МАТЕМАТИКА

Челябинский физико-математический журнал. 2018. Т. 3, вып. 3. С. 253–275.

УДК 512.552.7 DOI: 10.24411/2500-0101-2018-13301

ЛОКАЛЬНЫЕ ЕДИНИЦЫ ЦЕЛОЧИСЛЕННОГО ГРУППОВОГО КОЛЬЦА ЦИКЛИЧЕСКОЙ ГРУППЫ ПОРЯДКА 64 ДЛЯ ХАРАКТЕРА С ПОЛЕМ ХАРАКТЕРА $\mathbb{Q}_{64}$

Р. Ж. Алеев[1,2,a], **О. В. Митина**[1,2,b], **Т. А. Ханенко**[1,c]

[1] *Челябинский государственный университет, Челябинск, Россия*
[2] *Южно-Уральский государственный университет (национальный исследовательский университет), Челябинск, Россия*
[a] *aleev@csu.ru,* [b] *ovm@csu.ru,* [c] *tanja_1110_94@mail.ru*

Работа посвящена исследованию единиц целочисленного группового кольца циклической группы порядка 64. Группы единиц целочисленных групповых колец циклических групп порядков 2 и 4 тривиальны, для порядка 8 эта группа хорошо известна, для циклической группы порядка 16 — описана ранее. Исследование единиц целочисленного группового кольца циклической группы порядка 64 проводится в терминах локальных единиц, определяемых характерами циклической группы порядка 64 и единицами кольца целых кругового поля $\mathbb{Q}_{64}$, полученного присоединением к полю рациональных чисел примитивного корня из 1 степени 64. Важнейшую роль среди локальных единиц играют единицы для характера с полем характера $\mathbb{Q}_{64}$, поскольку они обеспечивают возможность индуктивного подхода к описанию групп единиц целочисленных групповых колец циклических 2-групп. Отметим, что ранее прямыми вычислениями авторы получили описание локальных единиц для характера с полем характера $\mathbb{Q}_{32}$ целочисленного группового кольца циклической группы порядка 32. Поэтому следующим естественным шагом является изучение локальных единиц для характера с полем характера $\mathbb{Q}_{64}$ целочисленного группового кольца циклической группы порядка 64. Для достижения поставленных целей разработан новый подход, который может быть применён для групп единиц целочисленных групповых колец циклических 2-групп порядка, большего чем 64.

Ключевые слова: *групповое кольцо, единица группового кольца, циклическая группа, круговое поле, целочисленное групповое кольцо.*

Введение

Эта работа продолжает статьи [1–3], посвящённые изучению индуктивного подхода к описанию групп единиц целочисленных групповых колец циклических 2-групп.

В работе [4, Определение 1] для любого неприводимого характера χ конечной группы G и любой единицы λ кольца целых поля характера $\mathbb{Q}(\chi)$ введено понятие

Работа выполнена при поддержке Правительства РФ (Постановление № 211 от 16.03.2013 г.), соглашение № 02.A03.21.0011, и при частичной поддержке Лаборатории квантовой топологии Челябинского госуниверситета (грант Правительства РФ № 14.Z50.31.0020).

локальной единицы $u_\chi(\lambda)$, которая в общем случае является центральной единицей рациональной групповой алгебры $\mathbb{Q}G$. Там же [4, Теорема 1] доказано, что в рассматриваемом случае найдётся такое натуральное число l, что $u_\chi(\lambda^l)$ является центральной единицей целочисленного группового кольца $\mathbb{Z}G$. На основе этого результата с использованием теоремы 2 из [5] в доказательстве теоремы 3 из [4] показано, что группа центральных единиц целочисленного группового кольца $\mathbb{Z}G$ состоит из произведений локальных единиц, которые определяются множеством представителей классов алгебраически сопряжённых характеров.

Применение указанных результатов в случае конечных циклических 2-групп даёт нам следующее. Пусть $G = \langle x \rangle$ — циклическая группа порядка 2^n, $n \in \mathbb{N}$, и ζ_{2^n} — примитивный (комплексный) корень из 1 степени 2^n. Для любого $j \in \{0, 1, \ldots, 2^n - 1\}$ определим комплексный неприводимый характер χ_j группы G по правилу $\chi_j(x^k) = \zeta_{2^n}^{jk}$ для любого $k \in \{0, 1, \ldots, 2^n - 1\}$. Ясно, что $\chi_0 = 1_G$ — главный характер. Из леммы 3 в [6] стандартными рассуждениями получим, что множеством представителей классов алгебраически сопряжённых характеров является множество $\mathrm{Irr}(G, alc) = \{1_G, \chi_1, \chi_2, \chi_4, \ldots, \chi_{2^s}, \ldots, \chi_{2^{n-1}}\}$. Поэтому для любой единицы u целочисленного группового кольца $\mathbb{Z}G$ имеем

$$u = u_{1_G}(\beta_0) \prod_{s=0}^{n-1} u_{\chi_{2^s}}(\beta_{2^s}),$$

где $\beta_0 \in \{1, -1\}$ и β_{2^s} — подходящая единица кольца целых поля характера χ_{2^s}. Отметим, что $\mathbb{Q}(\chi_{2^s}) = \mathbb{Q}(\zeta_{2^n}^{2^s})$ для всякого $s \in \{0, 1, \ldots, n-1\}$. Любая нормализованная единица v целочисленного группового кольца $\mathbb{Z}G$ имеет вид

$$v = \prod_{s=0}^{n-1} u_{\chi_{2^s}}(\beta_{2^s}),$$

где β_{2^s} — подходящая единица кольца целых поля характера $\mathbb{Q}(\chi_{2^s})$ для всякого $s \in \{0, 1, \ldots, n-1\}$.

Более точно. Пусть K — подполе поля комплексных чисел $\mathbb{C}$ и $\bar{\mathbb{Z}}$ — кольцо всех целых алгебраических чисел. Тогда обозначим через $\mathrm{Int}(K) = K \cap \bar{\mathbb{Z}}$ — кольцо целых поля K, через $\mathrm{Un}(\mathrm{Int}(K))$ — группу единиц кольца $\mathrm{Int}(K)$, через $\mathrm{V}(\mathbb{Z}G)$ — нормализованную группу единиц кольца $\mathbb{Z}G$. В этих обозначениях получим, что

$$\mathrm{V}(\mathbb{Z}G) \leqslant \prod_{s=0}^{n-1} \langle u_{\chi_{2^s}}(\beta_{2^s}) \mid \beta_{2^s} \in \mathrm{Un}(\mathrm{Int}(\mathbb{Q}(\chi_{2^s}))) \rangle .$$

С другой стороны, предложение 1 из [2] описывает периодическую часть группы $\mathrm{V}(\mathbb{Z}G)$. Также из этого результата следует, что множество

$$W = \left\{ \prod_{s=1}^{n-1} u_{\chi_{2^s}}(\beta_{2^s}) \in \mathrm{V}(\mathbb{Z}G) \mid \beta_{2^s} \in \mathrm{Un}(\mathrm{Int}(\mathbb{Q}(\chi_{2^s}))),\ s \in \{1, \ldots, n-1\} \right\}$$

есть подгруппа без кручения группы $\mathrm{V}(\mathbb{Z}G)$. Отметим, что подгруппа W изоморфна подгруппе группы единиц группового кольца $\mathbb{Z}\langle x^2 \rangle$, что позволяет применять индукцию. Оппонентом подгруппы W является подгруппа

$$W_1 = \langle u_{\chi_1}(\beta_1) \mid \beta_1 \in \mathrm{Un}(\mathrm{Int}(\mathbb{Q}(\chi_1))) \rangle ,$$

а произведение $W_1 \times W$ является подгруппой конечного индекса группы $\mathrm{V}(\mathbb{Z}G)$. Следует отметить, что для дальнейших приложений будет более удобной некоторая подгруппа $V_1 \leqslant W_1$, которую введём позднее, ибо её определение требует дополнительных понятий и обозначений.

Описание подгруппы W_1 было получено в статьях [2] и [1] для циклических групп G порядков 16 и 32. В общем случае описание получилось весьма длинным и довольно запутанным. Следует указать, что в силу определения единицы $u_{\chi_1}(\beta_1)$ всё сводится к изучению свойств элемента $\beta_1 \in \mathrm{Un}(\mathrm{Int}(\mathbb{Q}(\chi_1)))$. Поэтому было решено рассмотреть как модель случай циклической группы порядка 64, когда можно реально проследить все существенные моменты, возникающие при изучении подгруппы W_1 в общем случае.

Итак, в дальнейшем будет изучаться подгруппа W_1 группы единиц целочисленного группового кольца циклической группы порядка 64*, фактически будет изучаться группа единиц* $\mathrm{Un}(\mathbb{Z}[\zeta_{64}])$.

Круговое поле, полученное присоединением ζ_{2^n}, будем обозначать как $\mathbb{Q}(\zeta_{2^n})$ или $\mathbb{Q}_{2^n}$. Если циклическая группа G имеет порядок 64, то в качестве полей характеров будут круговые поля $\mathbb{Q}_{2^k}$ для $k \leqslant 6$, причём может встретиться любое такое k.

1. Круговое поле $\mathbb{Q}_{64}$

1.1. Общие сведения

Обозначение. Для удобства положим $\zeta_{64} = \alpha$ и, не ограничивая общности, можем считать, что

$$\alpha = e^{i\frac{2\pi}{64}} = \cos\frac{2\pi}{64} + i\sin\frac{2\pi}{64}.$$

Тогда, в частности, $\alpha^{32} = -1$, $\alpha^{16} = i$, $\alpha^8 = \frac{\sqrt{2}}{2}(1+i)$.

Хорошо известны следующие результаты.

Лемма 1. 1. *Круговое поле $\mathbb{Q}(\alpha)$ равно $\mathbb{Q}(\alpha) = \{f(\alpha) \mid f \in \mathbb{Q}[\![31]\!][t]\}$, где $\mathbb{Q}[\![31]\!][t]$ — множество (точнее, подпространство) всех многочленов с рациональными коэффициентами степени не выше* 31*. Иными словами, элементы $1, \alpha, \alpha^2, \ldots, \alpha^{31}$ образуют базис множества $\mathbb{Q}(\alpha)$ как векторного пространства над полем рациональных чисел $\mathbb{Q}$.*

2. *Группа Галуа $\mathrm{Gal}(\mathbb{Q}_{64})$ кругового поля $\mathbb{Q}_{64}$, или, равносильно, группа автоморфизмов имеет порядок, равный степени расширения $\mathbb{Q}(\alpha)$ над $\mathbb{Q}$:*

$$|\mathrm{Gal}(\mathbb{Q}_{64})| = [\mathbb{Q}(\alpha) : \mathbb{Q}] = 32.$$

3. *Более того, всякий автоморфизм σ поля $\mathbb{Q}_{64}$ является расширением по линейности отображения*

$$\sigma : \alpha \mapsto \alpha^k \text{ для подходящего нечётного } k \in \{1, 3, \ldots, 63\},$$

т. е. для любого элемента $\beta \in \mathbb{Q}_{64}$

$$\beta = b_{31}\alpha^{31} + \cdots + b_1\alpha + b_0, \text{ где } \{b_{31}, \ldots, b_1, b_0\} \subset \mathbb{Q}$$

имеем

$$\sigma(\beta) = b_{31}\sigma(\alpha^{31}) + \cdots + b_1\sigma(\alpha) + b_0 = b_{31}\alpha^{31k} + \cdots + b_1\alpha^k + b_0.$$

Таким образом, группа Галуа поля $\mathbb{Q}_{64}$ *имеет вид*

$$\mathrm{Gal}(\mathbb{Q}_{64}) = \left\{\sigma_k \mid \sigma_k(\alpha) = \alpha^k,\ k \in \{1, 3, \ldots, 63\}\right\}.$$

4. *Кольцом целых кругового поля* $\mathbb{Q}(\alpha) = \mathbb{Q}_{64}$ *является кольцо*

$$\mathbb{Z}[\alpha] = \{f(\alpha) \mid f \in \mathbb{Z}[\![31]\!][t]\},$$

где $\mathbb{Z}[\![31]\!][t]$ *— множество (точнее, конечно порождённая подгруппа) всех многочленов с целыми коэффициентами степени не выше* 31.

5. *Из пунктов* 1 *и* 4 *получим, что* $\{1, \alpha, \alpha^2, \ldots, \alpha^{31}\}$ *— целый базис расширения* $\mathbb{Q}(\alpha)/\mathbb{Q}$.

Определение 1. Для любого натурального n множество

$$2\mathbb{Z}[\zeta_{2^n}] = \{2\rho \mid \rho \in \mathbb{Z}[\zeta_{2^n}]\}$$

является идеалом в кольце $\mathbb{Z}[\zeta_{2^n}]$. Поэтому возникает *сравнимость элементов кольца* $\mathbb{Z}[\zeta_{2^n}]$ *по модулю этого идеала.* Для краткости будем писать для элементов $\rho, \sigma \in \mathbb{Z}[\zeta_{2^n}]$

$$\rho \equiv \sigma \pmod 2,$$

если $\rho \equiv \sigma \pmod{2\mathbb{Z}[\zeta_{2^n}]}$, т. е. $\rho \in \sigma + 2\mathbb{Z}[\zeta_{2^n}]$.

Замечание 1. В силу утверждения 5 леммы 1 имеем, что

$$2\mathbb{Z}[\alpha] = \left\{2\sum_{j=0}^{31} b_j\alpha^j \mid b_j \in \mathbb{Z},\ j \in \{0, 1, \ldots, 31\}\right\}.$$

В частности, получим, что для элемента $b = \sum_{j=0}^{31} b_j\alpha^j \in \mathbb{Z}[\alpha]$ сравнение

$$b \equiv 1 \pmod 2$$

выполняется тогда и только тогда, когда b_0 — нечётное число, b_j — чётное число для $j \in \{1, 2, \ldots, 31\}$.

1.2. Три полезных последовательности

1.2.1. Последовательность $\{s_j\}_{j\in\mathbb{Z}}$

Обозначение. Для любого целого j положим

$$s_j = \alpha^j + \alpha^{-j} = 2\cos\frac{\pi}{32}j.$$

Замечание 2. Для любого целого j число s_j инвариантно относительно действия автоморфизма кругового поля, индуцированного отображением $\alpha \longmapsto \alpha^{-1}$, и, очевидно, состоит из действительных чисел, т. е. $\{s_j\}_{j\in\mathbb{Z}} \subset \mathbb{R}$.

Свойства последовательности $\{s_j\}_{j\in\mathbb{Z}}$ изучены в лемме 2 работы [1], откуда для последующих применений извлечём очевидное, но весьма полезное следствие.

Лемма 2. *Последовательность* $\{s_j\}_{j\in\mathbb{Z}}$ *по модулю* 2 *периодична с периодом* 32 *и имеет следующие свойства.*

1. $s_0 \equiv s_{16} \equiv 0 \pmod 2$, $s_8 \equiv s_{24} \equiv \sqrt{2} \pmod 2$.

2. *Набор* $(s_0, s_1, \ldots, s_{32})$ *симметричен относительно центра, т. е. для всех* $j \in \{0, 1, 2, \ldots, 16\}$ $s_{32-j} \equiv s_j \pmod 2$. *Таким образом, по модулю* 2 *имеем следующие значения элементов последовательности* s_j :

j	0	1	...	7	8	9	...	15	16	17	...	23	24	25	...	31	32
s_j	0	s_1	...	s_7	$\sqrt{2}$	s_9	...	s_{15}	0	s_{15}	...	s_9	$\sqrt{2}$	s_7	...	s_1	0

3. *Для любых целых* j *и* l $s_j s_l = s_{j+l} + s_{l-j}$, *в частности,* $s_j^2 \equiv s_{2j} \pmod 2$ *и*

$$s_0^2 \equiv s_{16}^2 \equiv s_8^2 \equiv s_{24}^2 \equiv 0 \pmod 2.$$

1.2.2. Последовательность $\{t_j\}_{j\in\mathbb{Z}}$

Обозначение. Для любого целого j положим

$$t_j = 1 + s_j + s_{2j}.$$

Свойства последовательности $\{t_j\}_{j\in\mathbb{Z}}$ изучены в лемме 3 работы [1], которая влечёт очевидное, но весьма полезное следствие.

Лемма 3. *Последовательность* $\{t_j\}_{j\in\mathbb{Z}}$ *по модулю* 2 *периодична с периодом* 32 *и имеет следующие свойства.*

0. *Для любого целого* j *имеем* $t_j = 1+\alpha^j+\alpha^{-j}+\alpha^{2j}+\alpha^{-2j} = 1+2\cos\frac{\pi}{32}j+2\cos\frac{\pi}{32}(2j)$.

1. $t_0 \equiv t_{16} \equiv 1 \pmod 2$, $t_8 \equiv t_{24} \equiv 1 + \sqrt{2} \pmod 2$.

2. $t_{32-j} \equiv t_j \pmod 2$ *для любого* $j \in \{0, 1, 2, \ldots, 31\}$. *Таким образом, по модулю* 2 *имеем следующие значения элементов последовательности* t_j :

j	0	1	...	7	8	9	...	15	16	17	...	23	24	...	31	32
t_j	1	t_1	...	t_7	$1+\sqrt{2}$	t_9	...	t_{15}	1	t_{15}	...	t_9	$1+\sqrt{2}$	...	t_1	1

3. *Для любого целого* j

$$t_j^2 \equiv t_{2j} \pmod 2, \quad t_0^2 \equiv t_8^2 \equiv t_{16}^2 \equiv t_{24}^2 \equiv 1 \pmod 2.$$

1.2.3. Последовательность $\{r_j\}_{j\in\mathbb{Z}}$

Обозначение. Для любого целого j положим $r_j = s_j + s_{16-j}$.

Замечание 3. Ясно, что

$$r_j = s_j + s_{16-j} = 2\cos\frac{\pi}{32}j + 2\cos\frac{\pi}{32}(16-j) =$$
$$= 2\cos\frac{\pi}{32}j + 2\cos\left(\frac{\pi}{2} - \frac{\pi}{32}j\right) = 2\cos\frac{\pi}{32}j + 2\sin\frac{\pi}{32}j.$$

Лемма 4. *Последовательность* $\{r_j\}_{j\in\mathbb{Z}}$ *периодична с периодом* 64. *Кроме того, отрезок* $(r_0, \ldots, r_{63})$ *последовательности* $\{r_j\}_{j\in\mathbb{Z}}$ *разбивается на части*:

$$\{r_0 = 2\} \cup R_0 = \left(r_1, \ldots, r_8 = 2\sqrt{2}, \ldots, r_{15}\right),$$
$$\{r_{16} = 2\} \cup R_1 = \left(r_{17}, \ldots, r_{24} = 0, \ldots, r_{31}\right),$$
$$\{r_{32} = -2\} \cup R_2 = \left(r_{33}, \ldots, r_{40} = -2\sqrt{2}, \ldots, r_{47}\right),$$
$$\{r_{48} = -2\} \cup R_3 = \left(r_{49}, \ldots, r_{56} = 0, \ldots, r_{63}\right).$$

Упорядоченные наборы R_0, R_1, R_2 *и* R_3 *имеют следующие свойства.*
1. $R_2 = -R_0$ *и* $R_3 = -R_1$.

2. *Для любого целого числа* j $r_{16+j} = r_j - 2s_{16-j} = r_{-j}$.

3. *Каждый из наборов* R_0 *и* R_2 *центрально симметричен, т. е. для любого* $k \in \{0, 2\}$

$$R_k = \left(r_{16k+1}, \ldots, r_{8(2k+1)-1}, r_{8(2k+1)2}, r_{8(2k+1)-1}, \ldots, r_{16k+1}\right).$$

Каждый из наборов R_1 *и* R_3 *центрально антисимметричен, т. е. для любого* $k \in \{1, 3\}$

$$R_k = \left(r_{16k+1}, \ldots, r_{8(2k+1)-1}, 0, -r_{8(2k+1)-1}, \ldots, -r_{16k+1}\right).$$

Доказательство. Из леммы 2 в [1] следует, что последовательность $\{r_j\}_{j\in\mathbb{Z}}$ периодична с периодом 64.

Сначала вычислим r_{8k} для $k \in \{0, 1, \ldots, 7, \}$. В самом деле, по лемме 2 из [1] получим равенства

$$\begin{aligned}
r_0 &= s_0 + s_{16} = 2 + 0 = 2,\\
r_{32} &= s_{32} + s_{16} = -2 - 0 = -2,\\
r_{16} &= s_{16} + s_0 = 0 + 2 = 2,\\
r_{48} &= s_{48} + s_{32} = 0 - 2 = -2,\\
r_8 &= s_8 + s_8 = 2s_8 = 2\sqrt{2},\\
r_{24} &= s_{24} + s_8 = -\sqrt{2} + \sqrt{2} = 0,\\
r_{40} &= s_{40} + s_{24} = s_{24} + s_{24} = -\sqrt{2} - \sqrt{2} = -2\sqrt{2},\\
r_{56} &= s_{56} + s_{40} = s_8 + s_{24} = \sqrt{2} - \sqrt{2} = 0.
\end{aligned}$$

Исследуем свойства наборов R_0, R_1, R_2 и R_3.

1. Рассмотрим произвольный элемент r из $R_2 \cup R_3$. Тогда найдётся такой номер $j \in \{1, 2, \ldots, 15\} \cup \{17, 18, \ldots, 31\}$, что $r = r_{j+32}$. Поэтому из леммы 2 в [1] следует

$$r = s_{j+32} + s_{16-j-32} = -s_j - s_{16-j} = -r_j \in R_2 \cup R_3.$$

2. Имеем

$$r_{16+j} = s_{16+j} + s_{16-(16+j)} = -s_{-32+(16+j)} + s_{-j} = s_j - s_{-16+j} = s_j - s_{16-j} = r_j - 2s_{16-j}.$$

Кроме того,

$$r_{-j} = s_{-j} + s_{16+j} = s_j - s_{-32+(16+j)} + s_{-j} = s_j - s_{-16+j} = s_j - s_{16-j} = r_j - 2s_{16-j}.$$

3. В силу утверждения 1 достаточно рассмотреть R_0 и R_1. Пусть $j \in \{1, 2, \ldots, 7\}$. Элемент $r_j \in R_0$ в качестве центрально симметричного имеет элемент

$$r_{16-j} = s_{16-j} + s_{16-16+j} = s_{16-j} + s_j = r_j.$$

Элемент $r_{16+j} \in R_1$ в качестве центрально симметричного имеет элемент r_{32-j}. Применим утверждение 2 и получим

$$\begin{aligned}
&r_{16+j} = r_j - 2s_{16-j},\\
&r_{32-j} = r_{16+(16-j)} = r_{16-j} - 2s_{16-(16-j)} = r_j - 2s_j,\\
&r_{16+j} + r_{32-j} = r_j - 2s_{16-j} + r_j - 2s_j = 2r_j - 2r_j = 0.
\end{aligned}$$

□

Рассмотрим последовательность $\{r_j\}_{j\in\mathbb{Z}}$, приведённую по модулю 2.

Лемма 5. *Последовательность $\{r_j\}_{j\in\mathbb{Z}}$ по модулю 2 периодична с периодом 16. Более точно, в обозначениях леммы 4 последовательность $\{r_j\}_{j\in\mathbb{Z}}$ по модулю 2 имеет следующие свойства.*

1. $r_0 \equiv r_8 \equiv 0 \pmod 2$.
2. $R_0 \equiv R_1 \equiv R_2 \equiv R_3 \pmod 2$ — *здесь имеется в виду поэлементная сравнимость по модулю 2 упорядоченных наборов R_0, R_1, R_2 и R_3.*
3. *Набор R_0 центрально симметричен по модулю 2, т. е.*

j	0	1	...	7	8	9	...	15
r_j	0	r_1	...	r_7	0	r_7	...	r_1

4. *Для любых целых j и k*

$$\begin{aligned} r_j r_k &\equiv 0 \pmod 2,\\ s_{8k} r_j &\equiv 0 \pmod 2,\\ t_k r_j &\equiv r_j + r_{k+j} + r_{k-j} + r_{2k+j} + r_{2k-j} \pmod 2. \end{aligned}$$

Доказательство. 1–3. Утверждения очевидно следуют из леммы 4.

4. По лемме 2 из [1]

$$\begin{aligned} r_j r_k &= (s_j + s_{16-j})(s_k + s_{16-k}) = \\ &= (s_{j+k} + s_{j-k} + s_{16-k+j} + s_{16-k-j}) + (s_{16-j+k} + s_{16-j-k} + s_{32-j-k} + s_{-j+k}) = \\ &= (s_{j+k} + s_{32-j-k}) + (s_{j-k} + s_{-j+k}) + 2s_{16-j-k} + (s_{16-k+j} + s_{16-j+k}). \end{aligned}$$

По лемме 2 из [1] получим $s_{32-j-k} = -s_{j+k}$, $s_{16-j+k} = s_{32-(16+j-k)} = -s_{16+j-k}$, поэтому $r_j r_k = 0 + 2s_{j-k} + 2s_{16-j-k} + 0 \equiv 0 \pmod 2$. Далее, по лемме 2 из [1] достаточно рассмотреть $k = 1$. Получим

$$s_8 r_j = s_8(s_j + s_{16-j}) = (s_{j+8} + s_{j-8}) + (s_{16-j+8} + s_{16-j-8}) = (s_{j+8} + s_{j-8}) + (s_{24-j} + s_{8-j}).$$

По лемме 2 [1] имеем $s_{24-j} = s_{32-(8+j)} = -s_{8+j}$, и определение последовательности $\{s_j\}_{j\in\mathbb{Z}}$ даёт, что $s_8 r_j = 2s_{8-j} \equiv 0 \pmod 2$.

Рассмотрим

$$\begin{aligned} t_k r_j &= (1 + s_k + s_{2k})(s_j + s_{16-j}) = \\ &= r_j + s_{k+j} + s_{k-j} + s_{2k+j} + s_{2k-j} + \\ &+ s_{k+16-j} + s_{k-16+j} + s_{2k+16-j} + s_{2k-16+j} = \\ &= r_j + (s_{k+j} + s_{k-16+j}) + (s_{k-j} + s_{k+16-j}) + \\ &+ (s_{2k+j} + s_{2k-16+j}) + (s_{2k-j} + s_{2k+16-j}) = \\ &= r_j + (s_{k+j} + s_{-16+(k+j)}) + (s_{k-j} + s_{16+(k-j)}) + \\ &+ (s_{2k+j} + s_{-16+(2k+j)}) + (s_{2k-j} + s_{16+(2k-j)}) = \\ &= r_j + (s_{k+j} + s_{16-(k+j)}) + (s_{k-j} - s_{16-(k-j)}) + \\ &+ (s_{2k+j} + s_{16-(2k+j)}) + (s_{2k-j} - s_{16-(2k-j)}) \equiv \\ &\equiv r_j + r_{k+j} + (s_{k-j} + s_{16-(k-j)}) + \\ &+ r_{2k+j} + (s_{2k-j} + s_{16-(2k-j)}) = \\ &= r_j + r_{k+j} + r_{k-j} + r_{2k+j} + r_{2k-j} \pmod 2. \end{aligned}$$

□

1.3. Максимальное действительное подполе $\mathbb{Q}_{64} \cap \mathbb{R}$ кругового поля $\mathbb{Q}_{64}$

Следующая лемма доказана в работе [7].

Лемма 6. *Для любого целого j*

$$s_{2j} = s_1^{2j} + \sum_{n=0}^{j-1} (-1)^{j-n} \left(C_{j+n}^{j-n} + C_{j+n-1}^{j-n-1} \right) s_1^{2n},$$

$$s_{2j+1} = s_1^{2j+1} + \sum_{n=0}^{j-1} (-1)^{j-n} \left(C_{j+1+n}^{j-n} + C_{j+n}^{j-n-1} \right) s_1^{2n+1}.$$

Лемма 7. *Для максимального действительного подполя $\mathbb{Q}(\alpha) \cap \mathbb{R}$ кругового поля $\mathbb{Q}(\alpha)$ выполняются следующие утверждения.*

1. *Максимальное действительное подполе $\mathbb{Q}(\alpha) \cap \mathbb{R}$ кругового поля $\mathbb{Q}(\alpha)$ равно*
$$\mathbb{Q}(\alpha + \alpha^{-1}) = \left\{ f(\alpha + \alpha^{-1}) \mid f \in \mathbb{Q}[t] \right\}.$$

2. *Поле $\mathbb{Q}(\alpha) \cap \mathbb{R}$ абелево, его степень расширения $[\mathbb{Q}(\alpha) \cap \mathbb{R} : \mathbb{Q}] = 16$ и любой автоморфизм из группы $\mathrm{Gal}(\mathbb{Q}(\alpha) \cap \mathbb{R})$ индуцируется отображением $\alpha \mapsto \alpha^k$ для нечётного k. В частности,*
$$\mathbb{Q}(\alpha + \alpha^{-1}) = \left\{ f(\alpha + \alpha^{-1}) \mid f \in \mathbb{Q}[\![15]\!][t] \right\},$$
где $\mathbb{Q}[\![15]\!][t]$ — множество (точнее, подпространство) всех многочленов с рациональными коэффициентами степени не выше 15.

3. *Максимальное действительное подполе $\mathbb{Q}(\alpha) \cap \mathbb{R}$ кругового поля $\mathbb{Q}(\alpha)$ имеет два следующих целых базиса:*
   а) $1,\ s_1 = \alpha + \alpha^{-1},\ s_1^2 = (\alpha + \alpha^{-1})^2, \ldots, s_1^{15} = (\alpha + \alpha^{-1})^{15}$;
   б) $1,\ s_1 = \alpha + \alpha^{-1},\ s_2 = \alpha^2 + \alpha^{-2}, \ldots, s_{15} = \alpha^{15} + \alpha^{-15}$.

   В частности, кольцо целых $\mathrm{Int}\,(\mathbb{Q}(\alpha) \cap \mathbb{R})$ максимального действительного подполя $\mathbb{Q}(\alpha) \cap \mathbb{R}$ кругового поля $\mathbb{Q}(\alpha)$ равно
$$\mathbb{Z}[\alpha + \alpha^{-1}] = \left\{ f(\alpha + \alpha^{-1}) \mid f \in \mathbb{Z}[\![15]\!][t] \right\},$$
где $\mathbb{Z}[\![15]\!][t]$ — множество (точнее, конечно порождённая подгруппа) всех многочленов с целыми коэффициентами степени не выше 15.

Доказательство.

1. Ясно, что $\mathbb{Q}(\alpha^{-1}+\alpha) \subseteq \mathbb{Q}(\alpha) \cap \mathbb{R}$. Пусть $\beta = \sum_i a_i \alpha^i \in \mathbb{Q}(\zeta) \cap \mathbb{R}$, где для любого i число $a_i \in \mathbb{Q}$. Тогда $\bar{\beta} = \sum_i a_i \bar{\alpha}^i = \sum_i a_i \alpha^{-i}$. Так как в нашем случае $\bar{\beta} = \beta$, то $\beta = \sum_i \frac{a_i}{2} (\alpha^i + \alpha^{-i})$. Поскольку $\alpha^i + \alpha^{-i}$ по лемме 6 выражается с целыми коэффициентами через $\alpha + \alpha^{-1}$, то $\beta \in \mathbb{Q}(\alpha^{-1} + \alpha)$, т. е. $\mathbb{Q}(\alpha^{-1} + \alpha) \supseteq \mathbb{Q}(\alpha) \cap \mathbb{R}$. Таким образом, $\mathbb{Q}(\alpha^{-1} + \alpha) = \mathbb{Q}(\alpha) \cap \mathbb{R}$.

2. Ясно, что множество $\mathbb{Q}(\alpha^{-1} + \alpha) = \mathbb{Q}(\alpha) \cap \mathbb{R}$ неподвижное относительно комплексного сопряжения подполе поля $\mathbb{Q}(\alpha)$. Всё следует из леммы 1 по основной теореме теории Галуа [8, § 58] и теореме из [8, § 59, с. 202].

3. а. Это результат из [9].
   б. Данное утверждение следует из утверждения 3.а данной леммы и из леммы 6.

□

2. Подгруппа W_1

2.1. Разложение W_1

Во введении была определена подгруппа W_1 нормализованной группы единиц $\mathrm{V}(\mathbb{Z}G)$ целочисленного группового кольца $\mathbb{Z}G$ циклической группы G порядка 64:

$$W_1 = \langle u_{\chi_1}(\beta_1) \mid \beta_1 \in \mathrm{Un}(\mathrm{Int}(\mathbb{Q}(\chi_1)))\rangle\,.$$

Из определения единиц $u_{\chi_1}(\beta_1)$ в работе [4, определение 1] следует мультипликативность таких единиц, поэтому $W_1 = \{u_{\chi_1}(\beta_1) \mid \beta_1 \in \mathrm{Un}(\mathrm{Int}(\mathbb{Q}(\chi_1)))\}$. Как уже отмечалось ранее $\mathrm{Un}(\mathrm{Int}(\mathbb{Q}(\chi_1))) = \mathrm{Un}(\mathbb{Z}[\alpha])$.

Обозначение. Положим

$$T = \prod_{l=0}^{14} \langle t_{2l+1}\rangle = \langle t_1\rangle \times \langle t_3\rangle \times \cdots \times \langle t_{29}\rangle\,.$$

Как следствие леммы 11 [1] получим следующий результат.

Лемма 8. *При введённых выше обозначениях выполняются следующие утверждения.*

1. $\mathrm{Un}(\mathbb{Z}[\alpha]) = \langle\alpha\rangle \times T$.

2. $\mathrm{Un}(\mathrm{Int}(\mathbb{Q}[\alpha] \cap \mathbb{R})) = \mathrm{Un}(\mathbb{Z}[\alpha + \alpha^{-1}]) = \langle -1\rangle \times T$.

Доказательство.

1. Это непосредственное следствие леммы 11 из [1].

2. Следует из утверждения 1 и леммы 7.

□

Обозначение. Обозначим след элемента $c \in \mathbb{Q}_{64}$ через $\mathrm{tr}_{\mathbb{Q}_{64}}(c)$.

Как непосредственное следствие леммы 1 из [4] получим следующий результат.

Лемма 9. *Пусть* $\beta_1 \in \mathrm{Un}(\mathbb{Z}[\alpha])$, $u_{\chi_1}(\beta_1) = \sum_{j=0}^{63} \gamma_j x^j$. *Тогда для любого значения* $j \in \{0, 1, \ldots, 63\}$

$$\gamma_j = \begin{cases} 1 + \dfrac{\mathrm{tr}_{\mathbb{Q}_{64}}(\beta_1 - 1)}{64}, & \text{если } j = 0, \\ \dfrac{1}{64}\mathrm{tr}_{\mathbb{Q}_{64}}\left((\beta_1 - 1)\alpha^{-j}\right), & \text{если } j \in \{1, \ldots, 63\}. \end{cases}$$

Замечание 4. Наша цель — получить единицу $u_{\chi_1}(\beta_1)$ из нормализованной группы единиц кольца $\mathbb{Z}G$,

$$u_{\chi_1}(\beta_1) = \sum_{j=0}^{63} \gamma_j x^j.$$

Поэтому необходимо найти такие условия на элемент $\beta_1 \in \mathrm{Un}(\mathbb{Z}[\alpha])$, чтобы обеспечивалась целочисленность коэффициентов γ_j для всех значений $j \in \{0, 1, \ldots, 63\}$.

Следующая лемма очевидна в силу того, что многочлен $t^{32} + 1$ является минимальным многочленом числа α.

Лемма 10. 1. *Для любого* $j \in \{0, 1, \ldots, 63\}$

$$\mathrm{tr}_{\mathbb{Q}_{64}}(\alpha^{-j}) = \begin{cases} 32, & \text{если } j = 0, \\ -32, & \text{если } j = 32, \\ 0 & \text{для всех остальных } j. \end{cases}$$

2. Пусть $\beta_1 = \sum_{k=0}^{31} b_k \alpha^k \in \mathrm{Un}(\mathbb{Z}[\alpha])$. *Тогда для любого* $j \in \{0, 1, \ldots, 63\}$

$$\mathrm{tr}_{\mathbb{Q}_{64}}(\beta_1 \alpha^{-j}) = \begin{cases} 32b_j, & \text{если } j \in \{0, 1, \ldots, 31\}, \\ -32b_{j-32}, & \text{если } j \in \{32, 33, \ldots, 63\}. \end{cases}$$

Предложение 1. *Пусть* $\beta_1 \in \mathrm{Un}(\mathbb{Z}[\alpha])$. *Локальная единица* $u_{\chi_1}(\beta_1)$ *принадлежит* $\mathrm{V}(\mathbb{Z}G)$ *тогда и только тогда, когда* $\beta_1 \in \mathrm{Un}(\mathbb{Z}[\alpha + \alpha^{-1}]) = \langle -1 \rangle \times T$, *причём* $\beta_1 \equiv 1 \pmod 2$.

Доказательство. Докажем необходимость условий. Пусть $\beta_1 = \sum_{k=0}^{31} b_k \alpha^k$. Тогда по лемме 10

$$\begin{aligned} \gamma_0 \in \mathbb{Z} &\longleftrightarrow \mathrm{tr}_{\mathbb{Q}_{64}}(\beta_1 - 1) \equiv 0 \pmod{64} \longleftrightarrow \\ &\longleftrightarrow 32b_0 \equiv 32 \pmod{64} \longleftrightarrow b_0 \equiv 1 \pmod 2, \\ \gamma_{32} \in \mathbb{Z} &\longleftrightarrow \mathrm{tr}_{\mathbb{Q}_{64}}((\beta_1 - 1)(-1)) \equiv 0 \pmod{64} \longleftrightarrow \\ &\longleftrightarrow 32b_0 \equiv 32 \pmod{64} \longleftrightarrow b_0 \equiv 1 \pmod 2, \end{aligned}$$

для любого $j \in \{1, 2, \ldots, 31\}$

$$\begin{aligned} \gamma_j \in \mathbb{Z} &\longleftrightarrow \mathrm{tr}_{\mathbb{Q}_{64}}\left((\beta_1 - 1)\alpha^{-j}\right) \equiv 0 \pmod{64} \longleftrightarrow \\ &\longleftrightarrow 32b_j \equiv 0 \pmod{64} \longleftrightarrow b_j \equiv 0 \pmod 2, \end{aligned}$$

для любого $j \in \{32, 33, \ldots, 63\}$

$$\begin{aligned} \gamma_j \in \mathbb{Z} &\longleftrightarrow \mathrm{tr}_{\mathbb{Q}_{64}}\left((\beta_1 - 1)\alpha^{-j}\right) \equiv 0 \pmod{64} \longleftrightarrow \\ &\longleftrightarrow -32b_{j-32} \equiv 0 \pmod{64} \longleftrightarrow b_{j-32} \equiv 0 \pmod 2. \end{aligned}$$

Это даёт нам, что $\beta_1 \equiv 1 \pmod 2$.

С другой стороны, $\beta_1 \in \mathrm{Un}(\mathbb{Z}[\alpha]) = \langle \alpha \rangle \times T$. Поэтому $\beta_1 = \alpha^k \cdot t$, где $k \in \{0, 1, \ldots, 63\}$ и $t \in T$.

Предположим, что $k \notin \{0, 32\}$. В этом случае

$$\mathrm{НОД}(k, 64) = 2^s \in \{1, 2, 4, 8, 16\} \longleftrightarrow kk_1 + 64n_1 = 2^s$$

для подходящих целых k_1 и n_1. Отсюда $16 = k(k_1 \cdot 2^{4-s}) + 64(n_1 \cdot 2^{4-s})$, тогда

$$i = \alpha^{16} = \alpha^{k(k_1 \cdot 2^{4-s}) + 64(n_1 \cdot 2^{4-s})} = (\alpha^k)^{k_1 \cdot 2^{4-s}} (\alpha^{64})^{n_1 \cdot 2^{4-s}} = (\alpha^k)^{k_1 \cdot 2^{4-s}}$$

и также $\beta = \beta_1^{k_1 \cdot 2^{4-s}} = (\alpha^k)^{k_1 \cdot 2^{4-s}} \cdot t^{k_1 \cdot 2^{4-s}} = i \cdot t^{k_1 \cdot 2^{4-s}}$. По лемме 7 для подходящих $a_j \in \mathbb{Z}$ для всех $j \in \{0, 1, \ldots, 15\}$

$$\beta = i \left(a_0 + \sum_{j=1}^{15} a_j (\alpha^j + \alpha^{-j}) \right) = a_0 \cdot i + \sum_{j=1}^{15} a_j (\alpha^{j+16} + \alpha^{-j+16}).$$

Очевидно $\{j + 16, -j + 16 \mid j \in \{1, 2, \ldots, 15\}\} \cap \{0, 32\} = \varnothing$, что даёт противоречие с утверждением 1. Таким образом, $\beta_1 = \pm t$. Поэтому по лемме 8 получим

$$\beta_1 \in \mathrm{Un}(\mathbb{Z}[\alpha + \alpha^{-1}]) = \langle -1 \rangle \times T.$$

Достаточность следует из леммы 10. $\square$

Лемма 11. *При введённых ранее обозначениях* $\langle u_{\chi_1}(-1)\rangle = \langle x^{32}\rangle$.

Доказательство. Пусть

$$u_{\chi_1}(-1) = \sum_{j=0}^{63} \gamma_j x^j.$$

Тогда для любого $j \in \{0, 1, \ldots, 63\}$ по лемме 10 получим

$$\gamma_j = \begin{cases} 1 + \dfrac{\mathrm{tr}_{\mathbb{Q}_{64}}(-1-1)}{64} = 1 - \dfrac{64}{64} = 0, & \text{если } j = 0, \\ \dfrac{1}{64}\mathrm{tr}_{\mathbb{Q}_{64}}\left((-1-1)(-1)(-1)\right) = \dfrac{64}{64} = 1, & \text{если } j = 32, \\ \dfrac{1}{64}\mathrm{tr}_{\mathbb{Q}_{64}}\left((-1-1)\alpha^{-j}\right) = -2 \cdot 0 = 0 & \text{для всех остальных } j. \end{cases}$$

□

Обозначения. Введём следующие обозначения.

1. Положим $D = \{\lambda \in T \mid \lambda \equiv 1 \pmod 2\}$. Иными словами, $D = (1 + 2\mathbb{Z}[\alpha]) \cap T$.
2. Положим также $V_1 = \{u_{\chi_1}(\lambda) \mid \lambda \in D\}$.

Лемма 12. *Для любого* $l \in \{0, \ldots, 14\}$ $t_{2l+1}^{16} \equiv 1 \pmod 2$, *т. е.* $t_{2l+1}^{16} \in D$, *и для любого* $k \in \{0, 1, 2, 3\}$ $t_{2l+1}^{2^k} \not\equiv 1 \pmod 2$, *т. е.* $t_{2l+1}^{2^k} \notin D$.

Доказательство. Поскольку элемент t_{2l+1} для любого $l \in \{0, \ldots, 14\}$ алгебраически сопряжён с элементом $t_1 = 1 + s_1 + s_2 = 1 + \alpha + \alpha^{-1} + \alpha^2 + \alpha^{-2}$, то достаточно доказать лемму для t_1. По лемме 3 из [1] для любого целого j $t_j^2 \equiv t_{2j} \pmod 2$. По индукции получим, что для любого натурального k $t_1^{2^k} \equiv t_{2^k} \pmod 2$. В частности, по лемме 3 из [1] $t_1^{16} \equiv t_{16} = -1 \equiv 1 \pmod 2$. Допустим, что для некоторого $k \in \{0, 1, 2, 3\}$ $t_1^{2^k} \equiv t_{2^k} \equiv 1 \pmod 2$. Тогда по лемме 3 из [1]

$$t_1^8 \equiv t_8 = 1 + \sqrt{2} \equiv 1 \pmod 2.$$

Откуда $\frac{\sqrt{2}}{2} \in \mathbf{Z}[\alpha]$, что невозможно, ибо $\frac{\sqrt{2}}{2}$ не является целым алгебраическим числом. □

Предложение 2. 1. *Индекс* $|T : T^{16}| = (16)^{15} = (2^4)^{2^4-1} = 2^{4(2^4-1)} = 2^{60}$. *Равносильно, порядок фактор-группы* $|T/T^{16}| = (16)^{15} = 2^{4(2^4-1)} = 2^{60}$.

2. D является подгруппой группы T, содержащей T^{16}, *т. е.* $T^{16} \leqslant D < T$.

Доказательство. 1. Следует из определения группы T и леммы 12.

2. Из леммы 12 получим, что подгруппа T^{16} содержится в множестве D. Пусть $1 + 2\lambda$ и $1 + 2\mu$ — произвольные элементы D, где $\lambda, \mu \in \mathbb{Z}[\alpha]$. Так как

$$(1 + 2\lambda)(1 + 2\mu) = 1 + 2(\lambda + \mu) + 4\lambda\mu \in (1 + 2\mathbb{Z}[\alpha]) \cap T = D,$$

то множество D замкнуто относительно умножения. Поскольку D состоит из смежных классов, которые являются элементами конечной фактор-группы T/T^{16}, то получим конечную подгруппу D/T^{16}. Отсюда следует, что D является подгруппой T, содержащей T^{16}. □

Как непосредственное следствие предложений 1 и 2 и леммы 11 получим описание строения группы W_1.

Предложение 3. *При введённых ранее обозначениях*

1. V_1 — *подгруппа группы* W_1.
2. $W_1 = \langle x^{32}\rangle \times V_1$.

2.2. Подгруппа M

В этом разделе определена подгруппа M, которая будет ключевой в нахождении подгруппы D, что является целью наших исследований.

2.2.1. Построение воронки

По определению

$$T = \prod_{l=0}^{14} \langle t_{2l+1} \rangle ,$$

поэтому множеством индексов в этом произведении является состоящее из 15 элементов множество $A = \{1, 3, 5, \ldots, 29\}$.

Замечание 5. Построим разбиения (дизъюнктные объединения) множества A, которые будут определяться всё уменьшающимися частями множества A. Поэтому этот процесс назовём *воронкой*.

Обозначения. Обозначим $A_0 = \{1, 3, 5, \ldots, 15\} = \{2l + 1 \mid l \in \{0, \ldots, 7\}\}$, в этом множестве 8 элементов. Также обозначим

$$B_0 = A \setminus A_0 = \{32 - (2l + 1) \mid 2l + 1 \in A_0 \setminus \{1\}\} = \{29, 27, \ldots, 17\}.$$

Далее, $A_1 = \{1, 3, 5, 7\}$ и $B_1 = \{15, 13, 11, 9\}$. Наконец, $A_2 = \{1, 3\}$ и $B_2 = \{7, 5\}$.

Изобразим этот процесс таблично:

$A =$

l	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$2l+1$	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29

.

Шаг 0. Имеем

$A_0 =$

l	0	1	2	3	4	5	6	7
$2l+1$	1	3	5	7	9	11	13	15

,

$B_0 =$

l	8	9	10	11	12	13	14
$2l+1$	17	19	21	23	25	27	29

.

Шаг 1. Далее

$A_1 =$

l	0	1	2	3
$2l+1$	1	3	5	7

, $\quad B_1 =$

l	4	5	6	7
$2l+1$	9	11	13	15

.

Шаг 2. Наконец,

$A_2 =$

l	0	1
$2l+1$	1	3

, $\quad B_2 =$

l	2	3
$2l+1$	5	7

,

и на этом процесс закончен. Получили разбиение

$$A = \{1, 3\} \cup \{5, 7\} \cup \{9, 11, 13, 15\} \cup \{17, 19, 21, 23, 25, 27, 29\}.$$

Теперь очевидно получим следующий результат.

Лемма 13. *При указанных выше обозначениях получим разбиения*

$$A = A_0 \cup B_0 = A_1 \cup B_1 \cup B_0 = A_2 \cup B_2 \cup B_1 \cup B_0.$$

2.2.2. Сравнимость элементов воронки

Используя построенные в лемме 13 разбиения, изучим сравнимость по модулю 2 степеней порождающих группы T.

Лемма 14. *Для любых* $l, r \in \{0, \dots, 15\}$ *имеем* $t_{2l+1}^8 t_{2r+1}^8 \in D$. *В частности,* $t_1^{-8} t_3^8 \in D$.

Доказательство. По лемме 3 для любого целого j $t_j^2 \equiv t_{2j} \pmod 2$. Поэтому для любого $l \in \{0, 1, \dots, 7\}$ $t_{2l+1}^8 \equiv t_{8(2l+1)} \pmod 2$. Из леммы 3 следует, что $t_{8(2l+1)} = 1 \pm \sqrt{2}$. Так как $(1 \pm \sqrt{2})^2 = 1 \pm 2\sqrt{2} + 2 \equiv 1 \pmod 2$ и $(1+\sqrt{2})(1-\sqrt{2}) = 1 - 2 \equiv 1 \pmod 2$, то произведение любых двух таких элементов сравнимо с 1 по модулю 2.

В частности, из леммы 12 следует, что $t_1^{-8} t_3^8 = (t_1^{-16})(t_1^8 t_3^8) \in D$. □

Обозначения. Введём обозначения согласно шагам воронки.

Для шага 0. Для любого $2l + 1 \in \{3, \dots, 15\} = A_0 \setminus \{1\}$ положим

$$m(0, 2l+1) = t_{2l+1}^{-1} t_{32-(2l+1)}.$$

Для шага 1. Для любого $2l + 1 \in \{1, \dots, 7\} = A_1$ положим

$$m(1, 2l+1) = t_{2l+1}^{-1} t_{16-(2l+1)}.$$

Для шага 2 положим $m(2, 1) = t_1^{-1} t_7,\ m(2, 3) = t_3^{-1} t_5$.

Лемма 15. *При введённых ранее обозначениях*

$$T = \langle t_1 \rangle \times \langle t_1^{-1} t_3 \rangle \times \prod_{k=0}^{2} \prod_{2^{5-k} - (2l+1) \in B_k} \langle m(k, 2l+1) \rangle =$$

$$= \langle t_1 \rangle \times \langle t_1^{-1} t_3 \rangle \times \prod_{2l+1 \in A_0 \setminus \{1\}} \langle m(0, 2l+1) \rangle \times \prod_{k=1}^{2} \prod_{2l+1 \in A_k} \langle m(k, 2l+1) \rangle.$$

Доказательство. Будем рассматривать доказательство по шагам. Для шага 0 для любого $2l + 1 \in \{3, \dots, 15\} = A_0 \setminus \{1\}$ получим $t_{32-(2l+1)} = t_{2l+1} m(0, 2l+1)$. Поэтому

$$T = \prod_{2l+1 \in A_0} \langle t_{2l+1} \rangle \times \prod_{32-(2l+1) \in B_0} \langle t_{32-(2l+1)} \rangle =$$

$$= \prod_{2l+1 \in A_0} \langle t_{2l+1} \rangle \times \prod_{32-(2l+1) \in B_0} \langle t_{2l+1} m(0, 2l+1) \rangle =$$

$$= \prod_{2l+1 \in A_0} \langle t_{2l+1} \rangle \times \prod_{32-(2l+1) \in B_0} \langle m(0, 2l+1) \rangle = T_0 \times \prod_{32-(2l+1) \in B_0} \langle m(0, 2l+1) \rangle,$$

где

$$T_0 = \prod_{2l+1 \in A_0} \langle t_{2l+1} \rangle.$$

Для шага 1 рассмотрим T_0. Для любого $2l + 1 \in \{1, \dots, 15\} = A_1$ получим

$$t_{16-(2l+1)} = t_{2l+1} m(1, 2l+1).$$

Поэтому

$$T_0 = \prod_{2l+1\in A_1} \langle t_{2l+1}\rangle \times \prod_{16-(2l+1)\in B_1} \langle t_{16-(2l+1)}\rangle =$$
$$= \prod_{2l+1\in A_1} \langle t_{2l+1}\rangle \times \prod_{16-(2l+1)\in B_1} \langle t_{2l+1}m(1,2l+1)\rangle =$$
$$= \prod_{2l+1\in A_1} \langle t_{2l+1}\rangle \times \prod_{16-(2l+1)\in B_1} \langle m(1,2l+1)\rangle = T_1 \times \prod_{16-(2l+1)\in B_1} \langle m(1,2l+1)\rangle,$$

где

$$T_1 = \prod_{2l+1\in A_1} \langle t_{2l+1}\rangle.$$

Для шага 2 рассмотрим $T_1 = \langle t_1\rangle \times \langle t_3\rangle \times \langle t_5\rangle \times \langle t_7\rangle$. Поскольку $t_5 = t_1 m(2,3)$, $t_7 = t_3 m(2,1)$, то

$$T_1 = \langle t_1\rangle \times \langle t_3\rangle \times \langle t_5\rangle \times \langle t_7\rangle = \langle t_1\rangle \times \langle t_3\rangle \times \langle t_3 m(2,3)\rangle \times \langle t_1 m(2,1)\rangle =$$
$$= \langle t_1\rangle \times \langle t_3\rangle \times \langle m(2,3)\rangle \times \langle m(2,1)\rangle.$$

Последний шаг. Имеем $\langle t_1\rangle \times \langle t_3\rangle = \langle t_1\rangle \times \langle t_1(t_1^{-1}t_3)\rangle = \langle t_1\rangle \times \langle t_1^{-1}t_3\rangle$. В результате получим требуемое. □

Теперь по шагам воронки исследуем сравнимость с 1 по модулю 2 элементов подгрупп из разложения группы T, приведённого в лемме 15.

Лемма 16. *Имеем по шагам воронки*

0) *на шаге* 0

$$t_{32-(2l+1)} \equiv t_{2l+1} \pmod 2 \longleftrightarrow m(0,2l+1) = t_{2l+1}^{-1} t_{32-(2l+1)} \in D$$

для любого $2l+1 \in \{3,5,\dots,15\} = A_0 \setminus \{1\}$;

1) *на шаге* 1

$$t_{16-(2l+1)}^2 \equiv t_{2l+1}^2 \pmod 2 \longleftrightarrow m(1,2l+1)^2 = t_{2l+1}^{-2} t_{16-(2l+1)}^2 \in D \text{ и}$$
$$t_{16-(2l+1)} \not\equiv t_{2l+1} \pmod 2$$

для любого $2l+1 \in \{1,3,5,7\} = A_1$;

2) *на шаге* 2

$$t_{8-(2l+1)}^4 \equiv t_{2l+1}^4 \pmod 2 \longleftrightarrow m(2,2l+1)^4 = t_{2l+1}^{-4} t_{8-(2l+1)}^4 \in D \text{ и}$$
$$t_{8-(2l+1)}^2 \not\equiv t_{2l+1}^2 \pmod 2$$

для любого $2l+1 \in \{1,3\} = A_2$.

Доказательство. На нулевом шаге по утверждению 2 леммы 3 получим

$$t_{32-(2l+1)} \equiv t_{2l+1} \pmod 2$$

для любого $2l+1 \in \{3,5,\dots,15\}$.

Посмотрим, что будет на первом шаге. По лемме 3 (утверждения 3 и 2) получим, что для любого $2l+1 \in \{1,3,5,7\} = A_1$

$$t_{2l+1}^2 \equiv t_{2(2l+1)} \pmod 2 \text{ и } t_{16-(2l+1)}^2 \equiv t_{32-2(2l+1)} \equiv t_{2(2l+1)} \pmod 2.$$

Предположим, что $t_{2l+1} \equiv t_{16-(2l+1)} \pmod 2$, т. е.

$$1 + s_{2l+1} + s_{2(2l+1)} \equiv 1 + s_{16-(2l+1)} + s_{32-2(2l+1)} \pmod 2.$$

По лемме 2 $s_{32-2(2l+1)} \equiv s_{2(2l+1)} \pmod 2$, следовательно, $s_{2l+1} \equiv s_{16-(2l+1)} \pmod 2$, т. е. для некоторых целых чисел a_j

$$s_{2l+1} - s_{16-(2l+1)} = 2 + 2\sum_{j=1}^{16-1} a_j s_j,$$

что противоречит линейной независимоси $1, s_1, s_2, \ldots, s_{15}$ над $\mathbb{Q}$. (По лемме 7 элементы $1, s_1, s_2, \ldots, s_{15}$ образуют целый базис поля $\mathbb{Q}[\alpha] \cap \mathbb{R} = \mathbb{Q}[\alpha + \alpha^{-1}]$.) Предположение неверно, поэтому $t_{16-(2l+1)} \not\equiv t_{2l+1} \pmod 2$.

Для второго шага отметим, что $A_1 = A_2 \cup \{8 - (2l+1) \mid 2l+1 \in A_2\}$. По утверждению 3 леммы 3 получим, что для любого $2l+1 \in A_1$ $t_{2l+1}^4 \equiv t_{4(2l+1)} \pmod 2$. Поэтому для любого $2l+1 \in A_2$ по утверждению 2 леммы 3

$$t_{8-(2l+1)}^4 \equiv t_{4(8-(2l+1))} = t_{32-4(2l+1)} \equiv t_{4(2l+1)} \pmod 2.$$

Далее предположим, что для $2l+1 \in A_2$ $t_{2l+1}^2 \equiv t_{8-(2l+1)}^2 \pmod 2$, тогда

$$\begin{aligned} 1 + s_{2(2l+1)} + s_{4(2l+1)} &= t_{2(2l+1)} \equiv t_{2l+1}^2 \equiv t_{8-(2l+1)}^2 \equiv \\ &\equiv t_{2(8-(2l+1))} = t_{(16-2(2l+1))} = 1 + s_{16-2(2l+1)} + s_{32-4(2l+1)} \pmod 2. \end{aligned}$$

По утверждению 2 леммы 2 $s_{4(2l+1)} \equiv s_{32-4(2l+1)} \pmod 2$, следовательно,

$$s_{2(2l+1)} \equiv s_{16-2(2l+1)} \pmod 2.$$

Противоречие получится также, как на первом шаге. □

Обозначения. Введём обозначения согласно шагам воронки.
Для шага 0:

$$M_0 = \prod_{l=1}^{7} \langle t_{2l+1}^{-1} t_{32-(2l+1)} \rangle = \prod_{l=1}^{7} \langle m(0, 2l+1) \rangle = \prod_{2l+1 \in A_0 \setminus \{1\}} \langle m(0, 2l+1) \rangle.$$

Для шага 1 имеем

$$M_1 = \prod_{l=0}^{3} \langle t_{2l+1}^{-2} t_{16-(2l+1)}^2 \rangle = \prod_{l=0}^{3} \langle m(1, 2l+1)^2 \rangle = \prod_{2l+1 \in A_1} \langle m(1, 2l+1)^2 \rangle.$$

Для шага 2:

$$\begin{aligned} M_2 &= \prod_{l=0}^{1} \langle t_{2l+1}^{-4} t_{8-(2l+1)}^4 \rangle = \prod_{l=0}^{1} \langle t_{2l+1}^{-4} t_{8-(2l+1)}^4 \rangle = \langle t_1^{-4} t_7^4 \rangle \times \langle t_3^{-4} t_5^4 \rangle = \\ &= \langle m(2,3)^4 \rangle \times \langle m(2,1)^4 \rangle. \end{aligned}$$

Наконец,

$$M = \langle t_1^{16} \rangle \times \langle t_1^{-8} t_3^8 \rangle \times \prod_{k=0}^{2} M_k,$$

т. е.

$$M = \langle t_1^{16}\rangle \times \langle t_1^{-8}t_3^8\rangle \times \langle t_1^{-4}t_7^4\rangle \times \langle t_3^{-4}t_5^4\rangle \times \langle t_1^{-2}t_{15}^2\rangle \times \langle t_3^{-2}t_{13}^2\rangle \times \langle t_5^{-2}t_{11}^2\rangle \times \langle t_7^{-2}t_9^2\rangle \times$$
$$\times \langle t_3^{-1}t_{29}\rangle \times \langle t_5^{-1}t_{27}\rangle \times \langle t_7^{-1}t_{25}\rangle \times \langle t_9^{-1}t_{23}\rangle \times \langle t_{11}^{-1}t_{21}\rangle \times \langle t_{13}^{-1}t_{19}\rangle \times \langle t_{15}^{-1}t_{17}\rangle.$$

Лемма 17. *Множество M — подгруппа в D. Кроме того, $T^{16} < M \leqslant D < T$.*

Доказательство. Утверждение следует из лемм 12, 14 и 16.

По лемме 15 имеем

$$T^{16} = \langle t_1^{16}\rangle \times \langle (t_1^{-1}t_3)^{16}\rangle \times \prod_{2l+1\in A_0\setminus\{0\}} \langle m(0,2l{+}1)^{16}\rangle \times \prod_{k=1}^{2} \prod_{2l+1\in A_k} \langle m(k,2l{+}1)^{16}\rangle.$$

Поэтому $M > T^{16}$, дополнительное утверждение следует из предложения 2. □

2.3. Подгруппа $\sqrt{M}$

Обозначение. Обозначим $\sqrt{M} = \{t \in T \mid t^2 \in M\}$.

Лемма 18. *Множество $\sqrt{M}$ — подгруппа группы T, имеющая следующие свойства.*

1. *Фактор-группа*

$$\sqrt{M}/M = \langle t_1^8 M\rangle \times \langle (t_1^{-1}t_3)^4 M\rangle \times \prod_{k=1}^{2} \prod_{2l+1\in A_k} \langle m(k,2l+1)^{2^{k-1}} M\rangle$$

и является элементарной абелевой 2-группой, возможно, единичной.

2. $T^{16} < M \leqslant \sqrt{M} \cap D \leqslant \sqrt{M} < T$.

Доказательство. То, что $\sqrt{M}$ является подгруппой группы T, очевидно, так как T абелева. Дополнительные утверждения непосредственно следуют из определения подгруппы M и леммы 17. □

Далее исследуем представителей порождающих смежных классов фактор-группы $\sqrt{M}/M$, указанные в утверждении 1 леммы 18. Первый шаг будет состоять в исследовании множества $\{m(1,2l+1) \mid 2l+1 \in A_1 = \{1,3,5,7\}\}$.

Лемма 19. *При введённых ранее обозначениях*

$$m(1,1) \equiv 1 + r_7 + (r_2 + r_4) \pmod 2, \quad m(1,3) \equiv 1 + r_5 + (r_4 + r_6) \pmod 2,$$
$$m(1,5) \equiv 1 + r_3 + (r_4 + r_6) \pmod 2, \quad m(1,7) \equiv 1 + r_1 + (r_2 + r_4) \pmod 2.$$

Доказательство. Найдём $m(1,1)$ по модулю 2. Так как

$$1 = t_1 t_1^{-1} = (1 + s_1 + s_2)t_1^{-1} = (1 + s_2)t_1^{-1} + s_1 t_1^{-1},$$

то $(1 + s_2)t_1^{-1} \equiv 1 + s_1 t_1^{-1} \pmod 2$. Отсюда

$$m(1,1) = t_1^{-1}t_{15} = t_1^{-1}(1 + s_{15} + s_{30}) = t_1^{-1}(1 + s_{15} - s_2) \equiv$$
$$\equiv t_1^{-1}(1 + s_{15} + s_2) = t_1^{-1}(1 + s_2) + t_1^{-1}s_{15} \equiv 1 + s_1 t_1^{-1} + t_1^{-1}s_{15} =$$
$$= 1 + t_1^{-1}(s_1 + s_{15}) = 1 + t_1^{-1} \cdot r_1 \pmod 2.$$

По леммам 3 и 12 имеем $m(1,1) \equiv 1 + t_8 \cdot t_4 \cdot t_2 \cdot t_1 \cdot r_1 \pmod 2$.

Теперь по леммам 2 и 5

$$\begin{aligned}
t_1 r_1 &\equiv r_1 + r_2 + r_0 + r_3 + r_1 \equiv r_2 + r_3 \pmod 2,\\
t_2 t_1 r_1 &\equiv t_2(r_2 + r_3) \equiv r_2 + r_4 + r_0 + r_6 + r_2 + r_3 + r_5 + r_1 + r_7 + r_1 \equiv\\
&\equiv r_4 + r_6 + r_3 + r_5 + r_7 = r_3 + r_4 + r_5 + r_6 + r_7 \pmod 2,\\
t_4 t_2 t_1 r_1 &\equiv t_4(r_3 + r_4 + r_5 + r_6 + r_7) \equiv\\
&\equiv r_3 + r_7 + r_1 + r_{11} + r_5 + r_4 + r_8 + r_0 + r_{12} + r_4 +\\
&+ r_5 + r_9 + r_1 + r_{13} + r_3 + r_6 + r_{10} + r_2 + r_{14} + r_2 +\\
&+ r_7 + r_{11} + r_3 + r_{15} + r_1 \equiv\\
&\equiv r_3 + r_7 + r_1 + r_3 + r_5 + r_4 + 0 + 0 + r_4 + r_4 +\\
&+ r_5 + r_7 + r_1 + r_3 + r_3 + r_6 + r_2 + r_2 + r_6 + r_2 +\\
&+ r_7 + r_3 + r_3 + r_1 + r_1 \equiv\\
&\equiv r_7 + r_1 + r_5 + r_4 + r_5 + r_7 + r_1 + r_2 + r_7 \equiv\\
&\equiv r_7 + r_4 + r_2 \pmod 2,\\
t_8 t_4 t_2 t_1 r_1 &\equiv (1 + s_8 + s_{16})(r_7 + r_2 + r_4) = (1 + s_8)(r_7 + r_2 + r_4) \equiv\\
&\equiv r_7 + r_2 + r_4 \pmod 2.
\end{aligned}$$

Таким образом, $m(1,1) \equiv 1 + r_7 + (r_2 + r_4) \pmod 2$.

Пусть, как в лемме 1, $\sigma_k \in \mathrm{Gal}(\mathbb{Q}_{64})$ для $k \in \{3,5,7\}$, где $\sigma_k(\alpha) = \alpha^k$. Кроме того, по лемме 3

$$\begin{aligned}
\sigma_3(m(1,1)) =& \sigma_3(t_1^{-1} t_{15}) = t_3^{-1} t_{45} \equiv t_3^{-1} t_{13} = m(1,3) \pmod 2,\\
\sigma_5(m(1,1)) =& \sigma_5(t_1^{-1} t_{15}) = t_5^{-1} t_{75} = t_3^{-1} t_{11} = m(1,5),\\
\sigma_7(m(1,1)) =& \sigma_5(t_1^{-1} t_{15}) = t_7^{-1} t_{105} \equiv t_7^{-1} t_9 = m(1,7) \pmod 2.
\end{aligned}$$

Также по лемме 5

$$\begin{aligned}
m(1,3) = \sigma_3(m(1,1)) &\equiv \sigma_3(1 + r_7 + (r_2 + r_4)) = 1 + r_{21} + (r_6 + r_{12}) \equiv\\
&\equiv 1 + r_5 + (r_4 + r_6) \pmod 2,\\
m(1,5) = \sigma_5(m(1,1)) &\equiv \sigma_5(1 + r_7 + (r_2 + r_4)) = 1 + r_{35} + (r_{10} + r_{20}) \equiv\\
&\equiv 1 + r_3 + (r_4 + r_6) \pmod 2,\\
m(1,7) = \sigma_7(m(1,1)) &\equiv \sigma_7(1 + r_7 + (r_2 + r_4)) = 1 + r_{49} + (r_{14} + r_{28}) \equiv\\
&\equiv 1 + r_1 + (r_2 + r_4) \pmod 2.
\end{aligned}$$

□

Лемма 20. *При введённых ранее обозначениях*

$$m(2,1)^2 \equiv 1 + r_2 + r_4 \pmod 2, \quad m(2,3)^2 \equiv 1 + r_4 + r_6 \pmod 2.$$

Доказательство. Будем действовать, как в лемме 19. Найдём $m(2,1)^2$ по модулю 2. Используя леммы 3 и 12, получим

$$1 = t_1^2 t_1^{-2} \equiv t_2 t_1^{-2} = (1 + s_2 + s_4) t_1^{-2} = (1 + s_4) t_1^{-2} + s_2 t_1^{-2} \pmod 2.$$

Поэтому $(1 + s_4) t_1^{-2} \equiv 1 + s_2 t_1^{-2} \pmod 2$. Отсюда

$$\begin{aligned}
m(2,1)^2 = t_1^{-2} t_7^2 \equiv t_1^{-2} t_{14} = t_1^{-2}(1 + s_{14} + s_{28}) \equiv t_1^{-2}(1 + s_{14} + s_4) =\\
= t_1^{-2}(1 + s_4) + t_1^{-2} s_{14} \equiv 1 + s_2 t_1^{-2} + t_1^{-2} s_{14} = 1 + t_1^{-2}(s_2 + s_{14}) =\\
= 1 + t_1^{-2} \cdot r_2 \equiv 1 + t_8 \cdot t_4 \cdot t_2 \cdot r_2 \pmod 2.
\end{aligned}$$

По леммам 2 и 5

$$\begin{aligned} t_2 r_2 &\equiv r_2 + r_4 + r_0 + r_6 + r_2 \equiv r_4 + r_6 \pmod 2, \\ t_4 t_2 r_2 &\equiv t_4(r_4 + r_6) \equiv r_4 + r_8 + r_0 + r_{12} + r_4 + r_6 + r_{10} + r_2 + r_{14} + r_2 \equiv \\ &\equiv r_4 + r_2 \pmod 2, \\ t_8 t_4 t_2 r_2 &\equiv (1 + s_8 + s_{16})(r_2 + r_4) = (1 + s_8)(r_7 + r_2 + r_4) \equiv \\ &\equiv r_2 + r_4 \pmod 2. \end{aligned}$$

Поэтому $m(2,1)^2 \equiv 1 + r_2 + r_4 \pmod 2$.

Пусть, как в лемме 1, $\sigma_3 \in \mathrm{Gal}(\mathbb{Q}_{64})$, где $\sigma_3(\alpha) = \alpha^3$. Тогда по леммам 3 и 5 получим

$$\begin{aligned} \sigma_3(m(2,1)^2) \equiv &\sigma_3(t_1^{-2} t_7^2) = t_3^{-2} t_{21}^2 \equiv t_3^{-2} t_{42} \equiv t_3^{-2} t_{10} \equiv t_3^{-2} t_5^2 = m(2,3)^2 \pmod 2, \\ \sigma_3(m(2,1)^2) &\equiv \sigma_3(1 + r_2 + r_4) = 1 + r_6 + r_{12} \equiv 1 + r_4 + r_6 \pmod 2. \end{aligned}$$

□

Лемма 21. *При введённых ранее обозначениях* $\left(t_1^{-1} t_3\right)^4 \equiv 1 + r_4 \pmod 2$.

Доказательство. По лемме 14 имеем $t_1^{16} \equiv 1 \pmod 2$, поэтому по леммам 2 и 3

$$\begin{aligned} t_1^{-4} \equiv t_1^{12} = t_1^8 t_1^4 \equiv t_8 t_4 = (1 + s_8)(1 + s_4 + s_8) = \\ = (1 + s_4 + s_8) + (s_8 + s_4 + s_{12} + s_{16} + 2) \equiv 1 + s_{12} \pmod 2. \end{aligned}$$

Также по лемме 3 $t_3^4 \equiv t_{12} = 1 + s_{12} + s_{24} \equiv 1 + s_{12} + s_8 \pmod 2$. Следовательно, по лемме 2

$$\begin{aligned} \left(t_1^{-1} t_3\right)^4 &\equiv (1 + s_{12})(1 + s_{12} + s_8) = \\ &= (1 + s_{12} + s_8) + (s_{12} + s_{24} + 2 + s_4 + s_{20}) = \\ &= 1 + s_4 + s_{20} \equiv 1 + s_4 + s_{12} = 1 + r_4 \pmod 2. \end{aligned}$$

□

2.4. Разложение W_1 в прямое произведение циклических подгрупп

Теорема 1. *При введённых ранее обозначениях выполняются следующие утверждения.*

1. $M = D$, *и поэтому*

$$\begin{aligned} D = \langle t_1^{16} \rangle \times \langle t_1^{-8} t_3^8 \rangle \times \langle t_1^{-4} t_7^4 \rangle \times \langle t_3^{-4} t_5^4 \rangle \times \langle t_1^{-2} t_{15}^2 \rangle \times \langle t_3^{-2} t_{13}^2 \rangle \times \langle t_5^{-2} t_{11}^2 \rangle \times \langle t_7^{-2} t_9^2 \rangle \times \\ \times \langle t_3^{-1} t_{29} \rangle \times \langle t_5^{-1} t_{27} \rangle \times \langle t_7^{-1} t_{25} \rangle \times \langle t_9^{-1} t_{23} \rangle \times \langle t_{11}^{-1} t_{21} \rangle \times \langle t_{13}^{-1} t_{19} \rangle \times \langle t_{15}^{-1} t_{17} \rangle. \end{aligned}$$

2. $W_1 = \langle x^{32} \rangle \times V_1$, *где*

$$\begin{aligned} V_1 = \{ u_{\chi_1}(\lambda) \mid \lambda \in D \} = \\ = \langle u_{\chi_1}(t_1^{16}) \rangle \times \langle u_{\chi_1}(t_1^{-8} t_3^8) \rangle \times \left(\langle u_{\chi_1}(t_1^{-4} t_7^4) \rangle \times \langle u_{\chi_1}(t_3^{-4} t_5^4) \rangle \right) \times \\ \times \left(\langle u_{\chi_1}(t_1^{-2} t_{15}^2) \rangle \times \langle u_{\chi_1}(t_3^{-2} t_{13}^2) \rangle \times \langle u_{\chi_1}(t_5^{-2} t_{11}^2) \rangle \times \langle t_7^{-2} t_9^2 \rangle \right) \times \\ \times \left(\langle u_{\chi_1}(t_3^{-1} t_{29}) \rangle \times \langle u_{\chi_1}(t_5^{-1} t_{27}) \rangle \times \langle u_{\chi_1}(t_7^{-1} t_{25}) \rangle \times \langle u_{\chi_1}(t_9^{-1} t_{23}) \rangle \times \right. \\ \left. \times \langle u_{\chi_1}(t_{11}^{-1} t_{21}) \rangle \times \langle u_{\chi_1}(t_{13}^{-1} t_{19}) \rangle \times \langle u_{\chi_1}(t_{15}^{-1} t_{17}) \rangle \right). \end{aligned}$$

Доказательство. По предложению 3 утверждение 2 этой теоремы является непосредственным следствием утверждения 1. Докажем утверждение 1.

По леммам 17 и 18 достаточно доказать, что $\sqrt{M} \cap D = M$. По лемме 18 для этого достаточно доказать, что

$$d = t_1^{8\delta}(t_1^{-1}t_3)^{4\delta_0}(m(2,1))^{2\delta_{21}}(m(2,3))^{2\delta_{23}} \times \prod_{l=0}^{3}(m(1,2l+1))^{\delta_{1(2l+1)}} \in D$$

тогда и только тогда, когда

$$\delta \equiv \delta_0 \equiv \delta_{21} \equiv \delta_{23} \equiv \delta_{1(1)} \equiv \delta_{1(3)} \equiv \delta_{1(5)} \equiv \delta_{1(7)} \equiv 0 \pmod 2.$$

Естественно, можно считать, что $\{\delta, \delta_0, \delta_{21}, \delta_{23}, \delta_{1(1)}, \delta_{1(3)}, \delta_{1(5)}, \delta_{1(7)}\} \subseteq \{0,1\}$.

По леммам 2 и 3 $t_1^8 \equiv t_8 = 1 + s_8 + s_{16} = 1 + s_8 \pmod 2$. Поэтому по леммам 19, 20 и 21 имеем

$$\begin{aligned} d \equiv{}& (1+s_8)^{\delta}(1+r_4)^{\delta_0}(1+r_2+r_4)^{\delta_{21}}(1+r_4+r_6)^{\delta_{23}}\times \\ &\times (1+r_7+(r_2+r_4))^{\delta_{1(1)}}(1+r_5+(r_4+r_6))^{\delta_{1(3)}}(1+r_3+(r_4+r_6))^{\delta_{1(5)}}\times \\ &\times (1+r_1+(r_2+r_4))^{\delta_{1(7)}} \pmod 2. \end{aligned}$$

Поскольку все показатели степеней либо 0, либо 1, то

$$\begin{aligned} d \equiv{}& (1+\delta s_8)(1+\delta_0 r_4)(1+\delta_{21}(r_2+r_4))(1+\delta_{23}(r_4+r_6))\times \\ &\times (1+\delta_{1(1)}(r_7+(r_2+r_4)))(1+\delta_{1(3)}(r_5+(r_4+r_6)))\times \\ &\times (1+\delta_{1(5)}(r_3+(r_4+r_6)))(1+\delta_{1(7)}(r_1+(r_2+r_4))) \pmod 2. \end{aligned}$$

Далее в силу леммы 5 получим

$$\begin{aligned} d \equiv{}& 1+\delta s_8+\delta_0 r_4+\delta_{21}(r_2+r_4)+\delta_{23}(r_4+r_6)+ \\ &+\delta_{1(1)}(r_7+(r_2+r_4))+\delta_{1(3)}(r_5+(r_4+r_6)))+ \\ &+\delta_{1(5)}(r_3+(r_4+r_6))+\delta_{1(7)}(r_1+(r_2+r_4)) \pmod 2. \end{aligned}$$

Применяя лемму 7, получим, что $\delta_{1(1)} = \delta_{1(3)} = \delta_{1(5)} = \delta_{1(7)} = 0$. Поэтому имеем

$$d \equiv 1+\delta s_8+\delta_0 r_4+\delta_{21}(r_2+r_4)+\delta_{23}(r_4+r_6) \pmod 2.$$

Снова применяя лемму 7, получим, что $\delta = \delta_0 = \delta_{21} = \delta_{23} = 0$. □

Замечание 6. Т. А. Ханенко произвела вычисления в системе GAP [10], которые согласуются с утверждением 1 теоремы.

А именно, согласно лемме 17 для элементов $a = t_1^{i_1}t_3^{i_2}t_5^{i_3}t_7^{i_4}t_9^{i_5}t_{11}^{i_6}t_{13}^{i_7}t_{15}^{i_8}$ при $i_1 \in \{0,1,\ldots,15\}$; $i_2 \in \{0,1,\ldots,7\}$; $i_3, i_4 \in \{0,1,2,3\}$ и $i_5, i_6, i_7, i_8 \in \{0,1\}$ проверено (с помощью программы), существуют ли элементы, сравнимые с 1 по модулю 2.

Программа

```
a:=E(64);# Возвращает примитивный корень 64 степени из 1.
K:=CF(64);# Создает круговое поле Q_64
t:=[];
for j in [1..15] do
t[j]:=a^(2*j)+a^(j)+1+a^(-j)+a^(-2*j);
Add(t,t[j]);
```

```
od;
l:=[]; # список всех произведений
y:=[]; # список степеней
m:=[]; # список сумм
q:=[]; # список элементов, когда сумма = 1
h:=[]; # список степеней при которых сумма элементов =1
w:=[]; # список элементов
z:=[]; # список степеней
for i1 in [0..15] do
for i2 in [0..7] do
for i3 in [0..3] do
for i4 in [0..3] do
for i5 in [0..1] do
for i6 in [0..1] do
for i7 in [0..1] do
for i8 in [0..1] do
a:=t1^i1*t3^i2*t5^i3*t7^i4*t9^i5*t11^i6*t13^i7*t15^i8;
b:=CanonicalBasis(K); # Возвращает базис K
d:=Coefficients(b,a); # создаёт список коэффициентов элемента a
                      # в базисе b
f:=d mod 2; # приводит коэфициенты d по модулю 2
Add(l,f);
Add(m,d);
i:=[i1,i2,i3,i4,i5,i6,i7,i8];
Add(y,i);
od;
od;
od;
od;
od;
od;
od;
od;
k := Length(l); # количество элементов в списке
for j in [1..k] do
if l[j][1] = 1 then
if Sum(l[j]) = 1
then Add(q,l[j]);
Add(h,y[j]);
fi;
fi;
od;
gap > q;
[]
gap > h;
[]
```

ВЫВОД: В результате работы программы получено, что среди исследуемых элементов только один сравним с 1 по модулю 2. Это элемент, у которого все показатели степеней равны 0.

Список литературы

1. **Алеев, Р. Ж.** Сравнение по модулю 2 круговых единиц в полях Q_{16} и Q_{32} / Р. Ж. Алеев, О. В. Митина, Е. А. Христенко // Челяб. физ.-мат. журн. — 2016. — Т. 1, вып. 4. — С. 8–29.
2. **Алеев, Р. Ж.** Нахождение единиц целочисленных групповых колец циклических групп порядков 16 и 32 / Р. Ж. Алеев, О. В. Митина, Т. А. Ханенко // Челяб. физ.-мат. журн. — 2016. — Т. 1, вып. 4. — С. 30–55.
3. **Алеев, Р. Ж.** Описание групп единиц целочисленного группового кольца циклической группы порядка 16 / Р. Ж. Алеев, О. В. Митина, Т. А. Ханенко // Тр. Ин-та математики и механики УрО РАН. — 2017. — Т. 23, вып. 4. — С. 32–42.
4. **Алеев, Р. Ж.** Единицы полей характеров и центральные единицы целочисленных групповых колец конечных групп / Р. Ж. Алеев // Мат. тр. — 2000. — Т. 3, вып. 1. — С. 3–37.
5. **Aleev, R. Ž.** Higman's central unit theory, units of integer group rings of finite cyclic groups and Fibonacci numbers / R. Ž. Aleev // International Journal of Algebra and Computation. — 1994. — Vol. 4, no. 3. — P. 309–358.
6. **Алеев, Р. Ж.** Центральные элементы целочисленных групповых колец / Р. Ж. Алеев // Алгебра и логика. — 2000. — Т. 39, вып. 5. — С. 513–525.
7. **Алеев, Р. Ж.** Вычисление квантовых факториалов и к ним обратных / Р. Ж. Алеев, И. Р. Мухамадеева // Челяб. физ.-мат. журн. — 2016. — Т. 1, вып. 1. — С. 6–15.
8. **Ван дер Варден, Б. Л.** Алгебра / Б. Л. ван дер Варден. — 2-е изд-е. — М. : Наука, гл. ред. физ.-мат. лит., 1979. — 624 с.
9. **Liang, J. J.** On the integer basis of the maximal real subfield of a cyclotomic field / J. J. Liang // Journal für die reine und angewandte Mathematik. — 1976. — Band 286/287. — P. 223–226.
10. The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.7.7; 2015 [Электронный ресурс]. — URL: http://www.gap-system.org (дата обращения: 15.06.2018).

Поступила в редакцию 02.06.2018
После переработки 03.08.2018

Сведения об авторах

Алеев Рифхат Жалялович, доктор физико-математических наук, доцент, профессор кафедры компьютерной топологии и алгебры, Челябинский государственный университет, Челябинск, Россия; профессор кафедры системного программирования, Южно-Уральский государственный университет (национальный исследовательский университет), Челябинск, Россия; e-mail: aleev@csu.ru.

Митина Ольга Викторовна, кандидат физико-математических наук, доцент кафедры компьютерной топологии и алгебры, Челябинский государственный университет, Челябинск, Россия; доцент кафедры прикладной математики и программирования, Южно-Уральский государственный университет (национальный исследовательский университет), Челябинск, Россия; e-mail: ovm588@gmail.com.

Ханенко Татьяна Александровна, студентка математического факультета, Челябинский государственный университет, Челябинск, Россия; e-mail: tanja_1110_94@mail.ru.

Chelyabinsk Physical and Mathematical Journal. 2018. Vol. 3, iss. 3. P. 253–275.

DOI: 10.24411/2500-0101-2018-13301

LOCAL UNITS OF INTEGER GROUP RING OF CYCLIC GROUP OF ORDER 64 FOR CHARACTER WITH CHARACTER FIELD $\mathbb{Q}_{64}$

R.Zh. Aleev[1,2,a], O.V. Mitina[1,2,b], T.A. Khanenko[1,c]

[1] *Chelyabinsk State University, Chelyabinsk, Russia*
[2] *South Ural State University (National Research University), Chelyabinsk, Russia*
[a] *aleev@csu.ru,* [b] *ovm@csu.ru,* [c] *tanja_1110_94@mail.ru*

The work is devoted to the study of units of the integer group ring for order 64 cyclic group. The units groups of the integer group rings for the cyclic groups of the orders 2 and 4 are trivial, for the order 8 this group is well known, for the cyclic group of the order 16 such group is described earlier. The study of units of the integer group ring of the order 64 cyclic group is carried out in terms of local units defined by the characters of the order 64 cyclic group and by units of the ring of the circular field $\mathbb{Q}_{64}$, obtained by adjoining the degree 64 primitive root of 1 to the field of the rational numbers. The most important role among the local units is played by units for the character with the character field $\mathbb{Q}_{64}$, because they provide the possibility of the inductive approach to the description of the units groups of the integer group rings for the cyclic 2-groups. We note that earlier, by direct calculations, the authors obtained a description of the local units for a character with the character field $\mathbb{Q}_{32}$ of the integer group ring for the cyclic group of the order 32. Therefore, the next natural step is to study the local units for a character with the character field $\mathbb{Q}_{64}$ of the integer group ring for the order 64 cyclic group. To achieve these goals, a new approach has been developed, which can be applied to units groups of the integer group rings for the cyclic 2-groups of an order greater than 64.

Keywords: *group ring, unit of group ring, cyclic group, cyclotomic field, integer group ring.*

References

1. **Aleev R.Zh., Mitina O.V., Khristenko E.A.** Sravneniye po modulyu 2 krugovykh edinits v polyakh Q_{16} i Q_{32} [Congruence modulo 2 of circular units in the fields Q_{16} and Q_{32}]. *Chelyabinskiy fiziko-matematicheskiy zhurnal* [Chelyabinsk Physical and Mathematical Journal], 2016, vol. 1, iss. 4, pp. 8–29. (In Russ.).
2. **Aleev R.Zh., Mitina O.V., Khanenko T.A.** Nakhozhdeniye edinits tselochislennykh gruppovykh kolets tsiklicheskikh grupp poryadkov 16 i 32 [Finding of units for integer group rings of orders 16 and 32 cyclic groups]. *Chelyabinskiy fiziko-matematicheskiy zhurnal* [Chelyabinsk Physical and Mathematical Journal], 2016, vol. 1, no. 4, pp. 30–55. (In Russ.).
3. **Aleev R.Zh., Mitina O.V., Khanenko T.A.** Opisaniye edinits group tselochislennykh gruppovykh kolets tsiklicheskikh grupp poryadka 16 [Description of the unit group of the integer group ring of a cyclic group of order 16]. *Trudy Instituta Matematiki i Mekhaniki UrO RAN* [Proceedings of Istitute of Mathematics and Mechanics], 2017, vol. 23, iss. 4, pp. 32–42. (In Russ.).
4. **Aleev R.Zh.** Units of character fields and central units of integer group rings of finite groups. *Siberian Advances of Mathematics*, 2001, vol. 11, iss 1. pp. 1–33.
5. **Aleev R.Ž.** Higman's central unit theory, units of integer group rings of finite cyclic groups and Fibonacci numbers. *International Journal of Algebra and Computation*, 1994, vol. 4, no. 3, pp. 309–358.
6. **Aleev R.Zh.** Central elements of integer group rings. *Algebra and Logic*, 2000, vol. 39, no. 5, pp. 293–300.

7. **Aleev R.Zh., Mukhamadeeva I.R.** Vychisleniye kvantovykh faktorialov i k nim obratnykh [Computation of quantum factorials and their inverses]. *Chelyabinskiy fiziko-matematicheskiy zhurnal* [Chelyabinsk Physical and Mathematical Journal], 2016, vol. 1, iss. 1, pp. 6–15. (In Russ.).
8. **Van der Varden B.L.** *Algebra* [Algebra]: 2nd ed. Moscow, Nauka Publ., 1979. 624 p. (In Russ.).
9. **Liang J.J.** On the integer basis of the maximal real subfield of a cyclotomic field. *Journal für die reine und angewandte Mathematik*, 1976, Band 286/287, pp. 223–226.
10. *The GAP Group*, GAP — Groups, Algorithms, and Programming, Version 4.7.7; 2015. Availabel at: http://www.gap-system.org, accessed 15.06.2018.

Accepted article received 02.06.2018
Corrections received 03.08.2018