УДК 514.142

А. В. ПРОКОПЧУК, В. И. ЯНЧЕВСКИЙ

О ЛИНЕЙНЫХ ОБОЛОЧКАХ КОММУТАНТОВ УНИТАРНЫХ ГРУПП НЕКОММУТАТИВНЫХ КОНЕЧНОМЕРНЫХ АЛГЕБР С ДЕЛЕНИЕМ

Институт математики НАН Беларуси

(Поступила в редакцию 03.12.2014)

Исследованию унитарных групп изотропных эрмитовых форм над некоммутативными алгебрами с делением посвящен целый ряд работ. Основной вклад здесь принадлежит Ж. Дьёдонне и Дж. Уоллу (см., напр., [1, 2]). В теории линейных алгебраических групп важную роль играют унитарные группы эрмитовых форм над некоммутативными конечномерными алгебрами с делением. В то время как благодаря упомянутым результатам Ж. Дьёдонне и Дж. Уолла случай изотропных форм довольно хорошо изучен, анизотропный случай остается малоприступным. В настоящее время намечаются лишь некоторые подходы к нахождению решения этой проблемы. Для реализации одного из таких подходов весьма важным является изучение линейных оболочек унитарных, специальных унитарных групп и их коммутантов. Начало изучению задач такого типа было положено одним нижеприведенным результатом Ж. Дьёдонне [1]. Для его формулировки и формулировки основных результатов статьи нам потребуются следующие определения и обозначения.

Пусть K – квадратичное сепарабельное расширение поля k характеристики, отличной от 2 ($\mathrm{char}K \neq 2$), скажем, $K = k(\sqrt{\alpha})$, $\alpha \in k$, A – некоммутативная конечномерная центральная K-алгебра с делением. Пусть также τ – инволютивный K/k-антиавтоморфизм A. Пусть

$$S_\tau = \{a \in A : a^\tau = a\},$$
$$U(\tau, A) = \{a \in A : a^\tau a = 1\},$$
$$SU(\tau, A) = \{a \in U(\tau, A) : Nrd_A(a) = 1\},$$

где отображение Nrd_A – отображение приведенной нормы алгебры A. В [1, с. 367] Ж. Дьёдонне установил следующие результаты.

П р е д л о ж е н и е 1. *Для некоммутативной алгебры A с делением подкольцо, порожденное элементами из S_τ, совпадает с ней.*

В конечномерном случае (см. [3]) с предыдущим результатом связан следующий.

П р е д л о ж е н и е 2. *A совпадает с K-линейной оболочкой $K[S_\tau]$ множества S_τ.*

На последнем результате базируется ответ на вопрос об описании K-линейной оболочки $K[U(\tau, A)]$ группы $U(\tau, A)$.

Т е о р е м а 1. *A совпадает с $K[U(\tau, A)]$.*

З а м е ч а н и е 1. Отметим, что доказательство этого утверждения содержится в [4] при некоторых дополнительных органичениях. Однако, как отмечает автор работы, на самом деле при небольшой модификации оно сохраняется и в рассматриваемой ситуации. Этому доказательству будет посвящена другая его работа.

Поскольку $SU(\tau, A) \subsetneqq U(\tau, A)$, то естественно возникает вопрос о совпадении K-линейных оболочек $K[SU(\tau, A)]$ и $K[U(\tau, A)]$. Ответ содержится в следующей теореме.

Т е о р е м а 2. *$K[SU(\tau, A)]$ совпадает с A.*

З а м е ч а н и е 2. При условии взаимной простоты индекса char$K$ и индекса алгебы A или при условии char$K = 0$ теорема 2 доказана в [4], следует лишь выбор элемента z, фигурировавшего в доказательстве, дополнить условием, что его минимальный многочлен (над K) имеет ненулевой коэффициент при x^{d-2}. (Доказательство теоремы 2 в общей ситуации будет дано в следующей работе второго автора настоящей статьи.)

Пусть теперь $[U(\tau, A), U(\tau, A)]$ – коммутант унитарной группы $U(\tau, A)$ (т. е. группа, порожденная элементами вида $[a,b] = aba^{-1}b^{-1},\ a,b \in U(\tau, A)$).

Поскольку $[U(\tau, A), U(\tau, A)] \subsetneqq SU(\tau, A)$, то естественно сравнить их K-линейные оболочки. В связи с этим следующая гипотеза кажется нам правдоподобной.

Г и п о т е з а. В предыдущих обозначениях

$$K[[U(\tau, A), U(\tau, A)]] = K[SU(\tau, A)] = K[U(\tau, A)] = K[S_\tau] = A.$$

Целью настоящей статьи является доказательство вышеприведенной гипотезы в случае простого индекса алгебры A. Для этого мы сначала доказываем следующее утверждение, представляющее и самостоятельный интерес.

Т е о р е м а 3. *Пусть A – центральная некоммутативная K-алгебра с делением, где характеристика K – либо нуль, либо взаимно проста с индексом алгебры A. Тогда существует коммутатор $[a,b] \notin K$ такой, что $a,b \in U(A,\tau)$.*

Случай простого индекса. Для доказательства теоремы 3 установим справедливость следующей леммы.

Л е м м а 1. *Пусть A – центральная K-алгебра с делением индекса $d > 1$ и такого, что d взаимно просто с* char$K$, *если* char$K > 0$. *Тогда для любых элементов $a,b \in A$ таких, что $[a,b] = \varepsilon_d^n$, $n < d$, где ε_d – примитивный корень степени d из 1, $\varepsilon_d^n \in K$, и $K < a,b >= A$ (здесь $K < a,b >$ – K-алгебра с образующими a,b) следует, что $(n,d) = 1$ (т. е. $\varepsilon_d \in K$). Более того, $a^d, b^d \in K$.*

Д о к а з а т е л ь с т в о. Предположим, что $K < a,b >= A$ и $ab = \varepsilon_d^n \cdot ba$, где $\varepsilon_d^n \in K$ следует, что $K(a)$ и $K(b)$ порождают максимальные подполя в алгебре A, так как в противном случае K-линейная оболочка элементов вида $\sum_{i,j} k_{ij} a^i b^j$ имела бы размерность меньшую, чем d^2.

Пусть $q = (n,d)$ – наибольший общий делитель чисел n и d. Из равенства $[a,b] = \varepsilon_d^n$ следует, что $aba^{-1} = \varepsilon_d^n b$. Возведя последнее равенство в степень d/q, получим $ab^{d/q}a^{-1} = \varepsilon_d^{n\cdot d/q} b^{d/q}$. Так как число $n \cdot d/q$ кратно d, то получаем $ab^{d/q}a^{-1} = b^{d/q}$. Из последнего следует, что $b^{d/q}$ принадлежит централизатору $C_A(K(a))$ в A поля $K(a)$. Поскольку $K(a)$ – максимальное подполе алгебры A, то $b^{d/q} \in K(a)$.

Если $q > 1$, мы приходим к противоречию с условием, что K-линейная оболочка элементов вида $a^i b^j$ имеет размерность d^2. В самом деле, из условия $b^{d/q} \in K(a)$ следует, что элементы вида b^t, где $d/q \le t < d$, выражаются в виде K-линейной комбинации $\sum_{i,j=0}^{i<d, j<d/q} k_{ij} a^i b^j$, а потому размерность линейной оболочки элементов вида $\sum_{i,j} k_{ij} a^i b^j$ не больше, чем d^2/q.

Как показано выше, $b^{d/q} \in K(a)$, а взаимная простота n и d влечет $b^d \in K(a)$. Элемент b^d коммутирует с элементами a и b, и так как $A = K < a,b >$, то он централен, т. е. $b^d \in K$. Аналогичные рассуждения влекут $a^d \in K$. Лемма доказана.

П р е д л о ж е н и е 3. *Пусть A – центральная K-алгебра с делением простого индекса p и либо характеристика K равна нулю, либо взаимно проста с p. Тогда существует коммутатор $[a,b] \notin K$ такой, что $a,b \in U(A,\tau)$.*

Д о к а з а т е л ь с т в о от противного. Пусть $[a,b] \in K$ для всех $a,b \in U(A,\tau)$. В силу совпадения множеств $K[U(A,\tau)]$ и A (теорема 2), в алгебре A существуют некоммутирующие элементы a,b из группы $U(A,\tau)$. Тогда для $c = [a,b]$ имеем $c \in K \setminus 1$. Следовательно,

$$1 = Nrd_A([a,b]) = Nrd_A(c) = c^p,$$

что влечет $c = \varepsilon_p$, т. е. $aba^{-1} = \varepsilon_p b$. Возведя последнее равенство в степень p, получим $ab^p a^{-1} = b^p$. Так как элементы a и b не коммутируют, то $K < a,b >$ – алгебра размерности p^2 и потому совпадает с A. Поскольку элемент b^p коммутирует с элементами a и b, то $b^p \in K$. Рассуждая аналогично для равенства $b^{-1}ab = \varepsilon_p a$, заключаем, что $a^p \in K$. Значит, ввиду $K[U(A,\tau)] = A$, получаем, что p-я степень любого нецентрального элемента из группы $U(A,\tau)$ принадлежит полю K. Покажем, что это не так. Рассмотрим элемент

$$z = \frac{e + a}{e^\tau + a^{-1}},$$

где $e \in K$. Заметим, что $z \in U(A,\tau)$. В силу доказанного выше, $z^p = t$, $t \in K$. Поскольку z лежит в поле $K(a)$, элемент $(z/a)^p$ также принадлежит полю K, т. е. $(z/a)^p = l$, $l \in K$. Имеем

$$(e + a)^p = l(e^\tau a + 1)^p. \qquad (*)$$

Поскольку элемент a порождает поле $K(a)$ степени p, то элементы $1, a, \ldots, a^{p-1}$ линейно независимы над K. Сравнение коэффициентов при a и a^{p-1} в левой и правой частях равенства (*) приводят к соотношениям: $e^p - 1 = le^\tau$, $e = l(e^\tau)^{p-1}$. Деля левые и правые части двух последних равенств, заключаем, что

$$(ee^\tau)^{p-2} = 1.$$

Поскольку для $e = x + y\sqrt{\alpha}$, $x, y \in k$, $ee^\tau = x^2 - \alpha y^2$, таким образом, для получения противоречия достаточно показать, что последняя квадратичная форма от x, y не может принимать значений в конечном множестве при произвольных $x, y \in k$, что без труда устанавливается с помощью элементарных вычислений. Предложение доказано.

Доказательство теоремы 3. Воспользуемся индукцией по индексу алгебры A. Базу индукции составляет предложение 3. Пусть теперь для всех алгебр индекса меньшего, чем d, теорема справедлива. Покажем, что она верна и для любой алгебры A индекса d. Рассмотрим два некоммутирующих элемента a, b из группы $U(A,\tau)$ и рассмотрим K-подалгебру $D = K < a,b >$ алгебры A, которая является алгеброй с делением. Если $D \neq A$, то алгебра D имеет индекс меньший, чем d, предположению индукции в D существует коммутатор $[u,w]$, не принадлежащий центру D такой, что $u, v \in U(A,\tau)$, а значит, $[u,w] \notin K$. Следовательно, $K < a,b >= A$.

Обозначим через $c \in K$ коммутатор $[a,b]$. Тогда

$$1 = Nrd_A([a,b]) = Nrd_A(c) = c^d.$$

Значит, $c = \varepsilon_d^n$ для некоторого $0 < n < d$. Применяя лемму 1 к алгебре $A = K < a,b >$, получаем, что $(n,d) = 1$. Значит, можно считать, что $[a,b] = \varepsilon_d$ и $a^d, b^d \in K$. Рассмотрим подалгебру $B = K < a,b^p >$, где p – некоторое простое число, делящее d. Так как $ab^p = \varepsilon_d^p b^p a$, где $\varepsilon_d^p \neq 1$, то элементы a, b^p не коммутируют друг с другом и потому алгебра B некоммутативна, при этом она имеет индекс меньший, чем индекс алгебры A. В самом деле, B состоит из K-линейных комбинаций элементов вида $\{a^i b^{pj}\}_{i,j=0}^{i<d, j<d/p}$, которых равно d^2/p. Значит, в алгебре B по предположению индукции имеется коммутатор $[u,w]$, не принадлежащий центру B, такой, что $u, v \in U(A,\tau)$, а значит, $[u,w] \notin K$. Теорема 3 доказана.

Докажем теперь вышеупомянутую гипотезу для алгебр простого индекса.

Теорема 4. *Пусть индекс алгебры A – простое число p и либо* $\mathrm{char}K = 0$, *либо* $(\mathrm{char}K) = 1$. *Тогда*

$$K[[U(A,\tau), U(A,\tau)]] = A.$$

Доказательство. Ввиду теоремы 3 существует коммутатор $[a,b] \notin K$, $a, b \in U(A,\tau)$. Положим $L = k([a,b])$. Ясно, что $L \subset K[[U(A,\tau), U(A,\tau)]]$.

Пусть $u \in U(A,\tau)$. Если $uLu^{-1} \not\subset L$, тогда $u[a,b]u^{-1} \notin L$ и в силу равенства $u[a,b]u^{-1} = [uau^{-1}, ubu^{-1}]$ получим, что $[uau^{-1}, ubu^{-1}] \notin L$, а потому $K < [a,b], [uau^{-1}, ubu^{-1}] >= A$. Значит, $K[[U(A,\tau), U(A,\tau)]] = A$.

Предположим теперь, что для любого $u \in U(A,\tau)$ имеем $uLu^{-1} = L$. Обозначим через φ_u ограничение на L внутреннего автоморфизма алгебры A с помощью u. Если φ_u – тождественный автоморфизм, то u коммутирует с любым элементов из L, а значит, $u \in L$ ввиду максимальности L в алгебре A. Следовательно, для всех u автоморфизм φ_u не может быть тождественным и, следовательно, существует u, для которого φ_u нетривиально действует на L и является образущей группы Галуа L / K (поскольку $[L:K] = p$).

Рассмотрим элемент

$$z = \frac{k_1 + k_2 u}{k_1 + k_2 u^{-1}},$$

где $k_1 k_2 \neq 0, k_1 \neq \pm k_2, k_1, k_2 \in k = K_\tau$. Очевидно $z \in U(A,\tau)$. Далее, $z \notin L$, так как в противном случае $k_1 u + k_2 u^2 = z k_1 u + z k_2$ и потому ввиду линейно независимости $1, u, \ldots, u^{p-1}$ над L получим, что $k_1 = z k_1$. Значит, $z = 1$, и, стало быть, $k_1 + k_2 u = k_1 + k_2 u^{-1}$, откуда $u = \pm 1$, что противоречит $u \notin L$.

Покажем, что при наших предположениях произвольный элемент $v \in U(A,\tau)$ имеет вид $v = l_v u^t$ для некоторого $t \in \{0,1,\ldots,p-1\}$. Действительно, $\varphi_u^t = \varphi_v$ для подходящего $t \in \{0,1,\ldots,p-1\}$, так как φ_u – образующая группы Галуа поля L / K. Значит, $\varphi_u^t \varphi_v^{-1}$ – тождественный L-автоморфзим, что влечет $v = l_v u^t$ для некоторого элемента $l_v \in L$. Обратно, для элемента v с условием $v = l_v u^t$ будем иметь $\varphi_u^t = \varphi_v$. Следовательно, любой элемент v из группы $U(A,\tau)$ имеет вид $v = l_v u^t$.

Из предыдущего рассуждения следует, что $z = lu^t$, $l \in L$, $0 < t \leq p-1$. Домножая на $k_1 + k_2 u^{-1}$ обе части последнего равенства, получим

$$k_1 + k_2 u = k_1 l u^t + k_2 l t^{t-1}.$$

Если $t > 1$, то в последнем равенстве при любом $0 < t \leq p-1$ коэффициент в линейной комбинации при u^0 всегда равен k_1. Что немедленно влечет $k_1 = 0$, что противоречит условию $k_1 k_2 \neq 0$. При $t = 1$ получим $k_1 + k_2 u = k_1 l u + k_2 l$. Тогда $k_1 = k_2 l$ и $k_2 = k_1 l$, откуда следует $l = \pm 1$, что проворечит условию $k_1 \neq \pm k_2$. Следовательно, всегда существует $u \in U(A,\tau)$ такой, что $u_0 L u_0^{-1} \not\subset L$. Таким образом, $K[[U(A,\tau), U(A,\tau)]] = A$. Теорема доказана.

Литература

1. *Дьёдонне Ж.* Геометрия классических групп. М., 1974.
2. *Hahn A.* The classical groups and K-theory. Front Cover. Springer-Verlag, 1989.
3. *Albert A. A.* Structure of algebras, Colloquium publications 24, AMS, 2003.
4. *Янчевский В. И.* Приведенные группы Уайтхеда и проблема сопряженности для специальных унитарных групп анизотропных эрмитовых форм // Зап. науч. семинаров С.-Петерб. отд-ния мат. ин-та им. В. А. Стеклова РАН. 2012. Т. 400, № 23. С. 222–245.

A. V. PROKOPCHUK, V. I. YANCHEVSKII

ON LINEAR SPANS OF THE COMMUTATOR SUBGROUPS OF UNITARY GROUPS OF NON-COMMUTATIVE FINITE DIMENSIONAL DIVISION ALGEBRAS

Summary

Let K/k be a separable quadratic extension, char$K \neq 2$, A a non-commutative finite dimensional central K-division algebra with unitary k-involution. For algebras A of prime index relatively prime to char$K$ we prove the following conjecture: k-linear span of the commutator subgroup of a unitary group of A coincides with A.