ТРУДЫ ИНСТИТУТА МАТЕМАТИКИ И МЕХАНИКИ УрО РАН

Том 23 № 4 2017

УДК 512.552.7

ОПИСАНИЕ ГРУППЫ ЕДИНИЦ ЦЕЛОЧИСЛЕННОГО ГРУППОВОГО КОЛЬЦА ЦИКЛИЧЕСКОЙ ГРУППЫ ПОРЯДКА 16 [1]

Р. Ж. Алеев, О. В. Митина, Т. А Ханенко

Работа посвящена описанию группы U единиц целочисленного группового кольца циклической группы порядка 16. Группы единиц целочисленных групповых колец циклических групп порядков 2 и 4 тривиальны, а группа единиц целочисленного группового кольца циклической группы порядка 8 хорошо известна. Поэтому случай циклической группы порядка 16 является первым, для которого не проведено полное исследование строения группы единиц целочисленного группового кольца циклической 2-группы. При изучении групп единиц целочисленных групповых колец циклических 2-групп порядков более 16 обязательно возникнет потребность в информации о строении групп единиц целочисленных групповых колец циклических 2-групп меньших порядков, в частности, порядка 16. Таким образом, можно сказать, что случай группы порядка 16 является базисным для дальнейших исследований. Описание группы U получено в терминах локальных единиц, определяемых характерами циклической группы порядка 16 и единицами кольца целых кругового поля $\mathbf{Q}_{16}$, полученного присоединением к полю рациональных чисел примитивного корня из 1 степени 16. Поэтому потребовалось весьма подробное изучение строения группы единиц кольца целых кругового поля $\mathbf{Q}_{16}$. Кроме того в работе получены важные соотношения между коэффициентами произвольной единицы из U. Эти соотношения, очевидно, послужат образцами и примерами для получения подобных соотношений при исследовании единиц для случаев 2-групп порядков, больших 16. Наконец, отметим, что один из порождающих группы U является особой единицей, которая определяется двумя единицами кольца целых кругового поля $\mathbf{Q}_{16}$. Эта единица является произведением двух локальных единиц, каждая из которых не содержится в U.

Ключевые слова: циклическая группа, групповое кольцо, единица группового кольца, круговое поле, кольцо целых поля, единица кольца целых кругового поля, целочисленное групповое кольцо.

R. Zh. Aleev, O. V. Mitina, T. A. Khanenko. Description of the unit group of the integral group ring of a cyclic group of order 16.

The paper is devoted to the description of the group of units of the integral group ring of a cyclic group of order 16. The groups of units of the integral group rings of cyclic groups of orders 2 and 4 are trivial, and the group of units of the integral group ring of a cyclic group of order 8 is well known. Thus, the case of a cyclic group of order 16 is the first for which the structure of the group of units of the integral group ring of a cyclic 2-group has not been studied completely. When the groups of units of the integral group rings of cyclic 2-groups of orders greater than 16 are studied, it is necessary to have information on the structure of the groups of units of the integral group rings of cyclic 2-groups of lower orders, in particular, of order 16. Thus, we can say that the case of the group of order 16 is the basis for further research. We describe the group of units of the integral group ring of a cyclic group of order 16 in terms of local units defined by the characters of a cyclic group of order 16 and by the units of the ring of integers of the cyclotomic field $\mathbf{Q}_{16}$ obtained by adjoining a primitive root of unity of degree 16 to the field of rational numbers. That is why we study in detail the structure of the group of units of the ring of integers of the cyclotomic field $\mathbf{Q}_{16}$. In addition, we derive important relations between the coefficients of an arbitrary unit of the integral group ring of a cyclic group of order 16. These relations will obviously serve as patterns and examples for obtaining similar relations in studying the units for the cases of 2-groups of orders greater than 16. Finally, we note that one of the generators of the group of units of the integral group ring of a cyclic group of order 16 is a singular unit defined by two units of the ring of integers of the cyclotomic field $\mathbf{Q}_{16}$. This unit is the product of the two local units, each of which is not contained in the integral group ring of a cyclic group of order 16.

Keywords: cyclic group, group ring, unit of a group ring, cyclotomic field, ring of integers of a field, unit of the ring of integers of a cyclotomic field, integral group ring.

MSC: 16S34

DOI: 10.21538/0134-4889-2017-23-4-32-42

[1]Статья выполнена при поддержке Правительства РФ (постановление № 211 от 16.03.2013 г.), соглашение № 02.A03.21.0011.

К 70-летию академика С.В. Матвеева

Введение

Эта работа продолжает статьи [1;2] и в то же время открывает цикл работ, посвященных индуктивному подходу к описанию групп единиц целочисленных групповых колец циклических 2-групп. Многие результаты данной статьи легко переносятся на общий случай произвольных циклических 2-групп, но неизбежное в таких случаях усложнение формулировок и формул останавливает авторов от подобного шага.

1. Основные понятия и определения

1.1. Круговые поля

Обозначим через $\mathbf{Q}(\alpha_{16}) = \mathbf{Q}_{16}$ круговое поле, полученное присоединением к полю рациональных чисел $\mathbf{Q}$ примитивного корня $\alpha = \cos(2\pi/16) + i\sin(2\pi/16)$ степени 16 из единицы. Аналогично определяются круговые поля $\mathbf{Q}_8$ и $\mathbf{Q}_4 = \mathbf{Q}(i)$.

Кольцом целых кругового поля $\mathbf{Q}_{16}$ является

$$\mathbf{Z}[\alpha] = \{f(\alpha) \mid f \in \mathbf{Z}[t]\}$$

— множество значений от α всех многочленов с целыми коэффициентами.

Также через $\mathrm{tr}_{\mathbf{Q}_{2^n}}$ обозначим след в поле $\mathbf{Q}_{2^n}$ для $n \in \{2, 3, 4\}$.

Нам потребуется следующее небольшое уточнение леммы 1 из [2], которое, очевидно, получается из свойств следа.

Лемма 1. *Для любого* $\rho \in \mathbf{Z}[\alpha^{2^n}]$, *где* $n \in \{0, 1, 2\}$, *имеем* $\mathrm{tr}_{\mathbf{Q}_{2^{4-n}}}(\rho) \equiv 0 (\mathrm{mod}\ 2^{3-n})$. *Более точно, если*

$$\rho = \sum_{j=0}^{2^{3-n}-1} b_j \alpha^{2^n j}, \ \text{где}\ \{b_0, \ldots, b_{2^{3-n}-1}\} \subseteq \mathbf{Z},$$

то $\mathrm{tr}_{\mathbf{Q}_{2^{4-n}}}(\rho) = 2^{3-n} b_0 \equiv 0 (\mathrm{mod}\ 2^{3-n})$.

Обозначим через $U(\mathbf{Z}[\alpha])$ группу единиц (обратимых элементов) кольца $\mathbf{Z}[\alpha]$, и вообще группу единиц всякого ассоциативного кольца K с единицей будем обозначать через $U(K)$.

Положим для $k \in \{0, 1, 2\}$

$$t_{2k+1} = \alpha^{2(2k+1)} + \alpha^{2k+1} + 1 + \alpha^{-(2k+1)} + \alpha^{-2(2k+1)} \in \mathbf{Z}[\alpha + \alpha^{-1}].$$

Лемма 2. *Группы единиц колец целых круговых полей* $\mathbf{Q}_{2^n}$ *для* $n \in \{2, 3, 4\}$ *известны. Более точно имеем*

1) $U(\mathbf{Z}[\alpha^4])$ *тривиальна, т.е.* $U(\mathbf{Z}[\alpha^4]) = \{1, i, -1, -i\}$;
2) $U(\mathbf{Z}[\alpha^2]) = \langle \alpha^2 \rangle \times \langle 1 + \sqrt{2} \rangle$, *где* $\sqrt{2} = \alpha^2 + \alpha^{-2}$;
3) $U(\mathbf{Z}[\alpha]) = \langle \alpha \rangle \times \langle t_1 \rangle \times \langle t_3 \rangle \times \langle t_5 \rangle$.

Д о к а з а т е л ь с т в о. Утверждения 1 и 2 хорошо известны и нетрудно доказываются. Утверждение 3 — это следствие 2 в [1].

Лемма доказана.

Следующий результат является чисто техническим, он будет использоваться несколько раз.

Лемма 3. *Группа $U(\mathbf{Z}[\alpha^2])$ единиц кольца целых кругового поля $\mathbf{Q}_8$ имеет следующие свойства.*

1. *Для любого целого числа r положим $(1+\sqrt{2})^r = c_r + d_r\sqrt{2}$, где c_r и d_r — целые числа, тогда последовательность $\{(c_r, d_r)\}_{r\in\mathbf{Z}}$ по модулю 4 является периодической с периодом 4. Более точно, для любого целого числа m имеем*

$$\begin{cases} c_{4m} \equiv 1 \pmod 4 \\ d_{4m} \equiv 0 \pmod 4 \end{cases}, \begin{cases} c_{4m+1} \equiv 1 \pmod 4 \\ d_{4m+1} \equiv 1 \pmod 4 \end{cases}, \begin{cases} c_{4m+2} \equiv 3 \pmod 4 \\ d_{4m+2} \equiv 2 \pmod 4 \end{cases}, \begin{cases} c_{4m+3} \equiv 3 \pmod 4 \\ d_{4m+3} \equiv 1 \pmod 4 \end{cases}.$$

2. *Пусть $\beta = \alpha^{2s}(c_r + d_r\sqrt{2})$ — произвольный элемент группы $U(\mathbf{Z}[\alpha^2])$, где $s \in \{0, 1, \ldots, 7\}$ и $r \in \mathbf{Z}$. Пусть также $\beta = b_0 + b_1\alpha^2 + b_2\alpha^4 + b_3\alpha^6$ — разложение β по базису кругового поля $\mathbf{Q}_8$. Тогда коэффициенты b_0, b_1, b_2 и b_4 в зависимуости от s находятся следующим образом:*

s	b_0	b_1	b_2	b_3
0	c_r	d_r	0	$-d_r$
1	d_r	c_r	d_r	0
2	0	d_r	c_r	d_r
3	$-d_r$	0	d_r	c_r

и

s	b_0	b_1	b_2	b_3
4	$-c_r$	$-d_r$	0	d_r
5	$-d_r$	$-c_r$	$-d_r$	0
6	0	$-d_r$	$-c_r$	$-d_r$
7	d_r	0	$-d_r$	$-c_r$

.

Д о к а з а т е л ь с т в о. 1. Действуем стандартно. Так как

$$(1+\sqrt{2})^{r+1} = (c_r + d_r\sqrt{2})(1+\sqrt{2}) = (c_r + 2d_r) + (c_r + d_r)\sqrt{2},$$

то

$$\begin{cases} c_{r+1} = c_r + 2d_r, \\ d_{r+1} = c_r + d_r \end{cases} \longleftrightarrow \begin{pmatrix} c_{r+1} \\ d_{r+1} \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} c_r \\ d_r \end{pmatrix}.$$

Найдем характеристический многочлен получившейся матрицы

$$\det \begin{pmatrix} 1-\lambda & 2 \\ 1 & 1-\lambda \end{pmatrix} = (1-\lambda)^2 - 2 = \lambda^2 - 2\lambda - 1.$$

По теореме Гамильтона — Якоби

$$\begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}^2 = 2\begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} + 2\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Отсюда

$$\begin{pmatrix} c_{r+2} \\ d_{r+2} \end{pmatrix} = 2\begin{pmatrix} c_{r+1} \\ d_{r+1} \end{pmatrix} + \begin{pmatrix} c_r \\ d_r \end{pmatrix} \longleftrightarrow \begin{cases} c_{r+2} = 2c_{r+1} + c_r, \\ d_{r+2} = 2d_{r+1} + d_r \end{cases}$$

с начальными данными

$$(c_0, d_0) = (1, 0) \text{ и } (c_1, d_1) = (1, 1).$$

Получим, что последовательность $\{c_r\}_{r\in\mathbf{Z}}$ состоит из нечетных чисел. Элементы последовательности $\{c_r\}_{r=0}^{\infty}$ по модулю 4 таковы:

$$1, 1, 3, 3, 1, 1, \ldots .$$

Запишем элементы последовательности $\{d_r\}_{r=0}^{\infty}$ по модулю 4:

$$0, 1, 2, 1, 0, 1, 2, 1, \ldots .$$

Отметим, что в этой последовательности все элементы с четными номерами являются четными, а все элементы с нечетными номерами сравнимы с 1 по модулю 4.

Получим периодическую последовательность по модулю 4:

$$(c_r, d_r)_{r\in\mathbf{Z}} = \begin{cases} (1,0) & \text{при } r \equiv 0 \pmod 4, \\ (1,1) & \text{при } r \equiv 1 \pmod 4, \\ (3,2) & \text{при } r \equiv 2 \pmod 4, \\ (3,1) & \text{при } r \equiv 3 \pmod 4. \end{cases}$$

2. Поскольку $\alpha^{2(s+4)} = -\alpha^{2s}$, то достаточно рассмотреть случай, когда $s \in \{0,1,2,3\}$.

Для $s = 0$ имеем $\beta = c_r\alpha^0 + d_r\alpha^{2+0} + d_r\alpha^{-2+0} = c_r + d_r\alpha^2 - d_r\alpha^6$. Поэтому $b_0 = c_r$, $b_1 = d_r$, $b_2 = 0$ и $b_3 = -d_r$.

Для $s = 1$ имеем $\beta = c_r\alpha^2 + d_r\alpha^{2+2} + d_r\alpha^{-2+2} = d_r + c_r\alpha^2 + d_r\alpha^4$. Поэтому $b_0 = d_r$, $b_1 = c_r$, $b_2 = d_r$ и $b_3 = 0$.

Для $s = 2$ имеем $\beta = c_r\alpha^4 + d_r\alpha^{2+4} + d_r\alpha^{-2+4} = a_r\alpha^2 + c_r\alpha^4 + d_r\alpha^6$. Поэтому $b_0 = 0$, $b_1 = d_r$, $b_2 = c_r$ и $b_3 = d_r$.

Для $s = 3$ имеем $\beta = c_r\alpha^6 + d_r\alpha^{2+6} + d_r\alpha^{-2+6} = -d_r + d_r\alpha^4 + c_r\alpha^6$. Поэтому $b_0 = -d_r$, $b_1 = 0$, $b_2 = d_r$ и $b_3 = c_r$.

Лемма доказана.

1.2. Коэффициенты элементов группового кольца

Пусть $G = \langle x \mid x^{16} = 1\rangle$ — циклическая группа порядка 16.

Любой элемент u комплексной групповой алгебры $\mathbf{C}G$ группы G может быть представлен в виде

$$u = \sum_{j=0}^{15} \beta_j e_j = \sum_{k=0}^{15} \gamma_k x^k,$$

где $1, x, \ldots, x^{15}$ — элементы группы G; $e_0, e_1, \ldots, e_{15}$ — минимальные идемпотенты комплексной групповой алгебры $\mathbf{C}G$; коэффициенты β_j, γ_k принадлежат $\mathbf{C}$ для любых $j, k \in \{0, 1, \ldots, 15\}$.

По таблице характеров для циклической группы порядка 16 получим согласно [3, § 37], что для любого $k \in \{0, 1, \ldots, 15\}$

$$\gamma_k = \frac{1}{16}\sum_{j=0}^{15} \alpha^{-jk}\beta_j \text{ и } \beta_k = \sum_{j=0}^{15} \alpha^{jk}\gamma_j.$$

Пусть $V(\mathbf{Z}G)$ — нормализованная группа единиц кольца $\mathbf{Z}G$, т.е. группа таких единиц целочисленного группового кольца $\mathbf{Z}$, что при разложении их по элементам группы сумма всех коэффициентов разложения равна 1. Это равносильно тому, что $\beta_0 = 1$.

Лемма 4. *Пусть*

$$\sum_{j=0}^{15} \beta_j e_j = \sum_{k=0}^{15} \gamma_k x^k$$

— единица из группы $V(\mathbf{Z}G)$ и

$$\beta_1 = \sum_{l=0}^{7} a_l\alpha^l \text{ и } \beta_2 = \sum_{l=0}^{3} b_l\alpha^{2l}.$$

Если $a_0 + a_4$ — нечетное целое число, то выполняются следующие утверждения:

1) $\beta_8 = \beta_4 = 1$*;*

2) *если* $\beta_2 = \alpha^{2s}(c_r + d_r\sqrt{2})$, *где* $s \in \{0, 1, \ldots, 7\}$ *и* $r \in \mathbf{Z}$, *то* $b_2 = 0$ *и либо* $s = 0$, $r \equiv 0$, $b_0 = c_r \equiv 1 \pmod 4$ *и* $b_1 = -b_3 = d_r \equiv 0 \pmod 4$, *либо* $s = 4$, $r \equiv 2$, $b_0 = -c_r \equiv 1 \pmod 4$ *и* $b_1 = -b_3 = -d_r \equiv 2 \pmod 4$;

3) *имеем следующие выражения для коэффициентов* $\gamma_0,\dots,\gamma_{15}$:

$$\gamma_0=\frac{1}{4}\left(1+b_0+2a_0\right), \qquad \gamma_8=\gamma_0-a_0, \qquad \gamma_4=\frac{1}{4}\left(1-b_0+2a_4\right), \qquad \gamma_{12}=\gamma_4-a_4,$$
$$\gamma_2=\frac{1}{2}a_2, \qquad \gamma_{10}=-\gamma_2, \qquad \gamma_6=\frac{1}{2}a_6, \qquad \gamma_{14}=-\gamma_6,$$
$$\gamma_1=\frac{1}{4}\left(b_1+2a_1\right), \qquad \gamma_9=\gamma_1-a_1, \qquad \gamma_3=\frac{1}{4}\left(-b_1+2a_3\right), \qquad \gamma_{11}=\gamma_3-a_3,$$
$$\gamma_5=\frac{1}{4}\left(-b_1+2a_5\right), \qquad \gamma_{13}=\gamma_5-a_5, \qquad \gamma_7=\frac{1}{4}\left(b_1+2a_7\right), \qquad \gamma_{15}=\gamma_7-a_7.$$

Д о к а з а т е л ь с т в о. 1) По [4, лемма 6] для любого $k\in\{0,1,2,3,\dots,15\}$ имеем

$$\gamma_k=\frac{1}{16}\Big(1+\sum_{l=0}^{3}\mathrm{tr}_{\mathbf{Q}_{2^{4-l}}}\left(\alpha^{-k\cdot 2^l}\beta_{2^l}\right)\Big).$$

Отсюда по лемме 1 получим

$$\gamma_0=\frac{1}{16}\left(1+\beta_8+\mathrm{tr}_{\mathbf{Q}_4}(\beta_4)+\mathrm{tr}_{\mathbf{Q}_8}(\beta_2)+8a_0\right), \ \gamma_4=\frac{1}{16}\left(1+\beta_8+\mathrm{tr}_{\mathbf{Q}_4}(\beta_4)-\mathrm{tr}_{\mathbf{Q}_8}(\beta_2)+8a_4\right).$$

Следовательно,

$$\gamma_0+\gamma_4=\frac{1}{16}\left(2+2\beta_8+2\mathrm{tr}_{\mathbf{Q}_4}(\beta_4)+8(a_0+a_4)\right)=\frac{1}{8}\left(1+\beta_8+2\mathrm{tr}_{\mathbf{Q}_4}(\beta_4)+4(a_0+a_4)\right).$$

Поскольку a_0+a_4 — нечетное целое число, то

$$B=1+\beta_8+2\mathrm{tr}_{\mathbf{Q}_4}(\beta_4)\equiv 4(\mathrm{mod}\ 8).$$

Так как $\beta_8\in\{1,-1\}$, $\beta_4\in\{1,-1,i,-i\}$, $\mathrm{tr}_{\mathbf{Q}_4}(\beta_4)\in\{2,-2,0\}$ и $B\equiv 4 \pmod 8$, то

$$\beta_8=\beta_4=1.$$

2) Простыми вычислениями с использованием утверждения 1) этой леммы и леммы [4, лемма 6] получим следующие выражения для коэффициентов $\gamma_0,\dots,\gamma_{15}$:

$$\gamma_0=\frac{1}{4}\left(1+b_0+2a_0\right), \qquad \gamma_8=\gamma_0-a_0, \qquad \gamma_4=\frac{1}{4}\left(1-b_0+2a_4\right), \qquad \gamma_{12}=\gamma_4-a_4,$$
$$\gamma_2=\frac{1}{4}\left(b_2+2a_2\right), \qquad \gamma_{10}=\gamma_2-a_2, \qquad \gamma_6=\frac{1}{4}\left(-b_2+2a_6\right), \qquad \gamma_{14}=\gamma_6-a_6,$$
$$\gamma_1=\frac{1}{4}\left(b_1+2a_1\right), \qquad \gamma_9=\gamma_1-a_1, \qquad \gamma_3=\frac{1}{4}\left(b_3+2a_3\right), \qquad \gamma_{11}=\gamma_3-a_3,$$
$$\gamma_5=\frac{1}{4}\left(-b_1+2a_5\right), \qquad \gamma_{13}=\gamma_5-a_5, \qquad \gamma_7=\frac{1}{4}\left(-b_3+2a_7\right), \qquad \gamma_{11}=\gamma_7-a_7.$$

Из этих выражений следует система сравнений по модулю 4

$$\begin{cases} b_0\equiv -1-2a_0\equiv 1+2a_4 \pmod 4,\\ b_2\equiv -2a_2\equiv 2a_6 \pmod 4,\\ b_1\equiv -2a_1\equiv 2a_5 \pmod 4,\\ b_3\equiv -2a_3\equiv 2a_7 \pmod 4.\end{cases}$$

Из этой системы, используя лемму 3, получаем нужное утверждение.

3) По [4, лемма 6] для любого $k\in\{0,1,2,3,\dots,15\}$ из утверждения 2) данной леммы нетрудно получить нужные выражения.

Лемма доказана.

1.3. Локальные единицы

Циклическая группа $G = \langle x \rangle$ порядка 16 имеет 16 неприводимых комплексных характеров: $\chi_0 = 1_G$ — главный характер, $\chi_1, \ldots, \chi_{15}$, и для любых $j, k \in \{0, 1, \ldots, 15\}$ имеем

$$\chi_j(x^k) = \alpha^{jk}.$$

Хорошо известно, что группа Галуа поля $\mathbf{Q}_{16}$ состоит из автоморфизмов σ_k поля $\mathbf{Q}_{16}$, продолжающих отображения $\alpha \mapsto \alpha^{2k+1}$ для $k \in \{0, 1, \ldots, 7\}$. Поэтому для любого $k \in \{0, 1, \ldots, 7\}$ характер χ_{2k+1} алгебраически сопряжен с характером χ_1. Аналогично алгебраически сопряжены характеры χ_2, χ_6, χ_{10} и χ_{14}, а также характеры χ_4 и χ_{12}.

По каждому характеру и любому элементу кольца целых поля этого характера можно согласно определению 1 из [5] построить единицу кольца целых рациональной групповой алгебры $\mathbf{Q}G$. Такие единицы будем называть *локальными*.

Определим локальные единицы более точно. Для каждой единицы $\lambda_1 \in U(\mathbf{Z}[\alpha])$ можно определить элемент

$$u_1(\lambda_1) = \sum_{k=0}^{7} \sigma_k(\lambda_1) e_{2k+1} + \sum_{k=0}^{7} e_{2k},$$

принадлежащий группе единиц кольца целых рациональной групповой алгебры $\mathbf{Q}G$. Отметим, что при переходе к базису из элементов группы G такая единица имеет рациональные коэффициенты, которые не обязаны быть целыми.

Аналогично для каждой единицы $\lambda_2 \in U(\mathbf{Z}[\alpha^2])$ определяется элемент

$$u_2(\lambda_2) = \sum_{k=0}^{7} e_{2k+1} + \sum_{k=0}^{3} \sigma_k(\lambda_2) e_{4k+2} + \sum_{k=0}^{3} e_{4k},$$

принадлежащий группе единиц кольца целых рациональной групповой алгебры $\mathbf{Q}G$.

Также для каждой единицы $\lambda_4 \in U(\mathbf{Z}[\alpha^4])$ имеем

$$u_4(\lambda_4) = \sum_{k=0}^{7} e_{2k+1} + \sum_{k=0}^{3} e_{4k+2} + \lambda_4 e_4 + \overline{\lambda_4} e_{12} + e_0 + e_8.$$

В этом случае возникают всего 4 локальные единицы (следует из леммы 2)

$$u_4(1) = 1,\ u_4(i), u_4(-1) \text{ и } u_4(-i).$$

Наконец, имеем две локальные единицы

$$u_8(\pm 1) = \sum_{k=0}^{7} e_{2k+1} + \sum_{k=0}^{3} e_{4k+2} + e_4 + e_{12} + e_0 + (\pm e_8).$$

С другой стороны, пусть дана единица

$$v = \sum_{j=0}^{15} \beta_j e_j = \sum_{k=0}^{15} \gamma_k x^k \in V(\mathbf{Z}G).$$

По [4, лемма 6] из мультипликативности минимальных идемпотентов $e_0, e_1, \ldots, e_{15}$ следует, что

$$v = u_1(\beta_1) u_2(\beta_2) u_4(\beta_4) u_8(\beta_8).$$

2. Группа единиц с $\beta_1 = 1$

В этом разделе мы рассмотрим единицы из $V(\mathbf{Z}G)$, у которых $\beta_1 = 1$, т.е. рассмотрим подмножество

$$W = \{v = u_2(\beta_2)u_4(\beta_4)u_8(\beta_8) \mid v \in V(\mathbf{Z}G)\}\,.$$

Лемма 5. *W — подгруппа без кручения группы $V(\mathbf{Z}G)$.*

Д о к а з а т е л ь с т в о. Из мультипликативности минимальных идемпотентов следует, что W является подгруппой группы $V(\mathbf{Z}G)$. Отсутствие кручения следует из [2, предложение 1].

Лемма доказана.

Лемма 6. *Пусть*

$$\sum_{j=0}^{15} \beta_j e_j = \sum_{k=0}^{15} \gamma_k x^k$$

— единица из группы W. Тогда

1) $\beta_8 = \beta_4 = 1$ *и* $W = \{u_2(\beta_2) \in V(\mathbf{Z}G)\}$;

2) $\beta_2 \in \langle (1+\sqrt{2})^4 \rangle$;

3) *если* $\beta_2 = c_r + d_r\sqrt{2}$ *для* $r \equiv 0 (\mathrm{mod}\ 4)$, *то*

$$\gamma_0 = \frac{1}{4}\,(3 + c_r)\,,\ \gamma_8 = \gamma_0 - 1, \qquad \gamma_4 = \gamma_{12} = \frac{1}{4}\,(1 - c_r)\,,\ \gamma_2 = \gamma_{10} = \gamma_6 = \gamma_{14} = 0,$$
$$\gamma_1 = \gamma_9 = \gamma_3 = \gamma_{11} = \frac{1}{4}\,(d_r)\,, \qquad \gamma_5 = \gamma_{13} = \gamma_7 = \gamma_{15} = \frac{1}{4}\,(-d_r)\,.$$

Д о к а з а т е л ь с т в о. 1) Очевидно, что выполняются условия леммы 4, откуда получим требуемое.

2) Пусть $\beta_2 = \alpha^{2s}(c_r + d_r\sqrt{2})$, где $s \in \{0, 1, \ldots, 7\}$ и $r \in \mathbf{Z}$. Тогда по лемме 4 получим, что надо исключить случай $s = 4$. Действительно, по лемме 4 при $s = 4$ имеем $d_r \equiv 2 \pmod 4$. Это противоречит тому, что тогда $\gamma_1 = -d_r/4$.

3) Указанные выражения легко получаются из леммы 4.

Лемма доказана.

Предложение 1. *При введенных ранее обозначениях*

$$W = \left\langle u_2\left((1+\sqrt{2})^4\right)\right\rangle,$$

где

$$u_2\left((1+\sqrt{2})^4\right) = \sum_{k=0}^{7} e_{2k+1} + \sum_{k=0}^{3} e_{4k} + (1+\sqrt{2})^4(e_2 + e_{10}) + (1-\sqrt{2})^4(e_6 + e_{14})$$
$$= 5 + 3(x - x^3 - x^5 + x^7 + x^9 - x^{11} - x^{13} + x^{15}) + 4(-x^4 + x^8 - x^{12}).$$

Д о к а з а т е л ь с т в о. Из лемм 5 и 6 и мультипликативности минимальных центральных идемпотентов $e_0, e_1, \ldots, e_{15}$ следует, что

$$W = \left\{u_2\left((1+\sqrt{2})^4\right)\right\} = \left\langle u_2\left((1+\sqrt{2})^4\right)\right\rangle.$$

Коэффициенты при минимальных центральных идемпотентах $e_0, e_1, \ldots, e_{15}$ легко вычисляются из определения локальной единицы $u_2\left((1+\sqrt{2})^4\right)$. В самом деле, так как $(1+\sqrt{2})^4 = 17 + 12\sqrt{2}$, то по лемме 6 получим

$$\gamma_0 = \frac{1}{4}\,(3+17) = 5,\ \gamma_8 = \gamma_0 - 1 = 4, \quad \gamma_4 = \gamma_{12} = \frac{1}{4}\,(1-17) = -4,\ \gamma_2 = \gamma_{10} = \gamma_6 = \gamma_{14} = 0,$$
$$\gamma_1 = \gamma_9 = \gamma_3 = \gamma_{11} = \frac{1}{4}\,(12) = 3, \qquad \gamma_5 = \gamma_{13} = \gamma_7 = \gamma_{15} = \frac{1}{4}\,(-12) = -3.$$

Предложение доказано.

3. Переход к группе единиц без кручения

Пусть t_1, t_3 и t_5 — единицы кольца $\mathbf{Z}[\alpha]$ (см. определение перед леммой 2). Для удобства положим
$$T = \langle t_1\rangle \times \langle t_3\rangle \times \langle t_5\rangle,$$
тогда по лемме 2 имеем $U(\mathbf{Z}[\alpha]) = \langle\alpha\rangle \times T$.

Определим в группе $V(\mathbf{Z}G)$ подмножество
$$V_0 = \{u_1(\beta_1)u_2(\beta_2)u_4(\beta_4)u_8(\beta_8) \in V(\mathbf{Z}G) \mid \beta_1 \in T\}\,.$$

Предложение 2. *При введенных выше обозначениях имеем*
1) V_0 *является подгруппой без кручения группы* $V(\mathbf{Z}G)$;
2) $V(\mathbf{Z}G) = G \times V_0$.

Д о к а з а т е л ь с т в о. 1) Так как T — подгруппа группы $U(\mathbf{Z}[\alpha])$, то из мультипликативности минимальных центральных идемпотентов $e_0, e_1, \ldots, e_{15}$ следует, что V_0 является подгруппой группы $V(\mathbf{Z}G)$. Отсутствие кручения в V_0 следует из [2, предложение 1].

2) Пусть $v = u_1(\beta_1)u_2(\beta_2)u_4(\beta_4)u_8(\beta_8)$ — произвольный элемент группы $V(\mathbf{Z}G)$. По лемме 2 имеем $\beta_1 = \alpha^k t$, где $k \in \{0, 1, \ldots, 15\}$ и $t \in T$. По [2, предложение 1] получим, что $x^{-k} = u_1(\alpha^{-k})u_2(\alpha^{-2k})u_4(\alpha^{-4k})u_8(\alpha^{-k})$. Так как $\alpha^{-k}\beta_1 = t \in T$, то
$$\begin{aligned} x^{-k}v &= u_1(\alpha^{-k})u_2(\alpha^{-2k})u_4(\alpha^{-4k})u_8(\alpha^{-k}) \cdot u_1(\beta_1)u_2(\beta_2)u_4(\beta_4)u_8(\beta_8) \\ &= u_1(\alpha^{-k}\beta_1)u_2(\alpha^{-2k}\beta_2)u_4(\alpha^{-4k}\beta_4)u_8(\alpha^{-k}\beta_8) \in T. \end{aligned}$$
Отсюда следует утверждение 2).

Предложение доказано.

Определим в группе V_0 подмножество
$$V_1 = \{u_1(\beta_1)) \in V(\mathbf{Z}G) \mid \beta_1 \in T\}\,.$$
Как в случае V_0, также вполне очевидно, что V_1 — подгруппа в V_0.

Лемма 7 [2, теорема 1]. *Пусть*
$$h_1 = x + x^{-1} - x^7 - x^{-7},\ h_2 = x^2 + x^{-2} - x^6 - x^{-6},\ h_3 = x^3 + x^{-3} - x^5 - x^{-5}.$$
Тогда при введенных выше обозначениях имеем $V_1 = \langle v_1\rangle \times \langle v_2\rangle \times \langle v_3\rangle$, *где*
$$\begin{aligned} v_1 &= u_1(t_1^4) = 42 + 38h_1 + 29h_2 + 16h_3 - 41x^8, \\ v_2 &= u_1(t_1^2t_3^2) = 4 - 2h_1 - 4h_2 + 6h_3 - 3x^8, \\ v_3 &= u_1(t_3^3t_5) = 6 - 2h_1 - 4h_2 + 5h_3 - 5x^8. \end{aligned}$$

Положим $T_1 = \langle t_1^4\rangle \times \langle t_1^2t_3^2\rangle \times \langle t_3^3t_5\rangle$, тогда $V_1 = \{u_1(t) \mid t \in T_1\}\,.$

Лемма 8. *Фактор-группа* T/T_1 *имеет вид*
$$T/T_1 = \langle t_1T_1\rangle \times \langle t_1t_3T_1\rangle,$$
причем подгруппа $\langle t_1T_1\rangle$ *имеет порядок* 4, *а подгруппа*$\langle t_1t_3T_1\rangle$ — *порядок* 2.

Д о к а з а т е л ь с т в о. Пусть $t_1^{k_1}t_3^{k_3}t_5^{k_5}$ — произвольный элемент группы T (k_1, k_3 и k_5 — целые числа). Так как $t_1^{k_1}t_3^{k_3}t_5^{k_5} = t_1^{k_1}t_3^{k_3-3k_5}(t_3^3t_5)^{k_5} \in t_1^{k_1}t_3^{k_3-3k_5}T_1$, то достаточно рассматривать элементы $t_1^{k_1}t_3^{k_3}$.

Далее пусть $k_3 = 2l + \delta$, где $\delta \in \{0, 1\}$. Тогда

$$t_1^{k_1} t_3^{k_3} = t_1^{k_1-2l} t_3^{\delta} (t_1^2 t_3^2)^l \in t_1^{k_1-2l} t_3^{\delta} T_1.$$

Поскольку $t_1^4 \in T_1$, то фактор-группа имеет вид

$$T/T_1 = \left\{ t_1^{k_1} t_1^{k_2} T_1 \mid k_1 \in \{0, 1, 2, 3\}, k_3 \in \{0, 1\} \right\}.$$

Так как $(t_1 t_3)^2 = t_1^2 t_3^2 \in T_1$, то элемент $(t_1 t_3) T_1$ имеет порядок 2 и не принадлежит подгруппе $\langle t_1 T_1 \rangle$ порядка 4. Отсюда следует утверждение леммы.

Лемма доказана.

Лемма 9. *Пусть $u_1(\beta_1) u_2(\beta_2) u_4(\beta_4) u_8(\beta_8)$ — произвольный элемент группы $V(\mathbf{Z}G)$. Тогда*

$$\beta_1 \in \langle t_1^3 t_3 \rangle T_1.$$

Доказательство. По лемме 7 для любого $t \in T_1$ локальная единица $u_1(t)$ принадлежит $V(\mathbf{Z}G)$, поэтому ввиду леммы 8 достаточно, что

$$\beta_1 \notin \{t_1, t_1^2, t_1^3, t_1 t_3, t_1^2 t_3, t_3\}.$$

Далее, по лемме 8 квадраты всех элементов порядка 4 фактор-группы T/T_1 равны $t_1^2 T_1$.

Поэтому, если существует элемент в $V(\mathbf{Z}G)$ с коэффициентом $\beta_1 \in \{t_1, t_1^3, t_1^2 t_3, t_3\}$, то его квадрат равен

$$u_1(t_1^2) u_2(\beta_2^2) u_4(\beta_4^2) u_8(\beta_8^2) \in V(\mathbf{Z}G).$$

Поэтому достаточно доказать, что

$$\beta_1 \notin \{t_1^2, t_1 t_3\}.$$

Докажем методом от противного. Поскольку

$$t_1^2 = 5 + 4(\alpha + \alpha^{-1}) + 3(\alpha^2 + \alpha^{-2}) + 2(\alpha^3 + \alpha^{-3}) = 5 + 4\alpha + 3\alpha^2 + 2\alpha^3 - 2\alpha^5 - 3\alpha^6 - 4\alpha^7,$$
$$t_1 t_3 = -1 + (\alpha + \alpha^{-1}) + (\alpha^2 + \alpha^{-2}) - (\alpha^3 + \alpha^{-3}) = -1 + \alpha + \alpha^2 - \alpha^3 + \alpha^5 - \alpha^6 - \alpha^7,$$

то в обозначениях леммы 4 в обоих случаях a_2 нечетно. Это противоречит тому, что $\gamma_2 = a_2/2$ по утверждению 3) леммы 4.

Лемма доказана.

Лемма 10. *Пусть $\beta_1 = t_1^3 t_3$. Тогда*

$$u_1(t_1^2 t_3) u_2(-(1 + \sqrt{2})^2) \in V(\mathbf{Z}G).$$

Более точно

$$u_1(t_1^2 t_3) u_2(-(1+\sqrt{2})^2) = 2 + (x^3 + x^4 + x^{12} + x^{13}) + 3(x + x^2 - x^6 - x^8 - x^{10} + x^{14} + x^{15}) - 4(x^7 + x^9).$$

Доказательство. Непосредственный подсчет дает

$$t_1^3 t_3 = 5 + 7(\alpha + \alpha^{-1}) + 6(\alpha^2 + \alpha^{-2}) + (\alpha^3 + \alpha^{-3}) = 5 + 7\alpha + 6\alpha^2 + \alpha^3 - \alpha^5 - 6\alpha^6 - 7\alpha^7.$$

В обозначениях леммы 4 имеем

$$a_0 = 5,\ a_1 = 7,\ a_2 = 6,\ a_3 = 1,\ a_4 = 0,\ a_5 = -1,\ a_6 = -6,\ a_7 = -7.$$

Поэтому выполнены условия леммы 4. Тогда в обозначениях этой леммы $\gamma_1 = 1/4\,(b_1 + 14)$ и $b_1 \equiv 2 \pmod 4$.

По утверждению 2) леммы 4 имеем $\beta_2 = -(1 + \sqrt{2})^{4m+2}$. По предложению 1 получим, что $u_2((1 + \sqrt{2})^{4m}) \in V(\mathbf{Z}G)$, поэтому достаточно взять $\beta_2 = -(1 + \sqrt{2})^2 = -3 - 2\sqrt{2}$. Используя утверждение 3) леммы 4, получим нужные выражения для коэффициентов $u_1(t_1^2 t_3) u_2(-(1 + \sqrt{2})^2)$.

Лемма доказана.

4. Доказательство теоремы

Теорема 1. *Группа единиц $U(\mathbf{Z}G)$ целочисленного группового кольца $\mathbf{Z}G$ циклической группы G порядка 16 в определенных ранее обозначениях равна*

$$\langle -1\rangle \times G \times \langle u_2((1+\sqrt{2})^4)\rangle \times \langle u_1(t_1^4)\rangle \times \langle u_1(t_3^3 t_5)\rangle \times \langle u_1(t_1^3 t_3) u_2(-(1+\sqrt{2})^2)\rangle.$$

Доказательство. Так как $U(\mathbf{Z}G) = \langle -1\rangle \times V(\mathbf{Z}G)$ и по предложению 2 имеем $V(\mathbf{Z}G) = G \times V_0$, то достаточно описать подгруппу V_0, определенную предложением 2. Из предложения 1, лемм 7, 9 и 10 следует, что V_0 порождается элементами

$$u_2((1+\sqrt{2})^4),\ u_1(t_1^4),\ u_1(t_1^2 t_3^2),\ u_1(t_3^3 t_5),\ u_1(t_1^3 t_3) u_2(-(1+\sqrt{2})^2).$$

Так как

$$\Big(u_1(t_1^3 t_3) u_2(-(1+\sqrt{2})^2)\Big)^2 = u_1(t_1^6 t_3^2) u_2((1+\sqrt{2})^4) = u_1(t_1^2 t_3^2) u_1(t_1^4) u_2((1+\sqrt{2})^4),$$

то $u_1(t_1^2 t_3^2)$ можно исключить из списка порождающих, что завершает доказательство теоремы.

Теорема доказана.

Заключение

Доказанная теорема будет служить основой для изучения групп единиц целочисленных групповых колец циклических 2-групп порядка 2^n для $n \geqslant 5$. Кроме того, леммы и предложения этой работы содержат много полезной информации для изучения таких групп единиц.

СПИСОК ЛИТЕРАТУРЫ

1. **Алеев Р.Ж, Митина О.В., Христенко Е.А.** Сравнение по модулю 2 круговых единиц в полях Q_{16} и Q_{32} // Челяб. физ.-мат. журн. 2016. Т. 1, вып. 4. С. 8–29.
2. **Алеев Р.Ж, Митина О.В., Ханенко Т.А.** Нахождение единиц целочисленных групповых колец циклических групп порядков 16 и 32 // Челяб. физ.-мат. журн. 2016. Т. 1, вып. 4. С. 30–55.
3. **Кэртис Ч., Райнер И.** Теория представлений конечных групп и ассоциативных алгебр. М.: Наука, 1969. 668 с.
4. **Алеев Р.Ж.** Центральные элементы целочисленных групповых колец // Алгебра и логика. 2000. Т. 39, вып. 5. С. 513–525.
5. **Алеев Р.Ж.** Единицы полей характеров и центральные единицы целочисленных групповых колец конечных групп // Мат. тр. 2000. Т. 3, вып. 1. С. 3–37.

Алеев Рифхат Жалялович
д-р физ.-мат. наук, доцент
профессор кафедры системного программирования
Южно-Уральский государственный университет,
профессор кафедры компьютерной топологии и алгебры
Челябинский государственный университет
e-mail: aleevrz@susu.ru, aleev@csu.ru

Поступила 13.10.2017

Митина Ольга Викторовна
канд. физ-мат. наук, доцент
Челябинский государственный университет,
Южно-Уральский государственный университет
e-mail: ovm@csu.ru

Ханенко Татьяна Александровна
студент математического факультета
Челябинский государственный университет
e-mail: tanja_1110_94@mail.ru

REFERENCES

1. Aleev R.Zh., Mitina O.V., Khistenko E.A. Congruence modulo 2 of circular units in the fields Q_{16} and Q_{32}. *Chelyab. Fiz.-Mat. Zh.*, 2016, vol. 1, no. 4, pp. 8–29 (in Russian).
2. Aleev R.Zh., Mitina O.V., Khanenko T.A. Finding of units for integer group rings of orders 16 and 32 cyclic groups. *Chelyab. Fiz.-Mat. Zh.*, 2016, vol. 1, no. 4, pp. 30–55 (in Russian).
3. Curtis C.W., Reiner I. *Representation theory of finite groups and associative algebras.* Ser. Pure Appl. Math., vol. XI. N. Y.; London, Interscience Publishers, a division of John Wiley & Sons, 689 p. ISBN: 978-0-8218-4066-5. Translated to Russian under the title *Teoriya predstavlenii konechnykh grupp i assotsiativnykh algebr.* Moscow, Nauka Publ., 1969, 668 p.
4. Aleev R.Zh. Central elements of integral group rings. *Algebra and Logic*, 2000, vol. 39, no. 5, pp. 293–300. doi: 10.1007/BF02681613 .
5. Aleev R. Zh. Units of character fields and central units of integral group rings of finite groups. *Siberian Advances of Mathematics*, 2001, vol. 11, no. 1, pp. 1–33.

The paper was received by the Editorial Office on October 13, 2017.

Rifkhat Zhalyalovich Aleev, Dr. Phys.-Math. Sci., Prof., South Ural State University, Chelyabinsk State University, Chelyabinsk, 454080 Russia, e-mail: aleevrz@susu.ru, aleev@csu.ru .

Ol'ga Viktorovna Mitina, Cand. Sci. (Phys.-Math.), South Ural State University, Chelyabinsk State University, Chelyabinsk, 454080 Russia, e-mail: ovm@csu.ru .

Tat'yana Aleksandrovna Khanenko, student Chelyabinsk State University, Chelyabinsk, 454080 Russia, e-mail: tanja_1110_94@mail.ru .