S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru

Том ??, стр. ?–? (2024) УДК 512.554.7
DOI 10.17377/semi.2024.15.xxx
MSC 16R10, 17A30

О ТОЖДЕСТВАХ АЛГЕБРЫ БИЛИНЕЙНОЙ ФОРМЫ НАД КОНЕЧНЫМ ПОЛЕМ

И.М. ИСАЕВ

Abstract. Yu. A. Medvedev [7] proved that the variety generated by a finite Jordan algebra is Cross. In particular, it is shown that such a variety has a finite basis of identities. For the class $\mathfrak{R}$ of Jordan algebras of symmetric non-degenerate linear forms over finite fields, the present work constructs a finite basis of identities. This is done by studying critical algebras of the variety. Note that the basis of identities for the algebra of bilinear forms over an infinite field was found by S. Yu. Vasilovsky [9].

Keywords: polynomial identities, Cross varieties, Jordan algebras, simmetric bilinear form.

В работе Ю.А. Медведева [7] установлена кроссовость многообразия, порожденного конечной йордановой алгеброй. В частности, многообразие, порожденное конечной йордановой алгеброй, имеет конечный базис тождеств. Пусть $\mathfrak{R}$ - класс йордановых алгебр симметрических невырожденных билинейных форм над конечными полями. В данной работе строится конечный базис тождеств произвольной алгебры из класса $\mathfrak{R}$. Метод исследования связан с изучением критических алгебр многообразия. Отметим, что базис тождеств алгебры билинейной формы над бесконечным полем был найден С.Ю. Василовским [9].

1. Обозначения и общие замечания

Рассмотрим йорданову алгебру билинейной формы $B(\mu)$. Напомним определение этой алгебры. Пусть V - векторное пространство над полем F с заданной на нем симметрической билинейной формой $\mu = \mu(x, y)$. Рассмотрим прямую

Isaev, I.M., On the Identities of Jordan Algebras of Bilinear Forms Over Finite Fields .

Поступила ?? июля 2024 г., опубликована ?? декабря 20?? г.

сумму векторного пространства V и одномерного пространства $F \cdot 1$ с базисом 1 и зададим на B умножение следующим образом: $(\alpha \cdot 1 + x)(\beta \cdot 1 + y) = (\alpha\beta + \mu(x,y)) \cdot 1 + (\beta x + \alpha y)$, где $\alpha, \beta \in F, x, y \in V$. Эта алгебра обозначается $B(\mu)$ и является йордановой алгеброй с единицей 1 . Если форма μ - невырождена и $dim_F V > 1$, то йорданова алгебра $B(\mu)$ является простой [8](гл.3, упр.2). Цель настоящей работы - нахождение базиса тождеств алгебры $B(\mu)$ в случае, если основное поле F является конечным полем характеристики не 2.

Класс всех алгебр невырожденной билинейной формы над полем F обозначим $\Re(F)$. Следуя [1], симметрическую невырожденную билинейную форму мы будем называть метрикой.

Типом метрики μ называется класс метрик пространства V, эквивалентных μ.

Пусть $F = GF(p^n), p \neq 2; dim_F V = m$. Известно [1], что в этом случае существует ровно два типа возможных метрик на V. Пусть P_i $\left(i = 1, ..., [\frac{m}{2}]\right)$ - гиперболические плоскости в V, т.е. $P_i = \langle v_i \rangle + \langle w_i \rangle, v_i^2 = w_i^2 = 0, v_i w_i = 1$; W - плоскость, не содержащая изотропных векторов (т.е. таких u, что $u^2 = 0$); $W = \langle v \rangle + \langle w \rangle, v^2 = 1, w^2 = -\xi, vw = 0$, где ξ - порождающий элемент поля $GF(p^n)$. Тогда при нечетном m метрики V определяются разложениями:

$$V = P_1 \oplus P_2 \oplus ... \oplus P_{\frac{m-1}{2}} \oplus \langle v \rangle, v^2 = 1, \tag{1}$$

$$V = P_1 \oplus P_2 \oplus ... \oplus P_{\frac{m-1}{2}} \oplus \langle w \rangle, w^2 = \xi. \tag{2}$$

Если же m четно, то метрики V определяются разложениями:

$$V = P_1 \oplus P_2 \oplus ... \oplus P_{\frac{m}{2}}, \tag{3}$$

$$V = P_1 \oplus P_2 \oplus ... \oplus P_{\frac{m-2}{2}} \oplus W. \tag{4}$$

Пусть $u_1, ..., u_m$ - база V. Тогда матрица $\|\mu\|$, у которой на месте (i,j) стоит элемент $\mu(u_i, u_j)$, называется матрицей метрики μ ; квадратичный характер дискриминанта этой матрицы не зависит от выбора базы в V. Следовательно, тип метрики однозначно определяется заданием размерности V и квадратичным характером дискриминанта, т.е. заданием того, является дискриминант квадратом в F или нет. Дискриминанты метрик (1)-(4) равны, соответственно:

$$(-1)^{m-1/2}, (-1)^{m/2}\xi, (-1)^{m/2}, (-1)^{m/2}\xi. \tag{5}$$

Базу пространства V, в которой оно имеет один из видов (1)-(4), назовем стандартной.

Легко проверить, что изоморфным алгебрам конечной размерности из $\Re(F)$ соответствуют пространства одинаковых типов и наоборот. Поэтому имеет смысл говорить о типе конечномерной алгебры из $\Re(F)$, имея в виду тип метрики ее пространства.

Обозначим алгебру $A = F + V$ через $A_m = F + V_m$, если она имеет тип (1) или (3), и через $A'_m = F + V'_m$, если она типа (2) или (4). Метрику A_m (A'_m) обозначим через μ_m (μ'_m). Алгебрами A_m, A'_m $(m = 1, 2, ...)$ исчерпываются все конечномерные алгебры класса $\Re(F)$.

Символом A_∞ обозначим некоторую фиксированную бесконечномерную алгебру из $\Re(F)$.

Не всякое подпространство W метрического пространства V является метрическим. В частности, может существовать подпространство $U \subseteq W$, такое, что $UW = 0$. Максимальное такое подпространство U мы будет называть ядром W.

Класс $\mathfrak{T}(F)$ состоит из алгебр вида $C = F + W$, где W подпространство метрического пространства и ядро W одномерно.

2. Тождества алгебр класса $\Re(F)$

В этом разделе мы получим некоторые тождества алгебр класса $\Re(F)$ ($F = GF(p^n)$) и докажем ряд лемм, характеризующих многообразия, заданные этими тождествами.

Алгебры класса $\Re(F)$ мы будем рассматривать, как кольца характеристики p, или, что то же самое, как алгебры над $GF(p)$ - простым подполем поля F.

Наша цель - найти базис тождеств многообразия $GF(p)$-алгебр, порожденного произвольной фиксированной алгеброй из $\Re(F)$. Разумеется, в это многообразие попадут какие-то алгебры из $\Re(\Phi)$ ($\mathfrak{T}(\Phi)$), где Φ подполе поля F. Оказывается эти алгебры можно выделить в $\Re(\Phi)$ ($\mathfrak{T}(\Phi)$) на языке тождеств.

Произвольную алгебру из $\Re(\Phi)$ мы будем обозначать буквой B. По аналогии с предыдущим параграфом можно ввести также алгебры B_m, B'_m.

Как всегда, $[a, b] = ab - ba$ обозначает коммутатор элементов a и b; $(a, b, c) = (ab)c - a(bc)$ - ассоциатор элементов $a, b, c.$; $a \odot b = \frac{1}{2}(ab + ba)$.

Пусть $Y = (y_1, y_2, y_3), X_i = (x_{3i-2}, x_{3i-1}, x_{3i}), X_{ij} = X_i X_j$ $(i, j = 1, 2, ..., m)$. Отметим,что X_{ij} - центральный полином алгебр класса $\Re(F)$. Рассмотрим матрицу порядка m, у которой на месте (i, j) стоит элемент X_{ij}. Положим

$$d_m = det\|X_{ij}\|, \quad \Delta_m = (-1)^{[m/2]} d_m.$$

Введем вспомогательные многочлены:

$$\varphi_m = \Delta_m - \Delta_m^{\frac{q+1}{2}}, \quad \varphi'_m = \Delta_m + \Delta_m^{\frac{q+1}{2}},$$

$$\psi_m = \left(\prod_{i=1}^{m}(1 - (YX_i)^{q-1})\right)(Y - Y^{2q-1}).$$

Здесь и далее мы не указываем, от каких переменных зависят многочлены, считая их зависящими от переменных, указанных ранее в тексте. Кроме того, в тех местах, где не указана расстановка скобок, будем считать ее произвольной.

Определим многочлены:

$$f_m = \varphi_{m-2}\psi_{m-2}, \ f'_m = \varphi'_{m-2}\psi_{m-2}, \ g_m = d_{m-2}\psi_{m-2} (m \geq 3)$$

$$f_2 = \varphi_2, \ f'_2 = x - x^{q^2}, \ f'_1 = g_2 = (x, y, z), \ f_1 = x - x^q;$$

$$\theta_3 = (x - x^q)^2(1 - ((x - x^q)Y)^{q-1})(Y - Y^{2q-1}),$$

$$\theta'_3 = (x, y, Y)(1 - (x - x^q)^{2q-2})(1 - Y^{2q-2})(1 - (Yx)^{q^2-q})),$$

$$\theta_2 = (x, y, Y)((1 - Y^{2q-2})(1 - (Yx)^{q^2-q})).$$

ЛЕММА 1. Для алгебры $B \in \Re(\Phi), \Phi \subseteq F$ условия $1-3$ $(1'-3')$, приведенные ниже эквивалентны.

1. $GF(p)$-алгебра B вложима в алгебру A_m;

2. В алгебре B выполняются тождества f_m, g_{m+1};

3. $dim_\Phi B \leq m + 1$, причем если $dim_\Phi B = m + 1$, то либо $B = B_m$, либо элементы Φ являются квадратами в F.

$1'$. $GF(p)$-алгебра B вложима в алгебру A'_m (при $m = 1$ в A'_1 либо в A_1);

$2'$. В алгебре B выполняется тождество f'_m;

$3'$. $dim_{\Phi}B \leq m+1$, причем если $dim_{\Phi}B = m+1$, то при $m > 1$ $\;B = B'_m$ и существует элемент Φ, не являющийся квадратом в F.

ДОКАЗАТЕЛЬСТВО. $(1 \to 2)$. Достаточно показать, что алгебра A_m удовлетворяет тождествам f_m, g_{m+1}.

Для многочлена g с коэффициентами из $GF(p)$ и произвольной $GF(p)$-алгебры C значком $g^{\sigma}(C)$, или просто g^{σ} мы будем обозначать элемент алгебры C, являющийся значением многочлена g при некоторой фиксированной подстановке σ элементов алгебры C вместо переменных многочлена g. Заметим, что $g^{\sigma}(h_1,...,h_r) = g(h_1^{\sigma},...,h_r^{\sigma})$.

Покажем, что $f_m^{\sigma}(A_m) = 0$ для любой подстановки σ. Если $m \geq 3$, то элементы X_i^{σ}, Y^{σ} $(i = 1,2,...,m-2)$ принадлежат V_m. Выполнение условия $\psi_{m-2}^{\sigma} \neq 0$ влечет соотношения $(Y^{\sigma})^2 = X_i^{\sigma}Y^{\sigma} = 0$ $(i = 1,2,...,m-2), Y^{\sigma} \neq 0$. В этом случае, $V_m = V' \oplus P$, где вектор Y^{σ} принадлежит гиперболической плоскости P, а $X_i^{\sigma} = u_i + \alpha_i Y^{\sigma}, u_i \in V'$. Согласно (5), $det\|\mu_m\| = (-1)^{[m/2]}$, следовательно, $d_{m-2}^{\sigma} = det\|X_i^{\sigma}X_j^{\sigma}\| = (-1)^{\left[\frac{m-2}{2}\right]}k^2, k \in F$. В самом деле, если векторы $\{u_i \mid i = 1,...,m-2\}$ - линейно зависимы, то $d_{m-2}^{\sigma} = 0$, если же векторы $\{u_i \mid i = 1,...,m-2\}$ - базис V', то по формуле (3.7) ([1]) $d_{m-2}^{\sigma} = (-1)\cdot det\mu_m \cdot k^2 = (-1)^{\left[\frac{m-2}{2}\right]}k^2$. В результате $\varphi_{m-2}^{\sigma} = 0, f_m^{\sigma} = 0$. Если же $m = 2$, то $d_m^{\sigma} = -k'^2, k' \in F$; $\Delta_m^{\sigma} = k'^2$, $f_m = \varphi_m = 0$. Поскольку $A_1 \simeq F \oplus F$, то и при $m = 1$ тождество $f_m^{\sigma} = 0$ выполняется в A_m.

Покажем, что $g_{m+1}^{\sigma} = 0$. При $m = 1$ указанное равенство очевидно. Если же $m \geq 2$, то, как и выше, $X_i^{\sigma} = u_i + \alpha_i Y^{\sigma}(i = 1,...,m-1), u_i \in V', dim_F V' = m-2$. Следовательно,

$$g_{m+1}^{\sigma} = d_{m-1}^{\sigma}\psi_{m-1}^{\sigma} = det\|u_iu_j\| \cdot \psi_{m-1}^{\sigma} = 0.$$

$(3 \to 1)$. Если $dim_{\Phi}B = m+1$, то искомое вложение есть естественное вложение алгебры B в алгебру $B_F = B \otimes_{\Phi} F$, которая, очевидно, лежит в классе $\Re(F)$ $\;(B_F = 1 \otimes F + V \otimes F))$. Если элементы $u_1,...,u_m$ образуют стандартную базу алгебры алгебры B, то элементы $u_1 \otimes 1,...,u_m \otimes 1$ образуют базу алгебры B_F. Отсюда ясно, что $B_F = A_m$, если $B = B_m$, либо элементы Φ являются квадратами в F.

Пусть теперь $dim_{\Phi}B = k+1 < m+1$. В этом случае $B_F = A_k$, либо $B_F = A'_k$, и для вложимости алгебры B_F в алгебру A_m достаточно установить следующие вложения пространств с метрикой

$$V_s \subset V_{s+1}, V_s \subset V'_{s+1}, V'_s \subset V_{s+1}, V'_s \subset V'_{s+1}(s = 1,2,...).$$

В свою очередь, эти включения достаточно проверить в случае $s = 1,2$. Рассмотрим эти случаи. Задавая метрику, мы будем указывать только ненулевые произведения элементов базы.

$$V_1 = \langle v \rangle,\ v^2 = 1;\quad V'_1 = \langle v' \rangle,\ {v'}^2 = \xi;\quad V_2 = \langle v_1 \rangle + \langle v_2 \rangle,\ v_1v_2 = 1;$$

$$V'_2 = \langle v'_1 \rangle + \langle v'_2 \rangle,\ {v'_1}^2 = 1,\ {v'_2}^2 = -\xi;\quad V_3 = \langle w_1 \rangle + \langle w_2 \rangle + \langle w_3 \rangle\, w_1w_2 = 1,\ w_3^2 = 1;$$

$$V'_3 = \langle w'_1 \rangle + \langle w'_2 \rangle + \langle w'_3 \rangle,\ w'_1w'_2 = 1,\ {w'_3}^2 = \xi.$$

Построим таблицу неочевидных вложений. Первый столбец в ней указывает "что вкладывается", второй столбец - "куда вкладывается" , третий - "по какой причине".

V_1	V_2	$(v_1+\frac{1}{2}v_2)^2=1$
V_1'	V_2	$(v_1+\frac{\xi}{2}v_2)^2=\xi$
V_1'	V_2'	$(\alpha v_1'+\beta v_2')^2=\xi,\quad \alpha^2=(\beta^2+1)\xi$
V_2'	V_3	$(w_1-\frac{\xi}{2}w_2)^2=-\xi$
V_2'	V_3'	$(w_1'+\frac{1}{2}w_2')^2=1,(\alpha(w_1'-\frac{1}{2}w_2')+\beta w_3')^2=-\xi,\quad \alpha^2=(\beta^2+1)\xi$

Покажем, что равенство $\alpha^2=(\beta^2+1)\xi$ разрешимо в F относительно α и β. Допустим, что это неверно. Тогда β^2+1 является квадратом в F для всех β. Значит, -1 является квадратом. Отсюда получаем

$$(-1)\left(\frac{\xi-1}{\xi+1}\right)^2+1=\frac{4\xi}{(\xi+1)^2}$$

является квадратом в F, что неверно. Противоречие показывает, что искомые α,β существуют.

Приведенное рассуждение показывает, что $B\subseteq B_F\subseteq A_m$.

$(2\to 3)$. Пусть в алгебре B выполняются тождества f_m,g_{m+1}. В этом случае $dim_\Phi B\leq m+1$. Если $dim_\Phi B=m+1$ и не выполняется условие 3, то $B=B_m'$ и порождающий элемент η поля Φ не является квадратом в F. При $m\geq 3$ для пространства W_m' алгебры B_m' существует разложение $W_m'=W\oplus P$, где P - гиперболическая плоскость. Пусть подстановка σ такова, что $X_1^\sigma,...,X_{m-2}^\sigma$ - стандартная база W', а Y^σ - изотропный вектор P. Тогда, согласно (5),

$$d_{m-2}(X_1^\sigma,...,X_{m-2}^\sigma)=(-1)^{[\frac{m-2}{2}]}\eta,$$

$$\Delta_{m-2}(X_1^\sigma,...,X_{m-2}^\sigma)=\eta,\quad f_m^\sigma=\eta-\eta^{\frac{q+1}{2}}\neq 0.$$

При $m=2$ имеем $\Delta_2({X_1}^\sigma,{X_2}^\sigma)=\eta\quad$ (${X_1}^\sigma,{X_2}^\sigma$ - стандартная база ${W_2}'$), и снова ${f_m}^\sigma\neq 0$. Наконец, при $m=1$

$${W_m}'=\langle w'\rangle,{w'}^2=\eta,x^\sigma=w',{f_1}^\sigma=w'(1-\eta^{\frac{q-1}{2}})\neq 0.$$

Следовательно, рассматриваемые случаи невозможны, и импликация доказана.

Мы доказали эквивалентность утверждений 1,2,3. Доказательство $1'\sim 2'\sim 3'$ проводится аналогично. Специфичность случая $m=1$ в утверждениях $1'-3'$ заключается в том, что $A_1=GF(q)\oplus GF(q),A_1'=GF(q^2)$, следовательно, A_1 удовлетворяет всем тождествам A_1'.

ЛЕММА 2. Для алгебры $C\in\mathfrak{T}(\Phi),\Phi\subseteq F$ условия $1,2$ $(1',2')$, приведенные ниже, эквивалентны.

1. $GF(p)$-алгебра C вложима в A_m;

2. Выполняется неравенство $m\geq 2$, и алгебра C удовлетворяет тождествам f_m,g_{m+1} при $m\geq 4$; g_4,θ_3 при $m=3$; θ_2 при $m=2$.

$1'$. $GF(p)$-алгебра C вложима в A_m';

$2'$. Выполняется неравенство $m\geq 3$, и алгебра C удовлетворяет тождествам f_m' при $m\geq 4$; f_3',θ_3' при $m=3$.

ДОКАЗАТЕЛЬСТВО. ($1 \to 2$). Достаточно, с учетом предыдущей леммы, доказать, что θ_2 (θ_3, θ_3') тождество в A_2 (A_3, A_3'). Пусть σ - некоторая подстановка элементов A_2 в θ_2. Тогда Y^σ - элемент пространства V_2, причем $\left(1 - Y^{2q-2}\right)^\sigma \neq 0$, только если Y^σ - изотропный вектор. Пусть

$$w^2 = 0,\ wY^\sigma = 1,\ x^\sigma = \alpha \cdot 1 + \beta w + \gamma Y^\sigma.$$

Заметим, что $\left(1 - (Yx)^{q^2-q}\right)^\sigma \neq 0$, только если $\beta = 0$. Значит,

$$x^\sigma = \alpha \cdot 1 + \gamma Y^\sigma,\ (x^\sigma, y^\sigma, Y^\sigma) = 0,\ \theta_2^\sigma = 0.$$

Тождество $\theta_3^\sigma = 0$ $\left({\theta_3'}^\sigma = 0\right)$ в алгебре A_3 (${A_3}'$) устанавливается аналогично.

($2 \to 1$). Пространство W алгебры $C = F + W$ разлагается в прямую сумму $W = W' \oplus \langle w \rangle$, где W' - метрическое пространство, $w^2 = W'w = 0$. Пусть $m > 3$. Положим в доказательстве импликации ($2 \to 3$) леммы 1 вместо Y^σ элемент (u, u, w), где $u \in W', u^2 \neq 0$. Тогда $Y^\sigma = u^2 w$ - изотропный вектор, $W = W' \oplus \langle Y^\sigma \rangle \subset W' \oplus P$. Фактически, мы находимся в условиях импликации ($2 \to 3$) леммы 1, где от гиперболической плоскости P требуется лишь наличие изотропного вектора в ней. Таковой у нас есть. Значит, по лемме 1 алгебра C вложима в A_m.

Если $m = 3$, то выполнение тождества g_4 в C влечет одномерность пространства W', а выполнение θ_3 дает $W' = \langle w' \rangle, {w'}^2 = 1$. Теперь же вложение C в A_3 не вызывает затруднений. Если же $m = 2$, то равенство $\theta_2^\sigma(C) = 0$ влечет $W = \langle w \rangle, w^2 = 0$. Вложение C в A_2 также проблем не вызывает.

Эквивалентность $1' \sim 2'$ устанавливается аналогично. Отметим, что f_1, f_2' - тождества в $A_1, A_1'(A_2')$. Поэтому C, ввиду наличия в ней нильпотентных элементов, в эти алгебры не вложима. Лемма 2 доказана.

Рассмотрим следующие многочлены, являющиеся тождествами алгебр класса $\Re(F)$:

$$h_1 = ([x, y]^2, z, t)$$

($[x, y]^2$ - ассоциативная запись йорданова многочлена),

$$h_2 = ((x - x^q)(y - y^q), z, t),$$

$$h_3 = (x - x^q)(y - y^q) - ((x - x^q)(y - y^q))^q\,,$$

$$h_4 = (x_1, x_2, x_3)(y_1, y_2, y_3) - ((x_1, x_2, x_3)(y_1, y_2, y_3))^q\,.$$

ЛЕММА 3. Пусть поле $\Phi = GF(p^t), p \neq 2$ удовлетворяет тождеству $h_3 = 0$. Тогда Φ вложимо в $GF(q^2)$.

ДОКАЗАТЕЛЬСТВО. Действительно, пусть $\alpha - \alpha^{q^2} \neq 0$. Тогда равенство $h_3(\alpha, \alpha) = (\alpha - \alpha^{q^2})(\alpha - 2\alpha^q + \alpha^{q^2}) = 0$ влечет $\alpha - \alpha^q = \alpha^q - \alpha^{q^2} \neq 0$. Далее, $h_3(\alpha^2, \alpha^2) = 0$ 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 $\alpha + \alpha^q = \alpha^q + \alpha^{q^2}, \alpha = \alpha^{q^2}$.

ЛЕММА 4. Йорданова алгебра симметрических матриц третьего порядка $H(\Phi_3)$, $ch\Phi \neq 2$ не удовлетворяет тождеству h_1.

Действительно, при $x^\sigma = e_{12} + e_{21} + e_{22}, y^\sigma = e_{11} + e_{12} + e_{21}, z^\sigma = t^\sigma = e_{23} + e_{32}$ имеем $h_1^\sigma = 2(e_{22} - e_{33}) \neq 0$.

3. Критические алгебры многообразия $Var\Re(F)$

Основным результатом настоящей части работы является следующая

ТЕОРЕМА 1. Идеалы тождеств алгебр A_m, A'_m, A_∞ порождаются, соответственно, следующими наборами многочленов:

(T_m) $f_m, g_{m+1}, h_1, h_2, h_3, h_4$ (при $m = 3$ добавляется θ_3, при $m = 2$ многочлен θ_2);

(T'_m) f'_m, h_1, h_2, h_3, h_4 (при $m = 3$ добавляется θ'_3, при $m = 1$ многочлен f'_2);

(T_∞) h_1, h_2, h_3, h_4.

ДОКАЗАТЕЛЬСТВО. Существование конечного базиса тождеств алгебр A_m, A'_m следует из теоремы Ю.А.Медведева о кроссовости многообразия, порожденного конечным йордановым кольцом [7]. Настоящая теорема дает нам конкретный вид базиса тождеств не только алгебр A_m, A'_m, но и алгебры A_∞. Заметим, что указанные наборы многочленов не всегда являются независимым базисом (например, в случае A'_1 достаточно тождеств f'_1, f'_2. Теорема сформулирована и будет доказываться в таком виде в целях единообразия схемы изложения. Для каждой конкретной алгебры метрики, разумеется, эту теорему можно сформулировать более точно.

Пусть $\mathfrak{M}_m$ ($\mathfrak{M}'_m$, $\mathfrak{M}_\infty$) - многообразие $GF(p)$-алгебр, удовлетворяющих тождествам T_m (T'_m, T_∞). Тогда утверждение теоремы заключено в равенствах:

$$\mathfrak{M}_m = VarA_m,\ \mathfrak{M}'_m = VarA'_m,\ \mathfrak{M}_\infty = VarA_\infty.$$

Доказательство будем вести параллельно для многообразий $\mathfrak{M}_m$ $\mathfrak{M}'_m$, $\mathfrak{M}_\infty$. Если схема рассуждений будет едина, то эти многообразия мы будем обозначать через $\mathfrak{M}$, а соответствующую ему алгебру метрики через A. В остальных случаях будем указывать, чему равны $\mathfrak{M}$ и A.

Итак, нам нужно установить равенство $\mathfrak{M} = VarA$. Включение $\mathfrak{M} \subseteq VarA$ следует из лемм 1, 2. Докажем обратное включение. Так как в $\mathfrak{M}$ выполняется тождество $h_3(x, y)$, то $\mathfrak{M}$ - локально конечно [2], следовательно, порождается своими критическими алгебрами, которые в свою очередь конечны. Для доказательства теоремы достаточно установить, что всякая критическая алгебра из $\mathfrak{M}$ вложима в A. Заметим, что всякая критическая алгебра из $\mathfrak{M}$ подпрямо неразложима.

Если J - нильпотентная критическая алгебра из $\mathfrak{M}$, то из тождества $h_3 = 0$ получаем, что J удовлетворяет тождеству $xy = 0$. Ввиду подпрямой неразложимости, J является одномерной $GF(p)$-алгеброй с нулевым умножением. Очевидным образом J вложима в A, если в A есть нильпотентные элементы. В случае $A = A_1$ (A'_1, A'_2), наличие в $\mathfrak{M}$ тождества $f_1(f'_2)$ дает $J \notin \mathfrak{M}$.

Если R - простая критическая алгебра из $\mathfrak{M}$, то R - изоморфна одной из следующих алгебр:

1. $\Phi = GF(p^t)$ - конечное поле;
2. $\Phi + W$ - конечномерная йорданова алгебра метрики над полем $\Phi = GF(p^t)$;
3. $\Phi_k^{(+)}$ - йорданова алгебра матриц порядка $k, k \geq 3, \Phi = GF(p^t)$;
4. $H(D_k)$ - йорданова алгебра симметричных матриц порядка k в случае $D = \Phi = GF(p^t)$, и эрмитовых матриц порядка k в случае $D = \Phi_2$, где Φ_2 - расщепляемая алгебра кватернионов, $k \geq 3$;

5. $H(\mathbb{C}_3, J_a)$ - исключительная йорданова алгебра эрмитовых 3×3 - матриц над расщепляемой Φ- алгеброй Кэли-Диксона.

Это описание можно найти в [8].

Рассмотрим последовательно эти случаи.

1. $R = GF(p^t)$. Так как в $\mathfrak{M}$ выполняется тождество $h_3(x,y)$ то по лемме 3 $GF(p^t) \subseteq GF(q^2)$. Значит, если $A \neq A_1$, то $R \subseteq GF(q^2) \cong A_1' \subseteq A$. Если же $A = A_1$, то из тождества f_1 следует, что $R \subseteq GF(q)$ и, следовательно, $R \subseteq A$.

2. $R = \Phi + W,\ \ 2 \leq dim_\Phi W < \infty,\ \Phi = GF(p^t)$.

В этом случае алгебра R неассоциативна. Пусть η - порождающий $GF(p^t);\ w \in W,\ w^2 = \eta$. Тогда при $x^\sigma = \eta,\ y^\sigma = w$ имеем

$$h_2^\sigma = \Big((\eta - \eta^q)(1 - \eta^{\frac{q-1}{2}}) \cdot w, z^\sigma, t^\sigma\Big) = 0.$$

Это возможно только при условии $\eta - \eta^q = 0,\ \Phi \subseteq F = GF(q)$. Если $A = A_\infty$, то $R \subseteq A_s \subseteq A$, где $s > dim_\Phi W$ ввиду того, что в бесконечномерной алгебре метрики содержится любая s-мерная алгебра метрики. Если же A - конечномерна, то $R \subseteq A$ по лемме 5.

3-5. Во всех этих случаях $H(\Phi_3') \subseteq R, \Phi' = GF(p)$, поэтому по лемме 4 $R \notin \mathfrak{M}$.

Пусть теперь R - критическая алгебра из $\mathfrak{M}$, имеющая вид $R = B + J$, где B - полупростая алгебра, J - радикал, $B \neq 0, J \neq 0$. Тогда $B = B_1 \oplus ... \oplus B_s$, где B_i - простые алгебры из $\mathfrak{M}$, т.е. простые алгебры вида:

1. $B_i = GF(p^{t_i}) \subseteq GF(q^2)$;

2. $B_i = \Phi_i + W_i$, где $\Phi_i = GF(p^{t_i}) \subseteq F,\ 2 \leq dim_{\Phi_i} W_i < \infty$.

Пусть e - произвольный идемпотент в R. Так как оператор умножения на e в R удовлетворяет уравнению $(2x-1)(x-1)x = 0$, то R разлагается в прямую сумму пространств

$$R_\lambda = \{x \in R \mid xe = \lambda x\},\ (\lambda = 0,\ 1/2,\ 1).$$

Это разложение называется пирсовским разложением алгебры R относительно идемпотента e. Аналогичное разложение допускает радикал J, причем $J_\lambda \subseteq R_\lambda, (\lambda = 0,\ 1/2,\ 1)$. Хорошо известно, что умножение пирсовских компонент R_λ в йордановых алгебрах подчиняется следующим правилам:

$$R_\lambda^2 \subseteq R_\lambda, R_\lambda R_{1/2} \subseteq R_{1/2} (\lambda = 0, 1); R_{1/2}^2 \subseteq R_0 + R_1, R_0 R_1 = 0.$$

Пусть e_k - единица подалгебры B_k $(1 \leq k \leq s)$. Обозначим через $J_\lambda^{(k)}$ пирсовскую λ-компоненту относительно идемпотента e_k. Тогда $J_\lambda^{(k)} \triangleleft R$ и из неразложимости алгебры R следует, что $J = J_1^{(k)}$ либо $J = J_{1/2}^{(k)}$.

Любая йорданова алгебра удовлетворяет следующему тождеству [8] (с.374):

$$(x, y, wz) + (w, y, zx) + (z, y, xw) = 0. \tag{6}$$

Если подставить $x^\sigma = e_k,\ w^\sigma = z^\sigma = e_{k'}\ (k \neq k'),\ y^\sigma = j \in \Im$ в (6), то $je_ke_{k'} = je_{k'}e_k$ (расстановка скобок здесь и далее для произведения элементов алгебры R правонормированная). Если же $x^\sigma = j, y^\sigma = e_1, z^\sigma = e_2, w^\sigma = e_3$ в (6), то $je_2e_1e_3 + je_3e_1e_2 = 2je_1e_2e_3 = 0$. Так как $je_k \neq 0$ для произвольных $j \in \Im,\ 1 \leq k \leq s$ (это следует из неразложимости алгебры R), то из предыдущего равенства следует, что $s \leq 2$. Если $J = J_1^{(1)}$, то подставляя в (6) $x^\sigma = w^\sigma = e_1,\ y^\sigma = e_2,\ z^\sigma = j \in J$, получим $je_2e_1 = je_2 = 0$. Значит, в этом случае $B = B_1$. Таким образом, имеет место следующая

ЛЕММА 5. Пусть $R = B + J$ - критическая алгебра многообразия $\mathfrak{M}$, где B - полупростая алгебра, J - радикал, $B \neq 0, J \neq 0$. Тогда либо

1. $B = B_1, J = J_\lambda^{(1)}$, где $\lambda = 1$ или $\lambda = 1/2$; либо
2. $B = B_1 \oplus B_2,\ J = J_{1/2}^{(1)} = J_{1/2}^{(2)}$.

СЛУЧАЙ 1. $B_1 = \Phi_1 + W_1,\ \Phi_1 \subseteq F,\ 2 \leq dim W_1 < \infty$.

Покажем, что алгебра R в этом случае принадлежит классу $\mathfrak{T}(\Phi_1)$. Положим $x^\sigma = \alpha u_1,\ y^\sigma = u_2$, где $u_1, u_2 \in W_1, \alpha \in \Phi_1,\ u_1^2 \neq 0,\ u_2^2 \neq 0, u_1u_2 \neq 0$. Тогда из равенства $h_1^\sigma = 0$ следует, что

$$[x^\sigma, y^\sigma]^2 = -4u_1^2u_2^2\alpha^2 \in N(R),$$

где $N(R)$ - ассоциативный центр алгебры R. Значит $\gamma\alpha^2, \gamma(\alpha^2 + 1) \in N(R)$ для $\gamma = -4u_1^2u_2^2 \neq 0$ для всех $\alpha \in \Phi_1$. Отсюда, таким же образом, как в конце доказательства импликации $(3 \to 1)$ леммы 1, получаем $\Phi_1 \subseteq N(R)$. Следовательно, по лемме 5 $B = B_1, J = J_1^{(1)}$, так как в противном случае $(e_1, e_1, J) \neq 0$, что неверно ввиду включения $\Phi_1 \subseteq N(R)$.

Осталось показать, что $W_1J = 0$. Пусть

$$u, v \in W_1,\ u^2 \neq 0,\ v^2 = e_1,\ uv = 0,\ e = \frac{e_1 + v}{2},$$

и элемент j лежит в пирсовской компоненте $J_1(e)$ разложения радикала J относительно идемпотента e. Подставляя значения $x_1^\sigma = x_2^\sigma = x_5^\sigma = v, x_3^\sigma = x_4^\sigma = u, x_6^\sigma = j$ в тождество h_4, получим

$$(v, v, u)(u, v, j) = u(u, v, j) = jvuu = juu = 0.$$

С другой стороны, в силу (6), имеем

$$(u, u, vj) + (v, u, uj) = u^2j - juu - juuv = 0.$$

Объединяя оба равенства, получаем $u^2j = 0,\ j = 0$. Следовательно, $J_1(e) = 0$, и аналогично $J_0(e) = 0$. В итоге, $J = J_{1/2}(e)$, и так как W_1 порождается элементами w, такими, что $w^2 = 1$, то $W_1J = 0$. Пользуясь наконец леммой 2, получаем искомое вложение алгебры R в A.

СЛУЧАЙ 2. $B = B_1 \oplus B_2,\ B_i = GF(q_i),\ q_i = p^{t_i},\ (i = 1, 2);\ J = J_{1/2}^{(1)} = J_{1/2}^{(2)}$.

Соотношение $h_3(\alpha, j) = 0$, где $\alpha \in B_1, j \in J$, показывает, что $(\alpha - \alpha^q)j = 0$. С другой стороны,

$$h_2(\alpha, \alpha, e_1, j) = \frac{1}{2}(\alpha - \alpha^q)^2 j = 0.$$

Следовательно, $(\alpha - \alpha^q)^{q^2-1}j = 0$ и $\alpha - \alpha^q = 0$. В итоге получаем $GF(q_1) \subseteq GF(q)$; и аналогично $GF(q_2) \subseteq GF(q)$.

Докажем теперь, что $(B, J, B) = 0$. Если $\alpha_1 \in B_1,\ \alpha_2 \in B_2$, то равенство $(\alpha_1, J, \alpha_2) = 0$ легко следует из (6). Если же в (6) подставить элементы $x^\sigma = j, y^\sigma = z^\sigma = \alpha_1, w^\sigma = e_1$, то получим $2jR_{\alpha_1}^2 = jR_{\alpha_1^2}$ (здесь и дальше R_x - оператор правого умножения в алгебре R на элемент x). Отсюда, по индукции легко показать равенство

$$2^{k-1}jR_{\alpha_1}^k = jR_{\alpha_1^k}$$

для любого $k > 0$. Применяя это равенство к порождающему элементу поля $GF(q_1)$, получаем

$$(B_1, J, B_1) = 0,\ 2jR_{\alpha_1}R_{\beta_1} = jR_{\alpha_1\beta_1}\ (\alpha_1, \beta_1 \in B_1).$$

Аналогично получаем

$$(B_2, J, B_2) = 0,\ 2jR_{\alpha_2}R_{\beta_2} = jR_{\alpha_2\beta_2}\ (\alpha_2, \beta_2 \in B_2).$$

Обозначим $C = B_1 \otimes_{F(p)} B_2$ и определим на J структуру унитального правого C-модуля, полагая

$$j(a \otimes b) = 4jR_aR_b,$$

где $a \in B_1,\ b \in B_2$. Ввиду приведенных выше равенств ясно, что C-модуль J является ассоциативным, и структура B-модуля J однозначно определяется структурой C-модуля J.

Известно [3], что

$$C = B_1 \otimes_{F(p)} B_2 \cong \oplus_{i=1}^{d} K_i,$$

где $K_i \cong K$, где K - композит полей $GF(q_1)$, $GF(q_2)$ в $GF(q)$, $K = GF(p^t)$, $t =$НОК(t_1, t_2), $d =$НОД(t_1, t_2).

Разложению C в прямую сумму полей K_i отвечает разложение J в прямую сумму идеалов JK_i. Но алгебра R подпрямо неразложима, поэтому J совпадает с одним из JK_i и является, таким образом, K-алгеброй. Следовательно, $J = Kj$, где $K \cong C/AnnJ$. Определим вложения полей B_1, B_2 в поле K по правилу

$$\tau(a) = \overline{a \otimes e_2}, \tau(b) = \overline{e_1 \otimes b},$$

где $\overline{x \otimes y}$ образ элемента $x \otimes y$ при гомоморфизме $C \to C/AnnJ$. Тогда $R \cong \tau(B_1) + \tau(B_2) + Kj$. Другими словами, алгебра R имеет следующее матричное представление

$$R \cong \left\{ \begin{pmatrix} \alpha & \gamma \\ 0 & \beta \end{pmatrix} \mid \alpha \in B_1,\ \beta \in B_2,\ \gamma \in K \right\}^{(+)}.$$

Так как в R не выполняются тождества θ_2, θ_3', то алгебра R не принадлежит многообразиям $\mathfrak{M}_2, \mathfrak{M}_3'$. В остальных случаях (разумеется, $\mathfrak{M} \neq \mathfrak{M}_1,\ \mathfrak{M}_1',\ \mathfrak{M}_2'$) имеем $R \subseteq A$.

СЛУЧАЙ 3. $B = GF(p^t) \subseteq \overline{F} = GF(q^2)$.

Если $J = J_{1/2}^{(1)}$, то таким же образом, как в предыдущем случае, получаем

$$R \cong \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & 0 \end{pmatrix} \mid \alpha,\ \beta \in B \ \right\}^{(+)}.$$

Легко проверить, что и здесь выполняются все заключения случая 2.

Пусть теперь $J = J_1^{(1)}$. Если $GF(p^t) \not\subseteq GF(q)$, то $B = B' + B'u$, где $B' = GF(p^l), B' \subseteq GF(q)$, $u^2 = \eta'$ (η' - порождающий элемент поля B'). Пусть, кроме того, η - порождающий элемент поля B. Тогда для произвольного $\alpha \in B'$ имеем $\alpha^2(\eta - \eta^q)^2 \in N(R)$, ввиду тождества $h_2^{\sigma} = 0$. Отсюда, как и ранее, легко получить $B' \subseteq N(R)$. Очевидно проверяется, что

$$u = \eta^{\frac{p^l+1}{2}},\ u - u^q = 2\eta^{\frac{p^l+1}{2}} = 2u.$$

Так как $h_3(u, j) = 2uj = 0$ ($j \in J$), то, ввиду неразложимости алгебры R, получаем $R = \Phi_1 + \Phi_1 u + \Phi_1 j$, т.е. R принадлежит классу $\mathfrak{T}(\Phi_1)$. В итоге, алгебра R не лежит в многообразиях $\mathfrak{M}_2$, $\mathfrak{M}_3$, так как в R не выполняются тождества θ_2, θ_3. В остальных случаях, применяя лемму 2, получаем $R \subseteq A$.

Наконец, рассмотрим случай $J = J_1^{(1)}$, $B = GF(p^t) \subseteq GF(q)$. Структура йорданова B-бимодуля J полностью определяет алгебру R. Из леммы 2.5 [5] следует, что J является однопорожденным B-бимодулем. Значит, алгебра R

является двупорожденной йордановой алгеброй, и по теореме Ширшова [8] алгебра R - специальна. Следовательно ([4], с.106), J - специальный B-бимодуль, т.е. существует мультипликативная специализация δ алгебры B, такая, что $\delta = \frac{1}{2}(\delta_1 + \delta_2)$, где $\delta_1,\ \delta_2$ - ассоциативные специализации B, причем

$$jb_1^{\delta_1}b_2^{\delta_2} = jb_2^{\delta_2}b_1^{\delta_1}$$

для всех $j \in J, b_1, b_2 \in B$ (см. [4], с.100). Теперь на J можно определить структуру ассоциативного B-бимодуля по правилу:

$$j \cdot b = jb^{\delta_1},\ b \cdot j = jb^{\delta_2}.$$

Пусть $S = B + J$ расщепляемое расширение ассоциативного B-бимодуля J. Тогда строение йорданова B-бимодуля J определяется правилом:

$$jb = \frac{1}{2}(j \cdot b + b \cdot j) = j \odot b.$$

Так как йорданов B-бимодуль J неразложим, то и ассоциативный B-бимодуль неразложим, и алгебра S, в этом случае, имеет вид:

$$S \cong \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \sigma(\alpha) \end{pmatrix} \mid \alpha,\ \beta \in GF(p^t) \right\},$$

где σ - фиксированный автоморфизм поля $GF(p^t)$ (см. [6]).

Как йорданов B-бимодуль, J имеет вид Kj, где K - ассоциативная алгебра, порожденная элементами вида $\alpha + \sigma(\alpha)$ ($\alpha \in GF(p^t)$. В итоге, алгебра R имеет следующее матричное представление:

$$R \cong \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \sigma(\alpha) \end{pmatrix} \mid \alpha,\ \beta \in GF(p^t) \right\}^{(+)}.$$

Если $\sigma \neq id$, (id - тождественный автоморфизм поля $GF(p^t)$), то алгебра R неассоциативна, и выполняются все заключения случая 2. Если же $\sigma = id$, то $R \subseteq A$ ($A \neq A_1, A_1', A_2'$).

Тем самым теорема 1, сформулированная в начале параграфа, полностью доказана, причем результат остается верным, если алгебру A рассматривать как алгебру над фиксированным подполем поля $GF(q)$.

В заключение отметим следствие теоремы 1, дающее примеры почти кроссовых многообразий йордановых колец и линейных алгебр.

ТЕОРЕМА 2. Многообразие F-алгебр, порожденное бесконечномерной алгеброй билинейной формы над конечным полем $F, chF \neq 2$, является почти кроссовым.

ДОКАЗАТЕЛЬСТВО. Пусть $\mathfrak{M}_\infty$ - многообразие F-алгебр, порожденное F-алгеброй A_∞. Если $\mathfrak{M}$ - подмногообразие $\mathfrak{M}_\infty$, содержащее бесконечное число критических F-алгебр, то из описания критических алгебр в теореме 1 вытекает, что F-алгебры $A_s,\ A_s',\ s = 1, 2, ...$ лежат в $\mathfrak{M}$, и так как этими алгебрами порождается многообразие $\mathfrak{M}_\infty$, то $\mathfrak{M} = \mathfrak{M}_\infty$. Следовательно, каждое собственное подмногообразие, содержащееся в $\mathfrak{M}_\infty$, порождается конечной йордановой алгеброй, и по теореме Медведева [7] является кроссовым.

References

[1] Э. Артин Геометрическая алгебра. – М.: Наука, 1969.
[2] Е.И. Зельманов, “Абсолютные делители нуля и алгебраические йордановы алгебры”, Сиб. матем. журн., 23:6 (1982), 100–116.
[3] B.R. McDonald Finite rings with identity. Pure and Applied Mathematics, Vol. 28, Marcel Dekker, Inc., New York, 1974.
[4] N. Jacobson, “Structure and Representations of Jordan Algebras,” American Mathematical Society, Providence, R.I., 1968.
[5] И.В. Львов,О многообразиях ассоциативных колец. I, Алгебра и Логика,12:3 (1973),269–297. MR0389973.
[6] Ю.Н. Мальцев, Е.Н. Кузьмин,Базис тождеств алгебры матриц второго порядка надконечным полем, Алгебра и Логика,17:1 (1978), 28–32. MR0516388.
[7] Ю.А. Медведев, “Тождества конечных йордановых *Phi*-алгебр”, Алгебра и логика, 18:6 (1979), 723–748.
[8] К.А. Жевлаков, А.М. Слинько, И.П. Шестаков, А.И. Ширшов, Кольца, близкие к ассоциативным. – М.: Наука, 1978. – 432 с.
[9] С.Ю. Василовский, “Базис тождеств йордановой алгебры билинейной формы над бесконечным полем”, Тр. Ин-та математики, 16 (1989), 5–37

Ismail Musaevich Isaev
Altai State Pedagogical Univercity,
Molodeznaya st. 55,
656031, Barnaul, Russia
E-mail address: isaev@uni-altai.ru