

## ТОЖДЕСТВА КОНЕЧНОЙ АЛГЕБРЫ КЭЛИ-ДИКСОНА

И. М. ИСАЕВ

К. А. Жевлаков в "Днестровской тетради" сформулировал следующую проблему: найти базис тождеств алгебры Кэли-Диксона  $C(F)$  над полем  $F$  [1, вопрос 55]. В случае конечного поля  $F = GF(p^n)$  существование конечного базиса таких тождеств следует из теоремы И. В. Львова о кроссовости многообразия, порожденного конечным альтернативным кольцом [2]. Заметим, что алгебра Кэли-Диксона над конечным полем является расщепляемой, т. е. матричной (см. [3, с. 62]). В качестве подалгебры она содержит алгебру  $M_2(F)$  матриц второго порядка над полем  $F$ . Базис тождеств алгебры  $M_2(F)$  в случае, когда  $F = GF(p^n)$ , построен в [4]. В настоящей работе указывается явный вид образующих идеала тождеств алгебры Кэли-Диксона  $A = C(GF(q))$ ,  $q = p^n$ , которые в определенном смысле близки к тождествам из [4]. Доказана следующая

ТЕОРЕМА. Идеал тождеств алгебры  $A$  порождается многочленами  $f_1(x)$ ,  $f_2(x, y)$ ,  $f_3(x, y, z)$ , где

$$f_1(x) = (x - x^q)(x - x^{q^2}),$$

$$f_2(x, y) = (x - x^q)(y - y^q) - [(x - x^q)(y - y^q)]^q,$$

$$f_3(x, y, z) = g_1(x, y, z)g_2(y, z)g_3(x, y, z),$$

$$g_1(x, y, z) = (x - x^q)[(y - y^{q^2})(z - z^{q^2})],$$

$$g_2(y, z) = (1 - y^{q^2 - q})(1 - z^{q^2 - q})(1 - (y \cdot z)^{q - 1}),$$

$$g_3(x, y, z) = (1 - (x \cdot y)^{q^2 - q})(1 - (x \cdot z)^{q^2 - q})(1 - (x \cdot y \cdot z)^{q^2 - q}),$$

$x \circ y = xy + yx$  и расстановка скобок в  $f_3, g_2, g_3$  произвольная.

Алгебру  $\mathcal{A}$  мы будем рассматривать как кольцо характеристики  $p$  или, что то же самое, как алгебру над простым подполем  $GF(p)$  поля  $GF(q)$ .

Перечислим известные свойства расщепляемых алгебр Кэли-Диксона, которые нам понадобятся в дальнейшем.

Алгебра  $\mathcal{A} = C(F)$  обладает базисом  $\{e_1, e_2, u_1, u_2, u_3, v_1, v_2, v_3\}$ ,

где  $e_1, e_2$  - ортогональные идемпотенты,  $e_i u_i = u_i e_i = u_i$ ,

$v_i e_1 = e_2 v_i = v_i$ ,  $u_i v_i = e_1$ ,  $v_i u_i = e_2$  ( $i=1, 2, 3$ );  $u_i u_j = v_k = -u_j u_i$ ,  
 $v_i v_j = -u_k = -v_j v_i$  при  $(i, j, k) = (1, 2, 3), (2, 3, 1), (3, 1, 2)$ ; остальные произведения базисных элементов равны 0.

Элемент  $1 = e_1 + e_2$  является единицей алгебры  $C(F)$ , мы отождествляем его с единицей поля  $F$ . Алгебра  $\mathcal{A}$  квадратична: любой ее элемент  $x$  удовлетворяет уравнению

$$x^2 - t(x)x + n(x) = 0, \quad (1)$$

где  $t$  и  $n$  - линейная и квадратичная функции  $\mathcal{A} \rightarrow F$  (след и норма элемента  $x$ ). Если

$$x = \alpha e_1 + \beta e_2 + \sum_{i=1}^3 (\alpha_i u_i + \beta_i v_i),$$

то

$$t(x) = \alpha + \beta, \quad n(x) = \alpha\beta - \sum_{i=1}^3 \alpha_i \beta_i.$$

Уравнение (1) называется характеристическим уравнением для  $x$ . Если  $t(x) = 0$ , то  $x^2 = -n(x) \in F$ ; линейризация этого соотношения показывает, что если  $t(x) = t(y) = 0$ , то  $x \circ y \in F$ .

Подалгебра в  $\mathcal{A}$ , натянутая на элементы  $e_1, e_2, u_1, v_1$ , очевидно изоморфна  $M_2(F)$ ; соответствующий изоморфизм определяется отображением  $e_i \rightarrow e_{ii}$ ,  $u_1 \rightarrow e_{12}$ ,  $v_1 \rightarrow e_{21}$ .

Максимальные нильпотентные подалгебры в  $\mathcal{A}$  имеют размерность 3, одной из них является подалгебра с базисом  $\{u_1, u_2, u_1 u_2 = v_3\}$ . Все они изоморфны между собой, и любой изоморфизм максимальных нильпотентных подалгебр продолжается до автоморфизма алгебры  $\mathcal{A}$  (см. [6]).

Пусть  $\bar{F} = GF(q^2)$  - расширение степени 2 поля  $F$ ,  $\bar{\mathcal{A}} = C(\bar{F}) \cong \mathcal{A} \otimes_F \bar{F}$  - алгебра Кэли-Диксона над  $\bar{F}$  с тем же базисом, что и  $\mathcal{A}$ ;

алгебра  $\mathcal{A}$  естественным образом вложена в  $\bar{\mathcal{A}}$ .

ЛЕММА 1. Если  $a \in \mathcal{A}$ , то либо  $a = \lambda_1 \bar{e}_1 + \lambda_2 \bar{e}_2$ , где  $\lambda_1, \lambda_2 \in \bar{F}$ ,  $\bar{e}_1, \bar{e}_2$  — ортогональные идемпотенты в  $\bar{\mathcal{A}}$ ,  $\lambda_1 \neq \lambda_2$ ,  $\bar{e}_1 + \bar{e}_2 = 1$ , либо  $a = \lambda + u$ , где  $\lambda \in F$ ,  $u^2 = 0$ .

ДОКАЗАТЕЛЬСТВО. Пусть  $a \notin F$ . Рассмотрим двумерную подалгебру  $\langle a \rangle_F$  в  $\mathcal{A}$  с базисом  $\{1, a\}$ . Если  $\langle a \rangle_F$  полупроста, то, так как поле  $F$  совершенно, алгебра  $\langle a \rangle_F$  также полупроста,  $\langle a \rangle_F = \bar{F}\bar{e}_1 \oplus \bar{F}\bar{e}_2$ , откуда  $a = \lambda_1 \bar{e}_1 + \lambda_2 \bar{e}_2$ , где  $\lambda_1, \lambda_2$  — корни характеристического многочлена  $\lambda^2 - t(a)\lambda + n(a)$  элемента  $a$ . При  $\lambda_1 = \lambda_2 = \lambda$  получаем  $a = \lambda \in \bar{F} \cap \mathcal{A} = F$ . Если  $\langle a \rangle_F$  имеет ненулевой радикал, то в  $\langle a \rangle_F$  можно выбрать базис  $\{1, b\}$ , где  $b^2 = 0$ , откуда  $a = \lambda + \mu b = \lambda + u$ .

Обозначим через  $\mathcal{M}$  многообразие альтернативных алгебр над полем  $GF(p)$ , удовлетворяющих тождествам  $f_1 = f_2 = f_3 = 0$ .

ПРЕДЛОЖЕНИЕ 1.  $\text{Var } \mathcal{A} \subseteq \mathcal{M}$ .

ДОКАЗАТЕЛЬСТВО. Пусть  $x \in \mathcal{A}$ . Если  $x = \lambda_1 \bar{e}_1 + \lambda_2 \bar{e}_2$  ( $\lambda_1, \lambda_2 \in \bar{F}$ ), то  $x - x^q = 0$ . Если же  $x = \lambda + u$  ( $\lambda \in F$ ,  $u^2 = 0$ ), то  $x^q = \lambda^q + u^q = \lambda^q = \lambda = x^q$ , откуда  $x - x^q = x - x^{q^2} = u$ . В обоих случаях  $f_1(x) = 0$ . Если  $x, y \in \mathcal{A}$  и  $t(x) = t(y) = 0$ , то, как отмечалось выше,  $x \circ y \in F$ , откуда  $h(x, y) = x \circ y - (x \circ y)^q = 0$ . Так как для любых  $x, y \in \mathcal{A}$  элементы  $x - x^q$ ,  $y - y^q$  имеют след 0, то подстановка  $x \rightarrow x - x^q$ ,  $y \rightarrow y - y^q$  в  $h(x, y)$  дает соотношение

$$f_2(x, y) = 0.$$

Покажем, что при любом выборе элементов  $x, y, z \in \mathcal{A}$  одна из функций  $g_1(x, y, z)$ ,  $g_2(y, z)$ ,  $g_3(x, y, z)$  обращается в нуль. Как и выше, замечаем, что если  $g_1(x, y, z) \neq 0$ , то  $y = \lambda + u$ ,  $z = \mu + v$  для некоторых  $\lambda, \mu \in F$ ,  $u^2 = v^2 = 0$ , причем

$$(y - y^{q^2})(z - z^{q^2}) = uv \neq 0.$$

Так как  $y^q = \lambda$ ,  $z^q = \mu$ , то условие  $g_2(y, z) \neq 0$  влечет  $(1 - \lambda^{q-1}) \times (1 - \mu^{q-1}) \neq 0$ . Но тогда  $\lambda = \mu = 0$ , в частности,  $t(y) = t(z) = 0$ , откуда  $y \circ z \in F$ , и условие  $1 - (y \circ z)^{q-1} \neq 0$  влечет  $y \circ z = 0$ . Учитывая,

что  $y^2 = x^2 = 0$ ,  $yz \neq 0$ , находим, что элементы  $y, x, yz$  образуют базис 3-мерной нильпотентной подалгебры в  $\mathcal{A}$ . Без ограничения общности можем положить  $y = u_1$ ,  $x = u_2$ ,  $yz = v_3$ . Если  $x = \alpha e_1 + \beta e_2 + \sum_i \alpha_i u_i + \sum_i \beta_i v_i$ , то  $x \circ y = \beta_1 + (\alpha + \beta) u_1$ ,  $x \circ x = \beta_2 + (\alpha + \beta) u_2$ ,  $x \circ yz = \alpha_3 + (\alpha + \beta) v_3$  и условие  $g_3(x, y, z) \neq 0$  влечет  $\beta_1 = \beta_2 = \alpha_3 = 0$ . Но тогда  $t(x) = \alpha + \beta$ ,  $n(x) = \alpha\beta$ , и характеристический многочлен для  $x$  имеет вид  $\lambda^2 - (\alpha + \beta)\lambda + \alpha\beta = (\lambda - \alpha)(\lambda - \beta)$ . Следовательно, при  $\alpha \neq \beta$  элемент  $x$  приводится к виду  $\alpha e'_1 + \beta e'_2$ , где  $e'_1, e'_2$  — ортогональные идемпотенты алгебры  $\mathcal{A}$ . Отсюда  $x - x^2 = 0$ ,

$g_1(x, y, z) = 0$ . Если же  $\alpha = \beta$ , то  $x - x^2 = \alpha u_1 + \alpha u_2 + \beta v_3$ , и снова  $g_1(x, y, z) = (x - x^2)v_3 = 0$ .

ПРЕДЛОЖЕНИЕ 2.  $\mathcal{M} \subseteq \text{Var } \mathcal{A}$ .

ДОКАЗАТЕЛЬСТВО. Многообразие  $\mathcal{M}$  имеет конечный индекс и экспоненту. По теореме И. В. Львова [2],  $\mathcal{M}$  кроссово, в частности,  $\mathcal{M}$  порождается конечным числом критических алгебр, которые, в свою очередь, конечны. Напомним, что алгебра называется критической, если она не лежит в многообразии, порожденном ее собственными подалгебрами и гомоморфными образами; любая критическая алгебра подпрямно неразложима. Для доказательства предложения 2 достаточно установить, что всякая критическая алгебра из  $\mathcal{M}$  вложима в  $\mathcal{A}$ .

Если  $N$  — нильпотентная алгебра из  $\mathcal{M}$ , то из тождеств  $f_1 = f_3 = 0$  получаем, что  $N$  удовлетворяет тождествам  $x^2 = 0$ ,  $xyz = 0$ , так что  $N$  фактически будет ассоциативной алгеброй. Легко понять, что имеется всего две критических алгебры  $N$ : одномерная алгебра с нулевым умножением и 3-мерная алгебра с порождающими  $x, y$  и определяющими соотношениями  $x^2 = y^2 = x \circ y = 0$ . Обе они очевидным образом вкладываются в  $\mathcal{A}$ .

Если  $R$  — простая алгебра из  $\mathcal{M}$ , то  $R$  изоморфна либо  $M_k(GF(p^t))$ , либо алгебре Кэли-Диксона  $C(GF(p^t))$ . Покажем, что  $k \leq 2$ . Действительно, если  $k \geq 3$ , то  $M_k(GF(p^t))$  содержит нильпотентную подалгебру, порожденную матрицами  $e_{12}, e_{23}$ , которая не удовлетворяет тождеству  $f_2 = 0$ , в частности,  $f_2(e_{12}, e_{23}) = e_{13} \neq 0$ . Если  $k = 2$ , то равенство  $f_2(\alpha e_{11}, e_{12}) = (\alpha - \alpha^2)e_{12} = 0$  влечет  $\alpha - \alpha^2 = 0$  для любого  $\alpha \in GF(p^t)$ , откуда  $GF(p^t) \subseteq GF(q) = F$ . Так как  $M_2(GF(p^t)) \subseteq C(GF(p^t))$ ,

то при  $R = C(GF(p^t))$  снова имеем  $GF(p^t) \subseteq F$ . Таким образом, простые алгебры вида  $M_2(GF(p^t))$  и  $C(GF(p^t))$ , лежащие в  $\mathcal{M}$ , вкладываются в  $\mathcal{A}$ . Если же  $R = GF(p^t)$ , то из тождества  $f_1(x) = 0$  следует, что  $GF(p^t) \subseteq GF(q^s) = \bar{F}$ . Рассматривая  $\bar{F}$  как двумерную алгебру над  $F$  и используя ее регулярное представление, получаем вложение

$$\bar{F} \subset M_2(F) \subset \mathcal{A}.$$

Пусть теперь  $R$  - критическая алгебра из  $\mathcal{M}$ , имеющая вид  $R = B + N$ , где  $B$  - полупростая подалгебра,  $N$  - радикал,  $B \neq 0, N \neq 0$ . Тогда  $B = B_1 \oplus \dots \oplus B_s$ , где  $B_i$  - простые алгебры из  $\mathcal{M}$ . Заметим, прежде всего, что среди  $B_i$  нет алгебр, изоморфных  $C(GF(p^t))$ . В самом деле, если  $B_i = C(GF(p^t))$ , то, выбирая в  $B_i$  нильпотентные подалгебры  $U$ , скажем,  $U = (u_1, u_2, u_3)_F$ , будем иметь, что  $U + N$  - нильпотентная подалгебра в  $R$ , откуда  $U^2 N = N U^2 = 0$ , в частности,  $u_3 = u_1 u_2 \in \text{Ann}_R N$ . Так как  $\text{Ann}_R N \triangleleft R$ , то  $B_i \subseteq \text{Ann}_R N$ ,  $B_i N = N B_i = 0$ . Но тогда  $B_i \triangleleft R$  и  $B_i \cap N = 0$ , что противоречит подпрямой неразложимости алгебры  $R$ .

Пусть  $e$  - произвольный идемпотент из  $R$ . Так как операторы правого и левого умножения на  $e$  в  $R$  - перестановочные идемпотентные операторы, то  $R$  разлагается в прямую сумму подпространств

$$R_{ij} = \{x \in R \mid ex = ix, xe = jx\}, \quad i, j = 0, 1.$$

Это так называемое пирсовское разложение алгебры  $R$  относительно идемпотента  $e$ . Аналогичное разложение допускает любое подпространство, инвариантное относительно умножения на  $e$  слева и справа. Хорошо известно, что перемножение пирсовских компонент  $R_{ij}$  в альтернативных алгебрах подчиняется следующим правилам:

$$R_{ij} R_{jk} \subseteq R_{ik}; \quad R_{ij}^2 \subseteq R_{ji} \quad (i+j=1); \quad R_{ij} R_{kl} = 0 \quad (j \neq k, (i, j) \neq (k, l)).$$

Кроме того,  $x^2 = 0$  для любого  $x \in R_{ij}$ , где  $i+j=1$ .

Пусть  $e_k$  - единица подалгебры  $B_k$  ( $1 \leq k \leq s$ ),  $P = N \cap \text{Ann}_R N$ . Так как  $\text{Ann}_R N \triangleleft R$ , то  $P \triangleleft R$ . Обозначим через  $P_{ij}^{(k)} (R_{ij}^{(k)})$

пирсовскую  $(i, j)$ -компоненту идеала  $P$  (алгебры  $R$ ) относительно идемпотента  $e_k$ . Так как  $N$  - нильпотентный идеал, то  $P \neq 0$ ,  $P \supseteq N^2$ .

ЛЕММА 2.  $P = P_{ij}^{(k)}$  для некоторой пары  $(i, j) \neq (0, 0)$ .

ДОКАЗАТЕЛЬСТВО. Так как  $B \subseteq R_{00}^{(k)} + R_{11}^{(k)}$ , то  $P_{ij}^{(k)}$  выдерживает умножение на  $B$  (слева и справа). Кроме того,  $PN = NP = 0$ , следовательно,  $P_{ij}^{(k)} \triangleleft R$ , и из неразложимости алгебры  $R$  следует, что  $P = P_{ij}^{(k)}$  для некоторых  $i, j$ . Предположим, что  $e_k P = P e_k = 0$ . Используя стандартные обозначения для ассоциаторов  $(a, b, c) = (ab)c - a(bc)$  и антикоммутативность умножения в  $N$ , получаем, что для любых элементов  $a \in R, n_1, n_2 \in N$  имеют место соотношения

$$\begin{aligned} (n_1, n_2)a &= n_1(n_2 a) + (n_1, n_2, a) = -(n_2 a)n_1 + (n_1, n_2, a) = \\ &= -n_2(an_1) - (n_2, a, n_1) + (n_1, n_2, a) = -n_2(an_1) = (an_1)n_2 \end{aligned}$$

и аналогично  $a(n_1, n_2) = n_1(n_2 a)$ . Так как  $N^2 \subseteq P$ , то  $e_k N^2 = N^2 e_k = 0$ , откуда  $e_k N + N e_k \subseteq P$ . Но тогда  $e_k(e_k N) = e_k N \subseteq e_k P = 0$  и  $N e_k = 0$ . Так как  $\text{Ann}_R N \triangleleft R$ , то  $B_k \subseteq \text{Ann}_R N$ , а это противоречит неразложимости алгебры  $R$ .

Если  $s > 1$ ,  $B \supset B_{k'}, k' \neq k$ , то из включения  $e_{k'} \in R_{00}^{(k)}$  следует, что либо  $P = P_{10}^{(k)} = P_{01}^{(k')}$ , либо  $P = P_{01}^{(k)} = P_{10}^{(k')}$ . Таким образом, имеет место следующая дихотомия:

ЛЕММА 3. Л и б о  $B = B_1, P = P_{ij}^{(1)}, (i, j) \neq (0, 0)$ , л и б о  $B = B_1 \oplus B_2, P = P_{10}^{(1)} = P_{01}^{(2)}$ .

СЛУЧАЙ 1. Одна из подалгебр  $B_i$ , скажем,  $B_1$  изоморфна  $M_2(K)$ ,  $K \in F, \{e_{ij} \mid i, j = 1, 2\}$  - стандартный базис алгебры  $B_1$ . Так как  $\langle e_{12}, N \rangle$  - нильпотентная подалгебра в  $R$ , то  $e_{12} \circ n = 0$  для любого  $n \in N$  и аналогично  $e_{21} \circ n = 0$ , откуда  $a \circ n = 0$ , где  $a = e_{12} + e_{21}$ . Умножая это соотношение на  $a$  слева и справа, получаем  $a^2 n = -ana = na^2$  или  $en = ne$ , где  $e = a^2$  - единица алгебры  $B_1$ . Таким образом,  $P = P_{11}^{(1)}$ , откуда  $s = 1, B = B_1$ . Так как  $e_{ij} N^2 = 0$ ,

$(i, j) = (1, 2), (2, 1)$ , то  $aN^2 = 0$ ,  $eN^2 = 0$ , следовательно,  $N^2 = 0$ ,  $N = P$ -унитарный  $B$ -бимодуль (в категории альтернативных колец).

Отождествим элементы  $\alpha \in K$  с  $\alpha e \in B$ ; таким образом,  $1 \in K$  - единица алгебры  $R$ . Из тождеств Муфанг следует, что в любой альтернативной алгебре верно тождество

$$(x^n, y, z) = \sum_{i=0}^{n-1} x^i (x, y, z) x^{n-1-i} = (x, \sum_{i=0}^{n-1} x^{n-1-i} y x^i, z).$$

В частности, для любых  $\alpha \in K$ ,  $\beta \in B$ ,  $u \in N$  имеет место  $(\alpha, \beta, u) = (\alpha^q, \beta, u) = q(\alpha, \alpha^{q-1}\beta, u) = 0$  (напомним, что  $K \in F = GF(q)$ ). Далее,

$$\alpha e_{12} u = e_{12} \alpha u = e_{12} \alpha u = -u \cdot \alpha e_{12} = -u \alpha \cdot e_{12} = e_{12} \cdot u \alpha. \text{ Аналогично } e_{21} \alpha u = e_{21} \cdot u \alpha, \text{ следовательно, } a[\alpha, u] = 0, [\alpha, u] = 0, \alpha u = u \alpha$$

$R$  является алгеброй над полем  $K$ . Разложим  $B$  и  $N$  на пирсовские компоненты  $B_{ij}$ ,  $N_{ij}$  относительно идемпотента  $e_{11}$  ( $i, j = 0, 1$ ). Учитывая, что  $e_{12} \in B_{10}$ ,  $e_{21} \in B_{01}$ , находим  $e_{12} N_{11} = 0$ ,  $e_{21} N_{11} = N_{11} e_{21} = 0$  и аналогично  $e_{12} N_{00} = e_{21} N_{00} = 0$ , откуда  $N_{11} = N_{00} = 0$ ,  $e_{12} N_{01} = e_{21} N_{10} = 0$ . Так как  $a^2 = 1$  ( $a = e_{12} + e_{21}$ ), то оператор  $L_a: x \rightarrow ax$  определяет взаимно обратные отображения  $N_{10} \rightarrow N_{01}$  и  $N_{01} \rightarrow N_{10}$ . Для любого  $u \in N_{10}$  линейное  $K$ -подпространство, натянутое на элементы  $u, v$ , где  $v = au = e_{12}u \in N_{01}$ , является идеалом в  $R$ . Из подпрямой неразложимости  $R$  следует, что  $N$  совпадает с этим подпространством для некоторых  $u, v$ . Тогда соответствие  $e_{11} \rightarrow e_1, e_{22} \rightarrow e_2, e_{12} \rightarrow u_1, e_{21} \rightarrow v_1, u \rightarrow u_2, v \rightarrow v_3$  дает, очевидно, вложение алгебры  $R$  в  $C(K) \in \mathcal{A}$ .

СЛУЧАЙ 2.  $B = B_1 \oplus B_2$ ,  $B_i = GF(q_i)$ ,  $q_i = p^{t_i}$ ;  $i = 1, 2$ ;  $P = P_{10}^{(1)} = P_{01}^{(2)}$ . Так как  $B_i$  - 1-порожденные подалгебры, то  $(B_i, B_i, N) = 0$ , а так как  $B_2 \subseteq R_{00}^{(1)}$ , то  $(B_1, B_2, N) = 0$ . Таким образом,  $N$  - ассоциативный  $B$ -бимодуль, а  $P$  - его неприводимый подбимодуль. Соотношение  $f_2(\alpha, u) = 0$ , где  $\alpha \in B_1, u \in P$ , показывает, что  $GF(q_1) \subseteq F$ , и аналогично  $GF(q_2) \subseteq F$ . Если  $N^2 = 0$ ,  $N = P$ , то алгебра  $R$  ассоциативна. Как и в [4], заключаем, что элементы  $R$  представляются

матрицами вида

$$\begin{pmatrix} \alpha & \gamma \\ 0 & \beta \end{pmatrix}, \quad \alpha \in GF(q_1), \beta \in GF(q_2), \gamma \in K,$$

где  $K$  - композит подполей  $GF(q_1), GF(q_2)$  в  $GF(q)$ ,  $K = GF(p^t)$ ,  $t = \text{НОК}(t_1, t_2)$ . Следовательно,  $R \subset M_2(K) \subset \mathcal{A}$ .

Пусть  $N^2 \neq 0$ ,  $P = P_{01}^{(1)} = P_{10}^{(2)}$ . Так как  $N^2 \in P$ , то  $N^2 = P$ .

Все подпространства  $N_{ij}^{(k)}$  являются подбимодулями в  $N$ . Из антикоммутативности умножения в  $N$  следует, что  $N_{00}^{(k)} \triangleleft R$ ,  $N_{11}^{(k)} \triangleleft R$ . Следовательно,  $N_{00}^{(k)} = N_{11}^{(k)} = 0$  ( $k=1,2$ ),  $N = N_{10}^{(k)} + N_{01}^{(k)}$ . Так как

$$N_{01}^{(1)} N_{01}^{(1)} \subseteq N_{10}^{(1)} \cap P = 0,$$

то  $N_{01}^{(1)} \subseteq P$ ,  $N = N_{10}^{(1)} + P$ ,  $P = N^2 = N_{10}^{(1)} N_{10}^{(1)} = N_{01}^{(2)} N_{01}^{(2)}$ . Если  $N_{ij}, P_{ij}$  - пирсовские компоненты идеалов  $N, P$  относительно идемпотента  $e = e_1 + e_2$ , то они - также подбимодули в  $N$ , причем  $N_{00} = 0$ ,  $N_{11} \triangleleft R$ ,  $N_{10} + N_{01} \triangleleft R$ .

Так как  $P = P_{11}$ , то  $N = N_{11}$ , т.е.  $e$  - единица алгебры  $R$ . Отсюда

$$N_{01}^{(1)} = e N_{01}^{(1)} = e_2 N_{01}^{(1)} \subseteq N_{10}^{(2)}, \quad N_{01}^{(1)} = N_{10}^{(2)}, \quad N_{10}^{(1)} = N_{01}^{(2)}.$$

Обозначим  $C = B_1 \otimes_{F_p} B_2$  и определим на  $N$  структуру унитарного правого  $C$ -модуля, полагая  $x(\alpha \otimes \beta) = \alpha x \beta$ , если  $x \in N_{10}^{(1)}$ , и  $x(\alpha \otimes \beta) = \beta x \alpha$ , если  $x \in P$ . Ясно, что это определение корректно, и структура  $B$ -бимодуля  $N$  однозначно определяется структурой  $C$ -модуля  $N$ . Более того, так как

$$x(\alpha \otimes \beta)y = \alpha x \beta y = x \cdot \alpha y \beta = x \cdot y(\alpha \otimes \beta) = \beta(x y) \alpha = (x y)(\alpha \otimes \beta)$$

для любых  $x, y \in N_{10}^{(1)}$ , то  $N$  является  $C$ -алгеброй. Известно [7], что  $C \cong \bigoplus_{i=1}^d K_i$ , где  $K_i \cong K$  для всех  $i$ ,  $d = \text{НОД}(t_1, t_2)$ . Разложение  $C$  в прямую сумму полей  $K_i$  отвечает разложению  $N$  в прямую сумму идеалов  $NK_i$ . Но  $R$  подпрямо неразложима, поэтому  $N$  совпадает с одним из  $NK_i$  и является, таким образом,  $K$ -алгеброй. Из леммы 2.5

[5], доказанной для произвольных (неассоциативных) колец, следует, что эта

алгебра является 2-порожденной. Порождающие  $n_1, n_2$  можно выбрать из

$$N_{10}^{(1)}, \quad \text{тогда } N \text{ имеет } K\text{-базис } \{n_1, n_2, n_3\}, \quad \text{где } n_3 = n_1 n_2 \in P.$$

Отождествим  $B_1$  с подалгеброй  $GF(q_1)e_1 \subset C(F)$ ,  $B_2 = GF(q_2)e_2$ ,  $N_{10}^{(1)} = \alpha Ku_1 + Ku_2$  и  $P = Ku_3$ , тогда возникает вложение  $R \subset C(K) \subseteq A$ .  
 СЛУЧАЙ 3.  $B = GF(p^t) \subseteq \bar{F} = GF(q^t)$ .

Снова  $N$  является ассоциативным  $B$ -бимодулем и если  $N_{ij}$  ( $i, j = 0, 1$ )-линейские компоненты  $N$  относительно идемпотента  $e \in B$ , то  $N_{00} = 0, N_{11} \triangleleft R$ ,  $N_{10} + N_{01} \triangleleft R$  и либо  $N = N_{10} + N_{01}$ , либо  $N = N_{11}$ . Здесь возникает несколько подслучаев.

а)  $N = N_{10} + N_{01}$ ,  $B = GF(p^t) \subseteq GF(q)$ .

Если  $N^2 = 0$ , скажем,  $N = P_{10}$ , то  $R$  представляется матрицами вида

$$\begin{pmatrix} \alpha & \beta \\ 0 & 0 \end{pmatrix}, \quad \alpha, \beta \in GF(p^t),$$

т.е.  $R \subset M_2(GF(p^t))$ . Если  $N^2 \neq 0$ , скажем,  $N_{10}^2 \neq 0$ , то  $N^2 = P = P_{01} = N_{10}^2 = N_{01}$  алгебра  $R$  порождается множеством  $B \cup \{n_1, n_2\}$  для некоторых  $n_1, n_2 \in N_{10}$ . Обозначим  $n_3 = n_1 n_2$ . Так как  $\alpha n_1 \beta n_2 = (n_1 n_2) \alpha \beta$  для любых  $\alpha, \beta \in B$ , то соответствие  $e \rightarrow e_1, n_1 \rightarrow u_1, n_2 \rightarrow u_2, n_3 \rightarrow u_3$  определяет вложение  $R \rightarrow C(GF(p^t))$ .

б)  $N = N_{11}$  - унитарный  $B$ -бимодуль,  $P$  - его неприводимый подбимодуль.

Если  $N^2 = 0, N = P$ , то  $P$  представляется матрицами вида

$$\begin{pmatrix} \alpha & \beta \\ 0 & \sigma(\alpha) \end{pmatrix}, \quad \alpha, \beta \in GF(p^t),$$

где  $\sigma$  - некоторый автоморфизм поля  $GF(p^t)$  (см. [4]). Для любых  $u \in P, \alpha \in B$  имеем  $u\alpha = \sigma(\alpha)u$ . Равенство  $f_2(\alpha u) = (\alpha - \alpha^q)u = 0$  дает  $\alpha + \sigma(\alpha) = [\alpha + \sigma(\alpha)]^q$ , следовательно,  $t(\alpha) = \alpha + \sigma(\alpha) \in \Phi = GF(p^t) \cap GF(q)$ . Тогда также  $t(\alpha)^2 = t(\alpha^2) + 2\alpha\sigma(\alpha) \in \Phi$ , и либо  $chF \neq 2, n(\alpha) = \alpha \cdot \sigma(\alpha) \in \Phi$ , либо  $chF = 2, t(\alpha)^3 = t(\alpha^3) + n(\alpha) \cdot t(\alpha) \in \Phi$ . В последнем случае снова  $n(\alpha) \in \Phi$ , если  $t(\alpha) \neq 0$ ; если же  $t(\alpha) = 0$ , то  $\alpha = \sigma(\alpha), \alpha u = u\alpha$ , и равенство  $f_1(\alpha + u) = (\alpha - \alpha^q)u = 0$  влечет  $\alpha = \alpha^q \in \Phi$ . Элемент  $\alpha$  является корнем многочлена  $x^2 -$

$-t(\alpha)x+n(\alpha)\in\Phi[x]$ ; таким образом,  $GF(p^t)$  квадратично над  $\Phi$  и либо совпадает с  $\Phi$ , либо  $[GF(p^t):\Phi]=2$ . В первом случае получаем вложение  $R\subset M_2(\Phi)\subseteq M_2(F)$ .

Рассмотрим второй случай. Если  $\alpha\neq 0$ , то из включений  $\alpha\sigma(\alpha)\in\Phi$ ,  $G(\alpha)\cdot G^2(\alpha)\in\Phi$  следует, что  $G^2(\alpha)=\nu\alpha$  для некоторого  $\nu=\nu(\alpha)\in\Phi$ . С другой стороны,  $G^2(\alpha)=G[t(\alpha)-\alpha]=\alpha-t(\alpha)+\sigma t(\alpha)$ , следовательно, либо  $\alpha\in\Phi$ , либо  $\nu=1$ ,  $G^2(\alpha)=\alpha$ . Применяя это рассуждение к порождающему элементу  $\xi$  поля  $GF(p^t)$ , заключаем, что  $G^2=\text{id}$ , а неподвижное относительно  $G$  подполе совпадает с  $\Phi=GF(p^s)\subseteq F$ . Пусть минимальный многочлен для  $\xi$  над  $\Phi$  имеет вид  $x^2-\lambda x+\mu$ ;  $G(\xi)=\lambda-\xi$ . Если  $a=\lambda e_1+u_1-\mu v_1$ , то подалгебра  $\langle a \rangle_\Phi\subset C(\Phi)$  с базисом  $\{1, a\}$  изоморфна  $\Phi(\xi)$ . Так как  $a\cdot u_2=\lambda u_2$ , т.е.  $u_2 a=(\lambda-a)u_2$ , то  $\Phi$ -подалгебра в  $C(\Phi)$ , порожденная элементами  $a, u_2$ , изоморфна  $R$ .

Если  $N^2\neq 0$ ,  $N^2=P$ , то, как и ранее,  $P$  - неприводимый  $B$ -бимодуль,  $u\alpha=\sigma(\alpha)u$  для любых  $\alpha\in B, u\in P$ . Соотношение  $f_3(\alpha, n, n')==(\alpha-\alpha^q)nn'=0$  ( $\alpha\in B, n, n'\in N$ ) влечет, что  $GF(p^t)\subseteq F$ . Пусть

$\xi$  - порождающий элемент поля  $B=GF(p^t)$ . Так как  $\xi n\cdot n'=nn'\cdot\xi=G(\xi)nn'=n\sigma(\xi)n'$ , то  $\xi n-n\sigma(\xi)\in P$  для любого  $n\in N$ .

Снова используя лемму 2.5 И. В. Львова [5], заключаем, что для некоторых

$n_1, n_2\in N$  имеет место  $N=Bn_1+Bn_2+Bn_3$ , где  $n_3=n_1n_2$ . Пока-

жем, что  $n_1, n_2$  можно выбрать так, что  $\xi n_i=n_i\sigma(\xi)$ . Действительно, если  $\xi n_i=n_i\sigma(\xi)+\lambda_i n_3$ , то, заменяя  $n_i$  на  $n'_i=n_i+t_i n_3$  ( $i=1,2$ ), будем иметь  $n'_1 n'_2=n_3$ ,  $\xi n'_i=\xi n_i+\xi t_i n_3=n'_i\sigma(\xi)+[\lambda_i+t_i(\xi-\sigma^2(\xi))]n_3=n'_i\sigma(\xi)$  при подходящем  $t_i$ ,

если  $\xi\neq\sigma^2(\xi)$ . Если же  $\sigma^2(\xi)=\xi$ , т.е.  $G^2=\text{id}$ , то индукцией по

$k$  легко проверяется равенство  $\xi^k n_i=n_i\sigma(\xi)^k+k\lambda_i\xi^k n_3$  для любого

$k>1$ . В частности, при  $k=p^t$  имеем  $\xi n_i=n_i\sigma(\xi)$ , т.е. требуемое

равенство выполняется автоматически. Тогда также  $\alpha n_i=n_i\sigma(\alpha)$  для любого

$\alpha\in B, i=1,2$ . Легко видеть, что отображение  $\alpha\mapsto\sigma(\alpha)e_1+\alpha e_2$ ,

$n_1\rightarrow u_1, n_2\rightarrow u_2, n_3\rightarrow v_3$  продолжается до изоморфного вложения алгебры  $R$  в  $C(GF(p^t))$ .

Тем самым предложение 2 полностью доказано. Предложения 1, 2 в совокупности означают, что справедлива основная теорема, сформулированная в начале статьи, причем результат сохраняется, если алгебру  $A = C(GF(q))$  рассматривать как алгебру над фиксированным подполем поля  $GF(q)$ .

В заключение остановимся на вопросе о независимости тождеств  $f_1, f_2, f_3$ . Просматривая доказательство предложения 2, легко можно заметить, что тождество  $f_1$  используется только для того, чтобы показать, что любое поле  $\Phi$ , лежащее в  $\mathcal{M}$ , вкладывается в  $GF(q^2)$ . Но при  $p \neq 2$  для этой цели достаточно использовать тождество  $f_2$ .

ЛЕММА 4. Пусть  $q = p^n$ ,  $p \neq 2$  и поле  $\Phi = GF(p^t)$  удовлетворяет тождеству  $f_2(x, y)$ . Тогда  $\Phi$  вложимо в  $GF(q^2)$ .

ДОКАЗАТЕЛЬСТВО. Действительно, пусть  $\alpha - \alpha^{q^2} \neq 0$  для некоторого  $\alpha \in \Phi$ . Тогда равенство  $f_2(\alpha, \alpha) = 2(\alpha - \alpha^{q^2}) \times (\alpha - 2\alpha^q + \alpha^{q^2}) = 0$  влечет  $\alpha - \alpha^q = \alpha^q - \alpha^{q^2} \neq 0$ . Далее,  $f_2(\alpha^2, \alpha^2) = 0$  влечет, что либо  $\alpha^2 = \alpha^{2q^2}$ , либо  $\alpha^2 - \alpha^{2q} = \alpha^{2q} - \alpha^{2q^2}$ . Но первый случай невозможен, так как тогда  $\alpha^{q^2} = -\alpha$  и  $2\alpha^q = 0$ , откуда  $\alpha = 0$ . Следовательно,  $(\alpha - \alpha^q)(\alpha + \alpha^q) = (\alpha^q - \alpha^{q^2})(\alpha^q + \alpha^{q^2})$ , откуда  $\alpha + \alpha^q = \alpha^q + \alpha^{q^2}$ ,  $\alpha = \alpha^{q^2}$ .

СЛЕДСТВИЕ. Если  $q = p^n$ ,  $p \neq 2$ , то тождество  $f_1$  является следствием тождеств  $f_2, f_3$  в многообразии альтернативных  $GF(p)$ -алгебр.

Если  $q = 2^n$ , то алгебра над  $GF(q)$  с порождающим элементом  $u$  и определяющим соотношением  $u^3 = 0$  удовлетворяет тождествам  $f_2, f_3$  и не удовлетворяет тождеству  $f_1$ . Алгебра  $R$ , указанная в [4], удовлетворяет тождествам  $f_1, f_3$ , но не удовлетворяет тождеству  $f_2$ . Наконец, над произвольным полем  $F$  существует альтернативная нильпотентная алгебра размерности 7, в которой выполнены тождества  $f_1, f_2$  (т.е.  $x^2 = 0$ ), но не выполнено тождество  $f_3$  (т.е.  $xyz \neq 0$ ). Эта алгебра имеет базис  $\{a_1, a_2, a_3, b_1, b_2, b_3, c^3\}$  и таблицу умножения (с учетом антикоммутатив-

ности)  $a_i a_j = b_k$ , где  $(i, j, k) = (1, 2, 3), (2, 3, 1), (3, 1, 2)$ ,  $a_i b_i = c$  ( $i = 1, 2, 3$ ), остальные произведения базисных элементов полагаются равными 0.

Автор благодарен И. П. Шестакову и Е. Н. Кузьмину за внимание к работе и ценные замечания.

#### Л и т е р а т у р а

1. Днестровская тетрадь, Новосибирск, 1976.
2. И. В. ЛЬВОВ, О многообразиях, порожденных конечными альтернативными кольцами, Алгебра и логика, 17, № 3 (1978), 282-286.
3. К. А. ЖЕВЛАКОВ, А. М. СЛИНЬКО, И. П. ШЕСТАКОВ, А. И. ШИРШОВ, Кольца, близкие к ассоциативным, М., Наука, 1978.
4. Ю. Н. МАЛЫШЕВ, Е. Н. КУЗЬМИН, Базис тождеств алгебры матриц второго порядка над конечным полем, Алгебра и логика, 17, № 1 (1978), 28-32.
5. И. В. ЛЬВОВ, О многообразиях ассоциативных колец, 1, Алгебра и логика, 12, № 3 (1973), 269-297.
6. H.P.PETERSSON, Borel subalgebras of alternative and Jordan algebras, J.Algebra, 16, № 4 (1970), 541-560.
7. B.R.McDONALD, Finite rings with identity, New York, 1974.

Поступило 12 октября 1983 г.