S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports

http://semr.math.nsc.ru

Том 11, стр. 800–810 (2014) УДК 512.55
MSC 16P10 16W20

СТРОЕНИЕ КОЛЕЦ, УДОВЛЕТВОРЯЮЩИХ ТОЖДЕСТВУ ИНДЕКСА ДВА

Е.В. ЖУРАВЛЕВ, Ю.Н. МАЛЬЦЕВ

Abstract. We describe the structure of finite indecomposable rings and also (infinite) regular rings satisfying the identity of index two.

Keywords: finite ring, regular ring.

1. Введение

В работах [1, 2] доказано, что произвольное конечное ассоциативное кольцо R удовлетворяет тождествам

$$mx = 0, \quad x_1x_2\dots x_n = f(x_1, x_2, \dots, x_n), \tag{1}$$

где m – натуральное число и $f(x_1, \dots, x_n)$ – многочлен из свободного ассоциативного кольца $\mathbb{Z}\langle x_1, x_2, \dots\rangle$, являющийся суммой одночленов степени $\geq n+1$. Число n называется индексом конечного кольца R или индексом тождества (см. [1]). Если $n = 1$, то $R = \bigoplus\limits_{i=1}^{s} GF(q_i)$ и многообразие ассоциативных колец

$$\mathrm{var}\left\langle \mathrm{mx} = 0, \mathrm{x_1} - \mathrm{x_1^2 f(x_1)} = 0 \right\rangle,$$

определенное тождествами (1) при $n = 1$, порождается конечным числом конечных полей (см. [3]). В работе [4] доказано, что кольцо $M_2(GF(q))$ удовлетворяет тождеству

$$\left(x - x^q\right)\left(y - y^{q^2}\right)\left(1 - [x, y]^{q-1}\right) = 0.$$

Zhuravlev, E.V., Maltsev, Y.N., Structure of rings satisfying an identity of index two.

Вторым автором работа выполнена в рамках задания №2014-418 для государственных работ в сфере научной деятельности Министерства образования и науки РФ и при частичной финансовой поддержке РФФИ (код проекта № 12.01.00329а).

Поступила 23 июля 2014, опубликована 27 октября 2014 г.

Таким образом, индекс полного кольца матриц второго порядка над конечным полем равен двум. В работе [4] приведено также описание подпрямо неразложимых конечных колец из многообразия колец

$$\mathrm{var}\left\langle \mathrm{px}=0, \left(\mathrm{x}-\mathrm{x}^{\mathrm{q}}\right)\left(\mathrm{y}-\mathrm{y}^{\mathrm{q}^2}\right)\left(1-[\mathrm{x},\mathrm{y}]^{\mathrm{q}-1}\right)=0\right\rangle,$$

где $q=p^k$ и p – простое число.

Цель настоящей работы – описать строение колец, удовлетворяющих тождеству индекса два и либо являющихся конечными кольцами, неразложимыми в прямую сумму собственных ненулевых идеалов, либо являющимися регулярными (в смысле Неймана) кольцами.

2. Строение неразложимых конечных колец индекса два

Пусть конечное кольцо R удовлетворяет тождеству

$$xy=f(x,y), \tag{2}$$

где $f(x,y)\in\mathbb{Z}\langle x,y\rangle$ и f – сумма одночленов степени ≥ 3. Пусть также R не является прямой суммой собственных ненулевых идеалов. Обозначим через $J(R)$ радикал Джекобсона кольца R.

Предложение 1. *Если $R=J(R)$, то*

$$R=N_{0,p^m}=\langle a|\, a^2=0, p^m a=0\rangle,$$

где p – простое число.

Доказательство. Из тождества (2) следует, что $R^2=R^3=R^4=\ldots=R^N$ для любого целого числа $N\geq 2$. Так как $J(R)^k=0$ для некоторого числа $k\geq 1$ (см. [5]), то $R^2=0$.

Конечная абелева группа $\langle R,+\rangle$ раскладывается в прямую сумму конечного числа примарных циклических подгрупп, каждая из которых, в силу равенства $R^2=0$, является идеалом кольца R (см. [6]). Так как R неразложимо в прямую сумму собственных ненулевых идеалов, то $R=\langle a|\, a^2=0, p^m a=0\rangle$. Предложение доказано.

Предложение 2. *Если $R\neq J(R)$, то существует простое число p такое, что $p^2R=0$.*

Доказательство. Пусть $n=|R|=p_1^{\alpha_1}\ldots p_s^{\alpha_s}$ – каноническое разложение на простые числа и $R_i=\{a\in R|\, ap_i^{\alpha_i}=0\}$. Тогда $R_i\lhd R$, $i\leq s$ и $R=\bigoplus_{i=1}^{s} R_i$ (см. [6]). Так как R не является прямой суммой собственных ненулевых идеалов, то $|R|=p^\alpha$, где p – простое число.

Из тождества (2) следует, что для любых элементов $a,b\in R$

$$(pa)(pb)=p^3g(a,b)=p^4h(a,b)=\ldots=p^\alpha v(a,b)=0,$$

где $g(x,y)$, $h(x,y)$, $v(x,y)$ – некоторые многочлены из $\mathbb{Z}\langle x,y\rangle$. Следовательно, $p^2xy=0$ – тождество в кольце R. Если R содержит единицу e, то подставляя вместо $y=e$, получим, что $p^2R=0$.

Если R не содержит единицу, то существует идемпотент $e^2=e\in R$, являющийся прообразом единицы фактор-кольца $R/J(R)$ при естественном гомоморфизме R на $R/J(R)$ (см. [7]). Рассмотрим двустороннее пирсовское разложение кольца R

$$R = eRe \dot{+} eR(1-e) \dot{+} (1-e)Re \dot{+} (1-e)R(1-e).$$

Тогда $eR(1-e) \dot{+} (1-e)Re \dot{+} (1-e)R(1-e) \subseteq J(R)$, подкольцо eRe содержит единицу e и следовательно, удовлетворяет тождеству $p^2x = 0$. В частности, $p^2e = 0$. Из доказательства предложения 1 следует, что $J(R)^2 = 0$. Если $(1-e)R(1-e) \neq 0$, то R является прямой суммой двух ненулевых идеалов

$$A = eRe \dot{+} eR(1-e) \dot{+} (1-e)Re \quad \text{и} \quad B = (1-e)R(1-e).$$

Противоречие доказывает, что $(1-e)R(1-e) = 0$ и

$$p^2R = p^2(eRe \dot{+} eR(1-e) \dot{+} (1-e)Re) = 0.$$

Предложение доказано.

Предложение 3. *Если $R/J(R)$ – некоммутативное кольцо, то $R = M_2(GF(q))$, где $q = p^k$.*

Доказательство. Исходя из доказательства предложения 2, мы можем считать, что

$$R = eRe \dot{+} eR(1-e) \dot{+} (1-e)Re = eRe + J(R), \quad J(R)^2 = 0$$

и $eR(1-e) \dot{+} (1-e)Re \subseteq J(R)$. Так как eRe содержит единицу e, то согласно работе [8] $eRe = B \dot{+} M$, где M – (B,B)-бимодуль, содержащийся в $J(eRe) = eRe \bigcap J(R)$ (см. [7]) и $B = \bigoplus\limits_{i=1}^{s} M_{n_i}(GR(p^{t_ir_i}, p^{t_i}))$ – прямая сумма полных матричных колец над кольцами Галуа. В частности, $R = B + J(R)$, $R/J(R) \cong B/J(B) = \bigoplus\limits_{i=1}^{s} M_{n_i}GF(p^{r_i})$. Пусть $B_i = M_{n_i}(GR(p^{t_ir_i}, p^{t_i}))$, $i \leq s$. Если, например, $n_1 \geq 2$, то рассмотрим систему матричных единиц $\{e_{ij} | 1 \leq i,j \leq n_1\}$ кольца $M_{n_1}(GR(p^{t_1r_1}, p^{t_1}))$. Из равенства $J(R)^2 = 0$ и тождества (2) следует, что

$$e_{12}a = \lambda e_{12}ae_{12},$$

где a – произвольный элемент $J(R)$, $\lambda \in \mathbb{Z}$. Умножая полученное равенство справа на e_{12}, получаем, что $e_{12}ae_{12} = e_{12}a = 0$, а значит $e_{22}a = e_{21}(e_{12}a) = 0$. Рассуждая аналогично, получаем, что $B_1J(R) = J(R)B_1 = 0$. Так как $B_1B_i = B_iB_1 = 0$, при $i \geq 2$, (см. [8]), то $B_1 \lhd R$, $\bigoplus\limits_{i=2}^{s} B_i + M + eR(1-e) + (1-e)Re \lhd R$ и R – кольцо, разложимое в прямую сумму идеалов B_1 и $\bigoplus\limits_{i=2}^{s} B_i + M + eR(1-e) + (1-e)Re$. Следовательно, $R = B_1 = M_{n_1}(GR(p^{t_1r_1}, p^{t_1}))$, $n_1 \geq 2$. Ввиду тождества $x^2 = f(x,x) = x^3g(x)$, выполнимого в кольце R, нильпотентные элементы кольца в квадрате равны нулю. Так как $R/J(R)$ – некоммутативное кольцо, то $n_1 = 2$.

Докажем, что $pR = 0$. Иначе, $\begin{pmatrix} p & 1 \\ 0 & 0 \end{pmatrix}$ – нильпотентная матрица, квадрат которой не равен нулю. Противоречие доказывает, что $R = M_2(GF(q))$, где $q = p^{r_1}$. Предложение доказано.

Предложение 4. *Если $R/J(R)$ – коммутативное кольцо и $R \neq J(R)$, то*

$$R = \bigoplus_{i=1}^{s} GR(p^{t_ir_i}, p^{t_i}) + J(R),$$

где $J(R)^2 = 0$. *При этом* R *удовлетворяет тождеству вида*

$$(x - x^q)\,(y - y^q) = 0,$$

где $q = p^{r_1 \cdot \ldots \cdot r_s}$.

Доказательство. Если кольцо R содержит единицу, то согласно работе [8] (предложение 6) $R = B + M$, где $B = \bigoplus_{i=1}^{s} B_i$, $B_i = M_{n_i}(GR(p^{t_i r_i}, p^{t_i}))$, $i \le s$, M – (B, B)-бимодуль, содержащийся в $J(R)$ и $B/pB \cong R/J(R)$. Так как $R/J(R)$ – коммутативное кольцо, то $n_1 = n_1 = \ldots = n_s = 1$ и B – прямая сумма колец Галуа $GR(p^{t_i r_i}, p^{t_i})$, $i \le s$. Следовательно, $R/J(R) = \bigoplus_{i=1}^{s} GF(p^{r_i})$. Пусть $q_i = p^{r_i}$, $i \le s$. Тогда фактор-кольцо $R/J(R)$ удовлетворяет тождеству $x - x^q = 0$, где $q = p^{r_1 r_2 \cdots r_s}$, и, так как $J(R)^2 = 0$, то R удовлетворяет тождеству $(x - x^q)\,(y - y^q) = 0$.

Если же R не содержит единицу, то согласно доказательству предложения 3 имеем, что $R = eRe + J(R)$, где $e^2 = e$ – прообраз в R единицы фактор-кольца $R/J(R)$, $eRe = \bigoplus_{i=1}^{s} B_i \dotplus M$, где M – (B, B)-модуль, содержащийся в $J(R)$, $B_i = M_{n_i}(GR(p^{t_i r_i}, p^{t_i}))$, $i \le s$. Так как eRe содержит единицу e, то согласно предыдущим рассуждениям каждое кольцо $B_i = GR(p^{t_i r_i}, p^{t_i})$, $i \le s$ и

$$R = \bigoplus_{i=1}^{s} GR(p^{t_i r_i}, p^{t_i}) + J(R), \quad R/J(R) = \bigoplus_{i=1}^{s} GF(p^{r_i}).$$

В частности, R удовлетворяет тождеству $(x - x^q)\,(y - y^q) = 0$, где $q = p^{r_1 r_2 \cdots r_s}$. Предложение доказано.

Таким образом, доказана следующая теорема.

Теорема 1. *Конечное, неразложимое в прямую сумму ненулевых идеалов, кольцо* R *удовлетворяет тождеству*

$$xy = f(x, y),$$

где $f(x, y) \in \mathbb{Z}\langle x, y\rangle$ *является суммой одночленов степени* ≥ 3 *тогда и только тогда, когда* R *изоморфно одному из следующих колец:*

(1) $\langle a \,|\, a^2 = 0, p^m a = 0\rangle$, p – *простое число. В этом случае* R *удовлетворяет тождеству* $xy = 0$;

(2) $M_2(GF(q))$. *В этом случае* R *удовлетворяет тождествам*

$$px = 0, \qquad \left(x - x^q\right)\left(y - y^{q^2}\right)\left(1 - [x, y]^{q-1}\right) = 0,$$

где $q = p^k$ *и* p – *простое число;*

(3) $R = \bigoplus_{i=1}^{s} GR(p^{t_i r_i}, p^{t_i}) + J(R)$, *где* $J(R)^2 = 0$, $t_i \le 2$, $i \le s$. *В этом случае* R *удовлетворяет тождествам* $p^2 x = 0$, $(x - x^q)\,(y - y^q) = 0$, *где* $q = p^{r_1 r_2 \cdots r_s}$.

Следствие (см. [9]). *Пусть* R – *конечная* $GF(p)$-*алгебра с единицей, неразложимая в прямую сумму идеалов, такая, что* $J(R)$ *совпадает с множеством делителей нуля. Если* R *удовлетворяет тождеству* $xy = f(x, y)$, *где* $f(x, y) \in \mathbb{Z}\langle x, y\rangle$

является суммой одночленов степени ≥ 3*, то* R *изоморфно кольцу матриц вида*

$$\begin{pmatrix} a_1 & b_2 & b_3 & b_n \\ 0 & a_1^{p^{t_2}} & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_1^{p^{t_n}} \end{pmatrix},$$

где $a_1, b_2, \ldots, b_n \in GF(p^r)$, $t_2, \ldots, t_n$ *– некоторые фиксированные целые числа,* $1 \leq t_i \leq r$.

Приведем полный список неизоморфных, неразложимых в прямую сумму ненулевых идеалов, колец порядков p, p^2, p^3, p^4, удовлетворяющих тождеству $xy = f(x,y)$, где $f(x,y) \in \mathbb{Z}\langle x,y\rangle$ является суммой одночленов степени ≥ 3. Для этого воспользуемся теоремой 1 и результатами работ [10, 5, 11], в которых приведена полная классификация всех колец порядка p^n, $n \leq 4$.

Кольца порядка p:

(1) $N_{0,p}$ – кольцо с нулевым умножением на аддитивной группе $(\mathbb{Z}_p, +)$;
(2) $\mathbb{Z}_p$.

Кольца порядка p^2:

(1) N_{0,p^2} – кольцо с нулевым умножением на аддитивной группе $(\mathbb{Z}_{p^2}, +)$;
(2) $\mathbb{Z}_{p^2}$;
(3) $\left\{\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \middle| \ a, b \in \mathbb{Z}_p\right\}$;
(4) $\begin{pmatrix} \mathbb{Z}_p & 0 \\ \mathbb{Z}_p & 0 \end{pmatrix}$;
(5) $\begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ 0 & 0 \end{pmatrix}$;
(6) $GF(p^2)$.

Кольца порядка p^3:

(1) N_{0,p^3} – кольцо с нулевым умножением на аддитивной группе $(\mathbb{Z}_{p^3}, +)$;
(2) $\mathbb{Z}_{p^2}[px]/(px)^2$;
(3) $\begin{pmatrix} \mathbb{Z}_{p^2} & p\mathbb{Z}_{p^2} \\ 0 & 0 \end{pmatrix}$;
(4) $\begin{pmatrix} \mathbb{Z}_{p^2} & 0 \\ p\mathbb{Z}_{p^2} & 0 \end{pmatrix}$;
(5) $GF(p^3)$;
(6) $\begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ 0 & \mathbb{Z}_p \end{pmatrix}$;
(7) $\left\{\begin{pmatrix} a & b & c \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix} \middle| \ a, b, c \in \mathbb{Z}_p\right\}$;
(8) R – кольцо без единицы, $|J(R)| = p^2$, $(R, +) = \langle f\rangle \dot{+} \langle a\rangle \dot{+} \langle b\rangle$ и умножение задается одним и только одним из соотношений:
  (a) $f^2 = f$, $af = a$, $bf = b$, $a^2 = b^2 = fa = fb = ab = ba = 0$;
  (b) $f^2 = f$, $bf = b$, $af = fa = a$, $a^2 = b^2 = ab = ba = fb = 0$;

(c) $f^2 = f$, $fb = b$, $af = fa = a$, $a^2 = b^2 = ab = ba = bf = 0$;
(d) $f^2 = f$, $fb = b$, $af = a$, $a^2 = b^2 = ab = ba = bf = fa = 0$;
(e) $f^2 = f$, $fa = a$, $fb = b$, $a^2 = b^2 = af = bf = ab = ba = 0$.

Кольца порядка p^4:

(1) N_{0,p^4} – кольцо с нулевым умножением на аддитивной группе $(\mathbb{Z}_{p^4}, +)$;

(2) $\begin{pmatrix} \mathbb{Z}_{p^2} & \mathbb{Z}_{p^2} \\ 0 & 0 \end{pmatrix}$;

(3) $\begin{pmatrix} \mathbb{Z}_{p^2} & 0 \\ \mathbb{Z}_{p^2} & 0 \end{pmatrix}$;

(4) $GR(p^4, p^2)$;

(5) $\mathbb{Z}_{p^2}[x]/(x^2)$;

(6) R – кольцо без единицы, $(R, +) = \langle f\rangle \dot{+} \langle a\rangle \dot{+} \langle b\rangle$, $\mathrm{ord}\, \mathrm{f} = \mathrm{p}^2$, $\mathrm{ord}\, \mathrm{a} = \mathrm{p}$, $\mathrm{ord}\, \mathrm{b} = \mathrm{p}$ и умножение задается одним и только одним из соотношений:
(a) $f^2 = f$, $fa = a$, $bf = b$, $af = a$, $a^2 = 0$, $ab = fb = ba = b^2 = 0$;
(b) $f^2 = f$, $fa = a$, $fb = b$, $af = a$, $a^2 = 0$, $bf = ab = ba = b^2 = 0$;
(c) $f^2 = f$, $fa = a$, $fb = b$, $af = a^2 = ab = bf = ba = b^2 = 0$;
(d) $f^2 = f$, $fa = fb = 0$, $af = a$, $a^2 = ab = 0$, $bf = b$, $ba = b^2 = 0$;
(e) $f^2 = f$, $fa = 0$, $fb = b$, $af = a$, $ba = 0$, $bf = 0$, $ab = b^2 = a^2 = 0$;

(7) R – нелокальное кольцо с единицей, $(R, +) = \langle e_1\rangle \dot{+} \langle e_2\rangle \dot{+} \langle a\rangle$, $\mathrm{ord}\, \mathrm{e}_1 = \mathrm{p}^2$, $\mathrm{ord}\, \mathrm{e}_2 = \mathrm{p}$, $\mathrm{ord}\, \mathrm{a} = \mathrm{p}$, e_1, e_2 – ортогональные идемпотенты и умножение задается одним и только одним из соотношений:
(a) $e_1a = a$, $e_2a = ae_1 = 0$, $ae_2 = a$, $a^2 = 0$;
(b) $e_1a = 0$, $e_2a = a$, $ae_1 = a$, $ae_2 = a^2 = 0$;

(8) R – локальное кольцо с единицей, $(R, +) = \langle e\rangle \dot{+} \langle a\rangle \dot{+} \langle b\rangle$, $\mathrm{ord}\, \mathrm{e} = \mathrm{p}^2$, $\mathrm{ord}\, \mathrm{a} = \mathrm{p}$, $\mathrm{ord}\, \mathrm{b} = \mathrm{p}$ и $a^2 = ab = ba = b^2 = 0$;

(9) $GF(p^4)$;

(10) $M_2(\mathbb{Z}_p)$;

(11) $\left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \middle| \, a, b \in GF(p^2) \right\}$;

(12) $\left\{ \begin{pmatrix} a & b \\ 0 & a^p \end{pmatrix} \middle| \, a, b \in GF(p^2) \right\}$;

(13) $\left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \middle| \, a, b \in GF(p^2) \right\}$;

(14) $\left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \middle| \, a, b \in GF(p^2) \right\}$;

(15) R – кольцо с единицей, $(R, +) = \langle e_1\rangle \dot{+} \langle a\rangle \dot{+} \langle e_2\rangle \dot{+} \langle b\rangle$, $\mathrm{ord}\, \mathrm{e}_1 = \mathrm{ord}\, \mathrm{a} = \mathrm{ord}\, \mathrm{e}_2 = \mathrm{ord}\, \mathrm{b} = \mathrm{p}$, $|J(R)| = p^2$, $R/J(R) \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$, $a, b \in J(R)$, $J(R)^2 = 0$, e_1, e_2 – ортогональные идемпотенты и умножение задается одним и только одним из соотношений:
(a) $e_1a = a$, $e_1b = ae_1 = 0$, $be_1 = b$, $ae_2 = a$, $be_2 = e_2a = 0$, $e_2b = b$;
(b) $e_1a = a$, $e_1b = b$, $ae_1 = be_1 = 0$, $ae_2 = a$, $be_2 = b$, $e_2a = e_2b = 0$;
(c) $e_1a = a$, $e_1b = ae_1 = be_1 = 0$, $ae_2 = a$, $be_2 = b$, $e_2a = 0$, $e_2b = b$;
(d) $e_1a = e_1b = 0$, $ae_1 = a$, $be_1 = ae_2 = 0$, $be_2 = b$, $e_2a = a$, $e_2b = b$;

(16) R – кольцо без единицы, $(R,+) = \langle e_1\rangle \dot{+} \langle a\rangle \dot{+} \langle e_2\rangle \dot{+} \langle b\rangle$, $\mathrm{ord}\, \mathrm{e}_1 = \mathrm{ord}\, \mathrm{a} = \mathrm{ord}\, \mathrm{e}_2 = \mathrm{ord}\, \mathrm{b} = \mathrm{p}$, $|J(R)| = p^2$, $R/J(R) \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$, $a, b \in J(R)$, $J(R)^2 = 0$, e_1, e_2 – ортогональные идемпотенты и умножение задается одним и только одним из соотношений:
  (a) $e_1a = a$, $e_1b = e_2a = e_2b = ae_1 = 0$, $ae_2 = a$, $be_1 = b$, $be_2 = 0$;
  (b) $e_1a = a$, $e_1b = e_2a = ae_1 = e_2b = 0$, $ae_2 = a$, $be_1 = 0$, $be_2 = b$;
  (c) $e_1a = a$, $e_1b = b$, $e_2a = e_2b = ae_1 = 0$, $ae_2 = a$, $be_1 = be_2 = 0$;
  (d) $e_1a = a$, $e_1b = e_2a = 0$, $e_2b = b$, $ae_1 = 0$, $ae_2 = a$, $be_1 = be_2 = 0$;

(17) R – локальное кольцо с единицей, $(R,+) = \langle e\rangle \dot{+} \langle a\rangle \dot{+} \langle b\rangle \dot{+} \langle c\rangle$, $\mathrm{ord}\, \mathrm{e} = \mathrm{ord}\, \mathrm{a} = \mathrm{ord}\, \mathrm{b} = \mathrm{ord}\, \mathrm{c} = \mathrm{p}$, $|J(R)| = p^3$, $a, b, c \in J(R)$ и $a^2 = ab = ba = bc = cb = ac = ca = b^2 = c^2 = 0$;

(18) R – кольцо без единицы, $(R,+) = \langle f\rangle \dot{+} \langle a\rangle \dot{+} \langle b\rangle \dot{+} \langle c\rangle$, $\mathrm{ord}\, \mathrm{e} = \mathrm{ord}\, \mathrm{a} = \mathrm{ord}\, \mathrm{b} = \mathrm{ord}\, \mathrm{c} = \mathrm{p}$, $|J(R)| = p^3$, $a, b, c \in J(R)$ и умножение задается одним и только одним из соотношений:
  (a) $f^2 = f$, $fa = a$, $fb = b$, $fc = c$, $af = bf = cf = 0$;
  (b) $f^2 = f$, $fa = fb = fc = 0$, $af = a$, $bf = b$, $cf = c$;
  (c) $f^2 = f$, $fa = a$, $fb = b$, $fc = af = bf = 0$, $cf = c$;
  (d) $f^2 = f$, $fa = a$, $fb = b$, $fc = 0$, $af = a$, $bf = 0$, $cf = c$;
  (e) $f^2 = f$, $fa = a$, $fb = b$, $fc = c$, $af = a$, $bf = cf = 0$;
  (f) $f^2 = f$, $fa = a$, $fb = fc = 0$, $af = a$, $bf = b$, $cf = c$;
  (g) $f^2 = f$, $fa = a$, $fb = b$, $fc = c$, $af = a$, $bf = b$, $cf = 0$;
  (h) $f^2 = f$, $fa = a$, $fb = b$, $fc = 0$, $af = a$, $bf = b$, $cf = c$;
  (i) $f^2 = f$, $fa = a$, $fb = fc = af = 0$, $bf = b$, $cf = c$.

Отметим также, что в [12, 13] классифицированы все конечные кольца с единицей порядка p^5, а в [14, 15] некоторые из колец порядка p^6 характеристики p или p^2.

3. Строение регулярных колец

Кольцо R называется регулярным, если уравнение $axa = a$ разрешимо в R для любого элемента $a \in R$ (см. [16]). Примерами регулярных колец являются прямые произведения тел. В [16] доказано, что если R – регулярное кольцо, то $M_n(R)$ тоже регулярное кольцо. Мы рассмотрим строение произвольного регулярного кольца R, удовлетворяющего тождеству $xy = f(x,y)$, где $f(x,y) \in \mathbb{Z}\langle x,y\rangle$ – сумма одночленов степени ≥ 3.

Известно, что для регулярного кольца R его радикал Джекобсона $J(R) = 0$ (см. [7]). Поэтому, если R – конечное кольцо, то по теореме Веддерберна-Артина $R = \bigoplus\limits_{i=1}^{m} M_{n_i}(GF(q_i))$. Покажем, что $n_i \leq 2$, $i \leq m$. Если, например, $n_1 \geq 3$, то полагая в тождестве $x = y = e_{12} + e_{23}$ получим, что $(e_{12} + e_{23})^2 = e_{13} = f(e_{12} + e_{23}, e_{12} + e_{23}) = 0$. Противоречие доказывает, что $R = \bigoplus\limits_{i=1}^{m} M_{n_i}(GF(q_i))$, где $n_i \leq 2$.

Покажем, что верно и обратное утверждение. А именно, произвольное конечное кольцо $R = \bigoplus\limits_{i=1}^{m} M_{n_i}(GF(q_i))$, где $n_i \leq 2$, является регулярным и удовлетворяет некоторому тождеству индекса два $xy = g(x,y)$, где $g(x,y)$ – сумма одночленов степени ≥ 3. Регулярность кольца следует из [16] (теорема 3, стр. 24).

Рассмотрим $\operatorname{var} \mathrm{R}$ – многообразие колец, порожденное кольцом R. В кольце R нильпотентные подкольца удовлетворяют тождеству $xy = 0$ (см. [17]). В работе [1] доказано, что в этом случае все нильпотентные кольца из $\operatorname{var} \mathrm{R}$ имеют нулевое умножение и R удовлетворяет некоторому тождеству $xy = g(x, y)$, где $g(x, y)$ – сумма одночленов степени ≥ 3.

Рассмотрим строение произвольных (не обязательно конечных) регулярных колец, удовлетворяющих тождеству индекса два. Имеет место следующая теорема.

Теорема 2. *Пусть R – ненулевое регулярное кольцо. Тогда*

(1) *кольцо R не содержит ненулевых нильпотентных элементов и удовлетворяет тождеству $xy = f(x, y)$, где $f(x, y)$ – сумма одночленов степени ≥ 3 свободного ассоциативного кольца $\mathbb{Z}\langle x, y\rangle$, тогда и только тогда, когда существует конечное множество конечных полей $\mathfrak{M} = \{GF(q_1), \dots, GF(q_s)\}$ такое, что*

$$F \subseteq R \subseteq \prod_{i \in I} F_i,$$

где $\{F, F_i, i \in I\} \subseteq \mathfrak{M}$;

(2) *кольцо R содержит ненулевые нильпотентные элементы и удовлетворяет тождеству $xy = f(x, y)$, где $f(x, y)$ – сумма одночленов степени ≥ 3 свободного ассоциативного кольца $\mathbb{Z}\langle x, y\rangle$, тогда и только тогда, когда существует конечное множество конечных полей $\mathfrak{M} = \{GF(q_1), \dots, GF(q_s)\}$ такое, что*

$$M_2(F) \subseteq R \subseteq M_2\left(\prod_{i \in I} F_i\right),$$

где $\{F, F_i, i \in I\} \subseteq \mathfrak{M}$.

Доказательство. Заметим, что конечное поле $GF(q)$ удовлетворяет тождествам $x - x^q = 0$, $x - x^{(q-1)t+1} = 0$ для любого целого числа $t \geq 1$. Поэтому произвольное кольцо вида $\prod_{i \in I} F_i$, где $\{F_i, i \in I\} \subseteq \mathfrak{M} = \{GF(q_1), \dots, GF(q_s)\}$ удовлетворяет тождеству $x - x^N = 0$, где $N = (q_1 - 1) \dots (q_s - 1) + 1$. Следовательно, если $F \subseteq R \subseteq \prod_{i \in I} F_i$, где $\{F, F_i, i \in I\} \subseteq \mathfrak{M}$, то R – ненулевое кольцо без нильпотентных элементов, удовлетворяющее тождествам $x - x^N = 0$, $(x - x^N)y = 0$.

Докажем обратное утверждение. Пусть R – ненулевое регулярное кольцо без нильпотентных элементов, удовлетворяющее тождеству $xy = f(x, y)$, где f – сумма одночленов степени ≥ 3. Тогда R удовлетворяет тождеству

$$x^2 - f(x, x) = x^2 - x^3 g(x) = 0,$$

где $f(x, x) = x^3 g(x)$ и $g(x) \in \mathbb{Z}[x]$. Откуда следует, что $(a - a^2 g(a))^2 = 0$ для любого элемента $a \in R$. Так как R – редуцированное кольцо, то $x - x^2 g(x) = 0$ – тождество в R.

Из работы [3] следует, что R удовлетворяет некоторому тождеству $mx = 0$, где m – натуральное число, и является локально конечным кольцом. Пусть $a \in R$, $a \neq 0$. Тогда подкольцо $\langle a\rangle$, порожденное a, является конечной прямой суммой конечных полей

$$\langle a\rangle = GF(q_1)\oplus\ldots\oplus GF(q_s),$$

каждое из которых удовлетворяет тождествам $mx = 0$, $x-x^2g(x) = 0$. Заметим, что число таких полей конечно и $GF(q_i)\subseteq R$ ($q_i\le 2+\deg g(x)$, $i\le s$).

Далее, полупростое кольцо R является подпрямым произведением примитивных колец R/P_i, $i\in I$, каждое из которых удовлетворяет тождествам $mx = 0$, $x-x^2g(x) = 0$. По теореме Капланского (см. [7], стр. 327) каждое примитивное кольцо R/P_i, $i\in I$ является конечным полем $GF(q_i')$ и множество таких полей является конечным $\{GF(q_i')|\, i\in I\} = \{GF(q_1'),\ldots,GF(q_t')\}$. Пусть

$$\mathfrak{M} = \{GF(q_1), GF(q_1'),\ldots,GF(q_t')\}\,.$$

Тогда $GF(q_1)\subseteq R\subseteq\prod\limits_{i\in I} GF(q_i')$.

Докажем второе утверждение. Пусть R – регулярное кольцо, удовлетворяющее тождеству вида $xy = f(x,y)$, где f – сумма одночленов степени ≥ 3 и a – ненулевой нильпотентный элемент в R. Тогда $a^n = 0$, где $n\ge 2$ и $a\cdot a = f(a,a) = a^2(ag(a)) = a^2(ag(a))^2 = \ldots = a^n(ag(a))^n = 0$. По условию существует элемент $x\in R$ такой, что $axa = a$. Положим $b = xax$. Тогда $aba = a$ и $bab = b$. Пусть $f_{11} = ab(1-ba)$, $f_{12} = a$, $f_{21} = b(1-ba)$, $f_{22} = ba$ и $f = f_{11}+f_{22}$. Тогда $f_{ij}\cdot f_{jt} = f_{it}$, $f_{ij}f_{st} = 0$, если $j\ne s$, и $f^2 = f\in fRf$. Пусть

$$A = \{r\in fRf|\, rf_{ij} = f_{ij}r, 1\le i,j\le 2\}\,.$$

Тогда A – подкольцо кольца fRf, содержащего единицу f. Пусть c – произвольный элемент из fRf и $c_{ij} = \sum\limits_{k=1}^{2} f_{ki}cf_{jk} = f_{1i}cf_{j1} + f_{2i}cf_{j2}$, $1\le i,j\le 2$. Тогда $c_{ij}\in A$ и $c = \sum\limits_{i,j=1}^{2} c_{ij}f_{ij}$. Таким образом, $M_2(A)\subseteq fRf\subseteq R$. Если v – ненулевой нильпотентный элемент кольца A, то индекс нильпотентности элемента $\begin{pmatrix} v & 1\\ 0 & 0\end{pmatrix} = vf_{11}+f_{12}$ равен трем. Противоречие доказывает, что A – кольцо без нильпотентных элементов, удовлетворяющее тождеству $x-x^2g(x) = 0$, где $f(x,x) = x^3g(x)$.

Ранее мы заметили, что A удовлетворяет также тождеству $mx = 0$, где m – натуральное число и содержит конечное поле $GF(q)$, $q\le 2+\deg g(x)$. Следовательно, $M_2(GF(q))\subseteq R$. Так как $J(R) = 0$ (см. [7]), то $R = \sum\limits_{i\in I}\bigoplus\limits_{s} R/P_i$ – подпрямое произведение примитивных колец R/P_i, $i\in I$. По теореме Капланского (см. [7], стр. 327) каждое кольцо $R/P_i = M_{n_i}(D^{(i)})$, где $D^{(i)}$ – тело, конечномерное над своим центром $Z^{(i)}$. Поле $Z^{(i)}$ удовлетворяет тождеству $x^2-f(x,x) = x(x-x^2g(x)) = 0$. Следовательно, $|Z^{(i)}|\le 2+\deg g(x)$ и $D^{(i)}$ – конечное тело. По теореме Веддерберна (см. [7], стр. 266) $D^{(i)} = Z^{(i)}$, $i\in I$. Если $n_i\ge 3$, для некоторого $i\in I$, то

$$(e_{12}+e_{23})^2 = e_{13} = f(e_{12}+e_{23}, e_{12}+e_{23}) = 0.$$

Противоречие доказывает, что $n_i\le 2$, $i\in I$ и $D^{(i)} = GF(q_i)$, где $q_i\le 2+\deg g(x)$. Множество полей $\{GF(q_i)|\, i\in I\}$ является конечным, так как их порядки ограничены в совокупности. Следовательно, $R\subseteq\prod\limits_{i\in I} M_2(GF(q_i))$.

Так как $\prod\limits_{i\in I} M_2(GF(q_i)) \cong M_2(\prod\limits_{i\in I} GF(q_i))$, то существует мономорфизм кольца R в $M_2(\prod\limits_{i\in I} GF(q_i))$, где множество полей $\{GF(q), GF(q_i) |\, i \in I\}$ является конечным.

Докажем обратное утверждение. Если $M_2(GF(q)) \subseteq R$, то R содержит ненулевой нильпотентный элемент $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Теорема доказана.

В связи со вторым утверждением теоремы возникает вопрос: всякое ли регулярное кольцо, удовлетворяющее тождеству вида $xy = f(x,y)$, где $f(x,y)$ – сумма одночленов степени ≥ 3, и содержащее ненулевые нильпотентные элементы, изоморфно некоторому кольцу $M_2(A)$, где A – регулярное кольцо без нильпотентных элементов? Ответ на этот вопрос отрицательный. Кольцо $M_2(GF(p)) \oplus GF(p)$ удовлетворяет тождеству индекса два (см. [4])

$$\Big(x - x^p\Big)\Big(y - y^{p^2}\Big)\Big(1 - [x,y]^{p-1}\Big) = 0,$$

содержит нильпотентные элементы и имеет порядок p^5. Если предположить $M_2(GF(p)) \oplus GF(p) \cong M_2(A)$, где A – конечное регулярное кольцо без нильпотентных элементов, то $|A| \geq p^2$ и порядок $|M_2(A)| \geq p^8$. Противоречие.

Список литературы

[1] И.В. Львов, *О многообразиях ассоциативных колец. I*, Алгебра и Логика, **12**:3 (1973), 269–297. MR0389973

[2] R. Kruse, *Identities satisfied by a finite ring*, J. Algebra, **26**:2 (1973), 298–318. MR0325678

[3] A. Iskander, *Product of ring varieties and attainability*, Trans. Amer. Math. Soc., **193**(466) (1974), 231–238. MR0349753

[4] Ю.Н. Мальцев, Е.Н. Кузьмин, *Базис тождеств алгебры матриц второго порядка над конечным полем*, Алгебра и Логика, **17**:1 (1978), 28–32. MR0516388

[5] В.П. Елизаров, *Конечные кольца*, М.: Гелиос, 2006.

[6] А.И. Кострикин, *Введение в алгебру*, М.: Наука, 1977. MR0460008

[7] Н. Джекобсон, *Строение колец*, М.: Иностранная литература, 1961.

[8] R. Wilson, *On structure of finite rings II*, Pacific J. Math., **51**:1 (1974), 317–325. Zbl 0317.16009

[9] R. Raghavendran, *Finite associative rings*, Compos. Math., **21**:2 (1969), 27–59.

[10] В.П. Елизаров, *Ненильпотентные конечные кольца*, ДЕП ВИНИТИ, **1472-85**.

[11] В.А. Ратинов, *Полусовершенные кольца со специальными типами присоединенных групп*, канд. дисс., МГПИ, Москва, 1980.

[12] B. Corbas, G.D. Williams, *Rings of order p^5. Part 1. Nonlocal rings*, Journal of Algebra, **231** (2000), 677–690. Zbl 1017.16014

[13] B. Corbas, G.D. Williams, *Rings of order p^5. Part 2. Local rings*, Journal of Algebra, **231** (2000), 691–704. Zbl 1017.16015

[14] Е.В. Журавлев, *Конечные локальные кольца порядка p^6 и характеристики p, радикал Джекобсона которых имеет индекс нильпотентности четыре*, Известия АлтГУ, **1** (2006), 20–35.

[15] Е.В. Журавлев, *О классификации конечных локальных колец характеристики p^2, радикал Джекобсона которых имеет индекс нильпотентности четыре*, Известия АлтГУ, **1** (2008), 18–28.

[16] Л.А. Скорняков, *Дедекиндовы структуры с дополнениями и регулярные кольца*, М.: Физматлит, 1961. Zbl 0115.02802

[17] L. Rowen, *Polynomial identities in ring theory*, Academic Press, 1980. MR0576061

Евгений Владимирович Журавлев
Алтайский государственный университет,
пр. Ленина 61,
656049, Барнаул, Россия
E-mail address: evzhuravlev@mail.ru

Юрий Николаевич Мальцев
Алтайская государственная педагогическая академия,
ул. Молодежная 55,
656031, Барнаул, Россия
E-mail address: maltsevyn@gmail.com