KUMMER SUBSPACES OF TENSOR PRODUCTS OF CYCLIC ALGEBRAS

ADAM CHAPMAN

(Communicated by Jerzy Weyman)

Abstract. We discuss the Kummer subspaces of tensor products of cyclic algebras, focusing mainly on the case of cyclic algebras of degree 3. We present a family of maximal Kummer spaces in any tensor product of cyclic algebras of prime degree, classify all the monomial Kummer spaces in tensor products of cyclic algebras of degree 3, and provide an upper bound for the dimension of Kummer spaces in the generic tensor product of cyclic algebras of degree 3.

1. Introduction

Let \( p \) be a prime integer and \( F \) be an infinite field of characteristic not \( p \) containing a primitive \( p \)-th root of unity \( \rho \). A cyclic algebra of degree \( p \) over \( F \) is an algebra that can be presented as

\[
F[x, y : x^p = \alpha, y^p = \beta, yx = \rho xy]
\]

for some \( \alpha, \beta \in F^\times \). We denote this presentation by \((\alpha, \beta)_{p,F}\). A given algebra can have more than one presentation. Fixing a presentation, we call the elements of the form \( cx^i y^j \), where \( i \) and \( j \) are integers between 0 and \( p - 1 \) and \( c \in F \), “monomials”.

The same goes for tensor products of cyclic algebras; i.e., if we fix presentations

\[
F[x_k, y_k : x_k^p = \alpha_k, y_k^p = \beta_k, y_k x_k = \rho x_k y_k] = (\alpha_k, \beta_k)_{p,F}
\]

for \( k \in \{1, \ldots, n\} \), then the monomials in the tensor product \( \bigotimes_{k=1}^n (\alpha_k, \beta_k)_{p,F} \) are of the form \( c \prod_{k=1}^n x_k^{i_k} y_k^{j_k} \) where \( i_1, j_1, \ldots, i_n, j_n \) are integers between 0 and \( p - 1 \) and \( c \in F \).

Let \( A \) be a tensor product of \( n \) cyclic algebras of degree \( p \). Assume \( A \) is a division algebra. An element \( x \in A \) is called Kummer if \( x^p \in F \) and \( x^k \notin F \) for all \( k \in \{1, \ldots, p - 1\} \). An \( F \)-vector subspace of \( A \) is called Kummer if all its nonzero elements are Kummer. A necessary and sufficient condition for a space \( Fx_1 + \cdots + Fx_m \) to be Kummer is that \( x_1^{d_1} \cdots x_m^{d_m} \in F \) for every \( m \)-tuple of nonnegative integers \( d_1, \ldots, d_m \) satisfying \( d_1 + \cdots + d_m = p \) [CV12, Corollary 2.2].

The expression \( x_1^{d_1} \cdots x_m^{d_m} \) stands for the sum of all the words in which each \( x_k \) appears \( d_k \) times, e.g., \( x_1^2 x_2^3 = x_1 x_1 x_2 x_2 x_2 \). This notation was introduced in [Rev77]. Fixing the presentations of the cyclic algebras, a Kummer space is called “monomial” if it is spanned by monomials.

Received by the editors May 5, 2014 and, in revised form, October 18, 2016 and November 22, 2016.

2010 Mathematics Subject Classification. Primary 16K20; Secondary 05C38, 16W60.

Key words and phrases. Central simple algebras, cyclic algebras, Kummer spaces, generic algebras, graphs.
Any central simple algebra of exponent $p$ over $F$ is Brauer equivalent to a tensor product of cyclic algebras of degree $p$ by the renowned Merkurjev-Suslin theorem [MS82]. Its symbol length is the minimal number of cyclic algebras required in order to express its Brauer class. In [Mat16] Kummer spaces were used in bounding the symbol length from above when $F$ is a $C_m$ field. This motivates the study of such spaces, and in particular their structure and possible dimensions.

We conjecture that the maximal dimension of a Kummer subspace of $A$ is $np+1$. The conjecture is known to hold true in certain special cases: for $p = 2$ and any positive integer $n$ (an immediate result of the theory of Clifford algebras of quadratic forms; see [Lam73, Chapter 5, Section 2]), and for $p = 3$ and $n = 1$. In the latter case, the Kummer spaces were completely classified in [Rac09] and [MV12]. A classification of the Kummer spaces in the case of $p = n = 2$ can be found in [CV13, Section 5].

In [CGM16] the monomial Kummer spaces in division cyclic algebras of prime degree were classified. Furthermore, an upper bound of $p + 1$ was provided for the dimension of the Kummer subspaces of the generic cyclic algebra, i.e. the algebra $(\alpha, \beta)_{p,K}$ where $K = F(\alpha, \beta)$ is the function field in two algebraically independent variables over $F$.

In this paper we present some new results on the classification of Kummer spaces and their maximality. In Section 2 we present a family of maximal Kummer subspaces in any tensor product of cyclic algebras. This section is based on results from [Cha09, Chapter 2, Section 1] and [Cha13, Chapter 2, Section 2]. In Section 3 we classify the monomial Kummer subspaces of tensor products of cyclic algebras of degree 3. This section is based on results from [Cha13, Chapter 2, Section 6]. In Section 4 we provide an upper bound for the dimension of a Kummer subspace of the generic tensor product of cyclic algebras of degree 3.

2. MAXIMAL KUMMER SUBSPACES OF TENSOR PRODUCTS OF CYCLIC ALGEBRAS

Fix $A = \bigotimes_{k=1}^{n} (\alpha_k, \beta_k)_{p,K} = \bigotimes_{k=1}^{n} F[x_k, y_k : x_k^p = \alpha_k, y_k^p = \beta_k, y_kx_k = \rho x_ky_k]$. Assume $A$ is a division algebra. Let $V_0 = F$ and $V_k = F[x_k, y_k + V_{k-1}x_k]$ for every $k \in \{1, \ldots, n\}$. The dimension of each $V_k$ is $pk + 1$. These spaces appeared also in [Mat16, Section 3].

Proposition 2.1. For each $k \in \{1, \ldots, n\}$, $V_k$ is a Kummer space.

Proof. Assume $V_{k-1}$ is either Kummer or $F$ for a certain $k$. Every element of $V_k$ is of the form $f(x_k)y_k + vx_k$ for some $f(x_k) \in F[x_k]$ and $v \in V_{k-1}$. Since $v$ commutes with $x_k$ and $y_k$, and $y_kx_k = \rho x_ky_k$, $(f(x_k)y_k + vx_k)^p = (f(x_k)y_k)^p + v^p x_k^p = N_{F[x_k]/F}(f(x_k))\beta_k + v^p \alpha_k \in F$ (see [CV12, Remark 2.5]). For any $1 \leq m \leq p - 1$, if $f(x_k) \neq 0$, then the eigenvector of $(f(x_k)y_k + vx_k)^m$ corresponding to the eigenvalue $\rho^m$ with respect to conjugation by $x_k$ is $(f(x_k)y_k)^m$, which is not zero, and therefore $(f(x_k)y_k + vx_k)^m \notin F$. If $f(x_k) = 0$, then what is left is $vx_k$, and of course $v^m x_k^m \notin F$. Consequently, $V_k$ is Kummer. Since $V_0 = F$, by induction $V_k$ is Kummer for every $k \in \{1, \ldots, n\}$. □

Remark 2.2. If $uv = \rho^k vu$ for some $u, v \in A \setminus \{0\}$ and $k \in \{0, \ldots, p - 1\}$, then $u^{p-1} * v = 0$ if $k \neq 0$ and $u^{p-1} * v = pu^{p-1}v$ if $k = 0$. Hence, if $uv = vu$ and $Fu + Fv$ is a Kummer subspace of $A$, then $v$ is a scalar multiple of $u$. 

Theorem 2.3. For each $k \in \{1, \ldots, n\}$, $V_k$ is a maximal Kummer subspace of $A$ with respect to inclusion.

Proof. Fix some $k \in \{1, \ldots, n\}$. The Kummer space $V_k$ has a basis of monomials $B_k = \left\{ x_i^t y_i \left( \prod_{j=i+1}^{k} x_j \right) : 1 \leq i \leq k, 0 \leq \ell \leq p-1 \right\} \cup \{x_1x_2 \ldots x_k\}$.

Note that when $i = k$, $\prod_{j=i+1}^{k} x_j$ is the empty product and so it is 1, and therefore $x_i^t y_i \left( \prod_{j=i+1}^{k} x_j \right) = x_k^t y_k \in B_k$. Let $z$ be an element in $A$ and write $z = \sum_{\alpha} m_{\alpha}$ for some monomials $m_{\alpha}$. Assume $V_k + Fz$ is Kummer. Let $w$ be an element in $B_k$. Since $w^{p-1} * z \in F$, for every $\alpha$ either $m_{\alpha}$ is a scalar multiple of $w$ or it does not commute with $w$. Therefore, by subtracting from $z$ an element of $V_k$, we may assume that none of the monomials $m_{\alpha}$ commute with any $w$ in $B_k$.

It remains to show that every monomial commutes with some element in $B_k$, which implies that $z = 0$: Consider a monomial $t = c x_1^{d_1} y_1^{e_1} \ldots x_n^{d_n} y_n^{e_n}$. If $d_1 = e_2 = \ldots = e_n = 0$, then $t$ commutes with $x_1 x_2 \ldots x_k \in B_k$. Otherwise, let $i$ be the maximal integer in $\{1, \ldots, n\}$ with $e_i \neq 0$. Then $t$ commutes with $x_i^t y_i x_{i+1} \ldots x_k \in B_k$ where $\ell$ is the unique integer in $\{0, \ldots, p-1\}$ with $\ell \equiv d_i e_i^{-1} \pmod{p}$. \hfill $\square$

3. Monomial Kummer subspaces of tensor products of cyclic algebras of degree 3

Keep $A$ as before and assume $p = 3$. Let $\mathcal{X}$ be the set of all Kummer elements in $A$. We build a directed graph $(\mathcal{X}, E)$ by drawing an edge from $y$ to $x$,

$$y \rightarrow x,$$

if $yxy^{-1} = \rho x$. For any subset $B \subset \mathcal{X}$, $(B, E_B)$ is the subgraph obtained by taking the vertices in $B$ and all the edges between them. The set $B$ is called $\rho$-commuting if it is linearly independent over $F$ and for every two distinct elements $x, y \in B$, $yxy^{-1} = \rho^k x$ for $k \in \{0, 1, 2\}$. In particular, any set of linearly independent monomials is $\rho$-commuting.

Remark 3.1. If $\{x, y\}$ is a $\rho$-commuting set spanning a Kummer space, then either $x \rightarrow y$ or $x \leftarrow y$.

Proof. If $xy = yx$, then $x^2 * y = 3x^2 y \in F$, which means that $y \in Fx$, a contradiction. \hfill $\square$

According to [CV12 Corollary 2.2], a set $\{x_1, \ldots, x_m\}$ spans a Kummer space if and only if every subset of cardinality 3 $\{x_i, x_j, x_k\}$ spans a Kummer space. Therefore we will start with sets of cardinality 3.

Lemma 3.2. Given a $\rho$-commuting set $\{x, y, z\}$, $Fx + Fy + Fz$ is Kummer if and only if (up to some permutation on $\{x, y, z\}$) either

$$x \rightarrow y \quad \downarrow \quad z \rightarrow x$$
or $xyz \in F$, in which case

\[
x \leftarrow y \\
\downarrow \\
z
\]

Proof. From Remark 3.1, the only possible graphs (up to permutation of the vertices) are the two graphs above. In the first case, $x*y*z = 0$, so there are no extra conditions. In the second case, $x*y*z = -3\rho^{-1}xyz \in F$. The opposite direction is a straightforward computation. 

Let $B$ be a $\rho$-commuting set spanning a Kummer space. We will now study the properties of the directed graph $(B,E_B)$. By a cycle we always mean a simple directed cycle.

**Proposition 3.3.** If $(B,E_B)$ contains a cycle of length 3:

\[
x_0 \leftarrow x_1 \\
\downarrow \\
x_2
\]

then for every $y \in B \setminus \{x_0,x_1,x_2\}$, either $x_k \rightarrow y$ for all $k \in \{0,1,2\}$ or $x_k \leftarrow y$ for all $k \in \{0,1,2\}$.

Proof. If $x_0 \rightarrow y$ and $x_1 \leftarrow y$, then

\[
x_0 \leftarrow x_1 \\
\downarrow \\
y
\]

which means that $yx_0x_1 \in F$. Since $x_0x_1x_2 \in F$, we get $y \in Fx_2$, which contradicts the linear independence.

**Proposition 3.4.** The cycles in $(B,E_B)$ are vertex-disjoint.

Proof. First assume that

\[
x_0 \leftarrow x_1 \\
\downarrow \\
x_2 \downarrow y
\]

Then $yx_1x_2 \in F$ and $x_0x_1x_2 \in F$, which means that $y \in Fx_0$, and that contradicts the linear independence.

Assume that

\[
x_0 \leftarrow x_1 \leftarrow y_1 \\
\downarrow \\
x_2 \\
\downarrow y_2
\]

From Proposition 3.3, we have $x_0 \rightarrow y_2$ and $y_1 \rightarrow x_0$. But then

\[
x_0 \leftarrow y_1 \\
\downarrow \\
y_2 \\
\downarrow x_1
\]

and we already saw that this is impossible.

**Proposition 3.5.** There are no cycles of length greater than 3 in $(B,E_B)$. 

Proof. Assume

\[
\begin{array}{c}
\text{x}_1 & \xleftarrow{\text{x}_2} & \cdots & \xleftarrow{\text{x}_{r-1}} & \text{x}_r \\
\text{x}_r & \xrightarrow{} & \text{x}_1
\end{array}
\]

for some \( r \geq 4 \). Let \( i \) be the maximal integer between 1 and \( r \) such that \( \text{x}_i \xrightarrow{} \text{x}_1 \). Now, \( \text{x}_1 \xrightarrow{} \text{x}_{i+1} \). Therefore

\[
\begin{array}{c}
\text{x}_1 & \xleftarrow{\text{x}_i} & \text{x}_{i+1} \\
\text{x}_{i+1} & \xrightarrow{} & \text{x}_1
\end{array}
\]

If \( i \geq 3 \), then according to Proposition 3.3, \( \text{x}_1 \xrightarrow{} \text{x}_{i-1} \), which implies that \( i \neq 3 \), or in other words \( i \geq 4 \). Let \( j \) be the minimal index for which \( \text{x}_1 \xrightarrow{} \text{x}_{j+1} \). In particular \( \text{x}_j \xrightarrow{} \text{x}_1 \). Now, \( j + 1 \leq i - 1 \), which means that

\[
\begin{array}{c}
\text{x}_{i+1} & \xleftarrow{\text{x}_1} & \text{x}_j \\
\text{x}_j & \xrightarrow{} & \text{x}_{i+1} \\
\text{x}_i & \xrightarrow{} & \text{x}_{j+1}
\end{array}
\]

But this is impossible. If \( i = 2 \), then according to Proposition 3.3, \( \text{x}_4 \xrightarrow{} \text{x}_1 \), which contradicts the maximality of \( i \). □

As a consequence we obtain the following theorem:

**Theorem 3.6.** A \( \rho \)-commuting subset \( B \) of \( X \) spans a Kummer space if and only if the graph \((B, E_B)\) satisfies the following axioms:

1. For every two distinct elements \( x, y \in B \), either \( x \xrightarrow{} y \) or \( x \xleftarrow{} y \).
2. All cycles are of length 3.
3. The product of all the elements in a cycle is in \( F \).
4. The cycles are vertex-disjoint.

**Proof.** The straightforward direction is an immediate result of what we’ve done so far. The opposite direction is a result of the fact that every three elements in this set span a Kummer space according to Lemma 3.2. □

The following remark may help the reader get an idea of what the graph \((B, E_B)\) looks like:

**Remark 3.7.** Assume \( B \) is a \( \rho \)-commuting set spanning a Kummer space. Let \( \sim \) be the following equivalence relation: \( x \sim y \) if and only if \( x = y \) or \( x \xrightarrow{} y \) and \( y \xleftarrow{} x \) belong to the same cycle in \((B, E_B)\). As we already saw, this equivalence relation is also direction preserving in the sense that, assuming \( x \not\sim z \), if \( x \xrightarrow{} z \) and \( x \sim y \), then \( y \xrightarrow{} z \), and if \( z \xrightarrow{} x \) and \( x \sim y \), then \( z \xrightarrow{} y \). Define an order \( \leq \) on the equivalence classes: \([x] \leq [z]\) if \([x] = [z]\) or \( z \xrightarrow{} x \). Then the set of equivalence classes is a totally ordered set.

One can therefore visualize the graph as graded into levels, where in each level we have either one element or a cycle, and each element has edges going from it to all the elements in the lower levels.

**Corollary 3.8.** Given a \( \rho \)-commuting set \( B \) spanning a Kummer space, if \( \#B = m \), then the longest path \( \text{x}_1 \xrightarrow{} \text{x}_2 \xrightarrow{} \cdots \xrightarrow{} \text{x}_r \) in the graph \((B, E_B)\) satisfying \( \text{x}_i \xrightarrow{} \text{x}_j \) for any \( 1 \leq i < j \leq r \) is of length no less than \( m - \lfloor \frac{m}{3} \rfloor \).
Proof. Take $B$ and take off exactly one element from each cycle. The number of elements taken off is at most $\left\lceil \frac{m}{3} \right\rceil$, and what is left satisfies the required condition.

Corollary 3.9. The maximal $\rho$-commuting set spanning a Kummer space in $A = \bigotimes_{k=1}^{n} (\alpha_k, \beta_k)_F$ is of cardinality $3n + 1$.

Proof. We already know of the existence of monomial Kummer spaces of dimension $3n + 1$. According to the previous corollary, if we have a $\rho$-commuting set $B$ of size $3n + 2$ spanning a Kummer space, then we have a path in $(B, E_B)$ of length $2n + 2$,

$$x_1 \rightarrow x_2 \rightarrow \cdots \rightarrow x_{2n+2},$$

satisfying $x_i \rightarrow x_j$ for any $1 \leq i < j \leq 2n + 2$. Then the set $B$ generates over $F$ a tensor product of $n + 1$ cyclic algebras of degree $3$,

$$F[x_1, x_2] \otimes F[x_1 x_2^{-1} x_3, x_1 x_2^{-1} x_4] \otimes \cdots \otimes F[(\prod_{k=1}^{n} x_{2k-1} x_{2k}^{-1}) x_{2n+1}, (\prod_{k=1}^{n} x_{2k-1} x_{2k}^{-1}) x_{2n+2}],$$

a contradiction.

4. THE GENERIC TENSOR PRODUCT OF CYCLIC ALGEBRAS

Let $K = F(\alpha_1, \beta_1, \ldots, \alpha_n, \beta_n)$ be the function field in $2n$ algebraically independent variables over $F$. Fix $A = \bigotimes_{k=1}^{n} K\{x_k, y_k : x_k^p = \alpha_k, y_k^p = \beta_k, y_k x_k = \rho x_k y_k\}$.

Theorem 4.1. For any Kummer subspace of $A$ there exists a monomial Kummer space of the same dimension.

Proof. Write $V = Kv_1 + Kv_2 + \cdots + Kv_m$, where $m$ is the dimension of $V$. Each $v_k$ is the sum of monomials of the form $c x_1^{i_1} y_1^{j_1} \cdots x_n^{i_n} y_n^{j_n}$ where $i_1, j_1, \ldots, i_n, j_n$ are integers between $0$ and $p - 1$ and the coefficient $c$ is a quotient of two polynomials in the variables $\alpha_1, \beta_1, \ldots, \alpha_n, \beta_n$ over $F$. By multiplying by all the denominators, we can assume that the coefficients are polynomials.

Since $\alpha_i = x_i^p$ and $\beta_i = y_i^p$, each $v_k$ is also in the ring of twisted polynomials

$$R = F[x_1, y_1, \ldots, x_n, y_n : y_i x_j = x_j y_i, x_i x_j = x_j x_i, y_i y_j = y_j y_i \ \forall i \neq j]$$

over $F$. Consider the left-to-right lexicographical grading on $R$: the degree of a nonzero monomial $a x_1^{i_1} y_1^{j_1} \cdots x_n^{i_n} y_n^{j_n}$ is $(i_1, j_1, \ldots, i_n, j_n)$. There is a left-to-right lexicographical ordering on the degrees, i.e. $(i_1, j_1, \ldots, i_n, j_n) > (r_1, s_1, \ldots, r_n, s_n)$ if and only if either $i_1 = r_1, j_1 = s_1, \ldots, i_{k-1} = r_{k-1}, j_{k-1} = s_{k-1}$ and $i_k > r_k$ or $i_1 = r_1, j_1 = s_1, \ldots, i_{k-1} = r_{k-1}, j_{k-1} = s_{k-1}, i_k = r_k$ and $j_k > s_k$ for some $k \in \{1, \ldots, n\}$. Every twisted polynomial $v$ in $R$ has a “leading term”, i.e. a term of highest degree. We define $\text{deg}(v)$ to be the degree of its leading term.

We perform a Gram-Schmidt-like process on the basis $v_1, \ldots, v_m$ to obtain a new basis whose leading terms are linearly independent over $K$: Let $\text{deg}(v_1)$ be $(a_1, b_1, \ldots, a_n, b_n)$. Let $a_1', b_1', \ldots, a_n', b_n'$ be the unique integers between $0$ and $p - 1$ such that $(a_1, b_1, \ldots, a_n, b_n) \equiv (a_1', b_1', \ldots, a_n', b_n') \pmod{p}$. Recall that each $v_k$ is the sum of monomials of the form $c x_1^{i_1} y_1^{j_1}, \ldots, x_n^{i_n} y_n^{j_n}$ where $i_1, j_1, \ldots, i_n, j_n$ are integers between $0$ and $p - 1$ and the coefficient $c$ is a polynomial in $F[\alpha_1, \beta_1, \ldots, \alpha_n, \beta_n]$. For each $k \in \{1, \ldots, n\}$, let $c_k$ be the coefficient of $x_1^{a_1'} y_1^{b_1'}, \ldots, x_n^{a_n'} y_n^{b_n'}$ in $v_k$. 

For each \( i \in \{2, \ldots, m\} \) we replace \( v_i \) with \( c_1v_i - c_i v_1 \). Now the coefficient of \( x_1^{a_1} y_1^{b_1} \cdots x_n^{a_n} y_m^{b_m} \) in \( v_k \) is zero for every \( k \in \{2, \ldots, m\} \). We continue in this manner by fixing \( v_2 \) and changing \( v_3, \ldots, v_m \) similarly, and so on. In the end, we obtain a basis \( v_1, \ldots, v_m \) satisfying \( \deg(v_i) \neq \deg(v_j) \pmod{p} \) for any \( i \neq j \). Consequently, the leading terms of \( v_1, \ldots, v_m \) are linearly independent over \( K \).

For every \( k \in \{1, \ldots, m\} \), let \( w_k \) be the leading term of \( v_k \). The \( K \)-vector space \( Kw_1 + \cdots + Kw_m \) is of dimension \( m \) and spanned by monomials, so it remains to prove that it is Kummer. Let \( d_1, \ldots, d_m \) be nonnegative integers satisfying \( d_1 + \cdots + d_m = p \). It is easy to see that if the element \( w_1^{d_1} \cdots w_m^{d_m} \) is nonzero, then it is the leading term of \( v_1^{d_1} \cdots v_m^{d_m} \), which is in \( K \) because \( Kv_1 + \cdots + Kv_m \) is Kummer. Otherwise \( w_1^{d_1} \cdots w_m^{d_m} \) is zero, which is also in \( K \). Consequently \( Kw_1 + \cdots + Kw_m \) is a Kummer space.

**Corollary 4.2.** If \( p = 3 \), then the upper bound for the dimension of a Kummer subspace of \( A \) is \( 3n + 1 \).

**Proof.** Follows immediately from the previous theorem and Section 3. □

**Acknowledgements**

The author thanks Jean-Pierre Tignol, Uzi Vishne and the anonymous referee for their comments on the manuscript. At the time of submission, the author was visiting ICTEAM Institute at Université Catholique de Louvain. The visit was sponsored by Wallonie-Bruxelles-International.

**References**


**Department of Computer Science, Tel-Hai Academic College, Upper Galilee, 12208 Israel**

**E-mail address:** adam1chapman@yahoo.com