О представлении конечных колец матрицами над коммутативным кольцом

А. МЕКЕЙ
Монгольский государственный университет
e-mail: mekei@yahoo.com

УДК 512.552.4+512.552.18

Ключевые слова: кольца Галуа, конечное кольцо, автоморфизм кольца Галуа, подпрямо неразложимое кольцо, многообразие колец, тождество, конечно представимое многообразие колец, почти конечно представимое многообразие колец.

Аннотация

В работе доказано, что все конечные ассоциативные кольца, удовлетворяющие тождествам вида $nx = 0$, $x^3 f(x) + x^2 = 0$, где n — нечётное натуральное число, $f(x) \in \mathbb{Z}[x]$, представимы матрицами над коммутативным кольцом.

Abstract

A. Mekei, On the representation of finite rings by matrices over commutative rings, Fundamentalnaya i prikladnaya matematika, vol. 17 (2011/2012), no. 7, pp. 151—163.

In this paper, it is shown that all finite associative rings satisfying the identities $nx = 0$ and $x^3 f(x) + x^2 = 0$, where n is an odd natural number and $f(x) \in \mathbb{Z}[x]$, are embeddable in the ring of matrices over some suitable commutative ring.

1. Введение

Многообразие ассоциативных колец, все конечные кольца которых представимы матрицами (или вложимы в кольцо матриц) над коммутативным кольцом, будем называть *конечно представимым* (или *конечно вложимым*) *многообразием*. Многообразие ассоциативных колец назовём *почти конечно представимым многообразием*, если само многообразие не конечно представимое, но его любое собственное подмногообразие конечно представимое.

В [1] Ю. Н. Мальцев исследовал конечно представимые многообразия ассоциативных колец и поставил задачу описать конечно представимые многообразия ассоциативных колец.

Пусть p — простое число, $\mathbb{Z}_{p^2}$ и $\mathbb{Z}_p$ — циклические группы порядков p^2 и p соответственно, $B_{21} = \mathrm{End}(\mathbb{Z}_{p^2} \oplus \mathbb{Z}_p)$, $\mathrm{var}\, B_{21}$ — многообразие, порождённое кольцом B_{21}. В [1] показано, что $\mathrm{var}\, B_{21}$ — почти конечно представимое многообразие. Заметим, что там же доказано, что многообразие $\mathrm{var}\, B_{21}$ удовлетворяет тождеству

$$(x - x^p)(y - y^p)(z - z^p) = 0.$$

Фундаментальная и прикладная математика, 2011/2012, том 17, № 7, с. 151—163.

Данный результат показывает, что существует не конечно представимое многообразие ассоциативных колец, удовлетворяющее тождеству вида

$$x^4 f(x) + x^3 = 0.$$

Отсюда естественно вытекает вопрос: будет ли конечно представимым многообразие ассоциативных колец, удовлетворяющих тождеству вида

$$x^3 f(x) + x^2 = 0, \quad f(x) \in \mathbb{Z}[x] \tag{1}$$

В настоящей работе исследована конечная представимость многообразий, удовлетворящих тождеству вида (1).

Сначала введём некоторые обозначения и определения и напомним некоторые многократно используемые результаты других авторов.

Радикал Джекобсона кольца R будем, как всегда, обозначать через $J(R)$, через Λ будем обозначать кольцо Галуа $\mathbb{Z}[x]/\big(p^k, f(x)\big) = GR(p^k, p^{r\cdot k})$, где p — простое число, $k \geqslant 1$ — натуральное число, $f(x)$ — унитарный многочлен (коэффициент его старшего члена равен 1) с целыми коэффициентами, неприводимый по модулю p, $f(x) \in \mathbb{Z}[x]$, $\deg f(x) = r$. Группа обратимых элементов кольца Λ обозначается через Λ^*, группа автоморфизмов кольца Галуа Λ — через $\mathrm{Aut}(\Lambda)$.

В [5] показано, что в Λ и Λ^* соответственно $|\Lambda| = p^{rk}$, $|\Lambda^*| = (p^r - 1)p^{r(k-1)}$ элементов и Λ^* содержит единственную циклическую подгруппу $\Gamma(\Lambda) = \langle g \rangle$ порядка $p^r - 1$, причём любой элемент $\lambda \in \Lambda$ имеет единственное представление вида

$$\lambda = \lambda_0 + p\lambda_1 + p^2\lambda_2 + \ldots + p^{k-1}\lambda_{k-1}, \tag{2}$$

где $\lambda_i \in \Gamma(\Lambda) \cup \{0\}$, $i = 0, 1, 2, \ldots, k-1$. В [5, предложение 2] также доказано, что $\mathrm{Aut}(\Lambda) = \langle \sigma \rangle$ — циклическая группа порядка r, причём действие σ на элементы кольца Λ определяется образом $\sigma(g) = g^p$ элемента g.

Пусть M — (Λ, Λ)-бимодуль над кольцом Галуа Λ. Элемент $a \in M$ называется *отмеченным* над Λ, если для любого $\lambda \in \Lambda$ справедливо $a\lambda = \sigma_i(\lambda)a$ относительно некоторого автоморфизма $\sigma_i \in \mathrm{Aut}(\Lambda)$.

Пусть M — конечно порождённый левый Λ-модуль, $a_1, a_2, \ldots, a_m$ — его порождающие элементы. Эти элементы назовём *несократимыми*, если ни один из них не является линейной комбинацией остальных. Несократимая система порождающих элементов называется *базисом* Λ*-модуля* M. Базис (Λ, Λ)-бимодуля M называется *отмеченным*, если каждый элемент этого базиса является отмеченным элементом.

В [3] А. А. Нечаев показал, что если Λ — кольцо Галуа, M — конечно порождённый (Λ, Λ)-бимодуль, то для M существует отмеченный базис, базис левого Λ-модуля ${}_\Lambda M$ является базисом правого Λ-модуля M_Λ и обратное тоже верно. Мы будем использовать все эти результаты в дальнейшем. Обозначим также через $\mathbb{Z}\langle x_1, x_2, \ldots\rangle$ свободное ассоциативное кольцо с множеством свободных образующих $X = \{x_1, x_2, \ldots\}$.

Основным результатом настоящей работы является теорема 1.

Теорема 1. *Всякое многообразие ассоциативных колец, идеал тождеств которого содержит многочлены*

$$p^k x, \quad x^3 f(x) + x^2, \tag{3}$$

где $k \geqslant 1$, p — простое число, $p \neq 2$ и $f(x) \in \mathbb{Z}[x]$, является конечно представимым многообразием.

Из теоремы 1 следует, что все конечные кольца с тождествами вида (3) вкладываются в кольца матриц над коммутативными кольцами.

Следствие 1. *Всякое многообразие ассоциативных колец, идеал тождеств которых содержит многочлены*

$$nx, \quad x^3 f(x) + x^2,$$

где $n > 1$ — нечётное целое число, $f(x) \in \mathbb{Z}[x]$, является конечно представимым многообразием.

Следствие 2. *Всякое многообразие ассоциативных колец, идеал тождеств которого содержит многочлен*

$$xy - f(x, y), \tag{4}$$

где $\deg f(x, y) \geqslant 3$, $f(x, y) \in \mathbb{Z}\langle x, y\rangle$, $\mathbb{Z}\langle x, y\rangle$ — свободное ассоциативное кольцо, является конечно представимым многообразием. □

Напомним, что выражения «идеал тождеств содержит многочлен $f(x)$» и «в многообразии выполнено тождество $f(x) = 0$» эквивалентные.

2. Доказательство основной теоремы

Представимость всех конечных полупростых колец, удовлетворяющих тождествам вида (3), матрицами над коммутативным кольцом очевидна. Согласно результатам работы [4] все конечные нильпотентные кольца, удовлетворяющие тождествам вида (3), представимы матрицами над коммутативным кольцом. Известно, что любое кольцо является подпрямой суммой подпрямо неразложимых колец. Остаётся доказать представимость матрицами над коммутативным кольцом только для подпрямо неразложимых конечных колец с ненулевым радикалом Джекобсона, удовлетворяющих тождествам вида (3) и не совпадающих со своим радикалом.

Определение 1. Конечное кольцо R назовём *A-кольцом*, если оно удовлетворяет следующим свойствам:

1) R — подпрямо неразложимое кольцо;
2) $R \neq J(R) \neq (0)$, где $J(R)$ — радикал Джекобсона кольца R;
3) R удовлетворяет тождествам вида

$$p^k x = 0, \quad x^3 f(x) + x^2 = 0, \tag{5}$$

где p — простое число, $k > 1$ — целое число, $f(x) \in \mathbb{Z}[x]$;

4) R обладает идемпотентным элементом $e = e^2$, который является прообразом в R единицы $\bar{1}$ фактор-кольца $\bar{R} = R/J(R)$.

В дальнейшем используем пирсовское разложение А-кольца R

$$R = eRe + eR(1-e) + (1-e)Re + (1-e)R(1-e) \tag{6}$$

относительно идемпотентного элемента e кольца R.

Лемма 1. *Пусть R — А-кольцо, $J(R)$ — его радикал. Тогда*

1) *кольцо $J(R)$ удовлетворяет тождествам*

$$x^2 = 0, \quad xy + yx = 0; \tag{7}$$

2) *если $p \neq 2$, то кольцо $J(R)$ удовлетворяет тождеству $xyz = 0$, т. е. $J(R)^3 = 0$.*

Доказательство. Так как кольцо $J(R)$ нильпотентно, из второго тождества (5) следует, что в $J(R)$ выполняется тождество $x^2 = 0$. Тождество $xy + yx = 0$ является следствием тождества $x^2 = 0$. При $p \neq 2$ из второго тождества (7) легко получается, что в $J(R)$ выполняется тождество $xyz = 0$, т. е. $J(R)^3 = 0$. □

Лемма 2. *Всякое конечное А-кольцо R совпадает с одним из следующих колец*:

1) $R = eRe + eR(1-e)$;
2) $R = eRe + (1-e)Re$;
3) $R = eRe$, *причём e является единичным элементом кольца R.*

Доказательство. Пусть R — А-кольцо и (6) — его пирсовское разложение относительно идемпотента $e = e^2 \in R$. Ясно, что

$$J(R) = eJ(R)e + eR(1-e) + (1-e)Re + (1-e)R(1-e).$$

Из тождества (7) следует, что

$$eR(1-e)Re = (1-e)ReR(1-e) = eR(1-e)R(1-e) = (1-e)R(1-e)Re = 0.$$

Тогда $eR(1-e)$, $(1-e)Re$ и $(1-e)R(1-e)$ — идеалы кольца R. Кольцо R является подпрямо неразложимым, поэтому либо два из этих идеалов равны нулю, либо все они равны нулю. Кроме того, легко убедиться, что случай $(1-e)R(1-e) \neq 0$ не имеет места. Поэтому имеют место только следующие возможности: $R = eRe + eR(1-e)$, $eR(1-e) \neq 0$; $R = eRe + (1-e)Re$, $(1-e)Re \neq 0$ или $R = eRe$. □

Следствие 3. *Конечное А-кольцо R совпадает с одним из следующих колец*:

1) *алгеброй над конечным полем, обладающей левой единицей e, такой что $eJ(R) = J(R)$, $J(R)e = 0$;*
2) *алгеброй над конечным полем, обладающей правой единицей e, такой что $eJ(R) = 0$, $J(R)e = J(R)$;*

3) *кольцом с единицей и характеристикой p или p^2 (т. е. R удовлетворяет тождеству $p^2x = 0$ или $px = 0$).*

Доказательство. Кольцо R совпадает с одним из типов, указанных в лемме 2. Пусть R имеет вид

$$R = eRe + eR(1-e), \quad eR(1-e) \neq 0. \tag{8}$$

Тогда подкольцо eRe является кольцом с единицей e и согласно теореме Вильсона [6] имеет вид

$$eRe = Q + N,$$

где Q — подкольцо кольца eRe и Q — прямая сумма конечного числа матричных колец над кольцами Галуа, N — (Q,Q)-бимодуль, $N \subseteq J(eRe) = pQ + N = e(pQ+N)e$ и $Q \cap N = (0)$, т. е. $Q + N$ прямая сумма бимодулей.

Из тождества (7) следует, что $pQ + N$ и $eR(1-e)$ аннулируют друг друга и являются идеалами с тривиальным пересечением. Так как R — подпрямо неразложимое кольцо и $eR(1-e) \neq 0$, то $pQ + N = 0$. Это означает, что eRe — полупростое кольцо. Тем самым доказано, что R — алгебра над полем $GF(p)$. Из (8) следует, что e — левая единица кольца R со свойствами $eJ(R) = J(R)$, $J(R)e = 0$. Это доказывает утверждение 1). Аналогичное рассуждение доказывает 2). Случай 3) следует из леммы 1, так как $pR \subseteq J(R)$ и поэтому $pe \in J(R)$, $(pe)^2 = 0 = p^2e$, т. е. $p^2R = 0$ и $p^2x = 0$ — тождество в кольце $R = eRe$. Это означает, что либо $\operatorname{char} R = p$, либо $\operatorname{char} R = p^2$. □

Следствие 4. *Конечное А-кольцо R вида $R = eRe + eR(1-e)$, или $R = eRe + (1-e)Re$, или $R = eRe$, $\operatorname{char} R = p$, представимо матрицами над коммутативным кольцом.*

Следствие 4 следует из предыдущего следствия 3, так как в указанных случаях R является конечномерной алгеброй над полем и, следовательно, имеет регулярное представление матрицами над полем.

Далее рассмотрим А-кольцо R с единицей характеристики p^2, где p — нечётное простое число. Тогда согласно [6] кольцо R имеет вид

$$R = Q + N, \tag{9}$$

где Q — подкольцо R и прямая сумма конечного числа матричных колец над кольцами Галуа, N — (Q,Q)-бимодуль, $N \subseteq J(R) = pQ + N$ и $Q \cap N = (0)$, $Q + N$ — прямая сумма (Q,Q)-бимодулей.

Лемма 3. *Если R — А-кольцо с единицей и $\operatorname{char} R = p^2$, то $pJ(R) = 0$.*

Доказательство. Пусть $\operatorname{char} R = p^2$. Согласно [6] R имеет вид (9), поэтому $J(R) = pQ + N$ и, следовательно, $pJ(R) = pN$. Пусть $a \in N$ — произвольный элемент. Тогда $pa = (pe)a = -a(pe) = -pa$, т. е. $2pa = 0$. Так как p — нечётное простое число, то из $2pa = 0$ следует, что $pa = 0$ для любого $a \in N$. Значит, $pJ(R) = pN = (0)$. □

Пусть R — А-кольцо и

$$A\big(J(R)\big) = \operatorname{Ann}_{J(R)} J(R) = \{x \in J(R) \mid xJ(R) = J(R)x = 0\}.$$

Легко убедиться, что $A\big(J(R)\big)$ — идеал кольца R, и согласно пункту 2) леммы 1 имеем, что $J(R)^2 \subseteq A\big(J(R)\big)$.

Лемма 4. *Пусть R — А-кольцо с единицей характеристики p^2 и $R = Q + N$, где Q — подкольцо кольца R, являющееся прямой суммой конечного числа матричных колец над кольцами Галуа, N — (Q, Q)-бимодуль, $N \subseteq J(R) = pQ + N$ и $Q \cap N = (0)$. Тогда $A\big(J(R)\big) \cap N = (0)$ и если $N \neq 0$, то $0 \neq N^2 \subseteq pQ$. Кроме того, N не содержит ненулевых идеалов кольца R.*

Доказательство. Ясно, что $J(R) = pQ + N$. Предположим, что

$$N' = N \cap A\big(J(R)\big) \neq (0).$$

Покажем, что N' — идеал кольца R. Действительно, для любых $x \in N'$, $r \in R$ и $a \in J(R)$ в силу второго из тождеств (7)

$$a \cdot (rx) = -(rx)a = -r(xa) = 0, \quad a(xr) = (ax)r = 0,$$
$$(rx)a = r(xa) = 0, \quad (xr)a = -a(xr) = -(ax)r = 0.$$

Эти равенства показывает, что N' — идеал кольца R. Тогда $pQ \cap N' = (0)$, что противоречит подпрямой неразложимости кольца R. Следовательно, $N' = (0)$. Из условия $pQ \cap N = (0)$ вытекает, что $N^2 \neq (0)$.

Докажем, что $A\big(J(R)\big) = pQ$. Достаточно показать, что

$$A' = \operatorname{Ann}_N N = \{x \in N \mid xN = Nx = 0\} = 0,$$

т. е. для любого $0 \neq x \in N$ существует такой $y \in N$, что $xy \neq 0$. В самом деле, легко убедиться, что A' — идеал кольца R, содержащийся в N. Если $A' \neq 0$, то $0 = N \cap pQ \supseteq A' \cap pQ$, что противоречит подпрямой неразложимости кольца R. Поэтому $A' = 0$. Пусть $a + b \in A\big(J(R)\big)$, где $a \in pQ$, $b \in N$, причём $b \neq 0$. Ранее мы заметили, что существует элемент $c \in N \subseteq J(R)$, такой что $bc \neq 0$. Следовательно, $0 = (a + b) \cdot c = ac + bc = bc$. Противоречие. Отсюда следует, что $A\big(J(R)\big) = pQ$, и из пункта 2) леммы 1 следует, что если $N \neq 0$, то $0 \neq N^2 \subseteq A\big(J(R)\big) = pQ$. □

Лемма 5. *Всякое А-кольцо R с единицей характеристики p^2 имеет вид*

$$R = \Lambda + N, \tag{10}$$

где $\Lambda = \mathbb{Z}[x]/\big(p^2, f(x)\big)$ — кольцо Галуа, $\operatorname{char}\Lambda = p^2$, $pJ(R) = 0$, N — (Λ, Λ)-бимодуль, $N \subseteq J(R)$, p — простое число, $p \neq 2$, $r = \deg f(x)$, $f(x)$ — неприводимый унитарный многочлен по модулю p и если $N \neq 0$, то $0 \neq N^2 \subseteq p\Lambda$.

Доказательство. Согласно [6] R имеет вид (9) и

$$Q = \Lambda_1 + \Lambda_2 + \ldots + \Lambda_m + M_{m_1}(\Lambda_{m+1}) + \ldots + M_{m_k}(\Lambda_{m+k}), \tag{11}$$

где $m_i \geqslant 2$, $i = 1, 2, \ldots, k$, Λ_j, $j = 1, 2, \ldots, m + k$, — кольцо Галуа и по условию хотя бы для одного j, $1 \leqslant j \leqslant m+k$, $\operatorname{char}\Lambda_j = p^2$, $p \neq 2$, p — простое число. Если

для некоторого $m+i$, $m+1 \leqslant m+i \leqslant m+k$, $\operatorname{char}\Lambda_{i+m} = p^2$ и либо $m_i \geqslant 2$, либо Λ_j — поле и $m_j \geqslant 3$, то соответственно кольцо $M_{m_i}(\Lambda_{m+i})$ или $M_{m_j}(\Lambda_j)$ содержит нильпотентное подкольцо, не удовлетворяющее тождеству $x^2 = 0$. Поэтому Λ_{m+i} является полем и $m_i \leqslant 2$ для всех $i = 1, 2, \ldots, k$. Пусть $\Lambda_{m+i} = GF(p^{s_i})$. Тогда слагаемое $H = M_2\big(GF(p^{s_1})\big) + \ldots + M_2\big(GF(p^{s_k})\big)$ является алгеброй над полем $GF(p)$.

По условию $\operatorname{char} R = p^2$, поэтому среди $\Lambda_1, \ldots, \Lambda_m$ есть кольцо Галуа характеристики p^2. Не нарушая общности, предположим, что $\operatorname{char}\Lambda_1 = p^2$, $p\Lambda_1 \neq (0)$. Среди Λ_i тоже могут быть конечные поля, поэтому можем считать, что $\operatorname{char}\Lambda_i = p^2$ при $i = 1, 2, \ldots, r$, $\operatorname{char}\Lambda_{r+j} = p$, $r \geqslant 1$, $j = 1, 2, \ldots, m-r$, т. е. $\Lambda_{r+j} = GF(p^{d_j})$ — конечные поля. Значит, А-кольцо R имеет вид

$$R = \Lambda_1 + \Lambda_2 + \ldots + \Lambda_r + GF(p^{d_1}) + \ldots + GF(p^{d_{m-r}}) + \\ + M_2\big(GF(p^{s_1})\big) + \ldots + M_2\big(GF(p^{s_k})\big) + N, \quad (12)$$

где $\Lambda_i = \mathbb{Z}[x]/\big(p^2, f_i(x)\big)$, $p \neq 2$, p — простое число, $f_i(x)$ — унитарный неприводимый полином по модулю p, $pJ(R) = pN = 0$, N — (Q,Q)-бимодуль, $N \subseteq J(R)$ и единица кольца R записывается как

$$e = e_1 + \ldots + e_r + e_{r+1} + \ldots + e_m + e_{m+1} + \ldots + e_{m+k}. \quad (13)$$

Из (12) следует, что $pR = p\Lambda_1 + \ldots + p\Lambda_r$, причём каждый из $p\Lambda_i$, $i = 1, 2, \ldots, r$, является идеалом кольца R. Тогда ввиду подпрямой неразложимости кольца R имеем, что $r = 1$ и $p\Lambda_1 \neq 0$, $p\Lambda_1$ — идеал кольца R. Если $N = 0$, то из (12) следует, что $R = \Lambda_1$ является кольцом Галуа. Предположим, что $N \neq (0)$. Согласно лемме 4 случай $N^2 = 0$ не имеет места. Из $J(R)^3 = 0$ следует, что $N^2 \subseteq A\big(J(R)\big) = \operatorname{Ann}_{J(R)} J(R)$. Из равенств $J(R) = pQ + N$, $pR = pQ + pN = pQ = p\Lambda_1$ следует, что $p\Lambda_1 = pR \subseteq A\big(J(R)\big)$.

Рассмотрим разложение

$$N = eNe = \sum_{i,j=1}^{n} e_i N e_j, \quad (14)$$

где $n = m + k$. Нетрудно заметить, что каждый из e_iNe_j является (Q,Q)-бимодулем. Используя тождество $xy + yx = 0$, указанное в лемме 1, покажем, что $N = e_1Ne_1$ и $e_iNe_j = 0$ при $(i,j) \neq (1,1)$. В самом деле, из тождества $xy + yx = 0$ следует равенство $e_iNe_j \cdot e_sNe_q = 0$ при $j \neq s$, или $q \neq i$, или $i = q \neq s = j$. Тогда при $i \neq j$ e_iNe_j является идеалом кольца R. Рассмотрим e_iNe_i. Имеем

$$e_iNe_i \cdot e_iNe_i = (e_iNe_i)^2 \subseteq e_iN^2e_i \subseteq N^2.$$

Поэтому если $(e_iNe_i)^2 \neq 0$, то $(e_iNe_i)^2$ также является идеалом кольца R. Поскольку кольцо R подпрямо неразложимо, заключаем, что только одно из e_iNe_j, $i \neq j$, или $(e_iNe_i)^2$ может быть неравным нулю. Из того, что $0 \neq N^2 \subseteq \subseteq pQ = p\Lambda_1$ и $(e_1Ne_1)^2 \subseteq e_1N^2e_1 \subseteq N^2$, следует, что только $(e_1Ne_1)^2$ может быть ненулевым, а все остальные e_iNe_j при $i \neq j$ и $(e_kNe_k)^2$ при $k \geqslant 2$ равны

нулю. Отсюда вытекает, что $N = e_1Ne_1 = eNe$. Тогда все слагаемые кольца Q (за исключением Λ_1) — простые кольца. Из $N^2 \neq (0)$ следует, что $e_1Ne_1 \neq 0$. Из того, что $N = e_1Ne_1$, следует, что слагаемые Λ_i и $M_2\big(GF(p^{s_j})\big)$ при $i = 2, \ldots, m$, $j = 1, \ldots, k$ являются идеалами кольца R, имеющими тривиальное пересечение с идеалом $p\Lambda_1 \neq (0)$. Отсюда следует, что все эти слагаемые равны нулю и кольцо R имеет вид

$$R = \Lambda + N, \tag{15}$$

где $\Lambda = \Lambda_1$, $e = e_1$, $N = eNe$, p — простое число, $p \neq 2$, $\Lambda = \mathbb{Z}[x]/\big(p^2, f(x)\big)$, $f = f_1(x)$ — неприводимый унитарный полином степени $r = \deg f$, $\operatorname{char}\Lambda = p^2$, $\operatorname{char} J(R) = \operatorname{char} N = p$, если $N \neq (0)$, то $0 \neq N^2 \subseteq p\Lambda$, $e_1 = e$ — единица кольца R, N — (Λ, Λ)-бимодуль, $N \subseteq J(R)$. □

Далее будем рассматривать А-кольцо R вида (10) с указанными в лемме 5 свойствами. Как отмечено во введении,

$$\Lambda = \mathbb{Z}[x]/\big(p^2, f(x)\big) = GR(p^2, p^{2r}).$$

Пусть Λ^* — группа обратимых элементов кольца Λ. Тогда в кольце Λ и группе Λ^* соответственно $|\Lambda| = p^{2r}$, $|\Lambda^*| = (p^r - 1) \cdot p^r$ элементов, Λ^* содержит единственную циклическую подгруппу $\Gamma(\Lambda) = \langle g \rangle$ порядка $p^r - 1$, порождённую обратимым элементом $g \in \Lambda$, и согласно (2) любой элемент $\lambda \in \Lambda$ имеет единственную запись вида

$$\lambda = g_1 + pg_2, \tag{16}$$

где $g_1, g_2 \in \langle g \rangle \cup \{0\}$.

В [5] показано, что группа автоморфизмов $\operatorname{Aut}(\Lambda)$ циклическая и порождается одним элементом σ порядка r, т. е. $\operatorname{Aut}(\Lambda) = \langle \sigma \rangle$, причём действие σ на элементы $\lambda \in \Lambda$ однозначно определяется образом $\sigma(g) = g^p$, и поэтому $\sigma^s(g) = g^{p^s}$ и $g^{p^r} = g$.

Согласно (16) любой элемент кольца Галуа Λ имеет вид $\lambda = \lambda_1 + p\lambda_2$, где $\lambda_1, \lambda_2 \in \langle g \rangle \cup \{0\}$. Поэтому для любых элементов $\lambda \in \Lambda$ и $x \in N$ справедливы равенства

$$\lambda x = (\lambda_1 + p\lambda_2)x = \lambda_1 x, \quad x\lambda = x(\lambda_1 + p\lambda_2) = x\lambda_1.$$

Рассмотрим $\bar{\Lambda} = \Lambda/J(\Lambda)$-модуль N. Тогда $\bar{\lambda} = \lambda + J(\Lambda) = \lambda_1 + J(\Lambda)$, и поэтому

$$\bar{\lambda}x = \big(\lambda_1 + J(\Lambda)\big)x = \lambda_1 x, \quad x\bar{\lambda} = x\big(\lambda_1 + J(\Lambda)\big) = x\lambda_1.$$

Отсюда следует, что N-(Λ, Λ)-бимодуль совпадает с N-$(\bar{\Lambda}, \bar{\Lambda})$-бимодулем, где $\bar{\Lambda} = \Lambda/J(\Lambda) \equiv GF(p^r)$ — поле. Поэтому N является $\big(GF(p^r), GF(p^r)\big)$-бипространством.

Как отмечено во введении, для (Λ, Λ)-бимодуля N существует отмеченный базис, являющийся Λ-базисом модулей ${}_\Lambda N$ и N_Λ. Пусть $a_1, a_2, \ldots, a_n$ — отмеченный базис (Λ, Λ)-бимодуля N. Тогда элементы $a_1, a_2, \ldots, a_n$ линейно независимы над $\bar{\Lambda}$. Предположим противное. Пусть $\bar{\lambda}_1 a_1 + \bar{\lambda}_2 a_2 + \ldots + \bar{\lambda}_n a_n = 0$, $\bar{\lambda}_i \in \bar{\Lambda}$ и $\lambda_i = g^{k_i} \neq 0$ хотя бы для одного i. Тогда a_i линейно выражается

через остальные элементы отмеченного базиса над Λ, так как $\bar{\lambda}_i = \lambda_i + J(\Lambda)$, $\bar{\lambda}_i a_i = \big(\lambda_i + J(\Lambda)\big)a_i = \lambda_i a_i$. Отсюда следует, что

$$0 = \bar{\lambda}_1 a_1 + \bar{\lambda}_2 a_2 + \ldots + \bar{\lambda}_n a_n = \lambda_1 a_1 + \lambda_2 a_2 + \ldots + \lambda_n a_n$$

в ${}_{\Lambda}N$. Из обратимости элемента λ_i в R следует, что это равенство противоречит несократимости базиса. Это показывает, что отмеченный базис (Λ, Λ)-бимодуля N является базисом $\big(GF(p^r), GF(p^r)\big)$-бипространства N и размерности пространств ${}_{\bar{\Lambda}}N$ и $N_{\bar{\Lambda}}$ совпадают с числом элементов отмеченного базиса (Λ, Λ)-бимодуля N. Это даёт нам право применить индукцию по размерности $GF(p^r)$ пространства N.

Лемма 6. *Пусть A-кольцо $R = \Lambda + N$ удовлетворяет всем условиям леммы* 5. *Тогда*

1) *для (Λ, Λ)-бимодуля N существует отмеченный базис $a_1, b_1, a_2, b_2, \ldots, a_d, b_d$, удовлетворяющий соотношениям*

$$a_i^2 = b_i^2 = 0, \quad a_i b_i = -b_i a_i = p \cdot 1, \quad a_i a_j = b_i b_j = a_j b_i = b_i a_j = 0 \quad \text{при} \quad i \neq j, \quad i, j = 1, 2, \ldots, d, \tag{17}$$

   где $e = 1$ — единица кольца Λ;
2) *пусть N_i — (Λ, Λ)-биподмодуль, порождённый элементами a_i, b_i отмеченного базиса, где $i = 1, 2, \ldots, d$. Тогда $N = N_1 \oplus N_2 \oplus \ldots \oplus N_d$;*
3) *Λ-модули ${}_{\Lambda}N$ и N_{Λ} совпадают, т. е. для любых $x \in N$ и $\lambda \in \Lambda$ имеет место равенство $x\lambda = \lambda x$.*

Доказательство. Докажем лемму индукцией по размерности $GF(p^r)$-пространства N. Если $N = \{0\}$, то утверждение очевидно. Пусть $N \neq \{0\}$. Согласно лемме 5 $0 \neq N^2 \subset p\Lambda$ и N не является идеалом кольца R. Более того, N не содержит ненулевого идеала кольца. Отсюда следует, что $\dim N \neq 1$. Если $\dim_{GF(p^r)} N = 1$ и $N = \Lambda a_1 = a_1 \Lambda$, где a_1 — отмеченный базис, то для любых $x, y \in N$ имеем, что $x = \lambda a_1$, $y = \mu a_1$ и $xy = (\lambda a_1)(\mu a_1) = \lambda \sigma_1(\mu) a_1^2 = 0$, т. е. $N^2 = (0)$, где $\sigma_1 \in \mathrm{Aut}(\Lambda)$. Это противоречит условию $0 \neq N^2 \subset p\Lambda$.

Пусть $\dim_{GF(p^r)} N = 2$, и пусть $a, b \in N$ — отмеченный Λ-базис. Из условия $0 \neq N^2 \subset p\Lambda$ и из леммы 1 следует, что $a^2 = 0$, $b^2 = 0$, $ab = -ba = ph$, где $h \in \Lambda^*$. Обозначим $a_1 = a$, $b_1 = h^{-1}b$. Тогда ясно, что $a_1^2 = 0$, $b_1^2 = 0$, $a_1 b_1 = = -b_1 a_1 = p \cdot 1$ и, кроме того, a_1 и b_1 составляют отмеченный базис. В самом деле,

$$a_1\lambda = a\lambda = \sigma_1(\lambda)a = \sigma_1(\lambda)a_1,$$
$$b_1\lambda = (h^{-1}b)\lambda = h^{-1}(b\lambda) = h^{-1}\sigma_2(\lambda)b = \sigma_2(\lambda)(h^{-1}b) = \sigma_2(\lambda)b_1,$$

где $\sigma_1, \sigma_2 \in \mathrm{Aut}(\Lambda)$.

Пусть $n = \dim_{GF(p^r)} N > 2$ и $\{a_1, a_2, \ldots, a_m\}$ — некоторый отмеченный базис для (Λ, Λ)-бимодуля N. Заметим, что N не содержит ненулевого идеала кольца R и согласно лемме 4 $N^2 \neq (0)$, $N \cap A\big(J(R)\big) = (0)$. Отсюда следует, что для элемента a_1 существует a_i из базисных элементов, такой что $a_1 a_i \neq 0$ и $i \neq 1$.

Действительно, предположим противное, пусть $a_1a_i = -a_ia_1 = 0$ для любого $i = 2, 3, \ldots, m$. Тогда подпространство $GF(p^r)a_1$ является идеалом кольца R, содержащимся в N, что противоречит подпрямой неразложимости кольца R. Значит, не нарушая общности, можем предполагать, что $i = 2$, $a_1a_2 = -a_2a_1 \neq 0$. Из условия $0 \neq N^2 \subseteq p\Lambda$ следует, что мы можем также предполагать, что $a_1a_2 = -a_2a_1 = p\cdot 1$, заменяя a_2 новым элементом из Λ, если необходимо. Обозначим $b_1 = a_2$ и получим новый базис $a_1, b_1, a_3, a_4, \ldots, a_m$, причём $a_1b_1 = -b_1a_1 = p\cdot 1$. Рассмотрим $a_1 \cdot a_i$, где $i \geqslant 3$. Если для некоторого элемента, например для a_i, $i \geqslant 3$, имеет место $a_1a_i = \lambda(p \cdot 1) \neq 0$, где $\lambda \in \Lambda$ и λ — обратимый элемент, то сделаем преобразование

$$a_1a_i = \lambda p \cdot 1 = \lambda a_1b_1 = a_1(\sigma_1^{-1}(\lambda)b_1)$$

и

$$a_1(a_i - \sigma_1^{-1}(\lambda)b_1) = 0 = -(a_i - \sigma_1^{-1}(\lambda)b_1)a_1,$$

где σ_1 — некоторый автоморфизм, т. е. $\sigma_1 \in \mathrm{Aut}(\Lambda)$. Заменяя элементы a_i элементом $a_i' = a_i - \lambda' b_1$, где $\lambda' = \sigma_1^{-1}(\lambda)$, получаем новый несократимый базис $a_1, b_1, a_3', a_4', \ldots, a_m'$ со свойствами $a_1b_1 = -b_1a_1 = p \cdot 1$, $a_1a_i' = -a_i' \cdot a_1 = 0$ для всех $i \geqslant 3$. Рассмотрим b_1a_i' при $i \geqslant 3$. Если $b_1a_i' = \mu p \neq 0$, где $\mu \in \Lambda$ — обратимый элемент, то применим преобразование

$$0 = b_1a_i' - \mu p \cdot 1 = b_1a_i' + \mu b_1a_1 = b_1(a_i' + \sigma_2^{-1}(\mu)a_1) = -(a_i' + \sigma_2^{-1}(\mu)a_1)b_1 = 0,$$

где $\sigma_2^{-1} \in \mathrm{Aut}(\Lambda)$ — некоторый автоморфизм.

Заменим элемент a_i' через $a_i'' = a_i' + \sigma_2^{-1}(\mu)a_1$ и эти новые элементы базиса также обозначим через a_i''. Тогда получаем, что $b_1a_i'' = a_i''b_1 = 0$ при $i \geqslant 3$. Эти a_i'' тоже аннулирует a_1, так как

$$a_1a_i'' = a_1(a_i' + \sigma_2^{-1}(\mu)a_1) = a_1a_i' + \sigma_1\big(\sigma_2^{-1}(\mu)\big)a_1^2 = 0 + 0 = 0.$$

Тем самым получаем новый несократимый базис $a_1, b_1, a_3'', a_4'', \ldots, a_m''$, удовлетворящий равенствам

$$a_1b_1 = -b_1a_1 = p_1 \cdot 1, \quad a_1a_i'' = -a_i''a_1 = b_1a_i'' = -a_i''b_1 = 0, \quad i > 2. \tag{18}$$

Заметим, что элементы a_1 и b_1 — элементы отмеченного базиса.

Покажем, что пространство N представимо в виде прямой суммы (Λ, Λ)-бимодулей:

$$N = \Lambda\langle a_1, b_1\rangle \oplus \Lambda\langle a_3'', \ldots, a_m''\rangle, \tag{19}$$

где $N_1 = \Lambda\langle a_1, b_1\rangle$ — $\langle\Lambda, \Lambda\rangle$-подмодуль, порождённый элементами a_1 и b_1, $N' = \Lambda\langle a_3'', \ldots, a_m''\rangle$ — (Λ, Λ)-бимодуль, порождённый элементами $a_3'', \ldots, a_m''$. Ясно, что $N = \Lambda\langle a_1, b_1\rangle + \Lambda\langle a_2'', \ldots, a_m''\rangle$. Пусть $x \in \Lambda\langle a_1, b_1\rangle \cap \Lambda\langle a_3'', \ldots, a_m''\rangle$. Тогда x представи́м в виде

$$x = \lambda_1a_1 + \mu_1b_1 = \lambda_3a_3'' + \cdots + \lambda_ma_m'', \tag{20}$$

где

$$\lambda_1, \lambda_3, \ldots, \lambda_m, \mu_1 \in \Gamma(\Lambda) \cup \{0\} = \langle g \rangle \cup \{0\}.$$

Из (20) и (18) вытекает, что $xa_1 = -p\mu_1 = 0$, $xb_1 = p\lambda_1 = 0$. Следовательно, $\mu_1 = 0$, $\lambda_1 = 0$. Тогда из (20) выводим равенство $\lambda_3 a_3'' + \ldots + \lambda_m a_m'' = 0$. Так как $a_3'', \ldots, a_m''$ — элементы несократимого базиса, то $\lambda_i = 0$, $i = 3, \ldots, m$. Это показывает, что N — прямая сумма (Λ, Λ)-бимодулей $\Lambda\langle a_1, b_1\rangle$ и $\Lambda\langle a_3'', \ldots, a_m''\rangle$.

Рассмотрим (Λ, Λ)-бимодуль N', являющийся $\big(GF(p^r), GF(p^r)\big)$-бипространством, такой что $\dim N' < \dim N$, $0 \neq (N')^2 \subset p\Lambda$. Пусть N' не содержит ненулевых идеалов кольца R. Тогда, как легко убедиться, подкольцо $R_1 = \Lambda + N'$ является A-кольцом. По предположению индукции в N' существует отмеченный базис $a_2, b_2, \ldots, a_d, b_d$, такой что

$$a_i^2 = b_i^2 = 0, \quad a_i b_i = -b_i a_i = p \cdot 1, \quad a_i b_j = a_j a_i = b_i b_j = 0$$

для всех $i \neq j$, где $i, j = 2, \ldots, d$, $2d = m$. Согласно предположению индукции $N' = N_2 \oplus \ldots \oplus N_d$, и следовательно, $N = N_1 \oplus N_2 \oplus \ldots \oplus N_d$. Этим доказано существование отмеченного базиса $a_1, b_1, a_2, b_2, \ldots, a_d, b_d$ для (Λ, Λ)-бимодуля N, удовлетворяющего соотношениям (17), и утверждения 1) и 2) леммы 6.

Докажем утверждение 3). Как отмечено выше, любой элемент $\lambda \in \Lambda$ представи́м в виде $\lambda = g_1 + pg_2$, где $g_1, g_2 \in \langle g \rangle \cup \{0\}$. Пусть $x \in N$. Тогда $x\lambda = xg_1 + xpg_2 = xg_1$, $\lambda x = g_1 x + pg_2 x = g_1 x + g_2(px) = g_1 x$. Значит, действие элемента Λ на N определяется действием элемента g. Рассмотрим a_i, b_i — парные элементы отмеченного базиса (Λ, Λ)-модуля N. Тогда

$$(a_i g)b_i = (\sigma_i(g)a_i)b_i = \sigma_i(g)p \cdot 1 = a_i(gb_i) = -(gb_i)a_i = -g(b_i a_i) = ga_i b_i = gp \cdot 1,$$

т. е. $\sigma_i(g)p \cdot 1 = gp \cdot 1$, где σ_i — автоморфизм кольца Галуа Λ. Как показано в [5, с. 200], из условия $p(\sigma_i(g) - g) = 0$, т. е. из того, что $\sigma_i(g) - g = g^{p^{s_i}} - g \in \in J(R)$, следует равенство $\sigma_i(g) = g^{p^{s_i}} = g$ для всех $i = 1, 2, \ldots, d$, где $s_i \leqslant r$. Это означает, что $a_i g = \sigma_i(g)a_i = ga_i$ для всех i. Аналогичное рассуждение также даёт, что $b_i g = gb_i$, т. е. левый Λ-модуль N и правый Λ-модуль N совпадают. Значит, $x\lambda = \lambda x$ для всех $x \in N$ и $\lambda \in \Lambda$. □

Предложение 1. *Всякое A-кольцо R с единицей, удовлетворяющее тождествам $p^2 x = 0$ и $x^3 f(x) + x^2 = 0$, где p — нечётное простое число, $f(x) \in \mathbb{Z}[x]$, представимо матрицами над некоторым коммутативным кольцом.*

Доказательство. Пусть $\operatorname{char} R = p^2$. Согласно леммам 5 и 6 кольцо R имеет вид $R = \Lambda + N$, где Λ — кольцо Галуа, $\operatorname{char}\Lambda = p^2$, $N \subseteq J(R)$, N — (Λ, Λ)-бимодуль.

Если $N = 0$, то утверждение доказано. Пусть $N \neq (0)$. Тогда $0 \neq N^2 \subset \subset p\Lambda$, $pJ(R) = 0$. Кроме того, согласно лемме 6 для N существует отмеченный (Λ, Λ)-базис, удовлетворяющий соотношениям (17). Представление кольца R определим как в [1]. Возьмём коммутативное локальное кольцо K с единицей

$$K = \Lambda\big\langle x_2^{(i)}, \ldots, x_p^{(i)}, y_2^{(i)}, \ldots, y_p^{(i)},\ i = 1, 2, \ldots, d \mid$$
$$px_j^{(i)} = py_j^{(i)} = 0,\ x_2^{(i)} \cdot y_2^{(i)} = \ldots = x_p^{(i)} \cdot y_p^{(i)} = p \cdot 1,$$
где 1 — единица кольца Галуа Λ,
$$\big(x_j^{(i)}\big)^2 = \big(y_j^{(i)}\big)^2 = x_j^{(i)} x_s^{(t)} = y_j^{(i)} y_s^{(t)} = x_j^{(i)} y_s^{(t)} = 0,\ \text{если } (i,j) \neq (s,t)\big\rangle.$$

Определим линейное отображение $\varphi\colon R = \Lambda + N \to K_p$, где K_p — кольцо $(p \times p)$-матриц над кольцом K:

$$\varphi(1) = E, \quad \varphi(a_i) = \sum_{j=2}^{p} x_j^{(i)} e_{1j} - \sum_{j=2}^{p} x_j^{(i)} e_{j1}, \quad \varphi(b_i) = -\sum_{j=2}^{p} y_j^{(i)} e_{1j} - \sum_{j=2}^{p} y_j^{(i)} e_{j1}.$$

Тогда

$$\varphi(a_i b_i) = \sum_{j=2}^{p} x_j^{(i)} y_j^{(i)} e_{jj} - (p^2 - p) e_{11} = pE = \varphi(a_i)\varphi(b_i),$$

$$\varphi(b_i a_i) = (p^2 - p) e_{11} + \sum_{j=2}^{p} (-x_j^{(i)} y_j^{(i)}) e_{jj} = -pE = -\varphi(b_i)\varphi(a_i).$$

Это отображение продолжается по линейности до отображения кольца R в K_p, и φ является искомым вложением. □

Доказательство теоремы 1. Представимость конечных нильпотентных колец этого многообразия следует из [4]. Для полупростого конечного кольца представимость его матрицами над коммутативным кольцом очевидна. Все подпрямо неразложимые кольца с ненулевым радикалом рассматриваемого многообразия, удовлетворяющего тождествам (3), описаны в леммах 2 и 6. Представимость их матрицами над некоторым коммутативным кольцом следует из следствия 4 и предложения 1. □

Доказательство следствия 1. Если многообразие $\mathfrak{M}$ удовлетворяет тождеству $nx = 0$ и $n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_m^{k_m}$ — каноническое разложение на простые числа, то любое конечное кольцо R из $\mathfrak{M}$ разлагается в прямую сумму

$$R = R_{p_1} \oplus R_{p_2} \oplus \ldots \oplus R_{p_m},$$

где R_{p_i} — кольца характеристики $p_i^{k_i}$, $i = 1, 2, \ldots, m$. Представимость кольца R теперь следует из теоремы 1. □

Доказательство следствия 2. Достаточно доказать представимость подпрямо неразложимых конечных колец, удовлетворяющих тождествам вида (4). Из тождества (4) при $x = y$ следует тождество вида $x^2 + x^3 h(x) = 0$. Кроме того, подпрямо неразложимое конечное кольцо также удовлетворяет тождеству вида $p^k x = 0$ для некоторого простого числа p. Поэтому каждое подпрямо неразложимое кольцо из рассматриваемого многообразия содержится в некотором многообразии, удовлетворяющем тождеству вида (3). При $p \neq 2$ представимость конечных колец рассматриваемого многообразия следует из теоремы 1. Пусть

$p = 2$. Тогда из тождества (4) следует, что во всех ниль-подкольцах кольца R, в том числе и в $J(R)$, выполняется тождество $xy = 0$. В этом случае также справедливы утверждения леммы 2, следствий 3 и 4. Значит, нам остаётся рассмотреть конечное A-кольцо R характеристики p^2 при $p = 2$. Как замечено выше в (9), согласно результатам [6] R имеет вид $R = Q + N$ и $J(R) = pQ + N$. Тогда из тождества $xy = 0$ следует, что $N^2 = 0 = pQ \cdot N = N \cdot pQ = 0$, $p \cdot J(R) = 0$, так как $p \cdot e \in J(R)$ и $p \cdot e \cdot a = pa = 0$ для любого $a \in J(R)$. Если $pQ \neq 0$, то в силу подпрямой неразложимости кольца R имеем, что $N = 0$ и подпрямо неразложимое кольцо $R = Q$ является кольцом матриц над кольцом Галуа. Тогда из (4) следует, что R совпадает либо с кольцом Галуа, либо с матричным кольцом $M_2(\Lambda)$, где Λ — конечное поле. Всё это означает, что при $p = 2$ подпрямо неразложимое A-кольцо также представимо матрицами над коммутативным кольцом. □

Нетрудно заметить, что подпрямо неразложимые кольца этого многообразия совпадают с критическими кольцами, которые описаны в [2].

Автор благодарен Ю. Н. Мальцеву и А. А. Нечаеву за обсуждение работы и полезные замечания.

Литература

[1] Мальцев Ю. Н. О представлении конечных колец матрицами над коммутативным кольцом // Мат. сб. — 1985. — Т. 128 (170), № 3 (11). — С. 383—402.

[2] Мекей А. О многообразиях, порождённых конечными ассоциативными кольцами, и свойствах экстремальности и критичности: Дис.. . . докт. физ.-мат. наук. — М., 1995.

[3] Нечаев А. А. Конечные кольца главных идеалов // Мат. сб. — 1973. — Т. 91 (33), № 3 (7). — С. 350—366.

[4] Bergman G. M., Britten D. J., Lemire F. W. Embedding rings in completed graded rings. III. Algebras over general k // J. Algebra. — 1983. — Vol. 84, no. 1. — P. 42—61.

[5] Raghavendran R. Finite associative rings // Compositio Math. — 1969. — Vol. 21, no. 2. — P. 195—229.

[6] Wilson R. S. On structure of finite rings. II // Pasific J. Math. — 1974. — Vol. 51, no. 1. — P. 317—325.