\sqrt[3]{D}\omega$ переставляет $m_0$, $m_1$, $m_2$ по циклу $m_0 \to m_1 \to m_2 \to m_0$.

**Замечание 2.2.3.** Норма элемента $m \in \mathbb{Q}\left[\sqrt[3]{D}\right]$, отвечающего по Рамануджану унимодулярному циклическому кубическому полиному, равна кубу рационального числа:

$$m_0 m_1 m_2 = (a + b + c - 3)^3.$$

**Лемма 2.2.4.** *Рассмотрим кубическую иррациональность* $m_0 = k_0 + k_1\sqrt[3]{D} + k_2\sqrt[3]{D^2} \in \mathbb{Q}\left[\sqrt[3]{D}\right]$ *вместе с сопряженными с ней элементами* $m_1, m_2$. *Предположим, что* $\mathrm{Nm}(m_0) = m_0 m_1 m_2$ *является кубом рационального числа. Тогда равенство* $m_0+m_1+m_2 = 3\sqrt[3]{\mathrm{Nm}(m_0)}$ *равносильно тому, что элемент* $m_0$ *является домноженным на рациональное число кубом двучленной кубической иррациональности, т.е.* $m_0 = r\cdot\left(\ell_0 + \ell_1\sqrt[3]{D} + \ell_2\sqrt[3]{D^2}\right)^3$ *с рациональными* $r$, $\ell_0$, $\ell_1$, $\ell_2$ *такими, что* $\ell_0\ell_1\ell_2 = 0$.

**Доказательство.** Данный факт есть иллюстрация рациональной параметризации особой плоской кубической кривой. Кубическая иррациональность $m_0$ определяет точку $\left[k_0 : k_1 : k_2 : \sqrt[3]{\mathrm{Nm}(m_0)}\right]$ на кубической поверхности в проективном пространстве $\mathbf{P}^3(\mathbb{Q})$, с введенной системой однородных координат $[X, Y, Z, T]$, заданной уравнением $X^3 + DY^3 + D^2Z^3 - 3DXYZ - T^3 = 0$. Плоскость $X = T$ высекает из кубической гиперповерхности кубическую кривую, у которой имеется особенность в точке $[1 : 0 : 0 : 1]$. Проводя секущие $Z = sY$ через особую точку в плоскости $X = T$ получим рациональную параметризацию при помощи параметра $s$:

$$(X^3 - T^3) + DY^3 + s^3D^2Y^3 - 3DsXY^2 = 0,$$

откуда, в силу того, что слагаемое в скобках обнуляется на рассматриваемой плоскости, получаем $X = \dfrac{Ds^3+1}{3s}Y$; $Z = sY$ и

$$\begin{aligned}\frac{3s}{Y}\left(X + Y\sqrt[3]{D} + Z\sqrt[3]{D^2}\right) &= (1 + Ds^3) + 3s\sqrt[3]{D} + 3s^2\sqrt[3]{D^2}\\ &= \left(1 + s\sqrt[3]{D}\right)^3. \end{aligned}$$ □

Обратное соответствие Рамануджана должно задаваться формулами

$$\begin{aligned} &a = \left(\frac{\sqrt[3]{m_0} + \sqrt[3]{m_1} + \sqrt[3]{m_2}}{3}\right)^3;\ b = \left(\frac{\sqrt[3]{m_0} + \omega\sqrt[3]{m_1} + \omega^2\sqrt[3]{m_2}}{3}\right)^3;\\ &c = \left(\frac{\sqrt[3]{m_0} + \omega^2\sqrt[3]{m_1} + \omega\sqrt[3]{m_2}}{3}\right)^3. \end{aligned} \tag{3}$$

В методической заметке [6] показано, что для любой кубической иррациональности $m_0$, норма которой является кубом и для которой нормировочный множитель $k = m_0 + m_1 + m_2 - 3\sqrt[3]{m_0 m_1 m_2}$ не равен нулю, $\dfrac{27a}{k}$; $\dfrac{27b}{k}$; $\dfrac{27c}{k}$ окажутся корнями унимодулярного циклического кубического полинома или же рациональными числами. Обозначим через $\mathcal{M}_D$ подмножество в факторгруппе $\mathbb{Q}\left[\sqrt[3]{D}\right]^* / \mathbb{Q}^*$, состоящее из классов тех кубических иррациональностей, норма которых является кубом. Через $\mathcal{Z}_D \subset \mathcal{M}_D$ обозначим те классы $\overline{m}_0$, для которых $m_0 + m_1 + m_2 = 3\sqrt[3]{m_0 m_1 m_2}$. Таким образом соответствие Рамануджана задает биекцию между множеством $\mathcal{M}_D \setminus \mathcal{Z}_D$ и множеством ориентированных циклических кубических полиномов, подчиненных $D$.

Вместо ориентированных унимодулярных циклических кубических полиномов можно рассматривать циклические кубические полиномы, у которых свободный член является кубом, рассматривая их с точностью до пропорциональности, т.е. домножения корней на одно и то же рациональное число.

Включим в рассмотрение теперь и циклические кубические полиномы с нулевым свободным членом, но отличные от $X^3$. Такой полином с зафиксированной ориентацией $(0ab)$ его корней будем называть подчиненным классу $\dfrac{a}{b} \in \mathbb{Q}^* / (\mathbb{Q}^*)^3$. Полином с единственным ненулевым корнем будем считать подчиненным любому рациональному $D \in \mathbb{Q}^*$. Обозначим через $\mathcal{P}_D$ множество классов пропорциональности ориентированных циклических кубических полиномов, подчиненных данному $D \in \mathbb{Q}^* / (\mathbb{Q}^*)^3$.

Тогда соответствие Рамануджана биективно отображает $\mathcal{P}_D$ на $\mathcal{M}_D$. Основной результат текущего раздела состоит в описании операции на $\mathcal{P}_D$, которая при соответствии Рамануджана переходит в умножение кубических иррациональностей.

**Предложение 2.2.5.** *Рассмотрим два полинома, классы пропорциональности которых лежат в $\mathcal{P}_D$, и наборы их корней $(abc)$ и $(a'b'c')$ циклически упорядочены. Рассмотрим тройку*

$$\begin{gathered}\left(\sqrt[3]{aa'} + \sqrt[3]{bc'} + \sqrt[3]{cb'}\right)^3;\ \left(\sqrt[3]{cc'} + \sqrt[3]{ba'} + \sqrt[3]{ab'}\right)^3;\\ \left(\sqrt[3]{bb'} + \sqrt[3]{ca'} + \sqrt[3]{ac'}\right)^3,\end{gathered} \tag{4}$$

*циклически упорядоченную слева направо.*

*Тогда полином с указанными корнями имеет рациональные коэффициенты и с введенным циклическим порядком на корнях задает элемент из $\mathcal{P}_D$. Циклическая перестановка корней $(a, b, c)$ приводит к циклической перестановке трех элементов, определенных в* (4).

**Доказательство.** Рассмотрим случай $abc \neq 0$ и $a'b'c' \neq 0$, оставив читателю разбор случая с наличием нулевых корней. Тогда мы можем считать, что $abc = a'b'c' = 1$. Сохраняя введенные выше обозначения для $x, y, z, x', y', z'$, прямым раскрытием скобок в первом выражении из (4) получаем:

$$\widetilde{a} = aa' + bc' + cb' + 6 + \frac{x}{y'} + \frac{x'}{y} + \frac{y}{x'} + \frac{y'}{x} + \frac{z'}{z} + \frac{z}{z'};$$

во втором выражении получаем:

$$\widetilde{b} = cc' + ab' + ba' + 6 + \frac{x}{z'} + \frac{z'}{x} + \frac{x'}{z} + \frac{z}{x'} + \frac{y}{y'} + \frac{y'}{y};$$

в третьем выражении получаем

$$\widetilde{c} = bb' + ca' + ac' + 6 + \frac{z}{y'} + \frac{y'}{z} + \frac{z'}{y} + \frac{y}{z'} + \frac{x'}{x} + \frac{x}{x'}.$$

Так что $\widetilde{a}$, $\widetilde{b}$, $\widetilde{c}$ – это корни многочлена с рациональными коэффициентами. Очевидно,

$$\left(\sqrt[3]{\widetilde{a}} + \sqrt[3]{\widetilde{b}} + \sqrt[3]{\widetilde{c}}\right)^3 = (\sqrt[3]{a} + \sqrt[3]{b} + \sqrt[3]{c})^3(\sqrt[3]{a'} + \sqrt{b'} + \sqrt[3]{c'})^3,$$

так что построенная операция отвечает умножению кубических иррациональностей в $\mathbb{Q}\left[\sqrt[3]{D}\right]$. Проверим, что с введенной ориентацией циклический кубический полином с корнями $\widetilde{a}$, $\widetilde{b}$, $\widetilde{c}$ будет подчинен $D$. Для этого в силу переформулировки определения ориентации в терминах $m_0, m_1, m_2$, данной перед замечанием 2.2.3, достаточно проверить, что

$$\left(\sqrt[3]{\widetilde{a}} + \sqrt[3]{\widetilde{b}}\omega^2 + \sqrt[3]{\widetilde{c}}\omega\right)^3 = m_1 \cdot m_1',$$

где $m_1 = \left(\sqrt[3]{a} + \sqrt[3]{b}\omega^2 + \sqrt[3]{c}\omega\right)^3$ и $m_1' = \left(\sqrt[3]{a'} + \sqrt[3]{b'}\omega^2 + \sqrt[3]{c'}\omega\right)^3$. Что также непосредственно проверяется. □

**Замечание 2.2.6.** Интересен случай, когда $a$ и $a'$ являются кубами в поле $\mathbb{Q}[a, b, c]$ и поле $\mathbb{Q}[a', b', c']$ соотвественно. В этом случае циклические кубические полиномы подчинены $D = 1$, а этот случай мы не разбираем в подробностях. Формулы (4) превращаются в формулы для перемножения циклических кубических расширений, которые мы приводили в разделе 2.1. А соответствие Рамануджана будет сопоставлять циклическому кубическому расширению элемент в алгебре $\mathbb{Q}[X]/(X^3 - 1) = \mathbb{Q} \oplus \mathbb{Q}[\omega]$, являющийся кубом. На этом пути можно снова получить параметризацию (1) циклических кубических расширений.

**Замечание 2.2.7.** Описанная операция, примененная к шенксовым полиномам, даже и подчиненным одному и тому же $D$, вообще говоря, выводит из класса шенксовых полиномов. Мы считаем, что удовлетворительная модификация этой операции, определенная на шенксовых полиномах, приведена нами в следующем разделе.

## §3. Основной раздел

**3.1. Взаимная точка.** Кубическая иррациональность $x + y\sqrt[3]{D} + z\sqrt[3]{D^2}$, норма которой над $\mathbb{Q}$ является точным кубом и равна $t^3$, задает точку $[x : y : z : t]$ на норменной кубической поверхности в $\mathbf{P}^3(\mathbb{Q})$

$$X^3 + DY^3 + D^2Z^3 - 3DXYZ = T^3. \tag{5}$$

Умножение кубических иррациональностей задает операцию на точках кубической поверхности. Кроме того, на точках кубической поверхности имеется частично определенная классическая операция “проведения секущей”, которая широко популяризована в книге [5].

Наша гипотеза состоит в том, что эти две операции согласованы по модулю кубов, однако мы не приводим гипотетическую формулировку. Тем не менее мы приводим два результата, которые могут оказаться частными случаями искомой гипотетической формулировки.

**Предложение 3.1.1.** *Пусть* $P = [x : y : z : t]$ *– это точка на норменной кубической поверхности* (5), *такая, что* $x \neq t$. *Рассмотрим третью точку пересечения с поверхностью* (5) *прямой, проведенной через* $0 = [1 : 0 : 0 : 1]$ *и* $P$. *Обозначим её через* $P'$. *Тогда*

$$P' = \left[-t + D\frac{yz}{x-t} : y : z : -x + D\frac{yz}{x-t}\right].$$

*При этом произведение кубических иррациональностей, отвечающих точкам $P$ и $P'$ лежит в $\mathbb{Q}^* \cdot \mathbb{Q}\left[\sqrt[3]{D}\right]^*$, т.е. является точным кубом с точностью до домножения на рациональное число.*

**Доказательство.** Вычисление третьей точки пересечения прямой с поверхностью мы опустим. Прямой подсчет показывает, что имеет место тождество:

$$3(x + y\sqrt[3]{D} + z\sqrt[3]{D^2})\Big(-t(x-t) + Dyz + (x-t)(y\sqrt[3]{D} + z\sqrt[3]{D^2})\Big)$$
$$= \Big((x-t) + y\sqrt[3]{D} + z\sqrt[3]{D^2}\Big)^3 - (x^3 + Dy^3 + D^2z^3 - 3Dxyz - t^3). \square$$

**Замечание 3.1.2.** Если точка $P$ отвечает по Рамануджану унимодулярному циклическому кубическому полиному с корнями $a, b, c$, то точка $P'$ отвечает по Рамануджану циклическому кубическому полиному с корнями $\frac{1}{a}$; $\frac{1}{b}$; $\frac{1}{c}$ – см. заметку [6]. Это означает частичную согласованность умножения в циклическом кубическом расширении с операцией на кубической поверхности, заданной проведением секущих.

**3.2. Шенксов случай.** Другая операция, которую мы рассмотрим только для шенксовых расширений, задается сложением точек на кубической кривой.

Зафиксируем $D$, не являющееся кубом. Мы будем рассматривать шенксовы полиномы $X^3 - uX^2 - (u+3)X - 1$ с параметром $s = 2u+3$, для которых $\frac{1}{4}(s^2+27) = Dt^3$, т.е. полиномы, подчиненные $D$ в том смысле, как это было определено в разделе 1. Это условие означает, что по Рамануджану данному шенксову полиному соответствует двучленная кубическая иррациональность из поля $\mathbb{Q}\left[\sqrt[3]{D}\right]$.

Напомним, что если $a, b, c$ – корни шенксова полинома $X^3 - uX^2 - (u+3)X - 1$, то

$$\sqrt[3]{a} + \sqrt[3]{b} + \sqrt[3]{c} = \sqrt[3]{u + 6 - 3\sqrt[3]{u^2 + 3u + 9}}.$$

Другими словами, $[u+6 : -u+3 : 3]$ – это точка на кубической кривой $X^3 + Y^3 = DT^3$, где $D = u^2 + 3u + 9$.

Далее мы рассматриваем лишь двучленные кубические иррациональности $x - z\sqrt[3]{D}$ с нормой $-y^3$, которые отвечают точкам на эллиптической кривой $X^3 + Y^3 = DZ^3$, где за начало отсчета выбрана точка $[1 : -1 : 0]$.

**Теорема 3.2.1.** *Пусть $P$, $Q$ – две точки на указанной кривой, а $m_P, m_Q$ – нормализованные кубические иррациональности, им отвечающие. Тогда $\dfrac{m_{P+Q}}{m_P \cdot m_Q}$ – полный куб в $\mathbb{Q}\left[\sqrt[3]{D}\right]$.*

**Доказательство.** Рассмотрим сначала случай, когда $P = Q$. Пусть $P = [x : y : t]$. Тогда $P + P = [y(x^3 + Dt^3) : -x(y^3 + Dt^3) : t(y^3 - x^3)]$, где формула взята из заметки Сильвермана [7, p. 335]

Мы ожидаем, что $m_{P+P}$ и $m_{P'}$ отличаются умножением на куб. И в самом деле, $m_{P'} = y - t\sqrt[3]{D}$. Вычислим $m_{P'} \cdot (y + t\sqrt[3]{D})^3$:

$$\begin{aligned}(y - t\sqrt[3]{D})(y + t\sqrt[3]{D})^3 &= (y^2 - t^2\sqrt[3]{D^2})(y^2 + 2yt\sqrt[3]{D} + t^2\sqrt[3]{D^2})\\ &= y^4 - 2yDt^3 + (2y^3 - Dt^3)t\sqrt[3]{D}.\end{aligned}$$

Учитывая соотношение $x^3 + y^3 = At^3$ мы видим, что эта кубическая иррациональность отвечает точке $P + P$.

Теперь перейдем к общему случаю, $P \neq Q$. Пусть $P = [x : y : 1]$, $Q = [p : q : 1]$. Тогда $P + Q = [D(y - q) - xp(yp - xq) : (D(x - p) - yq(xq - yp) : xp(x - p) + yq(y - q)]$.

Мы хотим проверить, что кубическая иррациональность

$$\ell = (X - \sqrt[3]{D})(p - \sqrt[3]{D})(D(x-p) - yq(xq - yp) - (xp(x-p) + yq(y-q))\sqrt[3]{D})$$

является полным кубом, домноженным на рациональное число.

Норму $\ell$ легко вычислить как произведение норм сомножителей: $\mathrm{Nm}(\ell) = -y \cdot q \cdot (D(y - q) - xp(yp - xq))$.

$\mathrm{Tr}(\ell)$ – это утроенный коэффициент перед единицей после раскрытия скобок. Он равен

$$\begin{aligned}&xp(D(x - p) - y * q(xq - yp)) - D(xp(x - p) + yq(y - q))\\ &\qquad = yq(xp(yp - xq) - D(y - q)).\end{aligned}$$

Таким образом, мы попали в условия леммы 2.2.4, и теорема доказана. □

**Замечание 3.2.2.** Шенксовы полиномы $X^3 - uX^2 - (u+3)X - 1$, подчиненные $D$, имеют параметр $u$, удовлетворяющий условию $u^2 + 3u + 9 =$

$Dx^3$ для некоторого рационального $x$. Другими словами, такой шенксов полином отвечает точке на эллиптической кривой $y^2+3u+9=Dx^3$. Соответствие Рамануджана переводит сложение точек на этой эллиптической кривой в сложение точек на кривой Ферма $X^3+Y^3=DZ^3$.

Желательно было бы описать эту операцию на шенксовых полиномах в терминах их корней, но нам пока не удалось это сделать.

## Список литературы

1. И. А. Крепкий, К. И. Пименов, *Формулы Рамануджана и элементарная теория Галуа.* — Вестник СПбГУ. Серия 1. Математика, Механика, Астрономия. **2(60)б**, No. 4 (2015), 553–563.
2. D. Shanks, *The simplest cubic number fields.* — Math. Comp. **28** (1974), 1137–1152.
3. B. C. Berndt, *Ramanujan's Notebooks*, Part IV. New York: Springer-Verlag, 1994.
4. Н. Г. Чеботарев, *Теория Галуа.* — М.-Л.: Гл. ред. общетехн. лит. и номографии, 1936.
5. Ю. И. Манин, *Кубические формы.* — Алгебра, геометрия и арифметика. М.: Наука, 1972.
6. M. Antipov, K. Pimenov, *On Ramanujan cubic denesting formulae.* — In preparation.
7. J. G. Silverman, *Taxicabs and sums of two cubes.* — Amer. Math. Monthly, **100**, No. 4 (1993), pp. 331–340

Antipov M. A., Pimenov K. I. On certain multiplicative structures on cubic extensions.

Multiplicative properties of a certain correspondence between elements in cyclic cubic extension of rational number field and elements in adjusted pure cubic extensions are investigated. Shanks cubic polynomial case is considered to connect multiplication of pure cubic irrationals with a point summation on an associated elliptic curve.

С.-Петербургский
государственный университет
Университетский пр. 28, Петродворец,
198504 Санкт-Петербург, Россия
*E-mail*: hyperbor@list.ru
*E-mail*: k.pimenov@spbu.ru

Поступило 25 июня 2018 г.