Записки научных
семинаров ПОМИ
Том 388, 2011 г.

А. В. Прокопчук, В. И. Янчевский

ИНВАРИАНТНЫЕ ПОДАЛГЕБРЫ ИНВОЛЮТИВНЫХ КВАТЕРНИОННЫХ АЛГЕБР С ДЕЛЕНИЕМ

Пусть K – поле характеристики отличной от 2 и Q – кватернионная алгебра с делением над K (ниже мы всегда отождествляем K с подмножеством $1 \cdot K$, где 1 – единица алгебры Q). Хорошо известно, что Q обладает целым классом инволюций $\mathrm{Inv}(Q)$ (т.е. антиавтоморфизмов второго порядка). Ограничение всякой такой инволюции на K является либо тождественным автоморфизмом, либо автоморфизмом второго порядка; соответственно этому инволюция называется инволюцией первого либо второго рода. Обозначим через k поле инвариантов инволюции в K. Тогда $\mathrm{Inv}_{K/k}(Q)$ будет обозначать множество инволюций алгебры Q, ограничения которых на K совпадают с образующей группы Галуа расширения K/k.

Определение 1. *Пусть $\tau \in \mathrm{Inv}_{K/k}(Q)$. k-подалгебра A алгебры Q (Q является, очевидно, и k-алгеброй) называется τ-инвариантной, если $A^\tau = A$.*

В этой статье нас будет интересовать описание множества τ-инвариантных подалгебр алгебры Q при фиксированной инволюции τ.

Случай инволюций первого рода тривиален и описывается следующим утверждением.

Предложение 1. *Пусть τ – инволюция первого рода (т.е. $K = k$). Тогда всякая τ-инвариантная подалгебра A алгебры Q содержится в следующем списке τ-инвариантных подалгебр алгебры Q:*

(i) $A = k$;

(ii) $A = k(s)$, *где* $s \notin k$, $s^\tau = \pm s$;

(iii) $A = Q$.

Ключевые слова: Кватернионная алгебра, инволюция алгебры, каноническая инволюция алгебры кватернионов.

Работа выполнена в рамках совместного проекта, поддержанного Белорусским республиканским и Российским фондами фундаментальных исследований, проект No. Ф10Р-110.

В дальнейшем нам потребуются следующие обозначения и элементарные факты об алгебрах с инволюциями.

Ниже для всякого кольца R с единицей R^* обозначает группу его обратимых (относительно умножения) элементов, для простой центральной K-алгебры A через $\mathrm{Nrd}_A : A \longrightarrow K^*$ обозначен гомоморфизм приведённой нормы, а для расширения K/k через $N_{K/k} : K^* \longrightarrow k^*$ обозначен гомоморфизм, определяемый нормой из K в k.

Определение 2. *Элемент s простой центральной K-алгебры A с инволюцией τ, инвариантный относительно τ, называется симметрическим (или τ-симметрическим), а если $s^\tau = -s$ – кососимметрическим (τ-кососимметрическим).*

Множество τ-симметрических элементов обозначается через $S_\tau(A)$. Для множества τ-кососимметрических элементов в A используется обозначение $K_\tau(A)$. Для краткости, если подалгебра $B \subset A$ инвариантна относительно τ, то мы будем писать $S_\tau(B)$, $K_\tau(B)$ вместо $S_{\tau|_B}(B)$, $K_{\tau|_B}(B)$.

Хорошо известна следующая лемма (см. [1, 2]).

Лемма 1. *Множества $S_\tau(A)$ и $K_\tau(A)$ являются k-векторными пространствами такими, что*

$$A = S_\tau(A) \oplus K_\tau(A),$$

где знак $\oplus$ означает прямую сумму k-подпространств $S_\tau(A)$ и $K_\tau(A)$ в k-пространстве A.

Для размерностей пространств $S_\tau(A)$ и $K_\tau(A)$ имеются лишь следующие возможности (ниже $m^2 = [A : K]$):

(i) $\dim_k S_\tau(A) = \dim_k K_\tau(A) = m^2$, *$\tau$ – инволюция второго рода;*

(ii) $\dim_k S_\tau(A) = m(m-1)/2$, $\dim_k K_\tau(A) = m(m+1)/2$, *$\tau$ – инволюция первого рода;*

(iii) $\dim_k S_\tau(A) = m(m+1)/2$, $\dim_k K_\tau(A) = m(m-1)/2$, *$\tau$ – инволюция первого рода.*

Вернемся к доказательству предложения.

Лемма-обозначение 1 (см. [3]). *Во всякой кватернионной алгебре Q существует K-базис $\{1, u, v, uv\}$ такой, что $uv = -vu$, $u^2 = \alpha$, $v^2 = \beta$, $\alpha, \beta \in K^*$. Такой базис называется каноническим, а алгебра Q обозначается через $(\frac{\alpha,\beta}{K})$.*

Доказательство предложения 1. Поскольку $K = k$, то всякая τ-инвариантная подалгебра в Q может иметь размерность над K либо 1, либо 2, либо 4. Первый и последний случай соответствуют алгебрам (i) и (iii) из списка в формулировке предложения, которые, очевидно, τ-инвариантны. Поскольку алгебры из (ii) также τ-инвариантны, то остаётся показать, что всякая τ-инвариантная подалгебра A размерности 2 над K соответствует случаю (ii). Ввиду коммутативности A, которая вытекает из принадлежности A единицы 1_Q алгебры Q, содержащейся в центре Q (а следовательно, и A), и возможности включения 1_Q в K-базис алгебры A, алгебра является квадратичным расширением поля K. Значит, $A = K(\sqrt{a})$ для некоторого подходящего элемента $a \in K$. Стало быть, $s^\tau = -s$ либо $s^\tau = s$ для $s = \sqrt{a}$. Предложение доказано. □

В дальнейшем нам потребуется также следующее хорошо известное утверждение.

Лемма 2. *Алгебра Q обладает единственной инволюцией τ со свойством* $\dim_k(S_\tau(Q)) = 1$.

Доказательство. Пусть $\{1, u, v, uv\}$ – канонический базис Q. Для произвольного элемента $\varepsilon_1 + \varepsilon_2 u + \varepsilon_3 v + \varepsilon_4 uv$, $\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4 \in K$, положим $q^\tau = \varepsilon_1 - \varepsilon_2 u - \varepsilon_3 v - \varepsilon_4 uv$. Простое вычисление показывает, что отображение $q \longrightarrow q^\tau$ – инволюция первого рода (т.е. $K = k$) и $\dim_k S_\tau(Q) = 1$. Единственность τ устанавливается из следующего. Нетрудно видеть, что $K_\tau(Q)$ состоит из элементов Q с приведенным следом 0. Пусть теперь μ – другая инволюция первого рода со свойством $\dim_k S_\mu(Q) = 1$. В силу леммы 1 $\dim_k K_\mu(Q) = 3$ и, кроме того, квадрат любого элемента из $K_\tau(Q)$ принадлежит k ввиду $\dim_k S_\mu(Q) = 1$. Значит, минимальный многочлен любого ненулевого $t \in K_\mu(Q)$ имеет вид $z^2 - t^2$, а потому приведенный след t равен 0. Совпадение размерностей $K_\mu(Q)$ и $K_\tau(Q)$ и включение $K_\mu(Q) \subseteq K_\tau(Q)$ влечёт совпадение $K_\mu(Q) = K_\tau(Q)$, а также $S_\mu(Q) = S_\tau(Q) = k$, то из леммы 1 немедленно следует $\mu = \tau$. □

Единственность инволюции τ из предыдущей леммы приводит к следующему определению.

Определение 2. *Инволюция $\tau \in \mathrm{Inv}(Q)$ со свойством* $\dim_k S_\tau(Q) = 1$ *называется канонической инволюцией Q.*

Обратимся теперь к описанию τ-инвариантных подалгебр в случае инволюций второго рода, который кроме общего представляет и специальный интерес, связанный с изучением групп k-рациональных точек анизотропных алгебраических групп.

Более точно, пусть D – центральная конечномерная K-алгебра с делением,

$$\mathrm{SL}(D) := \{d \in D \mid \mathrm{Nrd}_D(d) = 1\}.$$

Эту группу можно рассматривать как группу K-рациональных точек односвязной K-группы, относящейся к внутренним формам ${}^2A_{d-1}$, где $d^2 = [D : K]$. Внешние формы таких групп тесно связаны со специальными унитарными группами $\mathrm{SU}(D, \tau)$, структура которых до настоящего времени мало изучена. При исследовании групп $\mathrm{SL}(D)$ важную роль играет коммутант $[D^*, D^*]$ мультипликативной группы D^* алгебры D. В унитарном случае возникает группа

$$U(D, \tau) := \{d \in D \mid dd^\tau = 1\}$$

и её коммутант $[U(D, \tau), U(D, \tau)]$. Тогда определены группы

$$\mathrm{SU}(D, \tau) := \mathrm{SL}(D) \cap U(D, \tau),$$
$$\mathrm{SUK}_1^{\mathrm{an}}(D, \tau) := \mathrm{SU}(D, \tau)/[U(D, \tau), U(D, \tau)].$$

Естественно, как и в случае групп $\mathrm{SL}(D)$, предварительно изучить группу $\mathrm{SUK}_1^{\mathrm{an}}(D, \tau)$. К сожалению, за исключением случая тел кватернионов до настоящего времени не существует более или менее общего описания этой группы. Известно лишь, что для некоторых специальных тел D она может быть бесконечной [4]. Кроме того, вторым автором недавно [5] было установлено существование эпиморфизма группы $\mathrm{SUK}_1^{\mathrm{an}}(D, \tau)$ на $\mathrm{SUK}_1(D, \tau)$ (так называемую приведенную унитарную группу Уайтхеда), что позволяет значительно расширить диапазон алгебр с делением с нетривиальной группой $\mathrm{SUK}_1^{\mathrm{an}}(D, \tau)$. Всё же в кватернионном случае $D = Q$ имеется определённый прогресс.

Точнее, пусть Q – кватернионная алгебра над K, обладающая кватернионной k-подалгеброй A. Рассмотрев каноническую инволюцию $\widetilde{\tau}$ на A и положив $\tau = \widetilde{\tau} \otimes \sigma$, где σ – образующая группы Галуа K/k, с учётом $Q = A \otimes_k K$, мы получим инволюцию второго рода алгебры Q такую, что A – τ-инвариантная подалгебра в Q. В этих обозначениях справедливо следующее утверждение, принадлежащее Б. Сури [6], вычисляющее группу $\mathrm{SUK}_1^{\mathrm{an}}(Q, \tau)$ в терминах τ-инвариантной подалгебры A, точнее, её мультипликативной группы A^*.

Предложение 2.

$$\mathrm{SUK}_1^{\mathrm{an}}(Q,\tau) \cong \mathrm{SL}(A)/[G,G],$$

где $G = \{a \in A^* \,|\, \mathrm{Nrd}_Q(a) \in N_{K/k}(K^*)\}$.

Варьирование τ-инвариантных алгебр A приводит (вообще говоря) к разным инволюциям τ и соответственно к разным группам $\mathrm{SUK}_1^{\mathrm{an}}(Q,\tau)$, что влечёт необходимость изучения τ-инвариантных подалгебр алгебры Q. С другой стороны, появляется проблема описания τ-инвариантных подалгебр алгебры Q, возникающих при ограничении фиксированной инволюции из $\mathrm{Inv}_{K/k}(Q)$. Решению этих задач и посвящена настоящая статья.

Ниже повсюду τ – инволюция второго рода и $K = k(\sqrt{\alpha})$, $\alpha \in k^*$.

Важную роль в этом описании играет следующий результат.

Предложение 3. *В алгебре Q с инволюцией τ существует единственная τ-инвариантная кватернионная подалгебра Q_τ над k, ограничение τ на которую совпадает с её канонической инволюцией.*

Доказательство. Существование алгебры Q_τ немедленно вытекает из доказательства одной теоремы А. Алберта, [1, теорема 21 а)]. Действительно, в доказательстве этой теоремы устанавливается существование канонического базиса $\{1, u, v, uv\}$ такого, что u, $v \in S_\tau(Q)$, а тогда линейная k-оболочка Q_τ базиса $\{1, u\sqrt{\alpha}, v\sqrt{\alpha}, uv\alpha\}$ является, как нетрудно видеть, k-кватернионной подалгеброй алгебры Q с каноническим ограничением τ на Q. Установим единственность Q_τ. Предположим, что Q'_τ – другая k-кватернионная τ-инвариантная подалгебра алгебры Q с каноническим ограничением $\tau|_{Q'_\tau}$. Тогда в силу леммы 1 $\dim_k K_{\tau|_{Q_\tau}}(Q_\tau) = \dim_k K_{\tau|_{Q'_\tau}}(Q'_\tau) = 3$, и, кроме того, $\dim_k K_\tau(Q) = 4$. Рассмотрим сумму k-подпространств $K_{\tau|_{Q_\tau}}(Q_\tau) + K_{\tau|_{Q'_\tau}}(Q'_\tau)$. Ввиду последнего замечания, $3 \leqslant \dim_k (K_{\tau|_{Q_\tau}}(Q_\tau) + K_{\tau|_{Q'_\tau}}(Q'_\tau)) \leqslant 4$. Пусть вначале $\dim_k (K_{\tau|_{Q_\tau}}(Q_\tau) + K_{\tau|_{Q'_\tau}}(Q'_\tau)) = 3$. Тогда ввиду трёхмерности $K_{\tau|_{Q_\tau}}(Q_\tau), K_{\tau|_{Q'_\tau}}(Q'_\tau)$ получаем $K_{\tau|_{Q_\tau}}(Q_\tau) = K_{\tau|_{Q_\tau}}(Q_\tau) + K_{\tau|_{Q'_\tau}}(Q'_\tau) = K_{\tau|_{Q'_\tau}}(Q'_\tau)$. Так как ещё $Q_\tau = k \oplus K_{\tau|_{Q_\tau}}(Q_\tau)$, $Q'_\tau = k \oplus K_{\tau|_{Q'_\tau}}(Q'_\tau)$, то $Q'_\tau = Q_\tau$. Покажем, что случай $\dim_k (K_{\tau|_{Q_\tau}}(Q_\tau) + K_{\tau|_{Q'_\tau}}(Q'_\tau)) = 4$ на самом деле невозможен, если считать, что $Q_\tau \neq Q'_\tau$. Предположим противное и воспользуемся стандартной формулой о размерности суммы

подпространств:

$$\begin{aligned} 6 &= \dim_k K_\tau(Q_\tau) + \dim_k K_\tau(Q'_\tau) \\ &= \dim_k (K_\tau(Q_\tau) + K_\tau(Q'_\tau)) + \dim_k (K_\tau(Q_\tau) \cap K_\tau(Q'_\tau)) \\ &= 4 + \dim_k (K_\tau(Q_\tau) \cap K_\tau(Q'_\tau)). \end{aligned}$$

Откуда $\dim_k (K_\tau(Q_\tau) \cap K_\tau(Q'_\tau)) = 2$. Пространства k и $K_\tau(Q_\tau) \cap K_\tau(Q'_\tau)$ имеют лишь нулевое пересечение. Тогда $\dim_k (k + K_\tau(Q_\tau) \cap K_\tau(Q'_\tau)) = 3$ и $k + K_\tau(Q_\tau) \cap K_\tau(Q'_\tau) \subset Q_\tau \cap Q'_\tau$, поэтому $\dim_k (Q_\tau \cap Q'_\tau) \geqslant 3$. С другой стороны, поскольку $Q_\tau \cap Q'_\tau$ — подалгебра в Q_τ, то её размерность должна быть делителем 4, который, как мы знаем, не меньше чем 3 и, стало быть, равен 4. Следовательно, $Q_\tau = Q_\tau \cap Q'_\tau$. Аналогично устанавливаем, что $Q'_\tau = Q_\tau \cap Q'_\tau$. Таким образом, $Q_\tau = Q'_\tau$ в противоречии с предположением $Q_\tau \neq Q'_\tau$. Предложение доказано. □

Предыдущее утверждение позволяет параметризовать все инволюции из $\mathrm{Inv}_{K/k}(Q)$ с фиксированным расширением K/k.

Теорема 1. *Пусть расширение K/k фиксировано и $\mathrm{Quat}_k(Q)$ – множество кватернионных подалгебр алгебры Q над k. Тогда отображение $\varphi_{K/k} : \mathrm{Inv}_{K/k}(Q) \longrightarrow \mathrm{Quat}_k(Q)$, задаваемое правилом $\varphi_{K/k}(\tau) = Q_\tau$, является биекцией.*

Доказательство. Корректность отображения $\varphi_{K/k}$ следует из предложения 3, его сюръективность устанавливается так. Пусть $B \in \mathrm{Quat}_k(Q)$ и δ – каноническая инволюция алгебры B. Продолжим δ до отображения $\tau : Q \longrightarrow Q$ формулой $(b_1 + b_2\sqrt{\alpha})^\tau = b_1^\delta - b_2^\delta \alpha$. Тогда прямое вычисление показывает, что τ – инволюция алгебры Q и $B = Q_\tau$, т.е. $\varphi_{K/k}(\tau) = B$. Для доказательства инъективности предположим, что $\tau, \mu \in \mathrm{Inv}_{K/k}(Q), \tau \neq \mu$, но $Q_\tau = Q_\mu$. В силу леммы 2 ограничения τ и μ совпадают на $Q_\tau = Q_\mu$ и потому $K_\tau(Q_\tau) = K_\mu(Q_\mu)$, а размерностные соображения показывают, что

$$\begin{aligned} K_\tau(Q) &= k\sqrt{\alpha} + K_\tau(Q_\tau), \\ K_\mu(Q) &= k\sqrt{\alpha} + K_\mu(Q_\mu), \end{aligned}$$

следовательно, $K_\tau(Q) = K_\mu(Q)$ и $S_\tau(Q) = S_\mu(Q)$, что влечёт в противоположность предположению $\tau \neq \mu$.

Таким образом, описание множества $\mathrm{Quat}_k(Q)$ приобретает значение и с точки зрения описания инволюций второго рода кватернионных алгебр.

Описание множества $\mathrm{Quat}_k(Q)$ с точностью до k-изоморфизма даётся следующим предложением.

Предложение 4. *Кватернионная алгебра B над k может быть k-изоморфно вложена в кватернионную алгебру Q с инволюцией τ тогда и только тогда, когда B Брауэр-эквивалентна алгебре $Q_\tau \otimes_k (\frac{\alpha,\beta}{k})$ для некоторого $\beta \in k^*$.*

Доказательство. Предположим, что $B \sim Q_\tau \otimes \left(\frac{\alpha,\beta}{k}\right)$, где $\sim$ означает Брауэр-эквивалентность. Умножим обе части эквивалентности тензорно на K (над k). Тогда

$$B \otimes_k K \sim \left(Q_\tau \otimes \left(\frac{\alpha,\beta}{k}\right)\right) \otimes_k K \sim (Q_\tau \otimes_k K) \otimes_K \left(\left(\frac{\alpha,\beta}{k}\right) \otimes_k K\right)$$
$$\sim Q_\tau \otimes_k K \sim Q.$$

Так как обе алгебры $B \otimes_k K$ и Q имеют одинаковые размерности над K, то они K-изоморфны, а ограничение этого изоморфизма на B и задаёт k-изоморфное вложение B в A. Обратно, пусть φ_B – k-изоморфизм, вкладывающий B в Q. Тогда нетрудно видеть, что $Q = \varphi(B) \otimes_k K$, а так как ещё $Q = Q_\tau \otimes_k K$, то алгебры $\varphi(B) \otimes_k K$ и $Q_\tau \otimes_k K$ K-изоморфны. Тогда алгебра $(\varphi(B) \otimes_k K) \otimes_K (Q_\tau \otimes_k K)$ является матричной над K, а так как ещё она имеет вид $(\varphi(B) \otimes_k Q_\tau) \otimes_k K$, то $\varphi(B) \otimes_k Q_\tau$ расщепляется квадратичным расширением $k(\sqrt{\alpha})$. Значит, $B \sim \varphi(B) \sim Q_\tau \otimes \left(\frac{\alpha,\beta}{k}\right)$, для подходящего $\beta \in k^*$. □

Следствие. *Пусть k – поле, $\mathrm{char}\, k \neq 2$, для которого выполнено условие: всякая центральная k-алгебра с делением экспоненты 2 кватернионна (в частности, глобальное поле, C_2-поле и т.п.). Тогда кватернионные k-алгебры, k-изоморфно вложенные в Q, параметризуются алгебрами с делением из смежного класса $Q_\tau + \mathrm{Br}(K/k)$ группы Брауэра поля по подгруппе $\mathrm{Br}(K/k)$ расщепимых над K элементов.*

Замечание. Из предыдущего следствия немедленно вытекает способ построения не k-изоморфных алгебр, k-изоморфно вложимых в Q (нужно только, чтобы группа $\mathrm{Br}(K/k)$ была нетривиальна).

Оказывается, что классы k-изоморфных элементов в $\mathrm{Quat}_k(Q)$ совпадают с классами сопряжённости в Q^*. Действительно, справедливо следующее

Предложение 5. *Две алгебры Q_1 и $Q_2 \in \mathrm{Quat}_k(Q)$ k-изоморфны в том и только с том случае, когда $Q_2 = gQ_1g^{-1}$ для некоторого $g \in Q$; τ-инвариантные алгебры Q_1 и Q_2 k-изоморфны тогда и только тогда, когда существует элемент $g \in Q^*$ такой, что $Q_2 = gQ_1g^{-1}$ и $(g^\tau g)Q_1(g^\tau g)^{-1} = Q_1$.*

Доказательство. Предположим, что $\varphi : Q_1 \longrightarrow Q_2$ – k-изоморфизм алгебр. Тогда алгебра Q может быть представлена и в виде $Q_1 \otimes_k K$, и в виде $Q_2 \otimes_k K$. Положим тогда $(q_1 + q_2\sqrt{\alpha})^\Phi = q_1^\varphi + q_2^\varphi\sqrt{\alpha}$. Прямое вычисление показывает, что $\Phi : Q \longrightarrow Q$ – K-автоморфизм алгебры Q, являющийся внутренним по теореме Сколема–Нётер (т.е. $\Phi(m) = gmg^{-1}$ для подходящего $g \in Q$ и произвольного $m \in Q$). Ясно, что ограничение Φ на Q_1 сопрягает Q_1 и Q_2. Обратно, если $Q_2 = gQ_1g^{-1}$, $g \in Q$, то ограничение внутреннего автоморфизма алгебры Q, индуцированного элементом g приводит к k-изоморфизму Q_1 и Q_2. Кроме того, если Q_1 и Q_2 τ-инвариантны, то из $Q_2 = gQ_1g^{-1}$ следует, что $g^{-\tau}Q_1^\tau g^\tau = Q_2^\tau$, и из этих двух последних совпадений получаем $(g^\tau g)Q_1(g^\tau g)^{-1} = Q_1$. Обратно, если для τ-инвариантной алгебры Q_1 существует элемент g такой, что $(g^\tau g)Q_1(g^\tau g)^{-1} = Q_1$, то подалгебра Q_2, равная gQ_1g^{-1} τ-инвариантна и сопряжена, а, следовательно, и k-изоморфна с алгеброй Q_1. □

Поскольку отыскание элемента g из предыдущего предложения в общем случае может вызвать определённые трудности, приведём другой способ, с помощью которого можно устанавливать сопряжённость τ-инвариантных подалгебр алгебры Q. Для этого заметим, что если Q_1, Q_2 – τ-инвариантные подалгебры алгебры Q, то k-пространства $S_\tau(Q_1), S_\tau(Q_2)$ либо оба трёхмерны, либо одно из них одномерно, а другое трёхмерно. Для рассмотрения первого случая нам потребуется

Лемма 3. *Пусть* $\dim_k S_\tau(Q_1) = \dim_k S_\tau(Q_2) = 3$. *Тогда алгебры Q_1, Q_2 обладают общим максимальным подполем, порождённым симметрическим элементом.*

Доказательство. Воспользуемся формулой о размерности суммы двух подпространств:

$$\begin{aligned}\dim_k(S_\tau(Q_1) + S_\tau(Q_2)) \\ = \dim_k S_\tau(Q_1) + \dim_k S_\tau(Q_2) - \dim_k(S_\tau(Q_1) \cap S_\tau(Q_2)).\end{aligned}$$

Тогда ввиду неравенства $\dim(S_\tau(Q_1) + S_\tau(Q_2)) \leqslant 4$ замечаем, что $\dim_k(S_\tau(Q_1) \cap S_\tau(Q_2)) \geqslant 2$. Следовательно, существует симметрический элемент из $S_\tau(Q_1) \cap S_\tau(Q_2)$, не принадлежащий k, который и порождает максимальное подполе и в Q_1, и в Q_2. □

Теперь критерий сопряжённости (k-изоморфности) для первого случая выглядит следующим образом.

Предложение 6. *Две τ-инвариантные подалгебры Q_1 и Q_2 алгебры Q с общим максимальным подполем, порождённым симметрическим элементом $\sqrt{p}$, $p \in k$, сопряжены тогда и только тогда, когда*

$$Q_1 = \left(\frac{p, q_1}{k}\right), \qquad Q_2 = \left(\frac{p, q_2}{k}\right)$$

и $q_1 q_2 \in N_{k(\sqrt{p})/k}(k(\sqrt{p})^*)$.

Доказательство. Заметим, что последнее условие в формулировке предложения эквивалентно их k-изоморфности, а тогда ввиду предложения 5 и их сопряжённости. □

Обратимся ко второму случаю.

Предложение 7. *Пусть $\dim_k S_\tau(Q_1) = 1, \dim_k S_\tau(Q_2) = 3$ и $Q_1 = (\frac{m,n}{k})$, $Q_2 = (\frac{m\alpha, n\alpha}{k})$. Тогда алгебры Q_1 и Q_2 сопряжены в том и только в том случае, когда алгебра $(\frac{\alpha, -mn}{k})$ – матричная алгебра над k.*

Доказательство. Сопряжённость алгебр Q_1 и Q_2 эквивалентна их k-изоморфности, что в свою очередь эквивалентно тому, что алгебра

$$\left(\frac{m, n}{k}\right) \otimes_k \left(\frac{m\alpha, n\alpha}{k}\right)$$

является матричной (над k). Но тогда ввиду

$$\left(\frac{m, n}{k}\right) \otimes_k \left(\frac{m\alpha, n\alpha}{k}\right) \sim \left(\frac{m, n}{k}\right) \otimes_k \left(\frac{m, \alpha}{k}\right) \otimes_k \left(\frac{n, \alpha}{k}\right) \otimes_k \left(\frac{m, n}{k}\right) \otimes_k \left(\frac{\alpha, \alpha}{k}\right)$$

$$\sim \left(\frac{m, \alpha}{k}\right) \otimes_k \left(\frac{n, \alpha}{k}\right) \otimes_k \left(\frac{\alpha, \alpha}{k}\right) \sim \left(\frac{\alpha, mn}{k}\right) \otimes_k \left(\frac{\alpha, -1}{k}\right) \sim \left(\frac{\alpha, -mn}{k}\right)$$

алгебра $\left(\frac{\alpha, -mn}{k}\right)$ – матричная алгебра над k, и обратно, что и требовалось. □

Несмотря на то, что алгебры Q_1 и Q_2 имеют специальный вид, предыдущее предложение завершает рассмотрение второго случая ввиду справедливости следующего утверждения. Предварим его формулировку введением следующей леммы-обозначения.

Лемма-обозначение 2. *Пусть* $Q_\tau = (\frac{m,n}{k})$, $\{1, u, v, uv\}$ *– канонический* k*-базис (т.е.* $u^2 = m$, $v^2 = n$, $uv = -vu$*) и* $Q_\tau(m,n)$ *–* k*-линейная оболочка элементов* $\{1, u\sqrt{\alpha}, v\sqrt{\alpha}^{-1}, uv\}$*. Тогда* $Q_\tau(m,n)$ *–* τ*-инвариантная подалгебра алгебры* Q *и ограничение* τ *на* $Q_\tau(m,n)$ *не является канонической инволюцией.*

Доказательство. Прямое вычисление. □

Теорема 2. *Всякая алгебра* $A \in \mathrm{Quat}_k(Q)$ τ*-инвариантна с неканоническим ограничением на* A *тогда и только тогда, когда существуют такие элементы* $m, n \in k$*, что*

$$Q_\tau = \left(\frac{m,n}{k}\right), A = Q_\tau(m,n).$$

Доказательство. Достаточность следует из предыдущей леммы. Необходимость устанавливается следующим образом. Пусть алгебра $A \in \mathrm{Quat}_k(Q)$ τ-инвариантна и ограничение τ на A не является каноническим. Тогда в A существует канонический базис $1, i, j, ij$ такой, что $i^\tau = i, j^\tau = j$. Действительно, пусть s – нецентральный симметрический элемент в A и $k(s) = k(\sqrt{a})$. Обозначим через g элемент из A^* такой, что $g\sqrt{a}g^{-1} = -\sqrt{a}$. Нетрудно видеть тогда, что $(g + g^\tau)\sqrt{a} = -\sqrt{a}(g + g^\tau)$. Таким образом, можно считать, что существует элемент b такой, что $b\sqrt{a}b^{-1} = -\sqrt{a}$ и $b^\tau = \pm b$ ($b = g$, если $g^\tau = g$, и $b = g + g^\tau$ в противном случае). Далее, ясно, что элементы $1, \sqrt{a}, b, \sqrt{a}b$ образуют канонический базис. Положим $i = \sqrt{a}$, $j = b$, если $b^\tau = b$, и $j = \sqrt{a}b$ в противном случае. Пусть $u = i\sqrt{\alpha^{-1}}, v = j\sqrt{\alpha}$. Тогда линейная k-оболочка $1, u, v, uv$ совпадает с Q_τ. Теперь для $m = u^2, n = v^2$, $Q_\tau = \left(\frac{m,n}{k}\right)$ и $A = Q_\tau(m,n)$. □

Замечание. Для получения аналога предложения 1 в случае инволюций второго рода к списку алгебр, возникающих в теореме 2, следует, очевидно, добавить лишь поле k и поля вида $K(s)$, где $s \in S_\tau(Q) \cup K_\tau(Q)$.

Последняя теорема показывает важность выяснения условия на пары $(m,n),(a,b)$ элементов из k для k-изоморфности алгебр с делением

$$\left(\frac{a,b}{k}\right),\left(\frac{m,n}{k}\right).$$

Решение этой задачи даёт следующая теорема (ниже знак $\sim$ означает сравнимость по модулю ${k^*}^2$ в группе k^*.

Теорема 3. *Пусть* $(\frac{a,b}{k})$ *– алгебра с делением. Алгебра* $(\frac{m,n}{k})$ *k-изоморфна алгебре* $(\frac{a,b}{k})$ *тогда и только тогда, когда выполнено одно из условий:*

(i) $m\sim b(\varepsilon_2^2-a\varepsilon_3^2)$, $n\sim a(M^2-b(\varepsilon_2^2-a\varepsilon_3^2)N^2)$, *где обе пары элементов* $(\varepsilon_2,\varepsilon_3)$ *и* (M,N) *не равны* $(0,0)$.

(ii) $m\sim(a+\delta_2^2b-\delta_3^2ab)$, $n\sim\frac{1}{a}(\delta_3\nu_3-\delta_2\nu_2)^2-\nu_2^2\frac{1}{b}-\nu_3^2ab$, *где* ν_2, ν_3 *одновременно не равны нулю, а* δ_2, δ_3 *– любые.*

Доказательство. Пусть 1, A, B, AB – канонический базис алгебры $(\frac{a,b}{k})$. Предположим, что алгебры $(\frac{a,b}{k})$ и $(\frac{m,n}{k})$ k-изоморфны. Тогда в $(\frac{a,b}{k})$ существуют два антикоммутирующих элемента таких, что их квадраты соответственно равны m и n, и потому следующая система

$$mx_4^2=x_1^2a+x_2^2b-x_3^2ab, \tag{1}$$

$$ny_4^2=y_1^2a+y_2^2b-y_3^2ab, \tag{2}$$

$$x_1y_1a+x_2y_2b-x_3y_3ab=0, \tag{3}$$

относительно неизвестных $x_1,\dots,x_4$, $y_1,\dots,y_4$ разрешима в k^8 таким образом, что существует решение $x_1=\varepsilon_1$, $x_2=\varepsilon_2$, $x_3=\varepsilon_3$, $x_4=\varepsilon_4$, $y_1=\mu_1$, $y_2=\mu_2$, $y_3=\mu_3$, $y_4=\mu_4$ такое, что не все ε_i и не все μ_i равны нулю.

Очевидно, верно и обратное. Таким образом, разрешимость системы (1), (2), (3) эквивалентна изоморфности алгебр $(\frac{a,b}{k})$ и $(\frac{m,n}{k})$.

Пусть ε_1, ε_2, ε_3, ε_4, μ_1, μ_2, μ_3, μ_4 – вышеуказанное решение системы (1), (2), (3).

Рассмотрим раздельно два случая: (i) $\varepsilon_1=0$; (ii) $\varepsilon_1\neq 0$.

Случай (i). Из (1) следует $m\sim b(\varepsilon_2^2-\varepsilon_3^2a)$, где ε_2, ε_3 одновременно не равны нулю. Ввиду изоморфизма $(\frac{a,b}{k})\cong(\frac{m,n}{k})$ тогда будем иметь

$$\left(\frac{a,b}{k}\right)\cong\left(\frac{b(\varepsilon_2^2-\varepsilon_3^2a),a}{k}\right)\cong\left(\frac{b(\varepsilon_2^2-\varepsilon_3^2a),n}{k}\right).$$

Следовательно,

$$n = aN_{k(\sqrt{b(\varepsilon_2^2-\varepsilon_3^2 a)})/k}(M + N\sqrt{b(\varepsilon_2^2 - \varepsilon_3^2 a)}) = a(M^2 - (b(\varepsilon_2^2 - \varepsilon_3^2 a))N^2)$$

для подходящих M, $N \in k$, не равных одновременно нулю. Заметим, что элемент $b(\varepsilon_2^2-\varepsilon_3^2 a)$ не является квадратом в k. В противном случае, $b \in N_{k(\sqrt{a})/k}$, а тогда $(\frac{a,b}{k}) \sim 1$. Таким образом, из условий $(\frac{a,b}{k}) \cong (\frac{m,n}{k})$ и $\varepsilon_1 = 0$ вытекает, что

$$m \sim b(\varepsilon_2^2 - \varepsilon_3^2 a), \tag{4}$$

$$n \sim a(M^2 - b(\varepsilon_2^2 - \varepsilon_3^2 a)N^2). \tag{5}$$

Обратно, пусть условия (4) и (5) выполнены. Тогда

$$\left(\frac{m,n}{k}\right) \cong \left(\frac{b(\varepsilon_2^2 - \varepsilon_3^2 a), a(M^2 - b(\varepsilon_2^2 - \varepsilon_3^2 a)N^2)}{k}\right)$$
$$\cong \left(\frac{b(\varepsilon_2^2 - \varepsilon_3^2 a), a}{k}\right) \cong \left(\frac{b,a}{k}\right) \cong \left(\frac{a,b}{k}\right).$$

Случай (ii). В этом случае из (1) получаем

$$m\left(\frac{\varepsilon_4}{\varepsilon_1}\right)^2 = a + \left(\frac{\varepsilon_2}{\varepsilon_1}\right)^2 b - \left(\frac{\varepsilon_3}{\varepsilon_1}\right)^2 ab.$$

Положим

$$\delta_2 = \left(\frac{\varepsilon_2}{\varepsilon_1}\right), \quad \delta_3 = \left(\frac{\varepsilon_3}{\varepsilon_1}\right), \quad \delta_4 = \left(\frac{\varepsilon_4}{\varepsilon_1}\right).$$

Тогда будем иметь

$$m\delta_4^2 = a + \delta_2^2 b - \delta_3^2 ab. \tag{1*}$$

Из (3) вытекает

$$\mu_1 a = \frac{\varepsilon_3}{\varepsilon_1}\mu_3 ab - \frac{\varepsilon_2}{\varepsilon_1}\mu_2 b, \quad \text{или} \quad \mu_1 a = \delta_3\mu_3 ab - \delta_2\mu_2 b.$$

Положим $\mu_1 a = \nu_1$, $\mu_2 = \nu_2$, $\mu_3 a = \nu_3$, $\mu_4 = \nu_4$. Умножим обе части равенства (2) на a, тогда в предыдущих обозначениях будем иметь

$$an\nu_4^2 = \nu_1^2 + \nu_2^2 ab - \nu_3^2 b. \tag{2*}$$

Кроме того из (3) получаем

$$\nu_1 = \delta_3\nu_3 b - \delta_2\nu_2 b. \tag{3*}$$

Заменим теперь в (2*) элемент ν_1^2 на его выражение из (3*). Тогда

$$an\nu_4^2 = b^2(\delta_3\nu_3 - \delta_2\nu_2)^2 + \nu_2^2 ab - \nu_3^2 b.$$

Разделив на ab^2 обе части, получим

$$n \sim \frac{1}{a}(\delta_3\nu_3 - \delta_2\nu_2)^2 + \nu_2^2\frac{1}{b} - \nu_3^2\frac{1}{a}\frac{1}{b}.$$

Обратно, положим

$$n \sim \frac{1}{a}(\delta_3\nu_3 - \delta_2\nu_2)^2 + \nu_2^2\frac{1}{b} - \nu_3^2\frac{1}{a}\frac{1}{b},$$

где ν_2 и ν_3 одновременно не равны нулю и $m \sim (a + \delta_2^2 b - \delta_3^2 ab)$. Нетрудно видеть, что элемент $(a + \delta_2^2 b - \delta_3^2 ab)$ отличен от нуля при любых δ_2, δ_3, поскольку является квадратом ненулевого кватерниона $A + \delta_2 B + \delta_3 AB$. Элемент

$$\frac{1}{a}(\delta_3\nu_3 - \delta_2\nu_2)^2 + \nu_2^2\frac{1}{b} - \nu_3^2\frac{1}{a}\frac{1}{b}$$

также отличен от нуля, поскольку является квадратом ненулевого кватерниона (напомним, что ν_2, ν_3 одновременно не равны нулю)

$$(\delta_3\nu_3 - \delta_2\nu_2)A^{-1} + \nu_2 B^{-1} + \nu_3 A^{-1}B^{-1}$$

в алгебре $(\frac{a^{-1},b^{-1}}{k})$, совпадающей, очевидно, с $(\frac{a,b}{k})$. Теперь уже ясно, что не ограничивая общности можно считать, что

$$n = \frac{1}{a}(\delta_3\nu_3 - \delta_2\nu_2)^2 + \nu_2^2\frac{1}{b} - \nu_3^2\frac{1}{a}\frac{1}{b}, \quad m = (a + \delta_2^2 b - \delta_3^2 ab).$$

Обращая предыдущие рассуждения при выбранных m и n, мы заключаем, что система (1), (2), (3) разрешима, и потому $(\frac{a,b}{k}) \cong (\frac{m,n}{k})$. Теорема доказана. □

Авторы признательны С. В. Тихонову за многочисленные полезные обсуждения.

Литература

1. A. A. Albert, *Structure of Algebras.* N.-Y., AMS. (1980), 210.
2. Ж. Дьёдонне, *Геометрия классических групп.* Мир, М., 1974.
3. Н. Бурбаки, *Алгебра. Модули, кольца, формы.* Наука, М., 1966.
4. B. A. Sethuraman, B. Sury, *On the special unitary group of a division algebra.* — Proc. Amer. Math. Soc. **134** (2005), 351–354.
5. В. И. Янчевский, *Об абелевых факторах специальных унитарных групп анизотропных форм.* — Докл. НАН Беларуси (2011) (принята к печати).
6. B. Sury, *On* $\mathrm{SU}(1,D)/[U(1,D),U(1,D)]$ *for a quaternion division algebra* D. — Arch. Math. **90** (2008), 493–500.

Prokopchuk A. V., Yanchevskiĭ V. I. Invariant subalgebras of involutorial quaternion division algebras.

Let K/k be a separable quadratic field extension. For quaternion division algebras with K/k involutions τ their τ-invariant k-subalgebras are studied. We give a complete description of such subalgebras up to k-isomorphisms.

Институт математики НАН Беларуси
E-mail: alexpro@im.bas-net.by, yanch@im.bas-net.by

Поступило 5 апреля 2011 г.