

О скрещенных групповых алгебрах над конечными полями

К. БУЗАШИ—Т. КРАУС—З. М. АБД ЕЛ МОНЕИМ (Дебрецен)

Пусть K — произвольное поле, L — тело, содержащее в своем центре поле K . Алгеброй типа E над полем K называется скрещенное произведение тела L либо с бесконечной циклической группой (a) :

$$\{L, a\}; \lambda a = a\lambda^a,$$

($\lambda \in L$; φ -автоморфизм тела L , оставляющий на месте элементы поля K), либо с бесконечной группой диэдра D :

$$\{L, a, b\}; \lambda a = a\lambda^a; \lambda b = b\lambda^b; b^{-1}ab = \gamma a^{-1}; b^2 = \mu.$$

($\lambda, \gamma, \mu \in L$; φ и ψ — K -автоморфизмы тела L).

В работах [3], [4] и [5] были описаны все алгебры типа E над полем действительных чисел. В этом случае в качестве тела L могут служить только само поле $\mathbf{R}$ вещественных чисел, поле комплексных чисел $\mathbf{C}$ и тело кватернионов Q , поэтому всех типов вещественных алгебр типа E всего 15.

В том случае, когда K — конечное поле, все расширения L будут полями, однако их очень много. Простейшим видом алгебр типа E над конечным полем K является такая скрещенная групповая алгебра, в которой L — расширение поля K степени 2. В настоящей работе будем заниматься описанием таких алгебр типа E .

Пусть K — фиксированное конечное поле характеристики $p (\neq 2)$, а L — расширение поля K степени 2.

Сначала сделаем несколько замечаний о K -автоморфизмах поля L . Так как $(L:K)=2$, то существует элемент $\theta \in L$, что $L=K(\theta)$, где θ — корень неприводимого над K полинома

$$p(x) = x^2 - \eta \in K[x].$$

Каждый элемент поля L представляется в виде

$$x = c_0 + c_1\theta \quad (c_i \in K).$$

Тогда любой K -автоморфизм поля L имеет вид

$$\varphi: c_0 + c_1\theta \rightarrow c_0 + c_1\theta_1,$$

где $p(\theta_1)=0$. Используя теорему Вьета, получаем

$$\theta_1 = -\theta.$$

Значит имеется точно два K -автоморфизма поля L :

$$(1) \quad \begin{aligned} \varphi_0: \alpha_0 + \alpha_1 \theta &\rightarrow \alpha_0 + \alpha_1 \theta, \\ \varphi_1: \alpha_0 + \alpha_1 \theta &\rightarrow \alpha_0 - \alpha_1 \theta. \end{aligned}$$

Введем обозначение

$$\varphi_1(x) = \bar{x} \quad (x \in L).$$

Будем описывать все алгебры типа E над полем K .

Теорема 1. *Существует точно два вида алгебр типа E , являющихся скрещенным произведением поля L на бесконечную циклическую группу (a) :*

$$(2) \quad A_1 = \{L, a\}; \lambda a = a\lambda, \quad (\lambda \in L),$$

$$(3) \quad A_2 = \{L, a\}; \lambda a = a\bar{\lambda}, \quad (\lambda \in L).$$

Ввиду замечаний о K -автоморфизмах поля L , существует всего 4 общих типов алгебр типа E над полем K , являющихся скрещенным произведением поля L на бесконечную группу диэдра D :

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

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

$$(III) \quad B_3 = \{L, a, b\}; \lambda a = a\lambda; \lambda b = b\bar{\lambda}; b^{-1}ab = \gamma a^{-1}; b^2 = \mu \quad (\lambda, \gamma, \mu \in L),$$

$$(IV) \quad B_4 = \{L, a, b\}; \lambda a = a\bar{\lambda}; \lambda b = b\bar{\lambda}; b^{-1}ab = \gamma a^{-1}; b^2 = \mu \quad (\lambda, \gamma, \mu \in L).$$

Замечание 1. *Общий тип алгебр, заданный соотношениями (II) путем замены базиса сводится к общему типу, заданному соотношениями (IV).*

Доказательство. Переходим к базису $a_1=a$; $b_1=ab$ и получаем

$$\lambda a_1 = \lambda a = a\bar{\lambda} = a_1\bar{\lambda},$$

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

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

$$b_1^2 = (ab)^2 = ab \cdot ab = b\gamma a^{-1}ab = \gamma b^2 = \gamma\mu = \mu_1 \quad (\mu_1 \in L).$$

Замечание 2. Пусть F_1 — множество квадратов элементов мультипликативной группы F поля L . Тогда F_1 — подгруппа группы F индекса 2 и

$$F = F_1 \cup \xi F_1,$$

$$\text{где } \xi \in F \text{ — фиксированный квадратный невычет в поле } L.$$

где $\xi \in L$ — фиксированный квадратный невычет в поле L .

Доказательство очевидно.

Теорема 2. *Общий тип алгебр (I) путем замены базиса сводится к видам алгебр типа E:*

$$(4) \quad A_3 = \{L, a, b\}; \lambda a = a\lambda; \lambda b = b\lambda; b^{-1}ab = a^{-1}; b^2 = 1,$$

$$(5) \quad A_4 = \{L, a, b\}; \lambda a = a\lambda; \lambda b = b\lambda; b^{-1}ab = \xi a^{-1}; b^2 = 1,$$

$$(6) \quad A_5 = \{L, a, b\}; \lambda a = a\lambda; \lambda b = b\lambda; b^{-1}ab = a^{-1}; b^2 = \xi,$$

где $\xi \in L$ определяется в замечании 2, $\lambda \in L$.

Доказательство. Если в алгебре B_1 элементы γ и μ принадлежат подгруппе F_1 (см. замечание 2), то замена базиса $a_1 = \sqrt{\gamma^{-1}}a$; $b_1 = \sqrt{\mu^{-1}}b$, ввиду перестановочности элементов a и b с элементами $\lambda \in L$, приводит к типу алгебр A_3 .

Если элемент γ является квадратным невычетом в L , то $\gamma = \xi f$, где $f \in F_1$ (см. замечание 2) — лежит в F_1 . Если при этом $\mu \in F_1$, то замена базиса $a_1 = \sqrt{f^{-1}}a$; $b_1 = \sqrt{\mu^{-1}}b$ приводит к типу алгебр A_4 .

Если $\gamma \in F_1$, а $\mu \notin F_1$, то, согласно замечанию 2, $\mu = \xi \cdot f_1$; $f_1 \in F_1$ и замена базиса $a_1 = \sqrt{\gamma^{-1}}a$; $b_1 = \sqrt{f_1^{-1}}b$ в алгебре B_1 приводит к типу алгебр A_5 .

Если $\gamma, \mu \notin F_1$, то они представляются в виде $\gamma = \xi f_2$; $\mu = \xi f_3$, ($f_2, f_3 \in F_1$) и замена базиса $a_1 = \sqrt{f_2^{-1}}a$; $b_1 = \sqrt{f_3^{-1}}b$ приводит к типу алгебр

$$A'_4 = \{L, a, b\}; \lambda a = a\lambda; b\lambda = \lambda b; b^{-1}ab = \xi a^{-1}; b^2 = \xi,$$

но дополнительная замена $a_1 = a$; $b_1 = \xi^{-1}ab$ в A'_4 приводит к типу A_4 . Теорема доказана.

Лемма 1. *Пусть элемент $\lambda \in L$ выдерживает автоморфизм φ поля L второго порядка. Тогда существует такой элемент $\delta \in F$, что $\lambda = \delta \cdot \delta^\varphi$.*

Доказательство. Пусть $|K| = p^m$. Так как φ — автоморфизм второго порядка, то $\lambda^\varphi = \lambda^{p^m}$. Пусть θ — образующий элемент мультипликативной группы F поля L . Так как F — циклическая группа, то для некоторого натурального k имеет место $\lambda = \theta^k$. Ищем элемент δ в виде $\delta = \theta^x$. Имеем

$$\theta^k = \theta^x \cdot \theta^{x p^m} = \theta^{x(p^m+1)},$$

откуда следует сравнение

$$(*) \quad x \cdot (p^m + 1) \equiv k \pmod{p^{2m} - 1}.$$

Из равенства $\lambda^{p^m} = \lambda$ получаем равенство $\theta^{k p^m} = \theta^k$, что ведет к сравнению

$$k(p^m - 1) \equiv 0 \pmod{p^{2m} - 1},$$

или $k \equiv 0 \pmod{p^m + 1}$. Учитывая этот факт, заключаем, что сравнение $(*)$ разрешимо. Лемма доказана.

Лемма 2. *Пусть дана алгебра*

$$A = \{L, a, b\}; \lambda a = a\lambda^\varphi; \lambda b = b\lambda, b^{-1}ab = \gamma a^{-1}; b^2 = \mu,$$

где $\lambda, \gamma, \mu \in L$; φ — произвольный K -автоморфизм поля L . Тогда алгебра A путем

замены базиса сводится к алгебре типа

$$B = \{L, a, b\}; \lambda a = a\lambda^q; \lambda b = b\bar{\lambda}, b^{-1}ab = \gamma a^{-1}; b^2 = 1.$$

Доказательство. Покажем, что элемент μ выдерживает автоморфизм $\lambda \rightarrow \bar{\lambda}$ поля L . Действительно,

$$\bar{\mu} = b^{-1}\mu b = b^{-1}b^2b = b^2 = \mu.$$

Ясно, что тогда и элемент μ^{-1} выдерживает этот автоморфизм. Согласно лемме 1, существует элемент $\mu_1 \in L$, что $\mu^{-1} = \mu_1 \cdot \bar{\mu}_1$. Сделаем подстановку $a_1 = a$; $b_1 = \mu_1 b$ и получаем

$$b_1^2 = \mu_1 b \cdot \mu_1 b = \mu_1 \cdot \bar{\mu}_1 b^2 = \mu_1 \cdot \bar{\mu}_1 \cdot \mu = 1,$$

$$b_1^{-1}a_1b_1 = (\mu_1 b)^{-1}a(\mu_1 b) = b^{-1} \cdot \mu_1^{-1}a\mu_1 b = (\bar{\mu}_1^{-1}) \cdot (\mu_1^q) \gamma a^{-1} = \gamma_1 a_1^{-1}, \quad (\gamma_1 \in L).$$

Получили алгебру типа B . Лемма доказана.

Используя лемму 2, очевидно следующее следствие:

Следствие 1. Общие типы алгебр B_3 и B_4 путем замены базиса сводятся к типам алгебр

$$B'_3 = \{L, a, b\}; \lambda a = a\lambda; \lambda b = b\bar{\lambda}; b^{-1}ab = \gamma a^{-1}; b^2 = 1,$$

$$B'_4 = \{L, a, b\}; \lambda a = a\bar{\lambda}; \lambda b = b\bar{\lambda}; b^{-1}ab = \gamma a^{-1}; b^2 = 1.$$

Теорема 3. Общий тип алгебр B'_3 (см. следствие 1) путем замены базиса сводится к алгебре типа

$$A_6 = \{L, a, b\}; \lambda a = a\lambda; \lambda b = b\bar{\lambda}; b^{-1}ab = a^{-1}; b^2 = 1.$$

Доказательство. Покажем, что элемент γ выдерживает автоморфизм $\lambda \rightarrow \bar{\lambda}$. Действительно,

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

откуда $\bar{\gamma} \cdot \gamma^{-1} = 1$, то есть $\bar{\gamma} = \gamma$. Тогда, согласно лемме 1, существует элемент $\gamma_1 \in L$, что $\gamma^{-1} = \gamma_1 \cdot \bar{\gamma}_1$. Сделаем замену $a_1 = a\gamma_1$; $b_1 = b$. Тогда

$$b_1^{-1}a_1b_1 = b^{-1}(a\gamma_1)b = (\gamma a^{-1})\bar{\gamma}_1 = (\gamma_1\bar{\gamma}_1)^{-1}\bar{\gamma}_1 a^{-1} = \gamma_1^{-1}a^{-1} = (\gamma_1 a)^{-1} = a_1^{-1}.$$

Теорема доказана.

Теорема 4. Общий тип алгебр B'_4 (см. следствие 1) путем замены базиса сводится к алгебрам типов

$$A'_7 = \{L, a, b\}; \lambda a = a\bar{\lambda}; \lambda b = b\bar{\lambda}; b^{-1}ab = a^{-1}; b^2 = 1,$$

$$A_8 = \{L, a, b\}; \lambda a = a\bar{\lambda}; \lambda b = b\bar{\lambda}; b^{-1}ab = \xi a^{-1}; b^2 = 1,$$

где $\lambda \in L$; ξ — фиксированный квадратный невычет в поле L .

Доказательство. Сделаем замену базиса $a_1 = at$; $b_1 = b$ при параметре $t \in L$. Имеем

$$b_1^{-1}a_1b_1 = b^{-1}(at)b = \gamma a^{-1}t = \gamma ta^{-1}.$$

С другой стороны

$$b_1^{-1} a_1 b_1 = \delta a_1^{-1} = \delta (at)^{-1} = \delta t^{-1} a^{-1}$$

для некоторого элемента $\delta \in L$. Сравнивая два равенства, получаем $\delta = \gamma \cdot t^2$. Это значит, что если элемент γ лежит в подгруппе F_1 , то подстановка, $a_1 = a\sqrt{\gamma^{-1}}$; $b_1 = b$ дает соотношение

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

и получаем алгебру типа A_7' . Если же элемент γ не лежит в подгруппе F_1 , то $\gamma = \xi f_1$ для некоторого $f_1 \in F_1$, где ξ — фиксированный квадратный невычет в поле L . Сделаем подстановку $b_1 = b$; $a_1 = a\sqrt{f_1^{-1}}$ и получаем

$$\begin{aligned} b_1^{-1} a_1 b_1 &= b^{-1} (a\sqrt{f_1^{-1}}) b = \gamma a^{-1} \sqrt{f_1^{-1}} = \gamma \sqrt{f_1^{-1}} a^{-1} = \xi \sqrt{f_1} a^{-1} = \\ &= \xi (a\sqrt{f_1^{-1}})^{-1} = \xi a_1^{-1}, \end{aligned}$$

что дает алгебру типа A_8 . Теорема доказана.

Замечание 3. Алгебра типа A_7' путем дополнительной замены базиса $a_1 = a$; $b_1 = ab$ сводится к типу

$$A_7 = \{L, a, b\}; \lambda a = a\bar{\lambda}; \lambda b = b\lambda; b^{-1}ab = a^{-1}; b^2 = 1.$$

Доказательство очевидно, так как $\lambda b_1 = \lambda(ab) = a\bar{\lambda}b = ab\lambda = b_1\lambda$.

Следствие 2. Все типы алгебр типа E над полем K характеристики $p (\neq 2)$ по отношению к полю L $((L:K)=2)$ задаются соотношениями

$$A_1 = \{L, a\} = L(a); \lambda a = a\lambda, \quad (\lambda \in L),$$

$$A_2 = \{L, a\}; \lambda a = a\bar{\lambda} \quad (\lambda \in L),$$

$$A_3 = \{L, a, b\}; \lambda a = a\lambda; \lambda b = b\lambda; b^{-1}ab = a^{-1}; b^2 = 1 \quad (\lambda \in L),$$

$$A_4 = \{L, a, b\}; \lambda a = a\lambda; \lambda b = b\lambda; b^{-1}ab = \xi a^{-1}; b^2 = 1 \quad (\lambda \in L),$$

$$A_5 = \{L, a, b\}; \lambda a = a\lambda; \lambda b = b\lambda; b^{-1}ab = a^{-1}; b^2 = \xi \quad (\lambda \in L),$$

$$A_6 = \{L, a, b\}; \lambda a = a\lambda; \lambda b = b\bar{\lambda}; b^{-1}ab = a^{-1}; b^2 = 1 \quad (\lambda \in L),$$

$$A_7 = \{L, a, b\}; \lambda a = a\bar{\lambda}; \lambda b = b\lambda; b^{-1}ab = a^{-1}; b^2 = 1 \quad (\lambda \in L),$$

$$A_8 = \{L, a, b\}; \lambda a = a\bar{\lambda}; \lambda b = b\bar{\lambda}; b^{-1}ab = \xi a^{-1}; b^2 = 1 \quad (\lambda \in L),$$

где ξ — фиксированный квадратный невычет в поле L .

Литература

- [1] С. Д. Берман—К. Бузаши, О представлениях бесконечной группы диэдра. *Publ. Math. (Debrecen)* **28** (1981), 173—187.
- [2] С. Д. Берман—К. Бузаши, О представлениях группы, содержащей бесконечную циклическую подгруппу конечного индекса. *Publ. Math. (Debrecen)* **29** (1982), 163—170.
- [3] С. Д. Берман—К. Бузаши, О модулях над групповыми алгебрами групп, содержащих бесконечную циклическую подгруппу конечного индекса. *Studia Sci. Math. Hungarica* **16** (1981), 455—470.
- [4] С. Д. Берман—К. Бузаши, Описание всех конечномерных вещественных представлений групп, содержащих бесконечную циклическую подгруппу конечного индекса. *Publ. Math. (Debrecen)* **31** (1984), 133—144.
- [5] Ч. Кертис—И. Райнер, Теория представлений конечных групп и ассоциативных алгебр. Изд. Наука, 1969.
- [6] N. JACOBSON, The theory of rings. *Amer. Math. Soc. New York*, 1943.

(Поступило 30. VI. 1984)