Acta Sci. Math., 52 (1988), 291—302

Описание скрещенных групповых алгебр над конечными полями

К. БУЗАШИ и Т. КРАУС

Пусть группа G содержит бесконечную циклическую подгруппу конечного индекса, K — произвольное поле (с некоторым ограничением на характеристику). В работе [1] показано, что изучение конечнопорожденных KG-модулей сводится к изучению алгебр типа E: скрещенных групповых алгебр над полем K либо бесконечной циклической группы

$$A = \{F, a\}; \quad a\lambda = \lambda^{\varphi} a;$$

либо бесконечной группы диэдра

$$B = \{F, a, b\}; \quad a\lambda = \lambda^{\varphi} a; \quad b\lambda = \lambda^{\psi} b; \quad b^{-1}ab = \gamma a^{-1}; \quad b^2 = \mu,$$

где F — тело, содержащее в своем центре поле K, $\lambda \in F$ — произвольный, $\gamma, \mu \in F$ — фиксированные элементы, φ и ψ — K-автоморфизмы тела F.

В работе [2] были описаны все алгебры типа E над полем $\mathbf{R}$ вещественных чисел, а в работе [3] — все алгебры типа E над конечным полем K, где F — расширение поля K степени 2. В статье [4] был рассмотрен вопрос об изоморфизме алгебр типа E, описанных в работе [3].

В настоящей работе описываются все алгебры типа E над произвольным конечным полем K по отношению к любому конечному расширению F поля K и выяснен вопрос об изоморфизме этих алгебр.

1.

Лемма 1. *Пусть K — конечное поле характеристики $p(\neq 2)$, F — конечное расширение поля K и задана скрещенная групповая алгебра бесконечной группы диедра*

$$B = \{F, a, b\}; \quad a\lambda = \lambda^{\varphi} a; \quad b\lambda = \lambda^{\psi} b; \quad b^{-1}ab = \gamma a^{-1}; \quad b^2 = \mu,$$

Поступило 27 марта 1985 г.

где $\lambda \in F$ — произвольный, γ, $\mu \in F$ — фиксированные элементы, φ и ψ — K-автоморфизмы поля F. Тогда K-автоморфизмы φ и ψ могут иметь порядок 2 или являются тождественными.

Доказательство. Используя определяющие соотношения алгебры B, имеем $b(b\lambda b^{-1})b^{-1} = b\lambda^{\psi} b^{-1} = \lambda^{\psi^2}$. С другой стороны $b(b\lambda b^{-1})b^{-1}b^2\lambda b^{-2} = \mu\lambda\mu^{-1} = \lambda$, значит $\lambda^{\psi^2} = \lambda$, то есть ψ имеет порядок 2 или тождественный автоморфизм.

Рассмотрим автоморфизм φ. С одной стороны $a(b\lambda b^{-1})a^{-1} = a\lambda^{\psi}a^{-1} = \lambda^{\psi\varphi}$, а с другой стороны

$$a(b\lambda b^{-1})a^{-1} = (ab)\lambda(ab)^{-1} = (b\gamma a^{-1})\lambda(b\gamma a^{-1})^{-1} =$$

$$= b\gamma a^{-1}\lambda a\lambda^{-1}b^{-1} = b\gamma\lambda^{\varphi^{-1}}\gamma^{-1}b^{-1} = b\lambda^{\varphi^{-1}}b^{-1} = \lambda^{\varphi^{-1}\psi}.$$

Значит имеем $\lambda^{\psi\cdot\varphi} = \lambda^{\varphi^{-1}\cdot\psi}$. Так как группа автоморфизмов поля F коммутативна, то из последнего равенства получаем $\varphi^2 = 1$. Значит φ либо тождественный автоморфизм поля F, либо имеет порядок 2. Лемма доказана.

Лемма 2. *Имеется 3 основных класса скрещенных групповых алгебр бесконечной группы диедра над K по отношению к полю F:*

(1) $B_1 = \{F, a, b\}$; $a\lambda = \lambda a$; $b\lambda = \lambda b$; $b^{-1}ab = \gamma a^{-1}$; $b^2 = \mu$;

(2) $B_2 = \{F, a, b\}$; $a\lambda = \lambda a$; $b\lambda = \bar{\lambda} b$; $b^{-1}ab = \gamma a^{-1}$; $b^2 = \mu$,

(3) $B_3 = \{F, a, b\}$; $a\lambda = \bar{\lambda} a$; $b\lambda = \bar{\lambda} b$; $b^{-1}ab = \gamma a^{-1}$; $b^2 = \mu$,

где $\lambda \in F$ — произвольный, γ, $\mu \in F$ — фиксированные элементы, $\lambda \to \bar{\lambda}$ — K-автоморфизм 2-го порядка поля F.

Доказательство. Из леммы 1 следует, что существует только 4 основные класса скрещенных групповых алгебр бесконечной группы диедра над полем K по отношению к полю F: алгебры B_1, B_2, B_3 и алгебра

(4) $B_3' = \{F, a, b\}$; $a\lambda = \bar{\lambda} a$; $b\lambda = \lambda b$; $b^{-1}ab = \gamma a^{-1}$; $b^2 = \mu$,

однако замена базиса $a_1 = a$; $b_1 = ab$ алгебру B_3' сводит к типу B_3. Действительно,

$$b_1\lambda = (ab)\lambda = a\lambda b = \bar{\lambda}(ab) = \bar{\lambda} b_1,$$

$$b_1^{-1}a_1b_1 = (ab)^{-1}a(ab) = b^{-1}ab = \gamma a^{-1} = \gamma a_1^{-1},$$

$$b_1^2 = (ab)^2 = abab = b\gamma a^{-1}ab = \gamma b^2 = \gamma\mu = \mu_1.$$

Лемма доказана.

Пусть порядок поля K равен $|K|=p^m$ и степень расширения $(F:K)=n$. Тогда порядок поля F равен $|F|=p^{nm}$ и все K-автоморфизмы поля F имеют вид $\lambda\to\lambda^{p^{im}}$ $(i=0, 1, \ldots, n-1)$.

Очевидна следующая

Теорема 1. *Все алгебры типа E над полем K по отношению к полю F, являющиеся скрещенными групповыми алгебрами бесконечной циклической группы (a), задаются формулой*

$$E_i = \{F, a\};\quad a\lambda = \lambda^{p^{im}}a\quad (\lambda\in F;\ i=0, 1, \ldots, n-1).$$

Замечание 1. Квадраты элементов мультипликативной группы F^* поля F образуют подгруппу F_1 группы F^* индекса 2, значит группа F^* разлагается в объединение смежных классов

$$F^* = F_1 \cup \xi\cdot F_1,$$

где $\xi\in F^*$ — фиксированный квадратный невычет в поле F.

Теорема 2. *Основной класс B_1 алгебр типа E (см.* (1)*) сводится к типам алгебр*

$$A_1 = \{F, a, b\};\quad a\lambda=\lambda a;\quad b\lambda = \lambda b;\quad b^{-1}ab = a^{-1};\quad b^2 = 1,$$

$$A_2 = \{F, a, b\};\quad a\lambda = \lambda a;\quad b\lambda = \lambda b;\quad b^{-1}ab = \xi a^{-1};\quad b^2 = 1;$$

$$A_3 = \{F, a, b\};\quad a\lambda = \lambda a;\quad b\lambda = \lambda b;\quad b^{-1}ab = a^{-1};\quad b^2 = \xi;$$

где $\lambda\in F$, ξ — фиксированный квадратный невычет в поле F.

Доказательство. В зависимости от того, элемент μ алгебры B_1 лежит в подгруппе F_1 (см. замечание 1) или нет, замена базиса $a_1=a$; $b_1=\sqrt{\mu^{-1}}\cdot b$ или $a_1=a$; $b_1=\sqrt{f^{-1}}\cdot b$, где $\mu=\xi\cdot f$; $f\in F_1$, приводит к соотношениям $b_1^2=1$ или $b_1^2=\xi$ в алгебре B_1, причем остальные соотношения не изменяются.

Теперь, в зависимости от того, элемент γ лежит в подгруппе F_1 или нет, сделаем опять замена базиса $a_1=\sqrt{\gamma^{-1}}\,a$; $b_1=b$, или $a_1=\sqrt{f_1^{-1}}\,a$; $b_1=b$ где $\gamma=\xi\cdot f_1$, $f_1\in F_1$, что ведет к соотношениям $b_1^{-1}a_1b_1=a_1^{-1}$ или $b_1^{-1}a_1b_1=\xi\cdot a_1^{-1}$.

В конечном счете получаем алгебры типов A_1, A_2, A_3 и алгебру

$$A_2' = \{F, a, b\};\quad a\lambda = \lambda a;\quad b\lambda = \lambda b;\quad b^{-1}ab = \xi a^{-1};\quad b^2 = \xi,$$

однако новая замена базиса $a_1=a$; $b_1=\xi^{-1}ab$:

$$(\xi^{-1}ab)^2 = \xi^{-2}abab = \xi^{-2}b\xi a^{-1}ab = \xi^{-1}b^2 = 1$$

приводит эту алгебру к типу A_2. Теорема доказана.

Замечание 2. Если степень расширения основного поля K неченое число: $(F:K)=2k+1$, то все алгебры типа E над полем K по отношению к полю F

осчерпываются алгебрами типов E_i, A_1, A_2, A_3 $(i=0, 1, \ldots, n-1)$, описанных в теоремах 1 и 2.

Доказательство. Так как группа K-автоморфизмов поля F имеет порядок $2k+1$, то K-автоморфизмов второго порядка поле F не имеет. Значит основных классов B_2 и B_3 алгебр типа E в этом случае не существует.

Рассмотрим случай, когда степень расширения поля K — четное число: $(F:K)=2k$. Тогда K-автоморфизм второго порядка поля F имеет вид $\lambda\to\lambda^{p^{km}}$.

В дальнейшем будем пользоваться следующей леммой, которая является частным случаем известного результата об автоморфизмах конечного порядка.

Лемма 3. *Пусть элемент $\alpha\in F$ выдерживает K-автоморфизм φ второго порядка поля F. Тогда существует такой элемент $\beta\in F$, для которого выполняется равенство*

$$\alpha = \beta\cdot\beta^{\varphi}. \tag{5}$$

Лемма 4. *Основные классы B_2 и B_3 алгебр типа E* (см. (2) и (3)) *сводятся к основным классам алгебр типа E над K:*

$$B_2' = \{F, a, b\};\quad a\lambda = \lambda a;\quad b\lambda = \lambda^{p^{km}}b;\quad b^{-1}ab = \gamma a^{-1};\quad b^2 = 1;$$

$$B_3' = \{F, a, b\};\quad a\lambda = \lambda^{p^{km}}a;\quad b\lambda = \lambda^{p^{km}}b;\quad b^{-1}ab = \gamma a^{-1};\quad b^2 = 1,$$

где $\lambda\in F$ — произвольный, $\gamma\in F$ — фиксированный элемент.

Доказательство. В алгебрах B_2 и B_3 элемент μ выдерживает автоморфизм $\mu\to\mu^{p^{km}}$. Действительно, $\mu^{p^{km}}=b\mu b^{-1}=bb^2b^{-1}=b^2=\mu$. Но тогда и элемент μ^{-1} выдерживает этот автоморфизм, и, согласно Лемме 3, существует такой элемент $\mu_1\in F$, что $\mu^{-1}=\mu_1\cdot\mu_1^{p^{km}}$. Сделаем замену базиса $a_1=a$; $b_1=\mu_1 b$ в обоих алгебрах B_2, B_3:

$$b_1^2 = (\mu_1 b)^2 = \mu_1 b\mu_1 b = \mu_1\mu_1^{p^{km}}b^2 = \mu^{-1}\mu = 1,$$

$$b_1^{-1}a_1b_1 = (\mu_1 b)^{-1}a(\mu_1 b) = b^{-1}\mu_1^{-1}a\mu_1 b = b^{-1}ab = \gamma a^{-1} = \gamma a_1^{-1}$$

в алгебре B_2, а в алгебре B_3:

$$b_1^{-1}a_1b_1 = (\mu_1 b)^{-1}a(\mu_1 b) = b^{-1}\mu_1^{-1}a\mu_1 b = \mu_1^{-p^{km}}\cdot\mu_1 b^{-1}ab = \gamma_1 a_1^{-1},$$

для некоторого $\gamma_1\in F$. Лемма доказана.

Теорема 3. *Общий класс алгебр B_2' (см. лемму 4) сводится к алгебре типа*

$$A_4 = \{F, a, b\};\quad a\lambda = \lambda a;\quad b\lambda = \lambda^{p^{km}}b;\quad b^{-1}ab = a^{-1};\quad b^2 = 1\quad (\lambda\in F).$$

Доказательство. Покажем, что в алгебре B_2' элемент γ выдерживает автоморфизм $\gamma \to \gamma^{p^{km}}$. Действительно, с одной стороны

$$b^{-1}(b^{-1}ab)b = b^{-1}\gamma a^{-1}b = \gamma^{p^{km}}(\gamma a^{-1})^{-1} = \gamma^{p^{km}}a\gamma^{-1} = \gamma^{p^{km}} \cdot \gamma^{-1} \cdot a,$$

а с другой стороны $b^{-1}(b^{-1}ab)b = b^{-2}ab^2 = a$. Значит $\gamma^{p^{km}} \cdot \gamma^{-1} = 1$ то есть $\gamma^{p^{km}} = \gamma$.

Тогда, используя лемму 3, для элемента γ^{-1} существует такой элемент $\gamma_1 \in F$, что $\gamma^{-1} = \gamma_1 \cdot \gamma_1^{p^{km}}$. Сделаем теперь подстановку $a_1 = \gamma_1 a$; $b_1 = b$ и получаем

$$b_1^{-1}a_1b_1 = b^{-1}(\gamma_1 a)b = \gamma_1^{p^{km}} \cdot \gamma^{-1}a = \gamma_1^{p^{km}} \cdot \gamma_1^{-1} \cdot \gamma_1^{-p^{km}}a^{-1} = (\gamma_1 a)^{-1} = a_1^{-1}.$$

Теорема доказана.

Теорема 4. *Общий класс алгебр B_3 (см. Лемму 4) сводится к алгебрам типов*

$$A_5 = \{F, a, b\}; \quad a\lambda = \lambda^{p^{km}} \cdot a; \quad b\lambda = \lambda b; \quad b^{-1}ab = a^{-1}; \quad b^2 = 1,$$

$$A_6 = \{F, a, b\}; \quad a\lambda = \lambda^{p^{km}} \cdot a; \quad b\lambda = \lambda^{p^{km}} \cdot b; \quad b^{-1}ab = \xi a^{-1}; \quad b^2 = 1,$$

где $\lambda \in F$ — произвольный элемент, ξ — фиксированный квадратный невычет в поле F.

Доказательство. Если элемент γ в алгебре B_3' является квадратом в поле F, то подстановка $a_1 = a \cdot \sqrt{\gamma^{-1}}$; $b_1 = b$ алгебру B_3' сводит к алгебре типа

$$A_5' = \{F, a, b\}; \quad a\lambda = \lambda^{p^{km}} \cdot a; \quad b\lambda = \lambda^{p^{km}} \cdot b; \quad b^{-1}ab = a^{-1}; \quad b^2 = 1.$$

Действительно,

$$b_1^{-1}a_1b_1 = b^{-1}(a\sqrt{\gamma^{-1}})b = \gamma a^{-1} \cdot \sqrt{\gamma^{-1}}^{p^{km}} = \gamma \cdot \sqrt{\gamma^{-1}}\, a^{-1} = (a\sqrt{\gamma^{-1}})^{-1} = a_1^{-1}.$$

Однако дополнительная замена $a_1 = a$; $b_1 = ab$ алгебру A_5' сводит к алгебре A_5:

$$(ab)\lambda = a\lambda^{p^{km}}b = \lambda(ab); \quad (ab)^{-1}a(ab) = b^{-1}ab = a^{-1}.$$

Если же элемент γ не является квадратом в поле F, то $\gamma = \xi f, f \in F_1$ (см. (4)), и замена базиса $a_1 = a\sqrt{f^{-1}}$; $b_1 = b$ алгебру B_3' сводит к алгебре A_6:

$$b_1^{-1}a_1b_1 = b^{-1}(a\sqrt{f^{-1}})b = \gamma a^{-1}\sqrt{f^{-1}}^{p^{km}} =$$

$$= \gamma\sqrt{f^{-1}}\,a^{-1} = \xi\sqrt{f}\,a^{-1} = \xi(a\sqrt{f^{-1}})^{-1} = \xi a_1^{-1}.$$

Теорема доказана.

Следствие 1. *Все алгебры типа E над конечным полем K характеристики $p(\neq 2)$ по отношению к полю F, где $|K| = p^m$, $(F:K) = n$ имеют вид:*

При нечетном n:

$$E_i = \{F, a\}; \quad a\lambda = \lambda^{p^{im}} \cdot a \quad (\lambda \in F;\ i = 0, 1, \ldots, n-1),$$

$$A_1 = \{F, a, b\}; \quad a\lambda = \lambda a; \quad b\lambda = \lambda b; \quad b^{-1}ab = a^{-1}; \quad b^2 = 1,$$

$$A_2 = \{F, a, b\}; \quad a\lambda = \lambda a; \quad b\lambda = \lambda b; \quad b^{-1}ab = \xi a^{-1}; \quad b^2 = 1,$$

$$A_3 = \{F, a, b\}; \quad a\lambda = \lambda a; \quad b\lambda = \lambda b; \quad b^{-1}ab = a^{-1}; \quad b^2 = \xi,$$

где $\gamma \in F$ — произвольный элемент, ξ — фиксированный квадратный невычет в поле F. Алгебра E_0 — групповая алгебра бесконечной циклической группы (a) над полем F, E_i $(i=1, 2, \ldots, n-1)$ — скрещенные групповые алгебры группы (a) над полем F. Алгебра A_1 — групповая алгебра бесконечной группы диэдра D над полем F; A_2, A_3 — скрещенные групповые алгебры группы D над F.

При четной степени $n=2k$ расширения поля K: Алгебры E_i $(i=0, 1, \ldots, n-1)$, A_1, A_2, A_3 и

$$A_4 = \{F, a, b\}; \quad a\lambda = \lambda a; \quad b\lambda = \lambda^{p^{km}} \cdot b; \quad b^{-1}ab = a^{-1}; \quad b^2 = 1,$$

$$A_5 = \{F, a, b\}; \quad a\lambda = \lambda^{p^{km}} \cdot a; \quad b\lambda = \lambda b; \quad b^{-1}ab = a^{-1}; \quad b^2 = 1,$$

$$A_6 = \{F, a, b\}; \quad a\lambda = \lambda^{p^{km}} \cdot a; \quad b\lambda = \lambda^{p^{km}} \cdot b; \quad b^{-1}ab = \xi a^{-1}; \quad b^2 = 1,$$

где $\gamma \in F$ — произвольный элемент, ξ — фиксированный квадратный невычет в поле F. Алгебры A_4, A_5, A_6 — скрещенные групповые алгебры группы D над полем F.

2.

В этом параграфе рассмотрим вопрос об изоморфизме K-алгебр E_i, A_j $(i=0, 1, \ldots, n-1;\ j=1, 2, \ldots, 6)$. В дальнейшем будем пользоваться следующей леммой, которая доказывается в работе [1].

Лемма 5. *Пусть $A=\{F, a, b\}$; $b^2=1$ — алгебра типа E с делителями нуля. Тогда существует не более четырех попарно неизоморфных A-модулей M, являющихся свободными циклическими $F(a)$-модулями. Если для некоторого элемента $\gamma \in F$ выполняется равенство $(\gamma ab)^2=1$, то A-модуль M изоморфен одному из модулей*

$$I_1 = A(1+b); \quad I_2 = A(1-b); \quad I_3 = A(1+\gamma ab); \quad I_4 = A(1-\gamma ab).$$

В противном случае модуль M изоморфен одному из модулей I_1, I_2. Модули I_1 и I_2 (соответственно I_3 и I_4) не изоморфны тогда и только тогда, когда элемент b (соответственно γab) перестановочен со всеми элементами поля F. Каждый из модулей I_3, I_4 не изоморфен ни одному из модулей I_1, I_2.

Также из работы [1] следует

Лемма 6. *Пусть* $A=\{F, a, b\}$; $b^2=1$ *и* $B=\{F, a, b\}$; $b^2=1$ — *изоморфные алгебры типа Е над полем К. Тогда числа неизоморфных А-модулей и В-модулей, являющихся свободными циклическими* $F(a)$*-модулями, равны.*

Теорема 6. *Алгебра* E_0 *не К-изоморфна ни одной из алгебр* E_i $(i=1, 2, \ldots, n-1)$, A_j $(j=1, 2, \ldots, 6)$.

Доказательство. Алгебра E_0 коммутативна, а все алгебры E_i, A_j $(i=1, 2, \ldots, n-1;\ j=1, 2, \ldots, 6)$ не коммутативны. Так как при изоморфизме коммутативность алгебр сохраняется, то теорема очевидна.

Теорема 6. *Алгебры* E_i $(i=1, 2, \ldots, n-1)$ *попарно К-изоморфны алгебрам* E_j $(j=1, 2, \ldots, n-1)$, $i\neq j$, *тогда и только тогда, когда* $j=n-i$, *и попарно не К-изоморфны алгебрам* A_l $(l=1, \ldots, 6)$.

Доказательство. Сначала докажем первое утверждение теоремы. Пусть

$$E_i=\{F, a_1\};\quad a_1\lambda=\lambda^{p^{im}}\cdot a_1\quad(\lambda\in F),\quad E_j=\{F, a_2\};\quad a_2\lambda=\lambda^{p^{jm}}\cdot a_2\quad(\lambda\in F)$$

для фиксированных $i\neq j$ $(i, j=1, 2, \ldots, n-1)$, и имеет место K-изоморфизм φ: $E_i\to E_j$. Так как множество элементов конечного порядка в обоих алгебрах совпадает с полем F, то ограничение $\varphi|_F$ K-изоморфизма φ на поле F является K-автоморфизмом поля F. Значит на поле F изоморфизм φ задается в виде φ: $\lambda\to\lambda^{p^{sm}}$, где s — фиксированное натуральное число $(1\leqq s\leqq n)$. Все обратимые элементы в E_j имеют вид δa_2^r $(\delta\in F)$. Так как элемент a_1 обратим в E_i, то $\varphi(a_1)=\delta a_2^r$ $(\delta\in F)$. Однако $\varphi(a_1^t)=(\delta a_2^r)^t=\delta_1 a_2^{tr}$. Элементы вида $\sum\limits_{\nu}\delta_\nu a^{\nu r}$ не исчерпывают все элементы алгебры E_j только в случае $r=\pm 1$, поэтому при изоморфизме φ алгебр E_i и E_j должно выполняться $\varphi(a_1)=\delta a_2$, или $\varphi(a_1)=\delta a_2^{-1}$. Рассмотрим первый случай.

С одной стороны для произвольного $\lambda\in F$ имеем

$$\varphi(a_1\lambda a_1^{-1})=\varphi(a_1)\varphi(\lambda)\varphi(a_1)^{-1}=\delta a_2\lambda^{p^{sm}}a_2^{-1}\delta^{-1}=\delta(\lambda^{p^{sm}})^{p^{jm}}\delta^{-1}=\lambda^{p^{(s+j)m}}.$$

С другой стороны

$$\varphi(a_1\lambda a_1^{-1})=\varphi(\lambda^{p^{im}})=(\lambda^{p^{sm}})^{p^{im}}=\lambda^{p^{(s+i)m}}.$$

Следовательно

$$p^{(s+i)m}\equiv p^{(s+j)m}\pmod{p^{nm}-1},$$

что означает $p^{nm}-1\,|\,p^{(i-j)m}-1$. Так как $1\leqq i\neq j\leqq n$, то последнее невозможно.

Рассмотрим теперь случай $\varphi(a_1)=\delta a_2^{-1}$. Повторяя рассуждения, сделанные в предыдущем случае, приходим к сравнению

$$p^{(s+i)m}\equiv p^{(s-j)m}\pmod{p^{nm}-1},$$

которое выполняется тогда и только тогда, когда $j\equiv -i \pmod n$. Это значит, что $E_i\cong E_j$ тогда и только тогда, когда $i=n-i$.

Покажем теперь, что каждая алгебра E_i $(i=1, \ldots, n-1)$ не K-изоморфна ни одной из алгебр $A_1, A_2, \ldots, A_6$. Действительно, алгебра E_i не содержит делителей нуля, значит она не может быть K-изоморфна ни одной из алгебр A_1, A_2, A_4, A_5, A_6, так как все они содержат делителей нуля (напр. $(1+b)\cdot (1-b)=0$).

Осталось показать, что алгебры E_i $(i=1, 2, \ldots, n-1)$ не K-изоморфны алгебре A_3. Действительно, пусть φ: $A_3\to E_i$ K-изоморфизм алгебры, заданной соотношениями

$$A_3 = \{F, a_1, b_1\};\quad a_1\lambda = \lambda a_1;\quad b_1\lambda = \lambda b_1;\quad b_1^{-1}a_1b_1 = a_1^{-1};\quad b_1^2 = \xi$$

на алгебру $E_i=\{F, a\}$; $a\lambda=\lambda^{p^{im}}\cdot a$. Так как элементы a_1 и b_1 обратимы в алгебре A_3, то их образы тоже обратимы в E_i, то есть

$$\varphi(a_1) = \delta a^s;\quad \varphi(b_1) = \delta_1 a^{s_1}\quad (\delta, \delta_1\in F).$$

Тогда, с одной стороны

$$\varphi(b_1^{-1}a_1b_1) = \varphi(b_1)^{-1}\varphi(a_1)\varphi(b_1) = a^{-s_1}\delta_1^{-1}\delta a^s\delta_1 a^{s_1} = \delta_2 a^s$$

для некоторого элемента $\delta_2\in F$, а с другой стороны

$$\varphi(b_1^{-1}a_1b_1) = \varphi(a_1^{-1}) = (\delta a^s)^{-1} = a^{-s}\delta^{-1} = \delta_3 a^{-s}\quad (\delta_3\in F).$$

Сравнивая два равенства, получаем $s=-s$, то есть $s=0$. Следовательно, $\varphi(a_1)=\delta$. Однако, в поле F элемент δ имеет конечный порядок, когда элемент a_1 — бесконечного порядка в алгебре A_3. Противоречие доказывает неизоморфность алгебр E_i и A_3. Теорема доказана.

Лемма 7. *Число n_i A_i-модулей $(i=1, 2, 4, 5, 6)$, являющихся свободными циклическими $F(a)$-модулями, задается следующим образом:*

1. $n_1=4$, *они изоморфны модулям*

$$I_1^{(1)} = A_1(1+b);\quad I_2^{(1)} = A_1(1-b);\quad I_3^{(1)} = A_1(1+ab);\quad I_4^{(1)} = A_1(1-ab).$$

2. $n_2=2$, *они изоморфны модулям*

$$I_1^{(2)} = A_2(1+b);\quad I_2^{(2)} = A_2(1-b).$$

3. $n_4=2$, *они изоморфны модулям*

$$I_1^{(4)} = A_4(1+b);\quad I_3^{(4)} = A_4(1+ab),$$

4. $n_5=3$, *они изоморфны модулям*

$$I_1^{(5)} = A_5(1+b);\quad I_2^{(5)} = A_5(1-b);\quad I_3^{(5)} = A_5(1+ab).$$

5. $n_6=1$, *он изоморфен модулю*

$$I_1^{(6)} = A_6(1+b).$$

Доказательство. Так как в алгебре A_1 выполняются равенства $b^2=1$, $(ab)^2=1$, кроме того элементы b и ab перестановочны со всеми элементами поля F, то, согласно Лемме 5, утверждение 1 доказано.

Покажем, что в алгебре A_2 нет таких элементов $\gamma\in F$, что $(\gamma ab)^2=1$. Действительно,

$$(\gamma ab)^2 = \gamma^2 abab = \gamma^2 b\xi a^{-1}ab = \gamma^2\xi b^2 = \gamma^2\xi = 1,$$

то есть $\gamma^2\in\xi^{-1}$. Однако последнее равенство противоречит тому, что элемент ξ — квадратный невычет в поле F. Так как в алгебре A_2 имеет место $b^2=1$ и элемент b перестановочен со всеми элементами поля F, то, используя лемму 5, отсюда получаем утверждение 2 леммы.

В алгебре A_4 выполняется $b^2=1$ и $(ab)^2=1$, но ни элемент b, ни элемент ab не перестановочны со всеми элементами поля F. Значит, согласно Лемме 5, имеет место утверждение 3 леммы.

В алгебре A_5 выполняются равенства $b^2=1$ и $(ab)^2=1$, элемент b перестановочен со всеми элементами поля F, однако $(ab)\lambda=a\lambda b=\lambda^{p^{km}}(ab)$, значит из леммы 5 следует утверждение 4 леммы.

Покажем, что в алгебре A_6 нет таких элементов $\gamma\in F$, что $(\gamma ab)^2=1$. Действительно,

$$(\gamma ab)^2 = \gamma ab\gamma ab = \gamma a\gamma^{p^{km}} bab = \gamma\gamma^{p^{2km}} abab = \gamma^2 b\xi a^{-1}ab = \gamma^2\xi^{p^{km}} = 1,$$

то есть $\gamma^2=\xi^{-p^{km}}$. Элемент ξ — квадратный невычет в поле F. Каждый примитивный элемент поля F лежит в смежном классе $\xi\cdot F_1$ (см. замечание 1), значит можно считать, что элемент ξ — примитивный в поле F. Ищем элемент γ в виде $\gamma=\xi^s$. Тогда $\xi^{2s}=\xi^{-p^{km}}$, что ведет к сравнению

$$2s \equiv -p^{km} \pmod{p^{2km}-1}.$$

Так как наибольший общий делитель $(2, p^{2km}-1)=2$, но число p — нечетно, то последнее сравнение неразрешимо.

В алгебре A_6 выполняется равенство $b^2=1$, но элемент b не перестановочен со всеми элементами поля F, поэтому из леммы 5 следует утверждение 5 леммы. Лемма доказана.

Теорема 7. *Алгебры* $A_1, A_2, \ldots, A_6$ *попарно не* K*-изоморфны.*

Доказательство. Покажем сначала, что алгебра A не содержит делителей нуля. Так как все алгебры A_1, A_2, A_4, A_5, A_6 содержат делителей нуля, то из этого будет следовать неизоморфность алгебры A_3 с алгебрами A_i $(i=1, 2, 4, 5, 6)$.

Пусть L — поле частных групповой алгебры $F(a)$ бесконечной циклической группы (a) над полем F. Тогда алгебра A_3 погружается в алгебру

$$A = \{L, b\}, \quad b^2 = \xi, \tag{6}$$

которая является скрещенным произведением поля L с автоморфизмом второго порядка, порожденным элементом b.

Согласно общей теории алгебр, A является либо полным матричным кольцом второго порядка (и тогда имеет делителей нуля), либо телом (см. например [5]). Первая возможность имеет место тогда и только тогда, когда элемент ξ (см. (6)) есть норма для некоторого элемента $x \in L$ относительно автоморфизма $\lambda \to \lambda^b$, то есть

$$\xi = x \cdot x^b. \tag{7}$$

Пусть

$$x = \frac{\sum_i \lambda_i a^i}{\sum_j \mu_j a^j} \quad (\lambda_i, \mu_j \in F).$$

Подставим выражение элемента x в формулу (7):

$$\frac{\sum_i \lambda_i a^i}{\sum_j \mu_j a^j} \cdot \frac{\sum_i \lambda_i a^{-i}}{\sum_j \mu_j a^{-j}} = \xi,$$

откуда получаем равенство

$$\sum_i \lambda_i a^i \cdot \sum_i \lambda_i a^{-i} = \xi \cdot \sum_j \mu_j a^j \cdot \sum_j \mu_j a^{-j}, \tag{8}$$

в групповой алгебре $F(a)$. Так как $F(a)$ — кольцо главных идеалов, то элемент $\sum_i \lambda_i a^i$ однозначно (с точностью до единиц кольца) представляется в виде произведения простых элементов

$$\sum_i \lambda_i a^i = \tau \cdot p_1 \cdot \ldots \cdot p_s \quad (p_i \in F(a), \tau \in F). \tag{9}$$

Тогда левая сторона равенства (9) имеет вид $\tau^2 \cdot p_i \cdot \ldots \cdot p_s \cdot p_1^b \cdot \ldots \cdot p_s^b$. Ввиду однозначности разложения элементов кольца $F(a)$ в произведение простых элементов, правая сторона равенства (8) разлагается в произведение тех же простых элементов кольца $F(a)$ причем с точностью до констант из F, что и левая сторона, ибо при

$$\sum_j \mu_j a^j = \delta a^b \cdot p_1 \cdot \ldots \cdot p_s$$

автоморфный образ этого элемента имеет вид

$$\left(\sum_j \mu_j a^j\right)^b = \delta a^{-b} \cdot p_1^b \cdot \ldots \cdot p_s^b,$$

то есть приходим к равенству

$$\tau^2 \cdot p_1 \cdot \ldots \cdot p_s \cdot p_1^b \cdot \ldots \cdot p_s^b = \xi \cdot \delta^2 \cdot p_1 \cdot \ldots \cdot p_s \cdot p_1^b \cdot \ldots \cdot p_s^b.$$

Отсюда следует $\tau^2 = \xi\delta^2$. Так как ξ — квадратный невычет в поле F, то последнее равенство невозможно. Противоречие доказывает, что алгебра не содержит делителей нуля.

Согласно лемме 7, число неизоморфных A_i-модулей $(i=1, 2, 4, 5, 6)$, являющихся свободными циклическими $F(a)$-модулями для этих модулей попарно различается, кроме алгебр A_2 и A_4. Поэтому, согласно лемме 6, среди алгебр A_1, A_2, A_4, A_5, A_6 могут быть K-изоморфны только алгебры A_2 и A_4.

Очевидно, центр алгебры A_2 совпадает с полем F, значит число обратимых элементов центра алгебры A_2 равно $p^{nm}-1$.

В то же время, если θ — примитивный элемент поля F, то группа всех обратимых элементов центра алгебры A_4 порождается элементом $\theta^{p^{km}+1}$, где $n=2k$. Действительно, из равенства

$$b \cdot \theta^x = (\theta^x)^{p^{km}} \cdot b = \theta^x b$$

следует сравнение

$$x(p^{km}-1) \equiv 0 \pmod{p^{nm}-1}$$

или

$$x \equiv 0 \pmod{p^{km}+1}.$$

Значит, число всех обратимых элементов центра алгебры равно числу $p^{km}=1$.

Так как при изоморфизме центральные элементы переходят в центральные, обратимые в обратимые, то алгебры A_2 и A_4 не K-изоморфны. Теорема доказана.

Следствие 2. *Все не K-изоморфные алгебры типа E над полем K характеристики p $(\neq 2)$ по отношению к полю F, где $|K|=p^m$, $(F: K)=n$ задаются алгебрами типов:*

При четном n: алгебры $E_i \left(i=0, 1, \ldots, \left[\frac{n}{2}\right]\right)$ *и* A_j $(j=1, 2, 3, 4, 5, 6)$.

При нечетном n: алгебры $E_i \left(i=0, 1, \ldots, \left[\frac{n}{2}\right]\right)$ *и* A_j $(j=1, 2, 3)$, *где алгебры* E_i, A_j *заданы в следствии* 1.

Литература

[1] С. Д. Берман—К. Бузаши, О модулях над групповыми алгебрами групп, содержащих бесконечную циклическую подгруппу конечного индекса, *Studia Sci. Math. Hungar,* **16** (1981), 455—470.

[2] С. Д. Берман—К. Бузаши, Описание всех конечномерных вещественных представлений групп, содержащих бесконечную циклическую подгруппу конечного индекса, *Publ. Math. Debrecen,* **31** (1984), 133—144.

[3] К. Бузаши—Т. Краус—Абд Эл Монеим, О скрещенных групповых алгебрах над конечными полями, *Publ. Math. Debrecen,* **33** (1986), 147—152.

[4] К. Бузаши, Об изоморфизме скрещенных алгебр над конечными полями, *Publ. Math. Debrecen,* **33** (1986).

[5] A. A. Albert, *Structure of Algebras,* Colloquium Publ., vol. 24, Amer. Math. Soc. (Providence, R. I., 1938).

[6] A. Weil, *Basic number theory,* Springer (Berlin, 1967).

KLTE MATEMATIKAI INTÉZET
PF. 12
4010 DEBRECEN, HUNGARY