УДК 511.625

АВТОМОРФИЗМЫ КОЛЕЦ ВЫЧЕТОВ КОЛЕЦ ЦЕЛЫХ КРУГОВЫХ ПОЛЕЙ

А.В. Шпонько[1]

Изучается структура колец вычетов колец целых круговых полей путем рассмотрения их кольцевых автоморфизмов. Выявлены связи особой подгруппы группы автоморфизмов с системой вложенных подколец кольца вычетов. Среди возникающих подколец выделено особо перспективное для изучения, и найдено множество его необратимых элементов для некоторых нетривиальных случаев.

Ключевые слова: абелевы поля, круговые поля, кольца целых, кольца вычетов, подкольца, автоморфизмы.

Пусть m – натуральное число. Обозначим через $\zeta_m = e^{\frac{2\pi i}{m}}$ – первообразный корень степени m из единицы. Тогда $Q(\zeta_m)$ называется m-круговым полем. Согласно теореме Кронекера–Вебера всякое абелево поле может быть вложено в круговое, что и обуславливает их важное значение в теории абелевых полей.

Пусть $I(Q(\zeta_m))$ – его кольцо целых. Известно, что оно состоит из элементов вида $\sum_{i=1}^{m-1}\alpha_i\zeta_m^i$, где $\alpha_i \in Z\,\forall i \in \{1,...,m-1\}$, то есть $I(Q(\zeta_m)) = \mathbb{Z}[\zeta_m]$. В частности, при $m=4$ имеем кольцо гауссовых целых. Мультипликативная структура этих колец известна лишь частично. В общем случае известны только подгруппы единиц конечного индекса. Поэтому нами изучается $I_m^p = I(Q(\zeta_m))/pI(Q(\zeta_m))$ – кольцо вычетов по модулю p кольца целых кругового поля. В дальнейшем значения p и m полагаются простыми и различными. В отличие от $I(Q(\zeta_m))$ эти кольца конечны, ввиду чего более удобны для изучения.

В [1] была также показана важность исследования колец вычетов абелевых полей (в особенности, круговых полей) для изучения центральных единиц целочисленных групповых колец конечных групп.

В [1, 2] начато исследование мультипликативной структуры колец вычетов кольца целых круговых полей. В частности известно, что

$$U(I_m^p) \cong \prod_{i=1}^{g} Z_{p^f-1},$$

где $f = \min\{j \geq 1 \mid p^j \equiv 1 (\mathrm{mod}\, m)\}$ и $fg = m-1$. Однако, сам изоморфизм не установлен, ввиду чего мы, в общем случае, не знаем порождающих элементов.

Пусть φ – произвольный кольцевой автоморфизм I_m^p. Тогда образ произвольного элемента I_m^p относительно φ можно представить в виде

$$\varphi\left(\sum_{i=1}^{m-1}\alpha_i\zeta^i\right) = \sum_{i=1}^{m-1}\alpha_i\varphi(\zeta)^i.$$

Тем самым автоморфизм однозначно определяется его образом $\varphi(\zeta)$.

Вообще говоря, отображение $\varphi: I_m^p \to I_m^p$ будет автоморфизмом I_m^p в том, и только в том случае, когда φ согласовано с кольцевыми операциями, $\mathrm{ord}(\varphi(\zeta)) = m$ и $\varphi(\zeta)$, $\varphi(\zeta)^2$,... $\varphi(\zeta)^{m-1}$ линейно независимы.

Автоморфизмы вида $\varphi(\zeta) = \zeta^k$, где $k = \{1,...,m-1\}$, обозначим как φ_k. Такие автоморфизмы назовем *целыми*. Они образуют в $Aut(I_m^p)$ подгруппу. Обозначим её $MAut(I_m^p)$.

[1] Шпонько Андрей Викторович – аспирант, кафедра алгебры, Южно-Уральский государственный университет
E-mail: ashponko@gmail.com

Легко показать, что если отображение $\psi: x \mapsto x^r$, где $x \in I_m^p, r \in N^+$ является автоморфизмом, то $\psi \in \langle \varphi_p \rangle \subseteq MAut(I_m^p)$. Поэтому подгруппа $\langle \varphi_p \rangle$ играет особую роль в $MAut(I_m^p)$, обозначим её через $PAut(I_m^p)$, а лежащие в ней автоморфизмы назовем *p-автоморфизмами.*

В [3] было доказано, что для произвольной подгруппы $A \subseteq PAut(I_m^p)$ множество устойчивых, относительно её действия, элементов

$$R(A) = \left\langle x \in I_m^p \mid \forall \sigma \in A \ \sigma(x) = x \right\rangle$$

является подкольцом в I_m^p. Более того, различным подгруппам соответствует различные подкольца и если выполнено $A \subseteq B \subseteq PAut(I_m^p)$, то $R(PAut(I_m^p)) \subseteq R(B) \subseteq R(A)$. Ввиду обозначенных свойств получаем множество подколец, структура вложенности которых в точности соответствует структуре вложенности подгрупп $PAut(I_m^p)$ (можно говорить об аналоге соответствия Галуа).

Обозначим для удобства $R(PAut(I_m^p))$ через RP_m^p и перейдем к его более детальному рассмотрению. Сперва заметим, что $RP_m^p = \left\langle x \in I_m^p \mid x^p = x \right\rangle$. Далее, найдем общий вид его элементов, характеризующим свойством которых является устойчивость к возведению в p-ю степень. Заметим, что

$$\left(\sum_{i=1}^{m-1} \alpha_i \zeta^i \right)^p = \sum_{i=1}^{m-1} \alpha_i^p \zeta^{ip} = \sum_{i=1}^{m-1} \alpha_i \zeta^{ip},$$

что доказывается идентично аналогичному свойству полей характеристики p. Отсюда следует

$$x = \sum_{i=1}^{m-1} \alpha_i \zeta^i \ x \in RP_m^p \Leftrightarrow \forall i,k \in Z_m^1 : j \equiv kp (\mathrm{mod}\, m) \rightarrow \alpha_j = \alpha_k,$$

это означает попарное равенство коэффициентов α_i для значений i, соответствующих одному смежному классу Z_m^* по $\langle p \rangle$. Теперь видно, что RP_m^p по сложению есть линейное пространство над Z_p размерности

$$g = \left| \langle p \rangle : Z_m^* \right|.$$

Его базис образован элементами

$$\theta_i = \sum\nolimits_{j \in P_i} \zeta^j, \qquad (1)$$

где $i \in \{1,...,g\}$, а P_i – смежные классы Z_m^1 по $\langle p \rangle$. Стоит отметить идентичность данных базисов для значений p сравнимых по модулю m, что обусловливает схожесть строения соответствующих колец вычетов, выявленную ранее в ходе численного эксперимента [2].

Обозначим через f – мощность $|PAut(I_m^p)|$. Очевидно $f = |\langle p \rangle|$ в Z_m^1. Отсюда видно, что для произвольного $a \in I_m^p$ справедливо $a^{p^f} = a$. Откуда, в частности, вытекает отсутствие в I_m^p нильпотентных элементов.

Рассмотрим функцию

$$P(x) = \prod_{\sigma \in PAut(I_m^p)} \sigma(x) = x^{1+p+\ +p^{f-1}} = x^{\frac{p^f-1}{p-1}},$$

ставящую в соответствие всякому элементу из I_m^p произведение всех его образов относительно p-автоморфизмов. Легко убедиться, что $P(x) \in RP_m^p$ для любого $x \in I_m^p$. Также легко показывается, что для любого $x \in RP_m^p$ имеем $P(x) = x$. Откуда следует, что $P: I_m^p \rightarrow RP_m^p$ является инъективным гомоморфизмом.

Поскольку P может быть сведено к возведению в степень, данное отображение сохраняет обратимость элемента. Обратимому элементу ставится в соответствие обратимый же, а необра-

тимому – необратимый. Это обуславливает интерес изучения $U(RP_m^p)$. Ввиду, как правило меньшей размерности RP_m^p, нежели I_m^p, его изучение может оказаться проще. Из результатов [1] следует

$$U(RP_m^p) \cong \prod_{i=1}^{g} Z_{p^i-1}, \tag{2}$$

однако сам изоморфизм пока, в общем случае, неизвестен, поскольку нет метода нахождения порождающих этих циклических групп.

Рассмотрим тривиальные случаи. При $g=1$ имеем кольцо RP_m^p, изоморфное (обычному) кольцу вычетов Z_p, строение которого хорошо известно. Если $g=m-1$, то RP_m^p совпадает со всем кольцом I_m^p.

Для простейшего нетривиального случая $g=2$ удалось получить следующие результаты.

Теорема 1. *Пусть $g=2$. θ_1, θ_2 – базис RP_m^p вида (1). Тогда таблица умножения базисных элементов имеет вид:*

$$\theta_1 * \theta_1 = -(a+1)\theta_1 - a\theta_2$$
$$\theta_1 * \theta_2 = \theta_2 * \theta_1 = a\theta_1 + a\theta_2,$$
$$\theta_2 * \theta_2 = a\theta_1 - (a+1)\theta_2,$$

где $a \in Z_p = \begin{cases} -\dfrac{m+1}{4}, \text{ если } m \equiv 3 (\mathrm{mod}\, 4) \\ \dfrac{m-1}{4}, \text{ если } m \equiv 1 (\mathrm{mod}\, 4) \end{cases}$.

Доказательство. Заметим, что $\theta_1 + \theta_2 = \sum_{i=1}^{m-1} \zeta^i = -1$. Также найдется $\psi \in MAut(I_m^p)$ такое, что $\psi(\theta_1) = \theta_2$ и $\psi(\theta_2) = \theta_1$.

Пусть $\theta_1 * \theta_2 = a\theta_1 + b\theta_2$. Однако $\theta_1 * \theta_2 = \theta_2 * \theta_1 = \psi(\theta_1 * \theta_2) = b\theta_1 + a\theta_2$. Откуда $b = a$ и, следовательно, $\theta_1 * \theta_2 = a\theta_1 + a\theta_2$.

В свою очередь $\theta_1 * \theta_1 + \theta_1 * \theta_2 = \theta_1(\theta_1 + \theta_2) = -\theta_1$. Откуда $\theta_1 * \theta_1 = -\theta_1 - \theta_1 * \theta_2 = -(a+1)\theta_1 - a\theta_2$.

В заключение имеем $\theta_2 * \theta_2 = \psi(\theta_1 * \theta_1) = -a\theta_1 - (a+1)\theta_2$.

Теперь найдем значение a, для чего определим сумму коэффициентов разложения $\theta_1 * \theta_1$ на базисные элементы, из предшествующих соображений равную $-(2a+1)$.

Поскольку $\theta_1 = \sum_{i=0}^{f-1} \zeta^{p^i}$, то

$$\theta_1 * \theta_1 = \sum_{i=0}^{f-1} \zeta^{p^i} \sum_{j=0}^{f-1} \zeta^{p^j} = \sum_{i=0}^{f-1} \sum_{j=0}^{f-1} \zeta^{p^i + p^j}.$$

Отметим, что каждое $\zeta^{p^i+p^j}$ либо входит в качестве одного из f слагаемых в θ_1 или θ_2 (см. формулу (1)), либо в случае $p^i + p^j \equiv 0 (\mathrm{mod}\, m)$ дает нам $1 = -(\theta_1 + \theta_2)$.

В первом случае имеем f^2 слагаемых вида $\zeta^{p^i+p^j}$, каждое из которых входит в разложение вида (1) для θ_1 либо θ_2. Поскольку θ_1 и θ_2 состоят каждое из f таких слагаемых, то искомая сумма есть $\frac{f^2}{f} = f$, откуда находим a.

Второй случай возможен лишь при условии разрешимости уравнения $p^x \equiv -1 (\mathrm{mod}\, m)$, что равносильно четности $\frac{m-1}{2}$ и соответственно условию $m \equiv 1 (\mathrm{mod}\ 4)$. Причем для заданного i су-

ществует единственное значение j, такое что $p^j + p^l \equiv 0(\mathrm{mod}\, m)$. Искомая сумма равна $-2f + \frac{f^2 - f}{f} = -f - 1$, откуда выражаем a. Теорема доказана.

Теорема 2. *Пусть* $g = 2$. *Тогда любой элемент* $x \in RP_m^p$ *представим в виде* $x = \alpha_1\theta_1 + \alpha_2\theta_2$, *где* $\alpha_1, \alpha_2 \in Z_p$.

$$x \notin U(RP_m^p) \Leftrightarrow \alpha_2 = c\alpha_1,$$

где $c \in Z_p$ *– один из корней уравнения*

$$\begin{cases} c + c^{-1} = \dfrac{2m-1}{m+1}, \text{ если } m \equiv 3(\mathrm{mod}\, 4), \\ c + c^{-1} = 2\dfrac{m-3}{m+1}, \text{ если } m \equiv 1(\mathrm{mod}\, 4), \end{cases}$$

обязанного в этом случае иметь два различных корня.

Доказательство.

Для $c \in Z_p$ справедливо $(\theta_1 + c\theta_2)(\theta_1 + c^{-1}\theta_2) = \theta_1\theta_1 + (c + c^{-1})\theta_1\theta_2 + \theta_2\theta_2 = 2a + 1 - (c + c^{-1})a$, где a – из теоремы 1.

Значит $\theta_1 + c\theta_2 \in U(RP_m^p)$ тогда, и только тогда, когда $2a + 1 - (c + c^{-1})a \neq 0$, что даст нам утверждение теоремы для элементов данного вида. Элементы вида $d\theta_1 + k\theta_2$, где $k \neq 0 \wedge d \neq 0$, можно свести к рассмотренному случаю домножением на d^{-1}, что никак не влияет на обратимость.

Обратимость остальных ненулевых элементов RP_m^p легко получить из теоремы 1. Из (2) следует наличие RP_m^p ровно $2p - 1$ необратимых элемента, откуда получаем необходимость существования корней у уравнения $2a + 1 - (c + c^{-1})a = 0$. Теорема доказана.

Таким образом, довольно подробно исследован случай, когда размерность $g = 2$. В настоящее время исследуются случаи большего значения g. Однако в силу того, что будут возникать уравнения более высоких степеней весьма проблематично найти такие же подробные описания колец RP_m^p для больших значений размерности g.

Теперь рассмотрим в качестве иллюстрации подкольца элементов устойчивых к *p-автоморфизмам* кольца вычетов 13-кругового поля по модулю $p = 41$. Заметим, что $41 \equiv 2(\mathrm{mod}13)$, а 2 – есть первообразный корень по модулю 13. Соответственно $g = 1$ даст нам $RP_{13}^{41} \cong Z_{41}$ и $PAut(I_{13}^{41}) = MAut(I_{13}^{41})$.

Перейдем к подгруппе $\langle \varphi_{41^2} \rangle = \langle \varphi_4 \rangle \subset PAut(I_m^p)$. Имеем $|\varphi_4 : PAut(I_m^p)| = 2$, а, значит, соответствующие подкольцо $R(\langle \varphi_4 \rangle)$ по сложению будет линейным пространством размерности 2 над Z_{41}. Его базисными элементами являются $\theta_1 = \zeta_{13}^4 + \zeta_{13}^3 + \zeta_{13}^{12} + \zeta_{13}^9 + \zeta_{13}^{10} + \zeta_{13}$ и $\theta_2 = \zeta_{13}^2 + \zeta_{13}^8 + \zeta_{13}^6 + \zeta_{13}^{11} + \zeta_{13}^5 + \zeta_{13}^7$.

Единственным подкольцом размерности 3, которое можно получить при помощи приведенных выше методов, будет $R(\langle \varphi_8 \rangle) = \langle x \in I_{13}^{41} \mid x^8 = x \rangle$. Его базисными элементами вида (1) будут $\theta_1 = \zeta_{13}^8 + \zeta_{13}^{12} + \zeta_{13}^5 + \zeta_{13}$, $\theta_2 = \zeta_{13}^2 + \zeta_{13}^3 + \zeta_{13}^{11} + \zeta_{13}^{10}$ и $\theta_3 = \zeta_{13}^4 + \zeta_{13}^6 + \zeta_{13}^9 + \zeta_{13}^7$. Попарно их перемножая, построим таблицу умножения:

$$\theta_1 * \theta_1 = -4\theta_1 - 3\theta_2 - 2\theta_3,$$
$$\theta_1 * \theta_2 = \theta_1 + 2\theta_2 + \theta_3,$$
$$\theta_1 * \theta_3 = 2\theta_1 + \theta_2 + \theta_3,$$
$$\theta_2 * \theta_2 = -2\theta_1 - 4\theta_2 - 3\theta_3,$$
$$\theta_2 * \theta_3 = \theta_1 + \theta_2 + 2\theta_3,$$

$$\theta_3 * \theta_3 = -3\theta_1 - 2\theta_2 - 4\theta_3,$$

откуда видно наличие автоморфизмов подкольца $\psi_1 : \theta_1 \to \theta_2 \to \theta_3 \to \theta_1$ и $\psi_2 : \theta_1 \to \theta_3 \to \theta_2 \to \theta_1$.

Нерассмотренными остались еще два собственных подкольца $R(\langle\varphi_{41^4}\rangle) = R(\langle\varphi_3\rangle)$ и $R(\langle\varphi_{41^6}\rangle) = R(\langle\varphi_{12}\rangle)$ размерностей 4 и 6 соответственно. Найденные подкольца образуют следующую структуру вложенности:

$$RP_{13}^{41} \subset R(\langle\varphi_4\rangle) \subset R(\langle\varphi_3\rangle) \subset I_{13}^{41},$$
$$RP_{13}^{41} \subset R(\langle\varphi_4\rangle) \subset R(\langle\varphi_{12}\rangle) \subset I_{13}^{41},$$
$$RP_{13}^{41} \subset R(\langle\varphi_8\rangle) \subset R(\langle\varphi_{12}\rangle) \subset I_{13}^{41},$$

что находится в полном соответствии с вложенностью соответствующих подгрупп $PAut(I_{13}^{41})$.

Литература

1. Алеев, Р.Ж. Центральные единицы целочисленных групповых колец конечных групп: дис. ... д-ра физ.-мат. наук / Р.Ж. Алеев. – Челябинск, 2002. – 354 с.

2. Шпонько, А.В. Порядки элемента в группах вычетов колец целых абелевых полей / А.В. Шпонько // Проблемы теоретической и прикладной математики: труды 40-й Всероссийской молодежной конференции. – Екатеринбург, 2009. – С. 72–75.

3. Шпонько, А.В. Подкольца колец вычетов целых круговых полей / А.В. Шпонько // Проблемы теоретической и прикладной математики: труды 42-й Всероссийской молодежной конференции. – Екатеринбург, 2011. – С. 256.

Поступила в редакцию 13 июля 2011 г.

AUTOMORPHISMS OF RESIDUE RINGS OF INTEGER RINGS OF CIRCULAR FIELDS

A.V. Shponko[1]

The authors research the structure of residue rings of integer rings of circular fields by analyzing their ring automorphisms. The connections between a special subgroup of the automorphism group and the system of the inserted subrings of the residue rings are found. Among the occurring subrings the authors found a very prospective one for further research as well as a multitude of its noninvertible elements for some nontrivial cases.

Keywords: Abelian fields, circular fields, integer rings, residue rings, subrings, automorphisms.

References

1. Aleev R.Zh. *Central'nye edinicy celochislennykh gruppovykh kolec konechnykh grupp: dis. d-ra. fiz.-mat. nauk* (The central units of integral group rings of finite groups: Thesis of Doctor of Physical and Mathematical Sciences). Cheljabinsk, 2002. 354 p.

2. Shponko A.V. Porjadki ehlementa v gruppakh vychetov kolec celykh abelevykh polejj (The orders of elements in groups of residue rings of Abelian fields). *Problemy teoreticheskojj i prikladnojj matematiki: Trudy 40-jj Vserossijjskojj molodezhnojj konferencii* (Proc. of the 40th All-Russian Youth Conference "Problems of Theoretical and Applied Mathematics"). Ekaterinburg, 2009. pp. 72–75. (in Russ.).

3. Shponko A.V. Podkol'ca kolec vychetov celykh krugovykh polejj (Subring of residue rings of integers of cyclotomic fields) // *Problemy teoreticheskojj i prikladnojj matematiki: Trudy 42-jj Vserossijjskojj molodezhnojj konferencii* (Proc. of the 42th All-Russian Youth Conference "Problems of Theoretical and Applied Mathematics"). Ekaterinburg, 2011. p. 256. (in Russ.).

[1] Shponko Andrey Victorovich is Post-graduate Student, Algebra Department, South Ural State University
E-mail: ashponko@gmail.com