УДК 512.552+519.713

©2011. **В. В. Скобелев**

СВОЙСТВА ДЕЛИТЕЛЕЙ НУЛЯ В АССОЦИАТИВНЫХ КОЛЬЦАХ

Систематически исследованы множества левых и правых делителей нуля в ассоциативных некоммутативных кольцах. Выделены два семейства множеств, определяемых, соответственно, левыми и правыми делителями нуля. Показано, что эти семейства множеств определяют два семейства, соответственно, правых и левых идеалов. Исследованы свойства этих семейств односторонних идеалов. Показано, что выделенные семейства множеств (а, следовательно, определяемые ими семейства односторонних идеалов) применимы для анализа структуры множества решений уравнений с параметрами, имеющими вид «произведение равно нулю», над ассоциативным некоммутативным кольцом.

Ключевые слова: *ассоциативные некоммутативные кольца, левые и правые делители нуля, односторонние идеалы*

1. Введение. В настоящее время наблюдается устойчивая тенденция использования вычислений в кольцах вычетов в процессе решения задач преобразования информации, в частности, криптографии (см., напр., [1-3]). Эта тенденция стимулировала, с одной стороны, исследование автоматно-алгебраических моделей над конечными кольцами, а, с другой стороны, исследование теоретико-множественных и алгебраических свойств структуры колец с целью разработки математического аппарата, применимого для систематического анализа соответствующих автоматно-алгебраических моделей.

Исследование линейных и некоторых классов нелинейных автоматов над конечными ассоциативно-коммутативными кольцами с единицей [4, 5] показало, что при их использовании в качестве математических моделей дискретных преобразователей информации актуальным становится анализ сложности решения задач идентификации (параметрической и начального состояния), а также структуры множеств неподвижных точек автоматных отображений. Указанный анализ автоматически сводится к анализу сложности решения систем уравнений (как правило, нелинейных) с параметрами над соответствующим кольцом.

Известно, что поиск решения уравнения 2-й степени со многими переменными над полем $GF(2^k)$ является NP-полной проблемой. Ситуация еще более усложняется при решении уравнений с параметрами над кольцами с делителями нуля. Поэтому актуальной становится задача систематического исследования свойств делителей нуля в ассоциативных кольцах.

Целью настоящей работы и является систематическое исследование свойств делителей нуля в ассоциативных не обязательно коммутативных кольцах с целью разработки математического аппарата, применимого при решении уравнений с параметрами, имеющих вид «произведение равно нулю».

Все не определяемые в работе алгебраические понятия – такие же, как и в [6].

2. Основные понятия. Всюду под кольцом $\mathcal{K} = (K, +, \cdot)$ ($|K| \geq 2$) понимается ассоциативное не обязательно коммутативное кольцо.

Известно, что $K = K^{inv} \cup K^{non-inv}$, где K^{inv} и $K^{non-inv}$ – множество, соответственно, обратимых и необратимых элементов кольца $\mathcal{K}$. Множество K^{inv} определяется следующим образом: $K^{inv} = \emptyset$, если $\mathcal{K}$ – кольцо без единицы, и $K^{inv} = \{x \in K | (\exists x^{-1} \in K)(xx^{-1} = x^{-1}x = 1)\}$, если $\mathcal{K}$ – кольцо с единицей. Отметим, что если $\mathcal{K}$ – кольцо с единицей и $u \in K^{non-inv}$, то $u^l \neq 1$ для всех $l \in \mathbb{N}$.

Замечание 1. В некоммутативном кольце $\mathcal{K}$ с единицей определяются множество $K^{l-inv} = \{x \in K | (\exists a \in K)(ax = 1)\}$ обратимых слева элементов, а также множество $K^{r-inv} = \{x \in K | (\exists b \in K)(xb = 1)\}$ обратимых справа элементов. Ясно, что $K^{l-inv} \supseteq K^{inv}$ и $K^{r-inv} \supseteq K^{inv}$, причем не исключается, что одно или оба из этих включений могут быть строгими.

Таким образом, $K^{non-inv} = K \backslash K^{inv}$. Отметим, что $K^{non-inv} \neq \emptyset$ для любого кольца, так как $0 \in K^{non-inv}$.

В свою очередь, известно, что $K^{non-inv} = K^{ld} \cup K^{rd} \cup K^{non-d} \cup \{0\}$, где K^{ld} (соответственно, K^{rd}) есть множество левых (соответственно, правых) делителей нуля, а $K^{non-d} = K \backslash (K^{ld} \cup K^{rd} \cup \{0\})$.

Замечание 2. Если $ab = 0$ ($a, b \in K^{non-inv} \backslash \{0\}$), то элемент a называется левым делителем нуля, а элемент b – правым делителем нуля. В коммутативном кольце $K^{ld} = K^{rd} = K^d$, а элементы множества K^d называются делителями нуля.

Нетрудно убедиться в том, что для множеств K^{ld} и K^{rd} истинны следующие утверждения.

Утверждение 1. *$K^{ld} \neq \emptyset$ тогда и только тогда, когда $K^{rd} \neq \emptyset$.*

Утверждение 2. *Если $x \in K^{ld}$, то $-x \in K^{ld}$, а если $y \in K^{rd}$, то $-y \in K^{rd}$.*

Утверждение 3. *Если $x \neq 0$, то $x \in K^{ld} \cap K^{rd}$ тогда и только тогда, когда существуют такие элементы $a \in K^{ld}$ и $b \in K^{rd}$, что $ax = 0$ и $xb = 0$.*

Утверждение 4. *Для любого элемента $x \in K^{ld}$*

$$ax \in \begin{cases} K^{ld}, & \text{если } a \in K^{inv} \cup K^{non-d} \\ K^{ld} \cup \{0\}, & \text{иначе,} \end{cases}$$

а для любого элемента $y \in K^{rd}$

$$ya \in \begin{cases} K^{rd}, & \text{если } a \in K^{inv} \cup K^{non-d} \\ K^{rd} \cup \{0\}, & \text{иначе.} \end{cases}$$

Из утверждения 4 вытекает, что истинны следующие три следствия.

Следствие 1. *Если $x \in K^{ld} \backslash K^{rd}$ (соответственно, $y \in K^{rd} \backslash K^{ld}$), то $ax \in K^{ld}$ (соответственно, $yb \in K^{rd}$) для любого элемента $a \neq 0$ (соответственно, для любого элемента $b \neq 0$).*

Следствие 2. *$yx \in K^{ld} \cap K^{rd} \cup \{0\}$ для любых $x \in K^{ld}$ и $y \in K^{rd}$.*

Следствие 3. *Если* $K^{ld} \neq \emptyset$ *(или, что то же самое,* $K^{rd} \neq \emptyset$*), то равенство* $K^{ld} \cap K^{rd} = \emptyset$ *истинно тогда и только тогда, когда* $(K^{ld}, \cdot)$ *и* $(K^{rd}, \cdot)$ *– подполугруппы полугруппы* $(K, \cdot)$*.*

Утверждение 5. *Для любого подкольца* $\mathcal{U} = (U, +\cdot)$ *кольца* $\mathcal{K} = (K, +, \cdot)$ *истинны равенства* $K^{ld} \cap U = U^{ld}$ *и* $K^{rd} \cap U = U^{rd}$ *(и, следовательно, если* $\mathcal{U}$ *– коммутативное подкольцо кольца* $\mathcal{K}$*, то* $K^{ld} \cap U = K^{rd} \cap U = U^{d}$*).*

Центром кольца $\mathcal{K}$ называется множество K_{zntr} всех таких элементов $a \in K$, что $ax = xa$ для всех $x \in K$. Для любого кольца $\mathcal{K}$ центр K_{zntr} – непустое множество (так как $0 \in K_{zntr}$), а $\mathcal{K}_{zntr} = (K_{zntr}, +, \cdot)$ – максимальное коммутативное подкольцо кольца $\mathcal{K}$.

Нетрудно убедиться в том, что истинны следующие утверждения, характеризующие множества K^{ld} и K^{rd} в терминах центра кольца.

Утверждение 6. *Истинно равенство* $K^{ld} \cap K_{zntr} = K^{rd} \cap K_{zntr}$*.*

Утверждение 7. $K^{ld} \subseteq K_{zntr}$ *тогда и только тогда, когда* $K^{rd} \subseteq K_{zntr}$*.*

Утверждение 8. *Если* $K^{ld} \subseteq K_{zntr}$ *(или, что то же самое,* $K^{rd} \subseteq K_{zntr}$*), то* $K^{ld} = K^{rd}$*.*

Нетрудно убедиться в том, что истинны следующие утверждения, характеризующие множества левых и правых делителей нуля в терминах гомоморфизмов колец.

Утверждение 9. *Если* φ *– гомоморфизм кольца* $\mathcal{K}_1 = (K_1, +_1, \cdot_1)$ *в кольцо* $\mathcal{K}_2 = (K_2, +_2, \cdot_2)$*, то* $\varphi(K_1^{ld}) \subseteq K_2^{ld} \cup \{0\}$ *и* $\varphi(K_1^{rd}) \subseteq K_2^{rd} \cup \{0\}$ *(в частности,* $\varphi(K^{ld}) \subseteq K^{ld} \cup \{0\}$ *и* $\varphi(K^{rd}) \subseteq K^{rd} \cup \{0\}$ *для любого эндоморфизма* φ *кольца* $\mathcal{K}$*).*

Утверждение 10. *Если* φ *– изоморфизм кольца* $\mathcal{K}_1 = (K_1, +_1, \cdot_1)$ *в кольцо* $\mathcal{K}_2 = (K_2, +_2, \cdot_2)$*, то* $\varphi(K_1^{ld}) \subseteq K_2^{ld}$ *и* $\varphi(K_1^{rd}) \subseteq K_2^{rd}$ *(в частности,* $\varphi(K^{ld}) \subseteq K^{ld}$ *и* $\varphi(K^{rd}) \subseteq K^{rd}$ *для любого изоморфизма* φ *кольца* $\mathcal{K}$ *в себя).*

Утверждение 11. *Если* φ *– автоморфизм кольца* $\mathcal{K}$*, то истинны равенства* $\varphi(K^{ld}) = K^{ld}$ *и* $\varphi(K^{rd}) = K^{rd}$*.*

Говорят, что в полугруппе $(G, \cdot)$ выполняется закон сокращения, если истинно следующее утверждение

$$(\forall a, b, c \in G)((ac = bc \Rightarrow a = b)\&(ca = cb \Rightarrow a = b)). \tag{1}$$

Известно, что полугруппа $(K^{inv} \cup K^{non-d}, \cdot)$ является максимальной подполугруппой полугруппы $(K, \cdot)$, удовлетворяющей закону сокращения (отсюда, в частности, вытекает, что для коммутативного кольца $\mathcal{K}$ существует расширение $\widetilde{\mathcal{K}}$, в котором каждый элемент множества K^{non-d} обратим). Таким образом, подмножество $K^{ld} \cup K^{rd} \subset K$ полностью характеризует все свойства, связанные с нарушением закона сокращения в кольце $\mathcal{K}$ (и во всех его расширениях).

Замечание 3. Формула (1) определяет двусторонний закон сокращения. В некоммутативном кольце $\mathcal{K}$ с единицей могут существовать такие обратимые слева элементы a, что $ax = ay \Rightarrow x = y$, но $xa = ya \not\Rightarrow x = y$, а также такие обратимые справа элементы b, что $xb = yb \Rightarrow x = y$, но $bx = by \not\Rightarrow x = y$. Таким образом, подмножество $K^{ld} \cup K^{rd} \subset K$ полностью характеризует все свойства, связанные с нарушением именно двустороннего закона сокращения в кольце $\mathcal{K}$.

Всюду в дальнейшем считаем, что $K^{ld} \neq \emptyset$ (и, следовательно, $K^{rd} \neq \emptyset$).

Множества K^{ld} и K^{rd} однозначно определяют в кольце $\mathcal{K}$ системы непустых множеств

$$A_x^r = \{u \in K^{rd} | xu = 0\} \ (x \in K^{ld}) \tag{2}$$

и

$$A_y^l = \{v \in K^{ld} | vy = 0\} \ (y \in K^{rd}). \tag{3}$$

Из (2) и (3) непосредственно вытекает, что истинно следующее утверждение:

$$(\forall a, b \in K^{non-inv} \backslash \{0\})((ab = 0) \Leftrightarrow (a \in A_b^l) \& (b \in A_a^r)).$$

Отметим, что если $\mathcal{K}$ – коммутативное кольцо, то $A_x^r = A_x^l = A_x$ $(x \in K^d)$.

Семейства множеств (2) и (3) играют важную роль для решения уравнений вида «произведение равно нулю» над кольцом $\mathcal{K}$. Проиллюстрируем это обстоятельство следующим примером.

Пример 1. 1. Для любых $n \in \mathbb{N}$ и $a_1, \ldots, a_n \in K^{non-inv} \backslash \{0\}$ решение системы уравнений $a_i x = 0$ $(i = 1, \ldots, n)$ имеет вид $x \in \{0\} \cup \bigcap\limits_{i=1}^{n} A_{a_i}^r$, а решение системы уравнений $x a_i = 0$ $(i = 1, \ldots, n)$ имеет вид $x \in \{0\} \cup \bigcap\limits_{i=1}^{n} A_{a_i}^l$.

2. Для любых $a \in K^{non-inv} \backslash \{0\}$ и $n \in \mathbb{N}$ решение уравнения $ax^n = 0$ имеет вид $x \in \{0\} \cup \{y \in K^{non-inv} | y^n \in A_a^r\}$, а решение уравнения $x^n a = 0$ имеет вид $x \in \{0\} \cup \{y \in K^{non-inv} | y^n \in A_a^l\}$.

3. Для любого $a \in K$ решение уравнения $x^2 + ax = 0$ имеет вид

$$x \in \{0, -a\} \cup \{b \in K^{non-inv} | (b + a \in K^{non-inv}) \& (b \in (A_b^l - a) \cap A_{b+a}^r)\},$$

а решение уравнения $x^2 + xa = 0$ имеет вид

$$x \in \{0, -a\} \cup \{b \in K^{non-inv} | (b + a \in K^{non-inv}) \& (b \in (A_b^r - a) \cap A_{b+a}^l)\}.$$

4. Решение уравнения $f_1(x) f_2(y) = 0$ имеет вид

$$(x, y) \in \{(a, b) \in K^2 | (f_1(a) = 0) \vee (f_2(b) = 0)\} \cup$$

$$\cup \{(a, b) \in K^2 | (f_1(a) \neq 0) \& (f_2(b) \neq 0) \& (f_1(a) \in A_{f_2(b)}^l) \& (f_2(b) \in A_{f_1(a)}^r)\}.$$

Рассмотренный пример показывает, что исследование теоретико-множественных и алгебраических свойств семейств множеств (2) и (3) имеет важное значение для анализа структуры множества решений уравнений с параметрами, имеющими вид «произведение равно нулю», над кольцом $\mathcal{K}$.

3. Свойства семейств множеств A_x^r $(x \in K^{ld})$ и A_y^l $(y \in K^{rd})$. Так как $\bigcup\limits_{x \in K^{ld}} A_x^r = K^{rd}$ и $\bigcup\limits_{y \in K^{rd}} A_y^l = K^{ld}$, то семейство множеств A_x^r $(x \in K^{ld})$ (соответственно, семейство множеств A_y^l $(y \in K^{rd})$) представляет собой покрытие множества K^{rd}

(соответственно, множества K^{ld}) непустыми подмножествами. Соотношение между этими покрытиями устанавливает следующее утверждение.

Предложение 1. Для любого кольца $\mathcal{K}$ истинны формулы

$$x \in \bigcap_{u \in A_x^r} A_u^l \ (x \in K^{ld}), \tag{4}$$

$$y \in \bigcap_{v \in A_y^l} A_v^r \ (y \in K^{rd}). \tag{5}$$

Доказательство. Из (2) вытекает, что истинна формула

$$(\forall x \in K^{ld})(\forall u \in A_x^r)(x \in A_u^l),$$

откуда следует, что истинна формула (4).

Аналогичным образом, из (3) вытекает, что истинна формула

$$(\forall y \in K^{rd})(\forall v \in A_y^l)(y \in A_v^r),$$

откуда следует, что истинна формула (5). □

Назовем множество $I_x^r = A_x^r \cup \{0\}$ $(x \in K^{ld})$ правым аннулятором элемента x, а множество $I_y^l = A_y^l \cup \{0\}$ $(y \in K^{rd})$ – левым аннулятором элемента y.

Отметим, что если $\mathcal{K}$ – коммутативное кольцо, то $I_x^r = I_x^l = I_x$ $(x \in K^d)$, а множество I_x $(x \in K^d)$ представляет собой аннулятор элемента x.

Предложение 2. Для любого кольца $\mathcal{K}$ каждое множество I_x^r $(x \in K^{ld})$ является правым идеалом, а каждое множество I_y^l $(y \in K^{rd})$ – левым идеалом.

Доказательство. Для любого $x \in K^{ld}$ и для любых $a, b \in I_x^r$

$$x(a \pm b) = xa \pm xb = 0 \pm 0 = 0,$$

откуда вытекает, что $a \pm b \in I_x^r$. Следовательно, $(I_x^r, +)$ $(x \in K^{ld})$ – подгруппа аддитивной группы кольца $\mathcal{K}$.

Аналогичным образом, для любого $y \in K^{rd}$ и для любых $a, b \in I_y^l$

$$(a \pm b)y = ay \pm by = 0 \pm 0 = 0,$$

откуда вытекает, что $a \pm b \in I_y^l$. Следовательно, $(I_y^l, +)$ $(y \in K^{rd})$ – подгруппа аддитивной группы кольца $\mathcal{K}$.

Для любого $x \in K^{ld}$ и для любых $a \in I_x^r$ и $b \in K$

$$x(ab) = (xa)b = 0b = 0,$$

откуда вытекает, что $ab \in I_x^r$ для любых $a \in I_x^r$ и $b \in K$. Следовательно, каждое множество I_x^r $(x \in K^{ld})$ является правым идеалом кольца $\mathcal{K}$.

Аналогичным образом, для любого $y \in K^{rd}$ и для любых $a \in I_y^l$ и $b \in K$

$$(ba)y = b(ay) = b0 = 0,$$

откуда вытекает, что $ba \in I_y^l$ для любых $a \in I_y^l$ и $b \in K$. Следовательно, каждое множество I_y^l $(y \in K^{rd})$ является левым идеалом кольца $\mathcal{K}$. □

Таким образом, в каждом кольце $\mathcal{K}$ семейство множеств A_x^r $(x \in K^{ld})$ определяет семейство правых идеалов I_x^r $(x \in K^{ld})$, а семейство множеств A_y^l $(y \in K^{rd})$ – семейство левых идеалов I_y^l $(y \in K^{rd})$. Охарактеризуем эти семейства идеалов.

Предложение 3. В каждом кольце $\mathcal{K}$ истинны равенства

$$I_{-x}^r = I_x^r \quad (x \in K^{ld}), \tag{6}$$

$$I_{-y}^l = I_y^l \quad (y \in K^{rd}). \tag{7}$$

Доказательство. Зафиксируем элемент $x \in K^{ld}$. Из утверждения 2 вытекает, что $-x \in K^{ld}$.

Пусть $a \in I_x^r$. Тогда $xa = 0$. Следовательно, $(-x)a = -xa = -0 = 0$, т.е. $a \in I_{-x}^r$. Итак, показано, что $I_x^r \subseteq I_{-x}^r$.

Пусть $a \in I_{-x}^r$. Тогда $(-x)a = 0$. Следовательно, $xa = -(-x)a = -0 = 0$, т.е. $a \in I_x^r$. Итак, показано, что $I_{-x}^r \subseteq I_x^r$.

Из включений $I_x^r \subseteq I_{-x}^r$ и $I_{-x}^r \subseteq I_x^r$ вытекает равенство (6).

Равенство (7) доказывается аналогично. □

Предложение 4. В каждом кольце $\mathcal{K}$ истинны включения

$$I_u^l \cap I_v^l \subseteq I_{u+v}^l \quad (u, v, u+v \in K^{rd}), \tag{8}$$

$$I_u^l \cap I_v^l \subseteq I_{u-v}^l \quad (u, v, u-v \in K^{rd}), \tag{9}$$

$$I_u^r \cap I_v^r \subseteq I_{u+v}^r \quad (u, v, u+v \in K^{ld}), \tag{10}$$

$$I_u^r \cap I_v^r \subseteq I_{u-v}^r \quad (u, v, u-v \in K^{ld}). \tag{11}$$

Доказательство. Зафиксируем элементы $u, v \in K^{rd}$. Пусть $a \in I_u^l \cap I_v^l$. Тогда $au = 0$ и $av = 0$. Следовательно,

$$a(u \pm v) = au \pm av = 0 \pm 0 = 0.$$

Отсюда вытекает, что если $u + v \in K^{rd}$, то $a \in I_{u+v}^l$, т.е. истинно включение (8), а если $u - v \in K^{rd}$, то $a \in I_{u-v}^l$, т.е. истинно включение (9).

Включения (10) и (11) доказываются аналогичным образом. □

Произведением подмножеств X $(X \subseteq K)$ и Y $(Y \subseteq K)$ назовем множество XY, состоящее из всех таких конечных сумм $\sum\limits_{i=1}^{n} x_i y_i$ $(n \in \mathbb{N})$, что $x_i \in X$ и $y_i \in Y$ для всех $i = 1, \ldots, n$.

Предложение 5. В каждом кольце $\mathcal{K}$ для любых элементов $x \in K^{ld}$ и $y \in K^{rd}$ множество $I_y^l I_x^r$ является двусторонним идеалом.

Доказательство. Так как $(I_x^r, +)$ $(x \in K^{ld})$ и $(I_y^l, +)$ $(y \in K^{rd})$ – подгруппы аддитивной группы кольца $\mathcal{K}$, то $(I_y^l I_x^r, +)$ также является подгруппой аддитивной группы кольца $\mathcal{K}$.

Пусть $u \in I_y^l I_x^r$. Тогда существует такое $n \in \mathbb{N}$, что $u = \sum\limits_{i=1}^{n} v_i w_i$, где $v_i \in I_y^l$ и $w_i \in I_x^r$ для всех $i = 1, \ldots, n$.

Так как множество I_y^l – левый идеал и $v_i \in I_y^l$ $(i = 1, \ldots, n)$, то $av_i = \alpha_i \in I_y^l$ $(i = 1, \ldots, n)$ для любого элемента $a \in K$. Следовательно,

$$au = a\sum_{i=1}^{n} v_i w_i = \sum_{i=1}^{n} (av_i) w_i = \sum_{i=1}^{n} \alpha_i w_i \in I_y^l I_x^r$$

для любого элемента $a \in K$, т.е. множество $I_y^l I_x^r$ – левый идеал.

Аналогичным образом доказывается, что множество $I_y^l I_x^r$ – правый идеал.

Так как множество $I_y^l I_x^r$ является как левым, так и правым идеалом, то оно является двусторонним идеалом кольца $\mathcal{K}$. □

Элементы семейства I_y^l $(y \in K^{rd})$, а так же семейства I_x^r $(x \in K^{ld})$ могут не быть попарно различными, соответственно, левыми или правыми идеалами кольца $\mathcal{K}$. Проиллюстрируем это обстоятельство следующим примером.

Пример 2. Для кольца вычетов $\mathcal{Z}_{p^k} = (\mathbb{Z}_{p^k}, \oplus, \circ)$ (p – простое число, а $k \in \mathbb{N}$), которое, как известно, является коммутативным, множество $\mathbb{Z}_{p^k}^{inv}$ состоит из всех чисел $a \in \mathbb{Z}_{p^k} \backslash \{0\}$, взаимно-простых с числом p, а

$$\mathbb{Z}_{p^k}^{d} = \mathbb{Z}_{p^k} \backslash (\mathbb{Z}_{p^k}^{inv} \cup \{0\}) = \{ap^i | a \in \mathbb{Z}_{p^k}^{inv};\ \ i = 1, \ldots, k-1\}.$$

Множества A_{ap^i} $(a \in \mathbb{Z}_{p^k}^{inv};\ \ i = 1, \ldots, k-1)$ имеют вид

$$A_{ap^i} = \{bp^j | b \in \mathbb{Z}_{p^k}^{inv};\ \ j = k-i, \ldots, k-1\}, \tag{12}$$

а идеалы $I_{ap^i} = A_{ap^i} \cup \{0\}$ $(a \in \mathbb{Z}_{p^k}^{inv};\ \ i = 1, \ldots, k-1)$ определяют все собственные идеалы кольца $\mathcal{Z}_{p^k}$.

Из (12) вытекает, что $A_{a_1 p^i} = A_{a_2 p^i}$ $(i = 1, \ldots, k-1)$ для любых $a_1, a_2 \in \mathbb{Z}_{p^k}^{inv}$ и, следовательно, $I_{a_1 p^i} = I_{a_2 p^i}$ $(i = 1, \ldots, k-1)$ для любых $a_1, a_2 \in \mathbb{Z}_{p^k}^{inv}$.

Определив на множестве K^{ld} отношение эквивалентности $\sim_l$ формулой

$$x_1 \sim_l x_2 \Leftrightarrow A_{x_1}^r = A_{x_2}^r \ \ (x_1, x_2 \in K^{ld}),$$

и выбрав по одному представителю a из каждого класса фактор-множества $K^{ld}/\sim_l$, получим все попарно-различные правые идеалы I_a^r, принадлежащие семейству правых идеалов I_x^r $(x \in K^{ld})$. Аналогичным образом, определив на множестве K^{rd} отношение эквивалентности $\sim_r$ формулой

$$y_1 \sim_r y_2 \Leftrightarrow A_{y_1}^l = A_{y_2}^l \ \ (y_1, y_2 \in K^{rd}).$$

и выбрав по одному представителю b из каждого класса фактор-множества $K^{rd}/\sim_r$, получим все попарно-различные левые идеалы I_b^l, принадлежащие семейству левых идеалов I_y^l $(y \in K^{rd})$.

Известно,что в любом кольце $\mathcal{K}$ для любого элемента $u \in K\backslash\{0\}$ последовательность элементов

$$u, u^2, \ldots, u^n, \ldots$$

удовлетворяет в точности одному из следующих трех условий:

Условие 1. Все элементы u^n $(n \in \mathbb{N})$ попарно различны (что возможно только в бесконечном кольце $\mathcal{K}$).

Условие 2. Существует такое натуральное число $n_u \geq 2$, что $u, \ldots, u^{n_u-1}$ – попарно различные элементы множества $K\backslash\{0\}$ и $u^{n_u} = 0$ (т.е. u – нильпотентный элемент).

Условие 3. Существует такое натуральное число $l_u \geq 2$, что $u, \ldots, u^{l_u-1}$ – попарно различные элементы множества $K\backslash\{0\}$ и $u^{l_u} = u^i$ для некоторого числа $i \in \mathbb{N}_{l_u-1}$.

Теорема 1. *В каждом кольце $\mathcal{K}$ для любого элемента $u \in K^{ld} \cup K^{rd}$, если $u, u^2, \ldots, u^k$ $(k \geq 2)$ – попарно различные элементы множества $K\backslash\{0\}$, то истинны включения*

$$I_u^r \subseteq I_{u^2}^r \subseteq \cdots \subseteq I_{u^k}^r \ (u \in K^{ld}), \tag{13}$$

$$I_u^l \subseteq I_{u^2}^l \subseteq \cdots \subseteq I_{u^k}^l \ (u \in K^{rd}). \tag{14}$$

Доказательство. Предположим, что $u \in K^{ld}$ и $u, u^2, \ldots, u^k$ $(k \geq 2)$ – попарно различные элементы множества $K\backslash\{0\}$.

Пусть $a \in I_{u^i}^r$ для некоторого $i \in \{1, \ldots, k-1\}$. Тогда $u^i a = 0$. Следовательно, $u^{i+1}a = u(u^i a) = u0 = 0$, т.е. $a \in I_{u^{i+1}}^r$.

Итак, показано, что $I_{u^i}^r \subseteq I_{u^{i+1}}^r$ для всех $i = 1, \ldots, k-1$. Отсюда вытекает, что включения (13) истинны.

Включения (14) доказываются аналогичным образом. □

Для элементов множества $K^{ld} \cup K^{rd}$ ситуацию, определяемую условием 3, характеризует следующая теорема.

Теорема 2. *В каждом кольце $\mathcal{K}$ с единицей для любого элемента $u \in K^{ld} \cup K^{rd}$, если $u, \ldots, u^{l_u-1}$ $(l_u \geq 2)$ – попарно различные элементы множества $K\backslash\{0\}$ и, кроме того, $u^{l_u} = u^i$ для некоторого числа $i \in \mathbb{N}_{l_u-1}$, то истинны формулы*

$$u^i \in A_{u^{l_u-i}-1}^l \cap A_{u^{l_u-i}-1}^r, \tag{15}$$

$$u^{l_u-1} \in (A_{u^i}^l + 1) \cap (A_{u^i}^r + 1). \tag{16}$$

Доказательство. Пусть выполнены условия теоремы.

Из равенства $u^{l_u} = u^i$ вытекает, что истинны равенства $u^i(u^{l_u-i} - 1) = 0$ и $(u^{l_u-i} - 1)u^i = 0$.

По условию теоремы $u^i \neq 0$. Кроме того, так как $u \in K^{non-inv}$, то $u^{l_u-i} \neq 1$, т.е. $u^{l_u-i} - 1 \neq 0$.

Следовательно, из равенства $u^i(u^{l_u-i} - 1) = 0$ вытекает, что $u^i \in A^l_{u^{l_u-i}-1}$ и $u^{l_u-1} \in A^r_{u^i} + 1$, а из равенства $(u^{l_u-i} - 1)u^i = 0$ вытекает, что $u^i \in A^r_{u^{l_u-i}-1}$ и $u^{l_u-1} \in A^l_{u^i} + 1$.

Из соотношений $u^i \in A^l_{u^{l_u-i}-1}$ и $u^i \in A^r_{u^{l_u-i}-1}$ вытекает, что истинна формула (15), а из соотношений $u^{l_u-1} \in A^r_{u^i} + 1$ и $u^{l_u-1} \in A^l_{u^i} + 1$ вытекает, что истинна формула (16). □

Из теоремы 2 непосредственно вытекает следующее следствие.

Следствие 4. *В кольце $\mathcal{K}$ с единицей для любого элемента $u \in K^{ld} \cup K^{rd}$, если $u, \ldots, u^{l_u-1}$ $(l_u \geq 2)$ – попарно различные элементы множества $K\backslash\{0\}$ и, кроме того, $u^{l_u} = u^i$ для некоторого числа $i \in \mathbb{N}_{l_u-1}$, то истинны формулы*

$$u^i \in (I^l_{u^{l_u-i}-1} \cap I^r_{u^{l_u-i}-1})\backslash\{0\},$$

$$u^{l_u-1} \in ((I^l_{u^i}\backslash\{0\}) + 1) \cap ((I^r_{u^i}\backslash\{0\}) + 1).$$

4. Заключение. В настоящей работе исследованы теоретико-множественные и алгебраические свойства семейств левых и правых идеалов, построенных на основе семейств подмножеств, определяемых, соответственно, правыми и левыми делителями нуля в ассоциативных некоммутативных кольцах. Анализ свойств этих семейств односторонних идеалов, формулируемых в терминах структуры тех или иных классов ассоциативных некоммутативных колец, представляет возможное направление исследований. Другое направление связано с разработкой на основе построенного математического аппарата методов анализа структуры множества решений различных типов уравнений с параметрами, имеющими вид «произведение равно нулю», над конечными ассоциативными некоммутативными кольцами.

1. *Алферов А.П., Зубов А.Ю., Кузьмин А.С. и др.* Основы криптографии. – М.: Гелиос АРВ, 2002. – 480 с.
2. *Харин Ю.С., Берник В.И., Матвеев Г.В. и др.* Математические и компьютерные основы криптологии. – Минск: Новое знание, 2003. – 382 с.
3. *Василенко О.Н.* Теоретико-числовые алгоритмы в криптографии. – М.: МЦМНО, 2003. – 328 с.
4. *Скобелев В.В., Скобелев В.Г.* Анализ шифрсистем. – Донецк: ИПММ НАНУ, 2009. – 479 с.
5. *Скобелев В.В., Глазунов Н.М., Скобелев В.Г.* Многообразия над кольцами. Теория и приложения. – Донецк: ИПММ НАНУ, 2009. – 323 с.
6. *Курош А.Г.* Лекции по общей алгебре. – М. Наука, 1973. – 400 с.

V. V. Skobelev

Properties of zero divisors in associative rings.

Sets of left and right divisors in associative non-commutative rings are examined systematically. There are extracted two families of sets determined via, correspondingly, left and right zero divisors. It is established that these families of sets determine two families of, correspondingly, left and right ideals.

Properties of these families of one-sided ideals are investigated. It is established that extracted families of sets (and, thus, determined families of one-sided ideals) can be applied into analysis the structure of the set of solutions for equations with parameters, of the form «some product is equal to zero», over associative non-commutative rings.

Keywords: *associative non-commutative rings, left and right zero divisors, one-sided ideals.*

В. В. Скобелєв

Властивості дільників нуля у асоціативних кільцях.

Систематично досліджено множини лівих та правих дільників нуля для асоціативних некомутативних кілець. Виділено дві сім'ї множин, які визначено, відповідно, лівими та правими дільниками нуля. Встановлено, що ці сім'ї множин визначають дві сім'ї множин, відповідно, правих та лівих ідеалів. Досліджено властивості цих сімей однобічних ідеалів. Встановлено, що виділені сім'ї множин (як наслідок, сім'ї однобічних ідеалів, які визначено цими сім'ями) може бути застосовано для аналізу структури множини розв'язків рівнянь з параметрами, які мають вигляд «добуток дорівнює нулю», над асоціативними некомутативними кільцями.

Ключові слова: *асоціативні некомутативні кільця, ліві та праві дільники нуля, однобічні ідеали.*

Ин-т прикл. математики и механики НАН Украины, Донецк
vv_skobelev@iamm.ac.donetsk.ua

Получено 30.12.11