УДК 512.552.4

А.Н. Федорова

О тождествах кольца матриц второго порядка над кольцом Галуа

A.N. Fedorova

On the Identities of the Second Order Matrix Ring over Galois Ringк

В работе получено некоторое описание вида тождеств кольца матриц второго порядка над кольцом Галуа.

Ключевые слова: кольца с тождествами, многообразия колец, матрицы над конечными кольцами, кольца Галуа.

In this paper we obtain a certain description for identities of the second order matrix ring over a Galois ring.

Key words: rings with identities, varieties of rings, matrices over finite rings, Galois rings.

В работе [1] найден базис тождеств кольца матриц второго порядка над кольцом Галуа характеристики p^2. В настоящей работе исследуется строение тождеств кольца матриц второго порядка над кольцом Галуа характеристики p^n при произвольном натуральном $n \geq 3$.

Введем необходимые обозначения. Положим $R_p^{(m,n)} = M_2(GR(p^m, n))$ – кольцо матриц второго порядка над кольцом Галуа, $A_p^n = M_2(GF(p^n))$ – кольцо матриц второго порядка над конечным полем. Пусть, далее, многообразие $\mathcal{A}_p^{(m,n)} = \mathsf{var}\ R_p^{(m,n)}$ и $\mathcal{N}_p^{(m,n)}$ – нильпотентное подмногообразие $\mathcal{A}_p^{(m,n)}$.

Как обычно, $T(R)$ – идеал тождеств кольца R, $J(R)$ – радикал Джекобсона кольца R, $\mathcal{L}_R(S)$ – линейная оболочка множества S над кольцом R.

Утверждение 1. *Индекс нильпотентности многообразия $\mathcal{N}_p^{(m,n)}$ равен $2m$.*

Доказательство. В работе [2] показано, что многочлен

$$f_1(x,y) = (x - x^{q^2})(y - y^{q^2})(1 - [x,y]^{q-1}) \in T(A_p^n),$$

$q = p^n$.

Отсюда следует, что для любых элементов $a, b \in R_p^{(m,n)}$ $f_1(a,b) \in J(R_p^{(m,n)})$. Так как $J(R_p^{(m,n)})^m = 0$, то $\prod_{i=1}^m f_1(a_i, b_i) = 0$ для любых элементов $a_i, b_i \in R_p^{(m,n)}$ $(i = \overline{1,m})$. Следовательно,

$$g(\bar{x}, \bar{y}) = \prod_{i=1}^{m} f_1(x_i, y_i) \in T(R_p^{(m,n)}).$$

Многочлен g можно переписать в виде

$$g(\bar{x}, \bar{y}) = x_1 y_1 x_2 y_2 \dots x_m y_m + h(\bar{x}, \bar{y}),$$

где h – сумма одночленов степени $\geq 2m + 1$.

Поэтому для любого кольца $K \in \mathcal{N}_p^{(m,n)}$ выполняется равенство $K^{2m} = (0)$.

Покажем, что $x_1 \dots x_{2m-1} \notin T(\mathcal{N}_p^{(m,n)})$. Пусть элемент $a = e_{12} + pe_{21} \in R_p^{(m,n)}$. Тогда

$$a^2 = pe,$$

$$a^{2m-1} = a^{2(m-1)} \cdot a = (pe)^{m-1} \cdot a =$$

$$= p^{m-1}(e_{12} + pe_{21}) = p^{m-1} e_{12} \neq 0$$

и

$$a^{2m} = (pe)^m = p^m e = 0.$$

Таким образом, кольцо $K = \langle a \rangle \in \mathcal{N}_p^{(m,n)}$ и $x_1 \dots x_{2m-1} \notin T(K)$.

Утверждение 2. *Пусть F – свободное кольцо многообразия $\mathcal{N}_p^{(m,n)}$. Тогда характеристика кольца F^t при $t = \overline{1, 2m-1}$ равна $p^{m-[\frac{t}{2}]}$.*

Доказательство. Аналогично утверждению 1, $f_1(a,b) \in J(R_p^{(m,n)})$ для любых элементов $a, b \in R_p^{(m,n)}$. Следовательно,

$$g(\bar{x}, \bar{y}) = p^{m-k} \prod_{i=1}^{k} f_1(x_i, y_i) \in T(R_p^{(m,n)})$$

для любого $k = \overline{1, m-1}$. Многочлен g перепишем в виде

$$g(\bar{x}, \bar{y}) = p^{m-k} x_1 y_1 \dots x_k y_k + p^{m-k} h(\bar{x}, \bar{y}),$$

где h – сумма одночленов степени $\geq 2k+1$. Тогда

$$g_1(\bar{x}, \bar{y}) =$$

$$= p^{m-k} x_1 y_1 \dots x_k y_k + p^{m-k} h_1(\bar{x}, \bar{y}) \in T(R_p^{(m,n)})$$

для некоторого многочлена h_1, являющегося суммой одночленов степени $\geq 2m$.

Поэтому $p^{m-k}x_1y_1\dots x_ky_k \in T(\mathcal{N}_p^{(m,n)})$ и $p^{m-k}x_1y_1\dots x_ky_kx_{k+1} \in T(\mathcal{N}_p^{(m,n)})$. То есть

$$p^{m-[\frac{t}{2}]}x_1\dots x_t \in T(\mathcal{N}_p^{(m,n)}).$$

Покажем, что $p^{m-[\frac{t}{2}]-1}x_1\dots x_t \notin T(\mathcal{N}_p^{(m,n)})$. Пусть элемент $a = e_{12} + pe_{21} \in R_p^{(m,n)}$. Тогда

$$a^t = a^{2\cdot[\frac{t}{2}]}\cdot a^{t-2\cdot[\frac{t}{2}]} = p^{[\frac{t}{2}]}e\cdot a^{t-2\cdot[\frac{t}{2}]}.$$

Следовательно, если $t \equiv 0 \pmod 2$, то

$$p^{m-[\frac{t}{2}]-1}a^t = p^{m-[\frac{t}{2}]-1}\cdot p^{[\frac{t}{2}]}e = p^{m-1}e \neq 0,$$

а если $t \equiv 1 \pmod 2$, то

$$p^{m-[\frac{t}{2}]-1}a^t = p^{m-[\frac{t}{2}]-1}\cdot p^{[\frac{t}{2}]}a =$$

$$= p^{m-1}a = p^{m-1}e_{12} \neq 0.$$

Следовательно, кольцо $K = \langle a\rangle \in \mathcal{N}_p^{(m,n)}$ и

$$p^{m-[\frac{t}{2}]-1}x_1\dots x_t \notin T(K).$$

Лемма 1. *Пусть $(0) \neq K$ – нильпотентное подкольцо в A_p^n. Тогда $K \leq \mathcal{L}_{GF(q)}(a)$, где a – один из следующих элементов:* $\begin{pmatrix} 1 & \beta \\ -\beta^{-1} & -1 \end{pmatrix}$ *($\beta \in GF(q)$), e_{12}, e_{21}.*

Доказательство. В силу тождества $f_1(x,y) = 0$ кольца A_p^n, $K^2 = (0)$. Пусть $0 \neq a_1, a_2 \in K$. Тогда $a_1^2 = a_2^2 = 0$. Поэтому $\operatorname{tr} a_i = \det a_i = 0$ $(i = 1,2)$. Следовательно, элемент a_i $(i = 1,2)$ имеет один из видов: $\alpha_i e_{12}$, $\alpha_i e_{21}$ или $\alpha_i \cdot \begin{pmatrix} 1 & \beta_i \\ -\beta_i^{-1} & -1 \end{pmatrix}$ $(\alpha_i, \beta_i \in GF(q))$. Так как $a_1a_2 = 0$, то элементы a_1 и a_2 имеют одинаковый вид. Предположим, что

$$a_i = \alpha_i \begin{pmatrix} 1 & \beta_i \\ -\beta_i^{-1} & -1 \end{pmatrix} \ (i = 1,2).$$

Тогда

$$a_1a_2 = \alpha_1\alpha_2\cdot(\beta_2-\beta_1)\begin{pmatrix} \beta_2^{-1} & 1 \\ -(\beta_1\beta_2)^{-1} & -\beta_1^{-1} \end{pmatrix} = 0.$$

Поэтому $\beta_1 = \beta_2$ и $a_2 \in \mathcal{L}_{GF(q)}(a_1)$. Лемма доказана.

Пусть B_t – подмножество свободного кольца $\mathbb{Z}_{p^m}[x_1,\dots,x_t]$, состоящее из элементов вида

$$x_{\alpha(1)}\dots x_{\alpha(t)} - x_{\beta(1)}\dots x_{\beta(t)} \ (\alpha,\beta \in S_t)$$

таких, что

$$\{\alpha(i) \mid 1 \leq i \leq t, i \equiv 1(\bmod 2)\} =$$

$$= \{\beta(i) \mid 1 \leq i \leq t, i \equiv 1(\bmod 2)\}.$$

Имеет место следующая

Теорема 1. $B_{2m-1} \subset T(\mathcal{N}_p^{(m,n)})$.

Доказательство. Пусть элементы $a_1,\dots,a_{2m-1} \in R_p^{(m,n)}$ и кольцо $K = \langle a_1,\dots,a_{2m-1}\rangle \in \mathcal{N}_p^{(m,n)}$. Напомним, что

$$\overline{R_p^{(m,n)}} = R_p^{(m,n)}/J(R_p^{(m,n)}) \cong A_p^n$$

и $\bar{a}$ – образ элемента $a \in R_p^{(m,n)}$ при естественном гомоморфизме $R_p^{(m,n)} \to \overline{R_p^{(m,n)}}$. Так как кольцо K нильпотентно, то $\overline{K}$ – нильпотентное подкольцо в $\overline{R_p^{(m,n)}}$.

Если $\overline{K} = (0)$, то $K \subseteq J(R_p^{(m,n)})$ и $K^m = 0$. Поэтому $B_{2m-1} \subset T(K)$.

Пусть $\overline{K} \neq (0)$. Тогда, в силу леммы 1, $\overline{K} \leq \mathcal{L}_{GF(q)}(\bar{a})$ для некоторого элемента $a \in R_p^{(m,n)}$.

Предположим, что $\overline{K} \leq \mathcal{L}_{GF(q)}(e_{12})$ (случай, когда $\overline{K} \leq \mathcal{L}_{GF(q)}(e_{21})$, рассматривается аналогично). Тогда можно считать, что

$$a_i = \begin{pmatrix} p\alpha_{11}^i & \beta_i + p\alpha_{12}^i \\ p\alpha_{21}^i & p\alpha_{22}^i \end{pmatrix},$$

где $\alpha_{ke}^i, \beta_i \in GR(p^m,n)$ $(i = \overline{1,2m-1})$. Индукцией по m покажем, что

$$a_1\dots a_{2m-1} =$$

$$= \begin{pmatrix} 0 & p^{m-1}\beta_1\alpha_{21}^2\beta_3\alpha_{21}^4\dots\beta_{2m-3}\alpha_{21}^{2m-2}\beta_{2m-1} \\ 0 & 0 \end{pmatrix}.$$

Прямым вычислением можно показать, что $a_1a_2a_3 = \begin{pmatrix} 0 & p\beta_1\alpha_{21}^2\beta_3 \\ 0 & 0 \end{pmatrix}$. Предположим, что требуемое равенство выполнено при $m = k$. Проверим его истинность при $m = k+1$. Заметим, что

$$a_1a_2\dots a_{2k-1} =$$

$$= \begin{pmatrix} 0 & p^{k-1}\beta_1\alpha_{21}^2\dots\alpha_{21}^{2k-1}\beta_{2k-1} \\ 0 & 0 \end{pmatrix} + p^k b$$

для некоторого $b \in R_p^{(k+1,n)}$. Кроме того, $a_{2k}a_{2k+1} \in J(R_p^{(k+1,n)})$. Тогда

$$a_1a_2\dots a_{2k-1}a_{2k}a_{2k+1} =$$

$$= \begin{pmatrix} 0 & p^{k-1}\beta_1\alpha_{21}^2\dots\alpha_{21}^{2k-1}\beta_{2k-1} \\ 0 & 0 \end{pmatrix}\cdot a_{2k}\cdot a_{2k+1} =$$

$$= \begin{pmatrix} 0 & p^{k-1}\beta_1\alpha_{21}^2\dots\alpha_{21}^{2k-1}\beta_{2k-1} \\ 0 & 0 \end{pmatrix}\cdot$$

$$\cdot\begin{pmatrix} p\alpha_{11}^{2k} & \beta_{2k} + p\alpha_{12}^{2k} \\ p\alpha_{21}^{2k} & p\alpha_{22}^{2k} \end{pmatrix}\cdot a_{2k+1} =$$

$$= \begin{pmatrix} 0 & p^k\beta_1\alpha_{21}^2\dots\alpha_{21}^{2k-1}\beta_{2k-1}\alpha_{21}^{2k}\beta_{2k+1} \\ 0 & 0 \end{pmatrix}.$$

Таким образом, требуемое равенство выполняется для всех $m \geq 2$. Причем произведение элементов $a_1, \dots, a_{2m-1}$ не изменяется при перестановке сомножителей, имеющих одинаковую четность индекса. Следовательно, $B_{2m-1} \subset T(K)$.

Пусть $\overline{K} \leq \mathcal{L}_{GF(q)}(\bar{a})$, где $a = \begin{pmatrix} 1 & \beta \\ -\beta^{-1} & -1 \end{pmatrix}$ $(\beta \in GR(p^m, n))$. Тогда можно считать, что $a_i = \alpha_i a + pb_i$, где $\alpha_i \in GR(p^m, n)$, $b_i \in R_p^{(m,n)}$. Заметим, что $a^2 = 0$ и $p^m R_p^{(m,n)} = (0)$. Поэтому

$$a_1 \dots a_{2m-1} =$$

$$= \prod_{i=1}^{2m-1} (\alpha_i a + pb_i) =$$

$$= \alpha_1 a \cdot pb_2 \cdot \alpha_3 a \cdot pb_4 \dots pb_{2m-2} \cdot \alpha_{2m-1} a =$$

$$= \prod_{i=1}^{m} \alpha_{2i-1} \cdot p^{m-1} \cdot ab_2 ab_4 \dots ab_{2m-2} a.$$

Пусть $b_i = (\gamma_{kj}^i)$ $(\gamma_{kj}^i \in GR(p^m, n))$. Тогда

$$ab_i = \begin{pmatrix} \delta_i & \epsilon_i \\ -\delta_i/\beta & -\epsilon_i/\beta \end{pmatrix},$$

где $\delta_i = \gamma_{11}^i + \beta\gamma_{21}^i$, $\epsilon_i = \gamma_{12}^i + \beta\gamma_{22}^i$.

По индукции легко показать, что

$$ab_2 ab_4 \dots ab_{2m-2} a = \prod_{i=1}^{m-1} (\delta_{2i} - (\epsilon_{2i}/\beta)) \cdot a.$$

То есть

$$a_1 \dots a_{2m-1} = \prod_{i=1}^{m} \alpha_{2i-1} \cdot p^{m-1} \cdot \prod_{i=1}^{m-1} (\delta_{2i} - (\epsilon_{2i}/\beta)) \cdot a.$$

Как и в предыдущем случае, произведение элементов $a_1, \dots, a_{2m-1}$ не изменяется при перестановке сомножителей, имеющих одинаковую четность индекса. Следовательно, $B_{2m-1} \subset T(K)$.

Таким образом, $B_{2m-1} \subset T(K)$ для любого нильпотентного кольца $K \leq R_p^{(m,n)}$. Так как многообразие $\mathcal{N}_p^{(m,n)}$ порождается нильпотентными подкольцами кольца $R_p^{(m,n)}$, то $B_{2m-1} \subset T(\mathcal{N}_p^{(m,n)})$.

Лемма 2. *Пусть полилинейный многочлен $f(x_1, \dots, x_{2m-1}) \in T(\mathcal{N}_p^{(m,n)})$. Тогда $f \in \mathcal{L}_{\mathbb{Z}_{p^m}}(B_{2m-1}) + p\mathcal{L}_{\mathbb{Z}_{p^m}}(x_{\sigma(1)} \dots x_{\sigma(2m-1)} | \sigma \in S_{2m-1})$.*

Доказательство. Пусть $f(x_1, \dots, x_{2m-1}) = \sum_{\sigma \in S_{2m-1}} \alpha_\sigma x_{\sigma(1)} \dots x_{\sigma(2m-1)}$. Определим отношение эквивалентности на множестве подстановок S_t $(3 \leq t \leq 2m-1)$, положив $\alpha \sim \beta$ $(\alpha, \beta \in S_t)$, если многочлен

$$x_{\alpha(1)} \dots x_t - x_{\beta(1)} \dots x_{\beta(t)} \in B_t.$$

Обозначим через M_t некоторое множество представителей классов эквивалентности, содержащее тождественную подстановку e. Тогда многочлен f можно представить в виде

$$f(x_1, \dots, x_{2m-1}) =$$

$$= g(x_1, \dots, x_{2m-1}) + \sum_{\sigma \in M_{2m-1}} \beta_\sigma x_{\sigma(1)} \dots x_{\sigma(2m-1)},$$

где $g \in \mathcal{L}_{\mathbb{Z}_{p^m}}(B_{2m-1})$, $\beta_\sigma \in \mathbb{Z}_{p^m}$.

Заметим, что $g \in T(\mathcal{N}_p^{(m,n)})$. Тогда

$$h(x_1, \dots, x_{2m-1}) =$$

$$\sum_{\sigma \in M_{2m-1}} \beta_\sigma x_{\sigma(1)} \dots x_{\sigma(2m-1)} \in T(\mathcal{N}_p^{(m,n)}).$$

Пусть $a_i = \begin{pmatrix} p\alpha_{11}^i & \beta_i + p\alpha_{12}^i \\ p\alpha_{21}^i & p\alpha_{22}^i \end{pmatrix}$, где $\alpha_{ke}^i, \beta_i \in GR(p^m, n)$ $(i = \overline{1, 2m-1})$.

Как и в теореме 1, кольцо $K = \langle a_1, \dots, a_{2m-1} \rangle \in \mathcal{N}_p^{(m,n)}$. Следовательно,

$$h(a_1, \dots, a_{2m-1}) = \sum_{\sigma \in M_{2m-1}} \beta_\sigma a_{\sigma(1)} \dots a_{\sigma(1)} = 0.$$

Положим $\alpha_{21}^{2i} = 1$ $(i = \overline{1, m-1})$, $\alpha_{21}^{2i-1} = 0$ $(i = \overline{1, m})$, $\beta_i = 1$ $(i = \overline{1, 2m-1})$. Тогда

$$a_1 \dots a_{2m-1} = p^{m-1} e_{12}$$

и

$$a_{\sigma(1)} \dots a_{\sigma(2m-1)} = 0$$

при $\sigma \neq e$. Поэтому

$$0 = h(a_1, \dots, a_{2m-1}) = \beta_e p^{m-1} e_{12}.$$

Таким образом, $\beta_e \equiv 0 \pmod{p}$. Аналогично получаем, что $\beta_\sigma \equiv 0 \pmod{p}$ для любой подстановки $\sigma \in M_{2m-1}$.

Теорема 2. *Пусть полилинейный многочлен $f(x_1, \dots, x_t) \in T(\mathcal{N}_p^{(m,n)})$ $(3 \leq t \leq 2m-1)$. Тогда $f \in \mathcal{L}_{\mathbb{Z}_{p^m}}(B_t) + p\mathcal{L}_{\mathbb{Z}_{p^m}}(x_{\sigma(1)} \dots x_{\sigma(t)} | \sigma \in S_t)$.*

Доказательство. Как и в доказательстве леммы 2, многочлен f можно представить в виде

$$f(x_1, \dots, x_t) = g(x_1, \dots, x_t) + \sum_{\sigma \in M_t} \beta_\sigma x_{\sigma(1)} \dots x_{\sigma(t)},$$

где $g \in \mathcal{L}_{\mathbb{Z}_{p^m}}(B_t)$.

Далее многочлен

$$h = f \cdot x_{t+1} \dots x_{2m-1} \in T(\mathcal{N}_p^{(m,n)}).$$

Тогда многочлен

$$r(x_1, \dots, x_t) =$$

$$= \sum_{\sigma \in M_t} \beta_\sigma x_{\sigma(1)} \dots x_{\sigma(t)} x_{t+1} \dots x_{2m-1} \in T(\mathcal{N}_p^{(m,n)}).$$

В силу леммы 2, $\beta_\sigma \equiv 0 \pmod p$ для любого $\sigma \in M_t$.

Из теоремы 2 очевидным образом вытекает

Следствие 1. *Пусть многочлен* $f(x_1, \dots, x_t) \in T(\mathcal{A}_p^{(m,n)})$ $(3 \le t \le 2m-1)$ *представим в виде*

$$f(x_1, \dots, x_t) = g(x_1, \dots, x_t) + h(x_1, \dots, x_t),$$

где g *– полилинейный многочлен; а* h *– сумма одночленов степени* $\ge 2m$. *Тогда* $g \in \mathcal{L}_{\mathbb{Z}_{p^m}}(B_t) + p\mathcal{L}_{\mathbb{Z}_{p^m}}(x_{\sigma(1)} \dots x_{\sigma(t)} | \sigma \in S_t)$.

Библиографический список

1. Олексенко А.Н. Базис тождеств алгебры матриц второго порядка над $GR(p^2, n)$ // Известия Алтайского государственного университета. – 2000. – №1.
2. Мальцев Ю.Н., Кузьмин Е.Н. Базис тождеств алгебры матриц второго порядка над конечным полем // Алгебра и логика. – 1978. – №1.