ПОДКОЛЬЦА КОЛЕЦ ВЫЧЕТОВ КРУГОВЫХ ПОЛЕЙ

А.В. Шпонько

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. 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 $I\big(Q(\zeta_m)\big) = \mathbb{Z}[\zeta_m]$. В частности, при $m = 4$ имеем кольцо гауссовых целых.

В [1] была 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. Поэтому нами изучается $I_m^p = I(Q(\zeta_m)) \Big/ pI(Q(\zeta_m))$ – кольцо вычетов по модулю p кольца целых кругового поля. В дальнейшем значения p и m полагаются простыми и различными.

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 $\varphi(\zeta)$.

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 $MAut(I_m^p)$.

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

$$\mathrm{R(A)} = \left\langle \mathrm{x} \in I_m^p \middle| \forall \sigma \epsilon \mathrm{A} \; \sigma(\mathrm{x}) = \mathrm{x} \right\rangle$$

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 соответ-

ствует структуре вложенности подгрупп $PAut(I_m^p)$ (можно говорить об аналоге соответсвия Галуа).

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

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

что доказывается идентично аналогичному свойству полей характеристики p. Отсюда следует

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

что означает попарное равенстов кооэфициентов 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

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

Его базис образован элементами

$$\theta_i = \sum_{j \epsilon P_i} \zeta^j, \qquad (1)$$

где $i \in \{1, .., g\}$, а P_i – смежные классы Z_m^* 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 $\left|PAut(I_m^p)\right|$. Очевидно $f = |\langle p \rangle|$ в Z_m^*. Отсюда видно, что для произвольного $a \in I_m^p$ справедливо $a^{p^f} = a$. Рассмотрим функцию

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

ставящую в соответствию элементу из I_m^p произведение всех его образов относительно автоморфизмов. Легко убедиться, что $\mathrm{P}(x) \in RP_m^p$ 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 $\mathrm{P}: I_m^p \rightarrow RP_m^p$ 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 необратимому – необратимый. Это обуславливает интерес изучения $U(RP_m^p)$. Ввиду, как правило, меньшей раз-

мерности RP_m^p, нежели I_m^p, его изучение может оказаться проще. Из результатов [1] следует:

$$U(RP_m^p) \cong \prod_{i=1}^{g} \mathrm{Z}_{p^f-1}, \quad (2)$$

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

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

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

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

Сопоставляя эту формулу с ранее доказанным, находим точное значение a. Оно зависите от разрешимости уравнения $p^x \equiv -1(mod\ m)$. Объем публикации не позволяет привести более подробные выкладки по этому вопросу. 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*

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

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 $\theta_1 + c\theta_2 \in U\left(RP_m^p\right)$ тогда, и только тогда, когда $2a + 1 - (c + c^{-1})a \neq 0$. Что дает нам утверждение теоремы для элементов данного вида. Элементы вида $d\theta_1 + k\theta_2$, где $\mathrm{k} \neq 0 \wedge d \neq 0$, 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.

Библиографический список

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. – 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. – 2011. – С. 256.