МАТЕМАТИКА

Челябинский физико-математический журнал. 2017. Т. 2, вып. 2. С. 133–151.

УДК 512.552.7+511.622

ГРУППЫ ЕДИНИЦ КЛАССОВЫХ КОЛЕЦ ХАРАКТЕРОВ ГРУППЫ РУДВАЛИСА

Р. Ж. Алеев[1,2,a], **М. И. Молодорич**[2,b]

[1] *Челябинский государственный университет, Челябинск, Россия*
[2] *Южно-Уральский государственный университет (национальный исследовательский университет), Челябинск, Россия*
[a] *aleevrz@susu.ru, aleev@csu.ru;* [b] *molodorichmi@susu.ru*

Рассматриваются классовые кольца характеров группы Ru, которые не являются подкольцами действительных квадратичных полей, и описаны их обратимые элементы.

Ключевые слова: *спорадическая группа, обратимый элемент, характер, групповое кольцо, классовое кольцо характера.*

1. Введение

Классовые кольца характеров группы были введены и изучены в [1].

Определение 1. Пусть G — конечная группа, $X(G)$ — множество представителей всех классов сопряжённости в G, $Irr(G)$ — множество всех неприводимых характеров группы G и $\chi \in Irr(G)$. Положим

$$\mathbf{Z}[cl,\chi] = \Big\{ \frac{1}{\deg\chi} \sum_{x\in X(G)} |x^G|\chi(x)\gamma(x) \;\Big|\; \gamma(x) \in \mathbf{Z}\ \forall x \in X(G) \Big\}.$$

$\mathbf{Z}[cl,\chi]$ называется *классовым кольцом характера* χ.

Исследование классовых колец характеров — важный шаг к описанию центральных единиц группы. Весьма полная информация о классовых кольцах характеров для всех спорадических групп получена в [2].

Также Молодорич получены описания групп единиц всех таких колец при условии, что классовое кольцо характера содержится в некотором действительном квадратичном поле [3]. Поэтому остаётся задача нахождения групп единиц таких классовых колец характеров спорадических групп, которые не содержатся в действительных квадратичных полях.

В [4] описаны группы единиц классовых колец характеров групп Янко J_1 и О'Нэна $O'N$, которые не содержатся в действительных квадратичных полях.

Справедлив следующий результат.

Статья выполнена при поддержке Правительства РФ (Постановление № 211 от 16.03.2013), соглашение № 02.A03.21.0011.

Лемма 1. *Неизвестны группы единиц классовых колец характеров, которые не содержатся в действительных квадратичных полях, только для следующих спорадических групп: J_3, J_4, Ly, Ru.*

2. Группа Рудвалиса

2.1. Начальные сведения

Лемма 2. [2]. *Группа Рудвалиса Ru имеет следующие классовые кольца характеров, которые не содержатся в действительных квадратичных полях:*

$$K_1 = \mathbf{Z} + 2^9 \cdot 13 \cdot 29A\mathbf{Z} + 2^9 \cdot 13 \cdot 29B\mathbf{Z},$$
$$K_2 = \mathbf{Z} + 2^9 \cdot 5^3 G\mathbf{Z} + 2^9 \cdot 5^3 H\mathbf{Z}, \text{ где}$$
$$A = -\zeta_7 + \zeta_7^2 + \zeta_7^3 + \zeta_7^4 + \zeta_7^5 - \zeta_7^6,$$
$$B = \zeta_7 - \zeta_7^2 + \zeta_7^3 + \zeta_7^4 - \zeta_7^5 + \zeta_7^6,$$
$$G = \zeta_{13} - \zeta_{13}^2 - \zeta_{13}^3 - \zeta_{13}^4 + \zeta_{13}^5 - \zeta_{13}^6 - \zeta_{13}^7 + \zeta_{13}^8 - \zeta_{13}^9 - \zeta_{13}^{10} - \zeta_{13}^{11} + \zeta_{13}^{12},$$
$$H = -\zeta_{13} - \zeta_{13}^2 - \zeta_{13}^3 + \zeta_{13}^4 - \zeta_{13}^5 + \zeta_{13}^6 + \zeta_{13}^7 - \zeta_{13}^8 + \zeta_{13}^9 - \zeta_{13}^{10} - \zeta_{13}^{11} - \zeta_{13}^{12}.$$

Здесь ζ_7 и ζ_{13} — примитивные корни из 1 степеней 7 и 13 соответственно.

Замечание 1. Согласно [5] кольцо K_1 — классовое кольцо характеров χ_{11}, χ_{12} и χ_{13} степени 27000, а K_2 — классовое кольцо характеров χ_{17}, χ_{18} и χ_{19} степени 43848. Также стоит отметить, что нецелыми значениями χ_{11}, χ_{12} и χ_{13} являются A, B и

$$C = \zeta_7 + \zeta_7^2 - \zeta_7^3 - \zeta_7^4 + \zeta_7^5 + \zeta_7^6,$$

а нецелыми значениями χ_{17}, χ_{18} и χ_{19} являются G, H и

$$I = -\zeta_{13} + \zeta_{13}^2 + \zeta_{13}^3 - \zeta_{13}^4 - \zeta_{13}^5 - \zeta_{13}^6 - \zeta_{13}^7 - \zeta_{13}^8 - \zeta_{13}^9 + \zeta_{13}^{10} + \zeta_{13}^{11} - \zeta_{13}^{12}.$$

Лемма 3.

1. *Для вышеуказанных чисел A, B и C имеем:*
   (a) $A + B + C = -1$;
   (b) $A^2 = 5 - 2A - 2B$, $B^2 = 7 + 2A$, $AB = -3 - A + B$, $ABC = 1$.
2. *Для вышеуказанных чисел G, H и I имеем:*
   (a) $G + H + I = 1$;
   (b) $G^2 = 11 + 2H$, $H^2 = 13 - 2G - 2H$, $GH = -7 + 3G + H$, $GHI = -25$.

Доказательство. Утверждение 1 (a) проверяется непосредственно, а доказательство утверждения 1 (b) можно найти в [2, Предложение 9].

Утверждение 2 (a) проверяется непосредственно, а утверждение 2 (b) содержится в [2, Предложение 10][1]. □

Лемма 4. *Пусть p — простое нечётное число не более 67 или $p = 9$, ζ_p — примитивный корень степени p из 1 и $\mathbf{Q}_p = \mathbf{Q}(\zeta_p)$ — круговое поле, полученное присоединением ζ_p к полю рациональных чисел.*

1. *Кольцо целых поля $\mathbf{Q}_p$ равно $\mathbf{Z}[\zeta_p]$.*

[1] К сожалению, в указанном источнике допущена опечатка: написано $GHI = -15$, что, впрочем, не влияет на результат.

2. *Пусть g — примитивный корень по модулю p, и положим $m = 2$ при $p = 9$ и $m = (p-3)/2$. Группа единиц кольца целых равна*
$$Un(\mathbf{Z}[\zeta_p]) = \langle -\alpha \rangle \times \prod_{k=0}^{m-1} \left\langle \frac{1-\zeta_p^{g^{k+1}}}{1-\zeta_p^{g^k}} \right\rangle.$$

3. *Если $g = 2$, то группа единиц кольца $\mathbf{Z}[\zeta_p] \cap \mathbf{R}$*
$$Un(\mathbf{Z}[\zeta_p] \cap \mathbf{R}) = \langle -1 \rangle \times \prod_{k=1}^{m} \left\langle \zeta_p^k + \zeta_p^{-k} \right\rangle.$$

4. *Если $g = 3$, то*
$$Un(\mathbf{Z}[\zeta_p] \cap \mathbf{R}) = \langle -1 \rangle \times \prod_{k=1}^{\frac{p-3}{2}} \left\langle \zeta_p^k + 1 + \zeta_p^{-k} \right\rangle.$$

Доказательство. Все сформулированные здесь утверждения можно получить довольно стандартными методами из классической книги [6].

Более подробно, утверждение 1 следует из теоремы 1 в § 5 главы V [6]. Утверждение 2 — частный случай теоремы 1 из [7] и [8], как указано во введении [7]. Доказательства утверждений 3 и 4 практически полностью совпадают. Поэтому докажем только утверждение 3 и только простой случай (случай $p = 9$ аналогичен).

Заметим, что
$$\frac{1-\zeta_p^2}{1-\zeta_p} = 1 + \zeta_p = 1 + \zeta_p^{p+1} = \zeta_p^{\frac{p+1}{2}}(\zeta_p^{\frac{p+1}{2}} + \zeta_p^{-\frac{p+1}{2}}).$$

Элемент $\zeta_p^{\frac{p+1}{2}} + \zeta_p^{-\frac{p+1}{2}} \in \mathbf{R}$ алгебраически сопряжён при действии группы Галуа с $\zeta_p + \zeta_p^{-1}$. Поэтому ясно, что группа $Un(\mathbf{Z}[\zeta_p] \cap \mathbf{R})$ является прямым произведением $\langle -1 \rangle$ и циклических подгрупп, порождённых элементами, алгебраически сопряжёнными при действии группы Галуа с $\zeta_p + \zeta_p^{-1}$.

С другой стороны, так как для любого $k \in \{1, \ldots, (p-1)/2\}$ имеем равенство $\zeta_p^k + \zeta_p^{-k} = \zeta_p^{p-k} + \zeta_p^{-p+k}$, норма в $\mathbf{Q}_p$ имеет вид
$$Norm(\zeta_p + \zeta_p^{-1}) = \prod_{k=1}^{p-1}(\zeta_p^k + \zeta_p^{-k}) = \left(\prod_{k=1}^{\frac{p-1}{2}}(\zeta_p^k + \zeta_p^{-k})\right)^2 = 1,$$

и потому
$$\prod_{k=1}^{\frac{p-1}{2}}(\zeta_p^k + \zeta_p^{-k}) = \pm 1.$$

□

2.2. Кольцо $\mathbf{K_1}$

2.2.1. Общие свойства

Положим для удобства $s_1 = \zeta_7 + \zeta_7^{-1}$, $s_2 = \zeta_7^2 + \zeta_7^{-2}$ и $s_3 = \zeta_7^3 + \zeta_7^{-3}$.

Лемма 5. *При введённых обозначениях имеют место следующие равенства:*

1) $A = -1 - 2\zeta_7 - 2\zeta_7^6 = -1 - 2s_1$;

2) $B = -1 - 2\zeta_7^2 - 2\zeta_7^5 = -1 - 2s_2$;

3) $C = -1 - 2\zeta_7^3 - 2\zeta_7^4 = -1 - 2s_4$;

4) $Un(\mathbf{Z}[\zeta_7] \cap \mathbf{R}) = Un(\mathbf{Z}[s_1]) = \langle -1 \rangle \times \langle 1 + s_1 \rangle \times \langle 1 + s_2 \rangle$;

5) $(1 + s_1)(1 + s_2)(1 + s_3) = -1$, $s_1 s_2 s_3 = 1$.

Доказательство. Утверждения 1–3 следуют из того, что

$$\zeta_7 + \zeta_7^2 + \zeta_7^3 + \zeta_7^4 + \zeta_7^5 + \zeta_7^6 = -1.$$

Утверждение 4 следует из леммы 4, поскольку 3 — примитивный корень по модулю 7. Утверждение 5 проверим непосредственно:

$$\begin{gathered}(1 + s_1)(1 + s_2)(1 + s_3) = (1 + s_1 + s_2 + s_3 + s_1)(1 + s_3) = s_1(1 + s_3) = \\ = s_1 + s_3 + s_2 = -1; \\ s_1 s_2 s_3 = (s_3 + s_1)s_3 = s_1 + 2 + s_3 + s_2 = 1.\end{gathered}$$

□

Лемма 6. *Кольцо K_1 удовлетворяет равенствам*

$$\begin{gathered}K_1 = \mathbf{Z} + 2^{10} \cdot 13 \cdot 29\mathbf{Z}s_1 + 2^{10} \cdot 13 \cdot 29\mathbf{Z}s_2 = \\ = \mathbf{Z} + 2^{10} \cdot 13 \cdot 29\mathbf{Z}(1 + s_1) + 2^{10} \cdot 13 \cdot 29\mathbf{Z}(1 + s_2).\end{gathered}$$

Доказательство. Равенства следуют из утверждений 1 и 2 леммы 5. □

Лемма 7. *Пусть $P = \mathbf{Q}(\zeta_7) \cap \mathbf{R} = \mathbf{Q}(s_1)$ и $p \in \{2, 13, 29\}$. Тогда*

1) *индекс ветвления $e = 1$ для всякого $p \in \{2, 13, 29\}$;*

2) *степень инерции $f = 3$ для $p = 2$ и $f = 1$ для $p \in \{13, 29\}$.*

Доказательство. Утверждения следуют из следствия [9, с. 247], так как $2 \not\equiv \pm 1 \pmod 7$, а $13 \equiv -1 \pmod 7$ и $29 \equiv 1 \pmod 7$. □

2.2.2. Модуль 2^{10}

Для каждого неотрицательного целого $n \in \{0, 1, 2, \dots\}$ введём в рассмотрение вспомогательные кольца $K(n) = \mathbf{Z} + 2^n\mathbf{Z}s_1 + 2^n\mathbf{Z}s_2$. Отметим сразу, что

$$\mathbf{Z}[s_1] = \mathbf{Z}[\zeta_7] \cap \mathbf{R} = K(0).$$

Обозначим через φ_2 автоморфизм поля $P = \mathbf{Q}[\zeta_7] \cap \mathbf{R} = \mathbf{Q}[s_1]$, индуцированный отображением $\zeta_7 \mapsto \zeta_7^2$.

Замечание 2. Легко понять, что группа Галуа поля P (над $\mathbf{Q}$) (равносильно: группа автоморфизмов поля P) равна $G(P) = \{1, \varphi_2, \varphi_4 = (\varphi_2)^2\} \cong \mathbf{Z}_3$.

Лемма 8. *Ряд $K(0) > K(1) > \dots > K(n) > \dots$ стабилизируется автоморфизмами из $G(P)$.*

Доказательство. Утверждение сразу следует из того, что $\varphi_2(s_1)$ и $\varphi_2(s_2) = s_3$, а $s_3 = -1 - s_1 - s_2$. □

Лемма 9. *Группа единиц* $Un(K_1) < Un(K(1)) = \langle -1\rangle \times \langle A\rangle \times \langle B\rangle$.

Доказательство. Ясно, что

$$K_1 = \mathbf{Z} + 2^{10}\cdot 13\cdot 29\mathbf{Z}s_1 + 2^{10}\cdot 13\cdot 29\mathbf{Z}s_2 < K(1) < \mathbf{Z}[s_1] = \mathbf{Z}[\zeta_7]\cap\mathbf{R}.$$

Поэтому для групп единиц

$$Un(K_1) < Un(K(1)) < Un(\mathbf{Z}[s_1]) = Un(\mathbf{Z}[\zeta_7]\cap\mathbf{R}) = \langle -1\rangle \times \langle 1+s_1\rangle \times \langle 1+s_2\rangle.$$

Согласно результатам из [10, § 3] получаем, используя лемму 7, что для любой единицы $\lambda \in K(0) = \mathbf{Z}[s_1] = \mathbf{Z}[\zeta_7]\cap\mathbf{R}$ выполняется $\lambda^7 \in Un(K(1))$. Однако условие возведения в 7-ю степень является достаточным, но не необходимым.

Проведём вычисления в GAP [5].

```
gap> P:=NF(7,[1,6]);
NF(7,[ 1, 6 ])
gap> b:=CanonicalBasis(P);
CanonicalBasis( NF(7,[ 1, 6 ]) )
gap> b[1];
E(7)+E(7)^6
gap> b[2];
E(7)^2+E(7)^5
gap> L1:=1+b[1];
-E(7)^2-E(7)^3-E(7)^4-E(7)^5
gap> L2:=1+b[2];
-E(7)-E(7)^3-E(7)^4-E(7)^6
gap> c:=Basis(P,[1,b[1],b[2]]);
Basis( NF(7,[ 1, 6 ]), [ 1, E(7)+E(7)^6, E(7)^2+E(7)^5 ] )
gap> pr:=[];
[  ]
gap> for i in [0..7] do
> for j in [0..7] do
> k:=Coefficients(c,L1^i*L2^j);
> if (k mod 2)=[1,0,0]
> then
> Add(pr,[i,j,k]);
> fi;
> od;
> od;
gap> pr;
[ [ 0, 0, [ 1, 0, 0 ] ], [ 0, 7, [ 101, -56, 70 ] ],
[ 1, 3, [ -3, 2, -2 ] ], [ 2, 6, [ 29, -16, 20 ] ],
[ 3, 2, [ 1, 2, 0 ] ], [ 4, 5, [ 9, -4, 6 ] ],
[ 5, 1, [ 17, 14, 6 ] ], [ 6, 4, [ 9, 4, 4 ] ],
[ 7, 0, [ 157, 126, 56 ] ], [ 7, 7, [ -19, 14, -14 ] ] ]
gap> quit;
```

Отсюда получаем, что

$$\big\{(1+s_1)(1+s_2)^3, (1+s_1)^2(1+s_2)^6, (1+s_1)^3(1+s_2)^2, (1+s_1)^4(1+s_2)^5,$$
$$(1+s_1)^5(1+s_2), (1+s_1)^6(1+s_2)^4\big\} \subset Un(K(1)).$$

Далее заметим, что имеют место равенства

$$\begin{aligned}
&\left((1+s_1)^3(1+s_2)^2\right)^2 = (1+s_1)^6(1+s_2)^4,\\
&\left((1+s_1)^3(1+s_2)^2\right)^3 = (1+s_1)^9(1+s_2)^6 = (1+s_1)^2(1+s_2)^6(1+s_1)^7,\\
&\left((1+s_1)^3(1+s_2)^2\right)^4 = (1+s_1)^{12}(1+s_2)^8 = (1+s_1)^5(1+s_2)(1+s_1)^7(1+s_2)^7,\\
&\left((1+s_1)^3(1+s_2)^2\right)^5 = (1+s_1)^{15}(1+s_2)^{10} = (1+s_1)(1+s_2)^3(1+s_1)^{14}(1+s_2)^7,\\
&\left((1+s_1)^3(1+s_2)^2\right)^6 = (1+s_1)^{18}(1+s_2)^{12} = (1+s_1)^4(1+s_2)^5(1+s_1)^{14}(1+s_2)^7.
\end{aligned}$$

Следовательно, $Un(K(1)) = \langle -1\rangle \times \langle (1+s_1)^7, (1+s_2)^7, (1+s_1)^3(1+s_2)^2\rangle$. Имеем $(1+s_1)^3(1+s_2)^2 = 1+2s_1 = -A$.

Из лемм 3 и 5 получаем, что

$$\begin{aligned}
B = \varphi_2(A) &= \varphi_2\left(-(1+s_1)^3(1+s_2)^2\right) = -(1+s_2)^3(1+s_3)^2 =\\
&= -(1+s_2)^3\left(-(1+s_1)(1+s_2)\right)^{-2} = -(1+s_1)^{-2}(1+s_2) =\\
&= -(1+s_1)^{-7}(1+s_1)^5(1+s_2) =\\
&= -(1+s_1)^{-7}\left((1+s_1)^3(1+s_2)^2\right)^4\left((1+s_1)^7(1+s_2)^7\right)^{-1} =\\
&= -(-A)^4(1+s_1)^{-14}(1+s_2)^{-7},
\end{aligned}$$

следовательно, $(1+s_1)^{14}(1+s_2)^7 = -A^4B^{-1}$;

$$\begin{aligned}
C = \varphi_4(A) &= \varphi_4\left(-(1+s_1)^3(1+s_2)^2\right) = -(1+s_3)^3(1+s_1)^2 =\\
&= -(1+s_1)^2\left(-(1+s_1)(1+s_2)\right)^{-3} = (1+s_1)^{-1}(1+s_2)^{-3} =\\
&= (1+s_1)^6(1+s_2)^4(1+s_1)^{-7}(1+s_2)^{-7} =\\
&= (-A)^2(1+s_1)^{-7}(1+s_2)^{-7},
\end{aligned}$$

поэтому $(1+s_1)^7(1+s_2)^7 = A^2C^{-1} = A^2(AB) = A^3B$. Отсюда

$$\begin{aligned}
&(1+s_1)^7 = (1+s_1)^{14}(1+s_2)^7\cdot\left((1+s_1)^7(1+s_2)^7\right)^{-1} = -A^4B^{-1}\cdot\left(A^3B\right)^{-1} = -AB^{-2},\\
&(1+s_2)^7 = (1+s_1)^7(1+s_2)^7\cdot(1+s_1)^{-7} = A^3B\cdot\left(-AB^{-2}\right)^{-1} = -A^2B^3.
\end{aligned}$$

Так как $ABC = 1$ по лемме 3 и $s_3 = -1-s_1-s_2$, то

$$A^{-1} = BC = (-1-2s_2)(-1-2s_3) \in K(1).$$

Аналогично $B^{-1} \in K(1)$. Таким образом, $Un(K(1)) = \langle -1\rangle \times \langle A\rangle \times \langle B\rangle$. □

Лемма 10. *Для любого $X \in \{A, B, AB\}$ и любого неотрицательного целого n $X^{\pm 2^n} \in K(n+1)\setminus K(n+2)$. Более точно, если $X^{\pm 2^n} = x_0 + 2^{n+1}x_1s_1 + 2^{n+1}x_2s_2$ для подходящих целых x_0, x_1 и x_2, то*

0) $x_0 \equiv 1 \pmod{2^{n+1}}$;

1) *по крайней мере одно из чисел x_1 и x_2 также должно быть нечётным.*

Доказательство. Сначала рассмотрим $X = A$ и A^{2^n}. Так как $A = -1-2s_1$, то получается базис для индукции по n. Пусть доказано, что $A^{2^{n-1}} \in K(n)\setminus K(n+1)$. Тогда $A^{2^{n-1}} = a_0 + 2^n a_1 s_1 + 2^n a_2 s_2$ для подходящих целых $a_0 \equiv 1 \pmod{2^n}$, a_1 и a_2. А так как $A^{2^{n-1}} \in K(n)\setminus K(n+1)$, то, по крайней мере, одно из чисел a_1 и a_2 также должно быть нечётным. При этом

$$A^{2^n} = \left(A^{2^{n-1}}\right)^2 = (a_0 + 2^n a_1 s_1 + 2^n a_2 s_2)^2 = a_0^2 + 2^{n+1}a_0a_1s_1 + 2^{n+1}a_0a_2s_2 + 2^{n+2}c$$

для некоторого $c \in \mathbf{Z}[s_1] = \mathbf{Z}[\zeta_7] \cap \mathbf{R}$. Поэтому $A^{2^n} \in K(n+1)$, а так как одно из чисел a_0a_1 или a_0a_2 обязательно нечётно и $a_0^2a_0 \equiv 1 \pmod{2^{n+1}}$, то в этом случае получаем требуемое.

Далее по лемме 3 $ABC = 1$. Поэтому

$$\begin{aligned} A^{-1} = BC = (-1-2s_2)(-1-2s_3) = 1+2s_2+2s_3+4(s_2+s_1) = \\ = -1+2(1+s_2+s_3+s_1)+2s_1+4s_2 = -1+2s_1+4s_2 \in K(1) \setminus K(2) \end{aligned}$$

и можно повторить рассуждения, как для A^{2^n}.

Таким образом, для любого неотрицательного целого n $A^{\pm 2^n} \in K(n+1)\setminus K(n+2)$. Применяя лемму 8 к $B = \varphi_2(A)$ и $C = \varphi_4(A)$, получаем для любого неотрицательного целого n $B^{\pm 2^n}, C^{\pm 2^n} \in K(n+1)\setminus K(n+2)$. Нужно лишь проверить утверждение 0) про свободный член. В самом деле, если $A^{\pm 2^{n-1}} = a_0 + 2^n a_1 s_1 + 2^n a_2 s_2$ для подходящих целых $a_0 \equiv 1 \pmod{2^n}$, a_1 и a_2, то

$$\begin{aligned} B^{\pm 2^{n-1}} &= \varphi_2(a_0 + 2^n a_1 s_1 + 2^n a_2 s_2) = a_0 + 2^n a_1 s_2 + 2^n a_2 s_3 = \\ &= a_0 + 2^n a_1 s_2 + 2^n a_2(-1-s_1-s_2) = \\ &= (a_0 - 2^n a_2) - 2^n a_2 s_1 + 2^n (a_1 - a_2) s_2, \end{aligned}$$

что и требовалось. Для величины C доказательство проводится аналогично.

Так как $AB = C^{-1}$, то лемма полностью доказана. □

Предложение 1. *Группа единиц* $Un(K_1) < Un(K(10)) = \langle -1 \rangle \times \langle A^{2^9} \rangle \times \langle B^{2^9} \rangle$.

Доказательство. Докажем по индукции, что $Un(K(n)) = \langle -1 \rangle \times \langle A^{2^{n-1}} \rangle \times \langle B^{2^{n-1}} \rangle$. Отсюда при $n = 10$ будет следовать утверждение леммы.

Базисом индукции является лемма 9. Допустим, что утверждение выполняется для натурального n, то есть $Un(K(n)) = \langle -1 \rangle \times \langle A^{2^{n-1}} \rangle \times \langle B^{2^{n-1}} \rangle$. Докажем для $n+1$. По лемме 10 $A^{2^n} \in K(n+1)$ и $B^{2^n} \in K(n+1)$. Поэтому

$$Un(K(n+1)) \geqslant \langle -1 \rangle \times \langle A^{2^n} \rangle \times \langle B^{2^n} \rangle.$$

Допустим, что существует $D = A^k B^l \in Un(K(n+1)) \setminus \langle A^{2^n} \rangle \times \langle B^{2^n} \rangle$. Без ограничения общности можно считать, что $0 \leqslant k, l < 2^n$, а по лемме 10 $0 < k, l$. Далее по предположению индукции имеем, что $k = l = 2^{n-1}$ и потому по лемме 10

$$D = (AB)^{2^{n-1}} \in K(n) \setminus K(n+1),$$

что невозможно, так как $D \in Un(K(n+1))$. Лемма доказана. □

2.2.3. Модуль 13

Введём в рассмотрение вспомогательное кольцо

$$L = \mathbf{Z} + 13 \cdot 2^{10}\mathbf{Z}s_1 + 13 \cdot 2^{10}\mathbf{Z}s_2 < K(10) = \mathbf{Z} + 2^{10}\mathbf{Z}s_1 + 2 \cdot 2^{10}\mathbf{Z}s_2.$$

Предложение 2. *Группа единиц* $Un(L) = \langle -1 \rangle \times \langle A^{1536} \rangle \times \langle A^{1024}B^{512} \rangle$.

Доказательство. Согласно результатам из [10, § 3] получаем, используя лемму 7, что для любой единицы $\lambda \in K(0) = \mathbf{Z}[s_1] = \mathbf{Z}[\zeta_7] \cap \mathbf{R}$ выполняется $\lambda^{12} \in Un(L_0)$, где $L_0 = \mathbf{Z} + 13\mathbf{Z}s_1 + 13\mathbf{Z}s_2$. Поэтому, если $\lambda \in Un(K(10))$, то $\lambda^{12} \in Un(L)$.

Однако условие возведения в такую степень является достаточным, но не необходимым. Проведём вычисления в GAP [5] с использованием предложения 1.

```
gap> P:=NF(7,[6]);
```

```
NF(7,[ 1, 6 ])
gap> b:=CanonicalBasis(P);
CanonicalBasis( NF(7,[ 1, 6 ]) )
gap> A:=-1-2*b[1];
-E(7)+E(7)^2+E(7)^3+E(7)^4+E(7)^5-E(7)^6
gap> B:=-1-2*b[3];
E(7)+E(7)^2-E(7)^3-E(7)^4+E(7)^5+E(7)^6
gap> c:=Basis(P,[1,b[1],b[2]]);
Basis( NF(7,[ 1, 6 ]), [ 1, E(7)+E(7)^6, E(7)^2+E(7)^5 ] )
gap> k:=Coefficients(c,A^512) mod 13;
[ 9, 8, 6 ]
gap> X1:=9+8*c[2]+6*c[3];
-E(7)-3*E(7)^2-9*E(7)^3-9*E(7)^4-3*E(7)^5-E(7)^6
gap> l:=Coefficients(c,B^512) mod 13;
[ 1, 11, 5 ]
gap> X2:=1+11*c[2]+5*c[3];
10*E(7)+4*E(7)^2-E(7)^3-E(7)^4+4*E(7)^5+10*E(7)^6
gap> k3:=Coefficients(c,X1^3) mod 13;
[ 1, 0, 0 ]
gap> l3:=Coefficients(c,X2^3) mod 13;
[ 1, 0, 0 ]
gap> pr:=[];
[  ]
gap> for i in [0..3] do
> for j in [0..3] do
> m:=(Coefficients(c,X1^i*X2^j) mod 13);
> if (m[2]=0) and (m[3]=0)
> then
> Add(pr,[i,j,m]);
> fi;
> od;
> od;
gap> pr;
[ [ 0, 0, [ 1, 0, 0 ] ], [ 0, 3, [ 1, 0, 0 ] ],
[ 1, 2, [ 9, 0, 0 ] ], [ 2, 1, [ 3, 0, 0 ] ],
[ 3, 0, [ 1, 0, 0 ] ], [ 3, 3, [ 1, 0, 0 ] ] ]
gap> quit;
```

Из этих вычислений следует, что

$$Un(L) = \langle -1 \rangle \times \langle A^{1536}, B^{1536}, A^{512}B^{1024}, A^{1024}B^{512} \rangle.$$

Так как $A^{512}B^{1024} \cdot A^{1024}B^{512} = A^{1536}B^{1536}$, то $Un(L) = \langle -1 \rangle \times \langle A^{1536}, B^{1536}, A^{1024}B^{512} \rangle$. Далее заметим, что $(A^{1024}B^{512})^3 = A^{3072}B^{1536} = (A^{1536})^2 B^{1536}$. Поэтому $Un(L) = \langle -1 \rangle \times \langle A^{1536} \rangle \times \langle A^{1024}B^{512} \rangle$. □

2.2.4. Модуль 29

Теорема 1. *Группа единиц* $Un(K_1) = \langle -1 \rangle \times \langle A^{512 \cdot 21} \rangle \times \langle A^{512 \cdot 17}B^{512} \rangle$.

Доказательство. Согласно результатам из [10, § 3] получаем, используя лемму 7, что для любой единицы $\lambda \in K(0) = \mathbf{Z}[s_1] = \mathbf{Z}[\zeta_7] \cap \mathbf{R}$ выполняется $\lambda^{28} \in Un(M)$, где

$M = \mathbf{Z} + 29\mathbf{Z}s_1 + 29\mathbf{Z}s_2$. Поэтому если $\lambda \in Un(L)$, то $\lambda^{28} \in Un(K_1)$. Однако условие возведения в такую степень является достаточным, но не необходимым.

Проведём вычисления в GAP [5] с использованием предложения 2.

```
gap> P:=NF(7,[6]);
NF(7,[ 1, 6 ])
gap> b:=CanonicalBasis(P);
CanonicalBasis( NF(7,[ 1, 6 ]) )
gap> c:=Basis(P,[1,b[1],b[2]]);
Basis( NF(7,[ 1, 6 ]), [ 1, E(7)+E(7)^6, E(7)^2+E(7)^5 ] )
gap> A:=-1-2*b[1];
-E(7)+E(7)^2+E(7)^3+E(7)^4+E(7)^5-E(7)^6
gap> B:=-1-2*b[2];
E(7)-E(7)^2+E(7)^3+E(7)^4-E(7)^5+E(7)^6
gap> kA:=Coefficients(c,A^1536) mod 29;
[ 12, 26, 3 ]
gap> kAB:=Coefficients(c,A^1024*B^512) mod 29;
[ 15, 6, 3 ]
gap> ZA:=12+26*c[2]+3*c[3];
14*E(7)-9*E(7)^2-12*E(7)^3-12*E(7)^4-9*E(7)^5+14*E(7)^6
gap> ZAB:=15+6*c[2]+3*c[3];
-9*E(7)-12*E(7)^2-15*E(7)^3-15*E(7)^4-12*E(7)^5-9*E(7)^6
gap> kA28:=Coefficients(c,ZA^28) mod 29;
[ 1, 0, 0 ]
gap> kA14:=Coefficients(c,ZA^14) mod 29;
[ 1, 0, 0 ]
gap> kA7:=Coefficients(c,ZA^7) mod 29;
[ 1, 0, 0 ]
gap> kA4:=Coefficients(c,ZA^4) mod 29;
[ 9, 26, 23 ]
gap> kAB28:=Coefficients(c,ZAB^28) mod 29;
[ 1, 0, 0 ]
gap> kAB14:=Coefficients(c,ZAB^14) mod 29;
[ 1, 0, 0 ]
gap> kAB7:=Coefficients(c,ZAB^7) mod 29;
[ 1, 0, 0 ]
gap> kAB4:=Coefficients(c,ZAB^4) mod 29;
[ 12, 26, 3 ]
gap> pr:=[];
[  ]
gap> for i in [0..7] do
> for j in [0..7] do
> m:=(Coefficients(c,ZA^i*ZAB^j) mod 29);
> if (m[2]=0) and (m[3]=0)
> then
> Add(pr,[i,j,m]);
> fi;
> od;
> od;
gap> pr;
```

```
[ [ 0, 0, [ 1, 0, 0 ] ], [ 0, 7, [ 1, 0, 0 ] ],
[ 1, 3, [ 1, 0, 0 ] ], [ 2, 6, [ 1, 0, 0 ] ],
[ 3, 2, [ 1, 0, 0 ] ], [ 4, 5, [ 1, 0, 0 ] ],
[ 5, 1, [ 1, 0, 0 ] ], [ 6, 4, [ 1, 0, 0 ] ],
[ 7, 0, [ 1, 0, 0 ] ], [ 7, 7, [ 1, 0, 0 ] ] ]
gap> quit;
```

Как в доказательстве леммы 9, из этих вычислений следует, что

$$Un(K_1) = \langle -1\rangle \times \left\langle A^{1536\cdot 7}, \left(A^{1024}B^{512}\right)^7, A^{1536\cdot 5}\cdot\left(A^{1024}B^{512}\right)\right\rangle.$$

Имеем $A^{1536\cdot 5}\left(A^{1024}B^{512}\right) = A^{1536\cdot 5+1024}B^{1536} = A^{512\cdot 17}B^{512}$. Для удобства положим $X = A^{512}$ и $Y = B^{512}$. В таких обозначениях $Un(K_1) = \langle -1\rangle \times \langle X^{21}, X^{14}Y^7, X^{17}Y\rangle$. Возникает матрица

$$\begin{pmatrix} 21 & 0\\ 14 & 7\\ 17 & 1\end{pmatrix},$$

над которой произведём элементарные преобразования:

$$\begin{pmatrix} 21 & 0\\ 14 & 7\\ 17 & 1\end{pmatrix} \longleftrightarrow \begin{pmatrix} 21 & 0\\ 14-119 & 0\\ 17 & 1\end{pmatrix} \longleftrightarrow \begin{pmatrix} 21 & 0\\ -105 & 0\\ 17 & 1\end{pmatrix} \longleftrightarrow \begin{pmatrix} 21 & 0\\ 17 & 1\end{pmatrix}.$$

Таким образом, получаем $Un(K_1) = \langle -1\rangle \times \langle A^{512\cdot 21}\rangle \times \langle A^{512\cdot 17}B^{512}\rangle$. □

2.3. Кольцо $\mathbf{K_2}$

2.3.1. Общие свойства

Положим для удобства для каждого $i \in \{1, 2, \ldots, 6\}$ $s_i = \zeta_{13}^i + \zeta_{13}^{-i}$.

Лемма 11. *При введённых обозначениях*

1) $G = s_1 - s_2 - s_3 - s_4 + s_5 - s_6 = 1 + 2s_1 + 2s_5$;
2) $H = -s_1 - s_2 - s_3 + s_4 - s_5 + s_6 = 1 + 2s_4 + 2s_6$;
3) $I = -s_1 + s_2 + s_3 - s_4 - s_5 - s_6 = 1 + 2s_2 + 2s_3$;
4) $Un(\mathbf{Z}[\zeta_{13}]\cap\mathbf{R}) = Un(\mathbf{Z}[s_1]) = \langle -1\rangle \times \langle s_1\rangle \times \langle s_2\rangle \times \langle s_3\rangle \times \langle s_4\rangle \times \langle s_5\rangle$;
5) $s_1s_2s_3s_4s_5s_6 = -1$ *u* $(s_1 + s_5)(s_2 + s_3)(s_4 + s_6) = -1$.

Доказательство. Утверждения 1–3 следуют из того, что

$$s_1 + s_2 + s_3 + s_4 + s_5 + s_6 = \sum_{j=1}^{12} \zeta_{13}^j = -1.$$

Утверждение 4 следует из леммы 4, поскольку 2 — примитивный корень по модулю 13. Утверждение 5 проверим непосредственно. Имеем

$$\begin{aligned} s_1s_2s_3s_4s_5s_6 &= (s_3 + s_1)(s_6 + s_1)(s_2 + s_1) =\\ &= (s_4 + s_3 + s_6 + s_5 + s_4 + s_2 + s_2 + 2)(s_2 + s_1) =\\ &= (s_6 + s_5 + s_4 + s_3 + s_2 + s_1 + 1 + s_4 + s_2 - s_1 + 1)(s_2 + s_1) =\\ &= (s_4 + s_2 - s_1 + 1)(s_2 + s_1) =\\ &= s_4(s_2 + s_1) + (s_2 - s_1)(s_2 + s_1) + (s_2 + s_1) =\\ &= s_6 + s_2 + s_5 + s_3 + s_4 - s_2 + s_2 + s_1 = -1. \end{aligned}$$

Так как $s_2s_3 = s_1 + s_5$, $s_4s_6 = s_2 + s_{10} = s_2 + s_3$ и $s_1s_5 = s_4 + s_6$, то утверждение доказано. □

Лемма 12. *Кольцо*

$$K_2 = \mathbf{Z} + 2^{10} \cdot 5^3\mathbf{Z}(s_1 + s_5) + 2^{10} \cdot 5^3\mathbf{Z}(s_4 + s_6) = \\ = \mathbf{Z} + 2^{10} \cdot 5^3\mathbf{Z}(s_1 + s_5) + 2^{10} \cdot 5^3\mathbf{Z}(s_2 + s_3).$$

Доказательство. Равенства следуют из утверждений 1 и 2 леммы 11. □

Пусть $F = \mathbf{Q}(s_1 + s_5, s_2 + s_3) < \mathbf{Q}(\zeta_{13}) \cap \mathbf{R}$. Группу Галуа поля F (над $\mathbf{Q}$) (равносильно: группу автоморфизмов поля F) обозначим $G(F)$.

Для каждого $i \in \{1, 2, \ldots, 12\}$ обозначим через ψ_i автоморфизм кругового поля $\mathbf{Q}(\zeta_{13})$, индуцированный отображением $\zeta_{13} \mapsto \zeta_{13}^i$.

Лемма 13. *Централизатором поля F в группе Галуа кругового поля $\mathbf{Q}(\zeta_{13})$ (над $\mathbf{Q}$) (равносильно: в группе автоморфизмов поля $\mathbf{Q}(\zeta_{13})$) является*

$$\{\psi_1, \psi_5, \psi_{12}, \psi_8\} = \langle\psi_5\rangle \cong \mathbf{Z}_4.$$

Другими словами, если для $i \in \{1, \ldots, 12\}$ обозначить через ϕ_i автоморфизм поля F, индуцированный ψ_i, то группа Галуа $G(F) = \{\phi_1, \phi_2, \phi_4\} = \langle\phi_2\rangle \cong \mathbf{Z}_3$.

Доказательство. Так как выполняются равенства

$$\psi_5(s_1 + s_5) = s_5 + s_{25} = s_5 + s_1,$$
$$\psi_5(s_2 + s_3) = s_{10} + s_{15} = s_3 + s_2,$$

то подгруппа $\langle\psi_5\rangle$ централизует поле F. Поскольку

$$5^2 = 25 \equiv 12 \pmod{13},\ 5^3 = 125 \equiv 8 \pmod{13} \text{ и } 5^4 = 625 \equiv 1 \pmod{13},$$

то $\langle\psi_5\rangle = \{\psi_1, \psi_5, \psi_{12}, \psi_8\} \cong \mathbf{Z}_4$. Заметим, что $\psi_2(s_1+s_5) = s_2+s_{10} = s_2+s_3$. Поэтому ψ_2 не централизует поле F, что завершает доказательство. □

Лемма 14. *Пусть $p \in \{2, 5\}$. Тогда для поля F*

1) *индекс ветвления $e = 1$ для всякого $p \in \{2, 5\}$;*
2) *степень инерции $f = 3$ для $p = 2$ и $f = 1$ для $p = 5$.*

Доказательство. По лемме 13 утверждения влечёт следствие [9, с. 247], так как $2 \notin \langle 5\rangle \pmod{13}$. □

Лемма 15. *Пусть L — кольцо целых поля F. Тогда*

1) $L = \mathbf{Z} + \mathbf{Z}(s_1 + s_5) + \mathbf{Z}(s_2 + s_3)$;
2) *группа единиц* $Un(L) = \langle-1\rangle \times \langle s_1 + s_5\rangle \times \langle s_2 + s_3\rangle$.

Доказательство. 1. По лемме 4 кольцо целых поля $\mathbf{Q}(\zeta_{13})$ равно

$$I = \left\{ \sum_{i=0}^{11} a_i\zeta_{13}^i \mid a_i \in \mathbf{Z}\ \forall i \in \{0, 1, \ldots, 11\} \right\}.$$

Пусть

$$a = \sum_{i=0}^{11} a_i\zeta^i \in I.$$

Из леммы 13 следует, что $a \in L \longleftrightarrow \psi_5(a) = a$. Имеем по модулю 13

i	1	2	3	4	5	6	7	8	9	10	11
$5i$	5	10	2	7	12	4	9	1	6	11	3

.

Кроме того,

$$\zeta_{12} = -\sum_{i=0}^{11} \zeta^i.$$

Теперь

$$\begin{aligned}
\psi_5(a) &= a_0 + a_1\zeta_{13}^5 + a_2\zeta_{13}^{10} + a_3\zeta_{13}^2 + a_4\zeta_{13}^7 + a_5\zeta_{13}^{12} + a_6\zeta_{13}^4 + a_7\zeta_{13}^9 + \\
&+ a_8\zeta_{13} + a_9\zeta_{13}^6 + a_{10}\zeta_{13}^{11} + a_{11}\zeta_{13}^3 = \\
&= a_0 + a_8\zeta_{13} + a_3\zeta_{13}^2 + a_{11}\zeta_{13}^3 + a_6\zeta_{13}^4 + a_1\zeta_{13}^5 + a_9\zeta_{13}^6 + a_4\zeta_{13}^7 + \\
&+ a_7\zeta_{13}^9 + a_2\zeta_{13}^{10} + a_{10}\zeta_{13}^{11} + a_5\zeta_{13}^{12} = \\
&= a_0 + a_8\zeta_{13} + a_3\zeta_{13}^2 + a_{11}\zeta_{13}^3 + a_6\zeta_{13}^4 + a_1\zeta_{13}^5 + a_9\zeta_{13}^6 + a_4\zeta_{13}^7 + \\
&+ a_7\zeta_{13}^9 + a_2\zeta_{13}^{10} + a_{10}\zeta_{13}^{11} - a_5\sum_{i=0}^{11}\zeta^i = \\
&= (a_0 - a_5) + (a_8 - a_5)\zeta_{13} + (a_3 - a_5)\zeta_{13}^2 + (a_{11} - a_5)\zeta_{13}^3 + \\
&+ (a_6 - a_5)\zeta_{13}^4 + (a_1 - a_5)\zeta_{13}^5 + (a_9 - a_5)\zeta_{13}^6 + (a_4 - a_5)\zeta_{13}^7 + \\
&+ (-a_5)\zeta_{13}^8 + (a_7 - a_5)\zeta_{13}^9 + (a_2 - a_5)\zeta_{13}^{10} + (a_{10} - a_5)\zeta_{13}^{11}.
\end{aligned}$$

Возникает система

$$\left\{\begin{array}{l} a_0 = a_0 - a_5 \\ a_1 = a_8 - a_5 \\ a_2 = a_3 - a_5 \\ a_3 = a_{11} - a_5 \\ a_4 = a_6 - a_5 \\ a_5 = a_1 - a_5 \\ a_6 = a_9 - a_5 \\ a_7 = a_4 - a_5 \\ a_8 = -a_5 \\ a_9 = a_7 - a_5 \\ a_{10} = a_2 - a_5 \\ a_{11} = a_{10} - a_5 \end{array}\right. \longleftrightarrow \left\{\begin{array}{l} a_0 = a_0 \\ a_1 = a_8 \\ a_2 = a_3 \\ a_3 = a_{11} \\ a_4 = a_6 \\ a_5 = a_1 \\ a_6 = a_9 \\ a_7 = a_4 \\ a_8 = 0 \\ a_9 = a_7 \\ a_{10} = a_2 \\ a_{11} = a_{10} \end{array}\right. \longleftrightarrow \left\{\begin{array}{l} a_0 = a_0 \\ a_1 = a_5 = a_8 = 0 \\ a_2 = a_3 = a_{10} = a_{11} \\ a_4 = a_6 = a_7 = a_9 \end{array}\right. .$$

Следовательно,

$$\begin{aligned}
a &= a_0 + a_2(\zeta_{13}^2 + \zeta_{13}^3 + \zeta_{13}^{10} + \zeta_{13}^{11}) + a_4(\zeta_{13}^4 + \zeta_{13}^6 + \zeta_{13}^7 + \zeta_{13}^9) = \\
&= a_0 + a_2(s_2 + s_3) + a_4(s_4 + s_6) = \\
&= a_0 + a_2(s_2 + s_3) + a_4(-1 - (s_1 + s_5) - (s_2 + s_3)) = \\
&= (a_0 - a_4) + (-a_4)(s_1 + s_5) + (a_2 - a_4)(s_2 + s_3),
\end{aligned}$$

что и требовалось.

2. Так как L содержится в $\mathbf{Z}[\zeta_{13}] \cap \mathbf{R}$, то по леммам 11 и 13 достаточно рассмотреть $u = s_1^{k_1}s_2^{k_2}s_3^{k_3}s_4^{k_4}s_5^{k_5} \in Un(L) \longleftrightarrow \psi_5(u) = u$ для $\{k_1, k_2, k_3, k_4, k_5\} \subset \mathbf{Z}$. В самом деле

$$\psi_5(u) = s_5^{k_1}s_3^{k_2}s_2^{k_3}s_6^{k_4}s_1^{k_5} = s_1^{k_5}s_2^{k_3}s_3^{k_2}s_5^{k_1}s_6^{k_4} = s_1^{k_5}s_2^{k_3}s_3^{k_2}s_5^{k_1}(-s_1s_2s_3s_4s_5)^{-k_4} =$$
$$= (-1)^{k_4}s_1^{k_5-k_4}s_2^{k_3-k_4}s_3^{k_2-k_4}s_4^{-k_4}s_5^{k_1-k_4}.$$

Отсюда возникает система

$$\begin{cases} k_4 \in 2\mathbf{Z} \\ k_1 = k_5 - k_4 \\ k_2 = k_3 - k_4 \\ k_3 = k_2 - k_4 \\ k_4 = -k_4 \\ k_5 = k_1 - k_4 \end{cases} \longleftrightarrow \begin{cases} k_4 = 0 \\ k_1 = k_5 \\ k_2 = k_3 \\ k_3 = k_2 \\ k_5 = k_1 \end{cases} \longleftrightarrow \begin{cases} k_4 = 0 \\ k_1 = k_5 \\ k_2 = k_3 \end{cases}.$$

Таким образом, $u = (s_1s_5)^{k_1}(s_2s_3)^{k_2}$, $s_1s_5 = s_6 + s_4$, $s_2s_3 = s_5 + s_1$. Из леммы 11 получаем требуемое.

□

2.3.2. Модуль 2^{10}

Для каждого неотрицательного целого $n \in \{0, 1, 2, \dots\}$ введём в рассмотрение вспомогательные кольца $L(n) = \mathbf{Z} + 2^n\mathbf{Z}(s_1 + s_5) + 2^n\mathbf{Z}(s_2 + s_3)$. Отметим сразу, что $L = L(0)$.

Лемма 16. *Ряд $L(0) > L(1) > \cdots > L(n) > \cdots$ стабилизируется автоморфизмами из $G(F)$.*

Доказательство. Утверждение сразу следует из того, что $\phi_2(s_1 + s_2) = s_2 + s_3$ и $\phi_2(s_2 + s_3) = s_4 + s_6$, а $s_4 + s_6 = -1 - (s_1 + s_5) - (s_2 + s_3)$. □

Лемма 17. *Для вышеуказанных чисел G и I имеем*

1) $G^2 = 13 - 2G - 2I$;
2) $I^2 = 11 + 2G$;
3) $GI = -7 + G + 3I$.

Доказательство. Равенства легко следуют из леммы 3. □

Лемма 18. *Группа единиц*

$$Un(K_1) < Un(L(1)) = \langle -1\rangle \times \left\langle (s_1 + s_5)^7, (s_1 + s_5)^5(s_2 + s_3)\right\rangle.$$

Причём

$$(s_1 + s_5)^7 = -183 + 286(s_1 + s_5) + 76(s_2 + s_3) = -364 + 143G + 38I,$$
$$(s_1 + s_5)^5(s_2 + s_3) = -11 + 10(s_1 + s_5) + 6(s_2 + s_3) = -19 + 5G + 3I.$$

Доказательство. Ясно, что

$$K_2 = \mathbf{Z} + 2^{10} \cdot 5^3\mathbf{Z}(s_1 + s_5) + 2^{10} \cdot 5^3\mathbf{Z}(s_2 + s_3) < L(1) < \mathbf{Z}[s_1] = \mathbf{Z}[\zeta_{13}] \cap \mathbf{R}.$$

Поэтому для групп единиц

$$Un(K_2) < Un(L(1)) < Un(L) = \langle -1\rangle \times \prod \langle s_1 + s_5\rangle \times \langle s_2 + s_3\rangle.$$

Согласно результатам из [10, § 3] получаем, используя лемму 7, что для любой единицы $\lambda \in \mathbf{Z}[s_1] = \mathbf{Z}[\zeta_{13}] \cap \mathbf{R}$ выполняется $\lambda^7 \in Un(L(1))$.

Однако условие возведения в 7-ю степень является достаточным, но не необходимым. Проведём вычисления в GAP [5].

```
gap> F:=NF(13,[5]);
NF(13,[ 1, 5, 8, 12 ])
gap> b:=CanonicalBasis(F);
CanonicalBasis( NF(13,[ 1, 5, 8, 12 ]) )
gap> b[1];
E(13)+E(13)^5+E(13)^8+E(13)^12
gap> u:=b[1];
E(13)+E(13)^5+E(13)^8+E(13)^12
gap> v:=b[2];
E(13)^2+E(13)^3+E(13)^10+E(13)^11
gap> c:=Basis(F,[1,b[1],b[2]]);
Basis( NF(13,[ 1, 5, 8, 12 ]), [ 1, E(13)+E(13)^5+E(13)^8+E(13)^12,
E(13)^2+E(13)^3+E(13)^10+E(13)^11 ] )
gap> d:=Basis(F,[1,1+2*b[1],1+2*b[2]]);
Basis( NF(13,[ 1, 5, 8, 12 ]), [ 1,
E(13)-E(13)^2-E(13)^3-E(13)^4+E(13)^5-E(13)^6-E(13)^7+E(13)^8
-E(13)^9-E(13)^10-E(13)^11+E(13)^12,
-E(13)+E(13)^2+E(13)^3-E(13)^4-E(13)^5-E(13)^6-E(13)^7-E(13)^8
-E(13)^9+E(13)^10+E(13)^11-E(13)^12 ] )
gap> pr:=[];
[  ]
gap> for i in [0..7] do
> for j in [0..7] do
> k:=Coefficients(c,u^i*v^j);
> l:=Coefficients(d,u^i*v^j);
> if (k mod 2)=[1,0,0]
> then
> Add(pr,[i,j,k,l]);
> fi;
> od;
> od;
gap> pr;
[ [ 0, 0, [ 1, 0, 0 ], [ 1, 0, 0 ] ],
[ 0, 7, [ -259, -76, 210 ], [ -326, -38, 105 ] ],
[ 1, 3, [ -7, -2, 6 ], [ -9, -1, 3 ] ],
[ 2, 6, [ 189, 56, -148 ], [ 235, 28, -74 ] ],
[ 3, 2, [ 5, 2, -4 ], [ 6, 1, -2 ] ],
[ 4, 5, [ -135, -40, 106 ], [ -168, -20, 53 ] ],
[ 5, 1, [ -11, 10, 6 ], [ -19, 5, 3 ] ],
[ 6, 4, [ 97, 28, -76 ], [ 121, 14, -38 ] ],
[ 7, 0, [ -183, 286, 76 ], [ -364, 143, 38 ] ],
[ 7, 7, [ -2479, -734, 1946 ], [ -3085, -367, 973 ] ] ]
gap> quit;
```

Как в вычислениях, обозначим для удобства $u = s_1 + s_5$ и $v = s_2 + s_3$. Получаем, что $\{uv^3, u^2v^6, u^3v^2, u^4v^5, u^5v, u^6v^4\} \subset Un(L(1))$. Далее заметим, что

$$\begin{aligned}
\left(uv^3\right)^2 &= u^2v^6,\\
\left(uv^3\right)^3 &= u^3v^9 = u^3v^2v^7,\\
\left(uv^3\right)^4 &= u^4v^{12} = u^4v^5v^7,\\
\left(uv^3\right)^5 &= u^5v^{15} = u^5vv^{14},\\
\left(uv^3\right)^6 &= u^6v^{18} = u^6v^4v^{14}.
\end{aligned}$$

Следовательно, $Un(L(1)) = \langle -1\rangle \times \langle u^7, v^7, uv^3\rangle$. Возникает матрица

$$\begin{pmatrix} 7 & 0\\ 0 & 7\\ 1 & 3 \end{pmatrix},$$

над которой произведём элементарные преобразования

$$\begin{pmatrix} 7 & 0\\ 0 & 7\\ 1 & 3 \end{pmatrix} \longleftrightarrow \begin{pmatrix} 7 & 0\\ -2 & 1\\ 1 & 3 \end{pmatrix} \longleftrightarrow \begin{pmatrix} 7 & 0\\ -2 & 1\\ 7 & 0 \end{pmatrix} \longleftrightarrow \begin{pmatrix} 7 & 0\\ 5 & 1 \end{pmatrix}.$$

Таким образом, получаем

$$Un(L(1)) = \langle -1\rangle \times \left\langle (s_1+s_5)^7\right\rangle \times \left\langle (s_1+s_5)^5(s_2+s_3)\right\rangle.$$

Оставшееся следует из вычислений. □

Далее можно рассуждать, как в лемме 10 и предложении 1, но мы проведём прямые вычисления.

Предложение 3. *Группа единиц*

$$Un(K_2) < Un(L(10)) = \langle -1\rangle \times \left\langle (s_1+s_5)^{7\cdot 512}\right\rangle \times \left\langle \left((s_1+s_5)^5(s_2+s_3)\right)^{512}\right\rangle.$$

Доказательство. Согласно результатам из [10, § 3 и лемма 32] получаем, используя лемму 7, что для любой единицы $\lambda \in L(1)$ выполняется $\lambda^{512} \in Un(L(10))$.

Проверим необходимость условия возведения в такую степень.

```
gap> F:=NF(13,[5]);
NF(13,[ 1, 5, 8, 12 ])
gap> b:=CanonicalBasis(F);
CanonicalBasis( NF(13,[ 1, 5, 8, 12 ]) )
gap> c:=Basis(F,[1,b[1],b[2]]);
Basis( NF(13,[ 1, 5, 8, 12 ]), [ 1,
E(13)+E(13)^5+E(13)^8+E(13)^12,
E(13)^2+E(13)^3+E(13)^10+E(13)^11 ] )
gap> p:=b[1]^7;
469*E(13)+259*E(13)^2+259*E(13)^3+183*E(13)^4+469*E(13)^5+
183*E(13)^6+183*E(13)^7+469*E(13)^8+183*E(13)^9+259*E(13)^10
+259*E(13)^11+469*E(13)^12
gap> q:=b[1]^5*b[2];
21*E(13)+17*E(13)^2+17*E(13)^3+11*E(13)^4+21*E(13)^5+
11*E(13)^6+11*E(13)^7+21*E(13)^8+11*E(13)^9+17*E(13)^10
+17*E(13)^11+21*E(13)^12
gap> Coefficients(c,p^512) mod 1024;
```

```
[ 1, 0, 0 ]
gap> Coefficients(c,p^256) mod 1024;
[ 1, 512, 512 ]
gap> Coefficients(c,q^512) mod 1024;
[ 1, 0, 0 ]
gap> Coefficients(c,q^256) mod 1024;
[ 513, 0, 512 ]
gap> pr:=[];
[  ]
gap> for i in [0..512] do
> for j in [0..512] do
> k:=(Coefficients(c,p^i*q^j) mod 1024);
> if (k[2]=0) and (k[3])=0
> then
> Add(pr,[i,j]);
> fi;
> od;
> od;
gap> pr;
[ [ 0, 0 ], [ 0, 512 ], [ 512, 0 ], [ 512, 512 ] ]
gap> quit;
```

□

2.3.3. Модуль 5^3

Теорема 2. *Группа единиц*

$$Un(K_2) = \langle -1 \rangle \times \left\langle (s_1 + s_5)^{7 \cdot 512 \cdot 25} \right\rangle \times \left\langle \left((s_1 + s_5)^5 (s_2 + s_3) \right)^{512 \cdot 25} \right\rangle .$$

Доказательство. Согласно результатам из [10, § 3 и лемма 32] получаем, используя лемму 7, что для любой единицы $\lambda \in \mathbf{Z}[s_1] = \mathbf{Z}[\zeta_7] \cap \mathbf{R}$ выполняется $\lambda^{100} \in Un(M)$, где $M = \mathbf{Z} + 5^3\mathbf{Z}s_1 + 5^3\mathbf{Z}s_2$. Поэтому, если $\lambda \in Un(L(10))$, то $\lambda^{100} \in Un(K_2)$.

Проведём вычисления в GAP [5] с использованием предложения 3, чтобы проверить необходимость возведения в такую степень.

```
gap> F:=NF(13,[5]);
NF(13,[ 1, 5, 8, 12 ])
gap> b:=CanonicalBasis(F);
CanonicalBasis( NF(13,[ 1, 5, 8, 12 ]) )
gap> c:=Basis(F,[1,b[1],b[2]]);
Basis( NF(13,[ 1, 5, 8, 12 ]), [ 1,
E(13)+E(13)^5+E(13)^8+E(13)^12,
E(13)^2+E(13)^3+E(13)^10+E(13)^11 ] )
gap> c1:=(Coefficients(c,b[1]^(7*512)) mod 125);
[ 86, 60, 20 ]
gap> c2:=(Coefficients(c,b[1]^2560*b[2]^512) mod 125);
[ 96, 15, 70 ]
gap> r:=86+60*b[1]+20*b[2];
-26*E(13)-66*E(13)^2-66*E(13)^3-86*E(13)^4-26*E(13)^5
-86*E(13)^6-86*E(13)^7-26*E(13)^8-86*E(13)^9-66*E(13)^10
-66*E(13)^11-26*E(13)^12
```

```
gap> t:=96+15*b[1]+70*b[2];
-81*E(13)-26*E(13)^2-26*E(13)^3-96*E(13)^4-81*E(13)^5
-96*E(13)^6-96*E(13)^7-81*E(13)^8-96*E(13)^9-26*E(13)^10
-26*E(13)^11-81*E(13)^12
gap> Coefficients(c,r^100) mod 125;
[ 1, 0, 0 ]
gap> Coefficients(c,r^50) mod 125;
[ 1, 0, 0 ]
gap> Coefficients(c,r^20) mod 125;
[ 76, 75, 25 ]
gap> Coefficients(c,r^25) mod 125;
[ 1, 0, 0 ]
gap> Coefficients(c,t^100) mod 125;
[ 1, 0, 0 ]
gap> Coefficients(c,t^50) mod 125;
[ 1, 0, 0 ]
gap> Coefficients(c,t^20) mod 125;
[ 26, 50, 25 ]
gap> Coefficients(c,t^25) mod 125;
[ 1, 0, 0 ]
gap> pr:=[];
[  ]
gap> for i in [0..25] do
> for j in [0..25] do
> k:=(Coefficients(c,r^i*t^j) mod 125);
> if (k[2]=0) and (k[3]=0)
> then
> Add(pr,[i,j]);
> fi;
> od;
> od;
gap> pr;
[ [ 0, 0 ], [ 0, 25 ], [ 25, 0 ], [ 25, 25 ] ]
gap> quit;
```

□

Список литературы

1. **Алеев, Р. Ж.** Центральные элементы целочисленных групповых колец / Р. Ж. Алеев // Алгебра и логика. — 2000. — Т. 39, № 5. — С. 513–525.
2. **Молодорич, М. И.** Классовые кольца характеров спорадических групп / М. И. Молодорич // Сиб. электрон. мат. изв. — 2014. — Т. 11. — С. 878–886.
3. **Молодорич, М. И.** Группы единиц классовых колец характеров спорадических групп / М. И. Молодорич // Сиб. электрон. мат. изв. — 2016. — Т. 13. — С. 38–48.
4. **Aleev, R. Zh.** Class character rings of groups J_1 and $O'N$ / R. Zh. Aleev, M. I. Molodorich // Groups and Graphs, Algorithms and Automata: Abstracts of the International Conference and PhD Summer School in honor of the 80th Birthday of Professor Vyacheslav A. Belonogov and of the 70th Birthday of Professor Vitaly A. Baransky. — 2015. — P. 31.

5. The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.8.3; 2016 [Электронный ресурс]. — URL: http://www.gap-system.org (дата обращения 12.03.2017).
6. **Боревич, З. И.** Теория чисел / З. И. Боревич, И. Р. Шафаревич. — М. : Наука, 1985. — 504 с.
7. **Алеев, Р. Ж.** Порождающие группы круговых единиц / Р. Ж. Алеев, В. С. Такшеева // Вестн. Челяб. гос. ун-та. — 2008. — № 6 (107). Математика. Механика. Информатика. Вып. 10. — С. 121–129.
8. **Masley, J. M.** Solution of small class number problems for cyclotomic fields / J. M. Masley // Compositio Mathematica. — 1976. — Vol. 33, fasc. 2. — P. 179–186.
9. **Narkiewicz, W.** Elementary and Analytic Theory of Algebraic Numbers / W. Narkiewicz.— Warsaw : PWN — Polish Sci. Publ., 1974. — 630 p.
10. **Алеев, Р. Ж.** Единицы полей характеров и центральные единицы целочисленных групповых колец конечных групп/ Р. Ж. Алеев // Мат. труды. — 2000. — Т. 3. — С. 3–37.

Поступила в редакцию 18.04.2017
После переработки 25.06.2017

Сведения об авторах

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

Молодорич Маргарита Ивановна, преподаватель кафедры системного программирования, Южно-Уральский государственный университет (национальный исследовательский университет), Челябинск, Россия; e-mail: molodorichmi@susu.ru.

Chelyabinsk Physical and Mathematical Journal. 2017. Vol. 2, iss. 2. P. 133–151.

THE UNIT GROUPS OF CLASS CHARACTER RINGS OF RUDVALIS GROUP

R.Zh. Aleev[1,2,a], **M.I. Molodorich**[2,b]

[1] *Chelyabinsk State University, Chelyabinsk, Russia*
[2] *South Ural State University (National Research University), Chelyabinsk, Russia*
[a] *aleevrz@susu.ru, aleev@csu.ru;* [b] *molodorichmi@susu.ru*

In our work we study the class character rings of group Ru, which are not the subrings of real quadratic fields. Their units are described.

Keywords: *sporadic group, unit, character, group rings, class character ring.*

References

1. **Aleev R.Zh.** Central elements of integral group rings. *Algebra and Logic*, 2000, vol. 39, no. 5, pp. 293–300.
2. **Molodorich M.I.** Klassovye kol'tsa kharakterov sporadicheskikh grupp [The class character rings of sporadic groups]. *Sibirskie elektronnye matematicheskiye izvestiya* [Siberian Electronic Mathematical Reports], 2014, vol. 11, pp. 878–886. (In Russ.).
3. **Molodorich M.I.** Gruppy yedinits klassovykh kolets kharakterov sporadicheskikh grupp [The unit groups of class character rings of sporadic groups]. *Sibirskie elektronnye matematicheskiye izvestiya* [Siberian Electronic Mathematical Reports], 2016, vol. 13, pp. 38–48. (In Russ.).
4. **Aleev R.Zh., Molodorich M.I.** Class character rings of groups J_1 and $O'N$. *Groups and Graphs, Algorithms and Automata: Abstracts of the International Conference and PhD Summer School in honor of the 80th Birthday of Professor Vyacheslav A. Belonogov and of the 70th Birthday of Professor Vitaly A.Baransky*, 2015, p. 31.
5. *The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.8.3; 2016.* Available at: http://www.gap-system.org, accessed 12.03.2017.
6. **Borevich Z.I., Shafarevich I.R.** *Number Theory.* New York, San Francisco, London, Academic Press, 1966. 435 p.
7. **Aleev R.Zh., Taksheeva V.S.** Porozhdayushchiye gruppy krugovykh edinits [Generators of the group of cyclotomic units]. *Vestnik Chelyabinskogo gosudarstvennogo universiteta* [Bulletin of Chelyabinsk State University], 2008, no. 6 (107), pp. 121–129. (In Russ.).
8. **Masley J.M.** Solution of small class number problems for cyclotomic fields. *Compositio Mathematica*, 1976, vol. 33, fasc. 2, pp. 179–186.
9. **Narkiewicz W.** *Elementary and Analytic Theory of Algebraic Numbers.* Warsaw, PWN — Polish Scientific Publishers, 1974. 630 p.
10. **Aleev R.Zh.** The units of character fields and the central units of integer group rings of finite groups. *Siberian Advances in Mathematics*, 2001, vol. 11, no. 1, pp. 1–33.

Accepted article received 18.04.2017
Corrections received 25.06.2017