BIMODULE STRUCTURE OF CENTRAL SIMPLE ALGEBRAS

ELIYAHU MATZRI, LOUIS H. ROWEN, DAVID J. SALTMAN, UZI VISHNE

ABSTRACT. For a maximal separable subfield $K$ of a central simple algebra $A$, we provide a semiring isomorphism between $K\cdot K$-bimodules $A$ and $H\cdot H$ bisets of $G = \text{Gal}(L/F)$, where $F = \mathbb{Z}(A)$, $L$ is the Galois closure of $K/F$, and $H = \text{Gal}(L/K)$. This leads to a combinatorial interpretation of the growth of $\dim_K((KaK)^i)$, for fixed $a \in A$, especially in terms of Kummer sets.

1. Introduction

$A$ always denotes a simple finite dimensional algebra of degree $n$ (i.e., dimension $n^2$) with center $F$, i.e., a central simple algebra $A/F$, and $K = F[\theta]$ is a given maximal subfield of $A$ that is a separable extension of $F$. Recall by the Koethe-Noether-Jacobson Theorem [Jac1, Theorem VII.11.1], [Jac4] that, for $A$ a division algebra, the set of such $\theta \in A$ is Zariski dense in $A$. The overall goal of this research is to investigate the internal structure of $A$ in terms of $K \subset A$ and an element $a \in A \setminus K$.

Notice that assuming $A$ is a division algebra is much too strong for the density statement. It is clear, for example, that such a field $K$ exists if $F$ has the property that every finite extensions $F^r$ of $F$ has a separable field extension of any degree. However, we will avoid these technicalities by simply assuming, in the whole paper, that $K$ is a maximal separable subfield of $A$.

We start by reviewing the well-known fact that there are $v \in A$ such that $A = KvK$ and in fact $A = \sum_{i,j=0}^{n-1} F^2 F v^{n-1-i}$ for suitable $v \in K$, and conversely, starting with any $v$, the set of $\theta$ for which $A = KvK$ is Zariski dense in $A$. Likewise, starting with $K$, the set of $v$ for which $A = KvK$ is Zariski dense in $A$. However, the situation can differ for $KaK$ for arbitrary $a \in A$, which is the subject of our paper.

We are interested in those $a \notin K$ for which $KaK \neq A$, since they may permit us to obtain more information about $A$. In this case we are also interested in examining $(KaK)^m$ for each $m \geq 1$. Another focus of this paper is spaces of Kummer elements. We say $a \in K$ is Kummer if and only if the characteristic polynomial of $a$ has the form $x^n - d$. We say a subspace $V \subset A$ is Kummer if and only if all $a \in V$ are Kummer.

One extreme case, since $KaK$ must contain $aK$, is that $KaK = aK$. Then $Ka = aK$. Since $K$ is a field, by Lemma 23, we can conclude that $a$ is invertible and $aKa^{-1} = K$. Some equivalent conditions in terms of traces are given in Theorem 45, which shows that if $Ka$ is Kummer ($v^n \in F$ for all $v \in Ka$), then $KaK$ is also...
Kummer. (We utilize characteristic free techniques, developed in Section 7 which are of independent interest).

We show that the sequence $\dim_K (KaK)^j : j = 1, 2, \ldots$ must stabilize at some $m \leq n$. Moreover, the sequence $(KaK)^j$ terminates in a finite cycle and we can characterize the resulting subspaces.

This is tied in with the behavior of the products $K(aKa^{-1})(a^2 Ka^{-2}) \cdots$ of fields conjugate to $K$, since

$$KaKa^{-1}(a^2 Ka^{-2}) = KaKaKa^{-2} = (KaK)(KaK)a^{-2}$$

(and also for longer products).

Our first main idea is that this question can be studied ring-theoretically. $A$ is a $K - K$ bimodule (i.e. a $K \otimes_F K$ module) and $(KaK)^m$ is a submodule, where the first $K$ acts by multiplication on the left and the second as multiplication on the right. Since we show $A = KrK$ for some $r$ we have that $A \cong K \otimes_F K$ as $K - K$ bimodules.

This sets the tone of our paper, in which we explore first what one can obtain using the bimodule structure, before studying how they interact in the multiplication of $A$.

Writing $f$ for the minimal polynomial of $\theta$ over $F$, we can factor $f$ over $K$ and have

$$f(x) = (x - \theta)f_1(x) \cdots f_s(x).$$

Thus, $K \otimes_F K$ is a semisimple ring, a direct sum of fields $K_0 \oplus K_1 \oplus \cdots \oplus K_s$ where $K_0 = K$ and $K_i = K[x]/K[x]f_i(x)$ for $1 \leq i \leq s$. As a bimodule $A$ is semisimple, i.e., is a finite direct sum of simple submodules. This gives us precisely the description of all sub-bimodules of $A$ (Remark 9). Of course, the $(KaK)^m$ for each $m$ are such sub-bimodules.

Furthermore, we can describe these $K_i$ in terms of the Galois group $G$ of the Galois closure $L/F$, generated over $F$ by the roots of $f(x)$. $G$ acts on these roots, enabling us to translate the theory to double cosets of $G$. Let $H \subset G$ be the Galois group of $L/K$. We call a subset $S \subseteq G$ an $H$-biset, if it is closed under multiplication by $H$ from left and right. Then (Corollary 4) there is a 1:1 correspondence between sub-bimodules of $K \otimes_F K$ and $H$-biset $S \subseteq G$, which is extended to an isomorphism of semirings in Theorem 19. This valuable tool enables us to relate the algebraic structure of $A$ to the growth of the series $\dim_K (KaK)^j$.

To relate these sub-bimodules to the multiplication in $A$, we embed $A$ into $\bar{A} = A \otimes_F L \cong M_n(L)$. Then $M_n(L)$ has an etale maximal subring $\bar{K} = K \otimes_F L$. After tensoring by $L$, sub-bimodules of $A$ become $K - \bar{K}$ sub-bimodules of $M_n(L)$. These later sub-bimodules are described in terms of matrix units and this is a powerful tool.

Another approach to studying $A$ in terms of $KaK$ is by means of Brauer factor sets, cf. [Jac3], and the corresponding description of $A$ as matrices of $M_n(K)$. Now $G$ acts naturally on the indices of the entries of the matrices, and $K$ corresponds to diagonal matrices. When $KaK \neq A$ this matrix description involves entries which are 0.

2. Writing $A = KaK$.

The fact that we can write $A = KaK$ is known, cf. [AI], [Jac1 Theorem VII.3], [Jac2], and [G]. Let us provide the quick argument.
We recall from [R1] Theorem 1.4.34 that over any field \( F \), the Capelli polynomial
\[ c_{n^2}(x_1, \ldots, x_{n^2}, y_1, \ldots, y_{n^2}) \]
has the property of vanishing whenever \( x_1, \ldots, x_{n^2} \) are specialized to sets of matrices that do not span \( M_n(F) \), but does not vanish when \( x_1, \ldots, x_{n^2} \) and \( y_1, \ldots, y_{n^2} \) each are specialized to sets of matrices that do span \( M_n(F) \). Define \( \tilde{x}_{ni+j+1} = y^i x^j y \) for \( 0 \leq i, j \leq n-1 \), and
\[ \tilde{c}(x, y) = c_{n^2}(\tilde{x}_1, \ldots, \tilde{x}_{n^2}, \tilde{x}_1, \ldots, \tilde{x}_{n^2}). \]

**Lemma 1.** \( A \) is spanned by \( S = \{ \theta^i a \theta^j : 0 \leq i, j \leq n - 1 \} \) iff \( \tilde{c}(a, \theta) \neq 0 \).

**Proof.** An immediate consequence of the previous paragraph. \( \square \)

**Remark 2.** Lemma 1 transfers the condition of generation over the center to a criterion about polynomial identities (or generalized identities), which for algebras over infinite fields is known to pass to tensor extensions (cf. [R1, Corollary 2.3.32]), and being a non-identity, is a Zariski open condition on \( A \). Of course, when we fix \( \theta \) and being a non-identity, is a Zariski open condition on \( A \). Hence, the matrix algebra \( A \) is Zariski dense in \( K \). For any such \( a \),
\[ \dim_F(KaK) = \dim_K((K \otimes K)(1 \otimes a)(K \otimes K)) = n^2, \]
implies \( K a K = A \), as desired.

If \( F \) is finite, then \( A \) already is a matrix algebra, and \( K/F \) is necessarily cyclic. Hence, the matrix algebra \( M_n(K) \) can be presented as a cyclic algebra \( \sum K z^i \) where \( z K z^{-1} = K \). Considering \( A \) as a subalgebra of \( M_n(K) \), and conjugating so that \( K \) is the diagonal, every element of the form \( \sum \alpha_i z^i \) with nonzero coefficients has non-zero entries as a matrix. \( \square \)

3. Bimodule decomposition of \( KaK \)

We fix a central simple algebra \( A \) and a separable maximal subfield \( K \).

### 3.1. A as a bimodule.

The algebra \( A \) has the structure of a \( K - K \) bimodule, where the first \( K \) acts by multiplication on the left and the second as multiplication on the right. Of course this is the same as saying that \( A \) is a module over \( K \otimes_F K \). Moreover, since by Proposition 3 there is \( a \in A \) such that \( A = KaK \), we conclude:
Lemma 4. $A \cong K \otimes_F K$ as $K$–$K$ bimodules.

Note that since $K/F$ is separable, $K \otimes_F K$ is a commutative semisimple algebra with all irreducibles appearing with multiplicity one, and thus can be written uniquely as a direct sum of simple modules. This implies that:

Lemma 5. Any two sub-$K$–$K$-bimodules of $A$ that are isomorphic as bimodules are equal as subsets.

In other words, the isomorphism type determines the submodule as a subset. Also note that since $K \otimes_F K$ is semisimple, all submodules are cyclic. From this we get:

Lemma 6. The possible $KvK \subseteq A$, ranging over $v \in A$, are exactly the $K$–$K$ submodules of $A$.

Following Lemma 4 we study the bimodule decomposition of $K \otimes_F K$. Since $K/F$ is separable,
\[
K \cong F[x]/F[x]f(x)
\]
for an irreducible polynomial $f(x)$ over $F$. The image of $x$ defines a canonical root $\theta \in K$ of $f(x)$, and we have an irreducible decomposition over $K$, \( f(x) = (x - \theta)f_1(x) \cdots f_s(x) \).

Extending scalars in (1), we have $K \otimes_F K \cong K[x]/K[x]f(x)$, where $\theta \otimes 1 \mapsto \theta$ and $1 \otimes \theta \mapsto x$. Thus:

Lemma 7. $K \otimes_F K$ is a direct sum of fields $K_0 \oplus K_1 \oplus \cdots \oplus K_s$ where $K_0 = K$ and $K_i = K[x]/K[x]f_i(x)$ for $1 \leq i \leq s$. Each $K_i$ is an irreducible $K$–$K$ bimodule.

In other words, the $K_i$ are precisely the irreducible $K$–$K$ sub-bimodules of $A$. Passing to $A$, there are $v_0, \ldots, v_s$ such that $A = \bigoplus Kv_iK$, and for each $i$, $Kv_iK \cong K_i$ as $K$-$K$-bimodules.

3.2. Galois structure of $K/F$.

We can think about the $K_i$ of Lemma 7 in terms of the Galois group of $K$. Explicitly, let $L/F$ be the Galois closure of $K/F$, so $L$ is generated over $F$ by the roots of $f(x)$. Let $\theta_i$ be a root of $f_i$, so $K_i = K(\theta_i)$. Then the projection $K \otimes_F K \twoheadrightarrow K_i$ can be defined by $\theta \otimes 1 \mapsto \theta$ and $1 \otimes \theta \mapsto \theta_i$.

Let $G$ be the Galois group of $L/F$ and $H \subset G$ the Galois group of $L/K$. That is, viewing $G$ as a permutation group on the roots of $f(x)$, $H$ is the stabilizer of $\theta$. Another way of saying this is that the set of right cosets $G/H = \{gH \mid g \in G\}$ corresponds to the embeddings $K \hookrightarrow L$, where $gH$ corresponds to the embedding defined by $\theta \mapsto g(\theta)$. It then follows that the roots of each $f_i(x)$ (including $f_0(x) = x - \theta$) are orbits of $H$ with respect to the action of $H \subseteq G$ on the roots of $f(x)$.

It is useful to get away from relying on a specific choice of polynomial, which now is easy. Let $\Theta$ denote the set of roots of $f(x)$ in $L$, which is isomorphic as a $G$-set to $G/H$ (via $g \mapsto g(\theta)$) and thus to the set of embeddings $K \hookrightarrow L$ (where $G$ acts via left composition).

The orbits of $H$ on $\Theta$ are the roots of each $f_i$; the orbits of $H$ on the embeddings are the embeddings of $K$ into $K_i$; and clearly, the orbits of $H$ on $G/H$ are the double cosets $HgH$, $g \in G$. This gives a correspondence between double cosets $HgH$ and the $K_i$, given by $\theta_i = g(\theta)$, and hence on the simple direct summands of $K \otimes K$. Note that this is really independent of the choice of $f$. Indeed, $K_i$ is isomorphic to the subfield of $L$ generated by $K$ and $g(K)$. Therefore, the subfield
\(K(\theta)\) corresponds to the double coset \(HgH\), and we denote this field, up to \(K\)-isomorphism, as \(K[g]\), as writing the double coset in a subscript seems unwise.

We have shown:

**Lemma 8.** The simple direct summands of \(K \otimes_F K\) are in one to one correspondence with the double cosets \(HgH\) of \(H\) in \(G\), given by \(HgH \mapsto K[g]\).

For future use, we generalize this correspondence to all the sub-bimodules. We call a subset \(S \subseteq G\) an \(H\)-biset, if it is closed under multiplication by \(H\) from left and right. In other words, an \(H\)-biset is the union of double cosets of \(H\).

**Corollary 9.** There is a one to one correspondence between sub-bimodules of \(K \otimes_F K\) and \(H\)-bises \(S \subseteq G\), given by \(S \mapsto \sum_{HgH \subseteq S} K[g]\).

Lemma 8 implies, for example, the following observation (for \(s = 2\)):

**Remark 10.** \(K \otimes_F K = K \oplus K_1\), the sum of two fields, if and only if \(G\) acts doubly transitively on the roots of \(f(x)\).

So, for example, if \(K/F\) has degree \(n\) and \(G = S_n\) then \(K \otimes_F K = K \oplus K_1\).

Counting degrees in Lemma 8 we have:

**Corollary 11.** The dimension of \(K[g] \subset K \otimes_F K\) over \(K\) is the quotient \(|HgH|/|H|\). More generally the dimension of the bimodule corresponding to any \(H\)-biset \(S\) is \(|S|/|H|\).

**Proof.** The length of the orbits of \(H\) on \(G/H\) is exactly the number of roots of the minimal polynomial \(f_i\) of \(g(\theta)\) over \(K\). \(\square\)

The object \(K[g]\) is being viewed here in a number of ways, and we need to describe them and keep them distinct. Of course we began by viewing \(K[g]\) as a submodule of \(K \otimes K\). Up to isomorphism, there is a unique \(K \otimes K\)-module corresponding to \(HgH\). However, being a simple \(K \otimes K\)-module \(K[g]\) is \((K \otimes K)/M\) for a maximal ideal \(M\), and then \(K[g]\) is a field, which by our description is isomorphic to \(Kg(K)\) \(\subset L\). Equivalently, \(K[g] \cong \Gamma H(g)\) where \(H(g) = H \cap gHg^{-1}\). Note that the field structure of \(K[g]\) does not determine \(HgH\). For example, if \(K/F\) is Galois (so \(H = \langle 1 \rangle\)) then all the \(K[g]\)'s are isomorphic to \(K\). More generally, for any \(f \in G\), \(f(Kg(K)) \subset L\) is also isomorphic to \(K[g]\) and not equal to \(Kg(K)\) unless \(f\) is in the normalizer of \(H(g)\). In other words, knowing \(K[g]\) as a field DOES NOT uniquely define the bimodule structure. To make \(K[g]\) a bimodule we need to define \((k \otimes k') \cdot a\) which amounts to defining two embeddings \(K \rightarrow K[g]\) (actions of \(K \otimes 1\) and \(1 \otimes K\)) and if we, for the moment, identify \(K[g]\) with \(Kg(K) \subset L\) then these two embeddings are the identity and \(g\). It is natural, whenever we view \(K[g]\) as a subfield of \(L\), to choose the first embedding always to be the identity. That is, we only consider subfields \(f(Kg(K)) \subset L\) where \(f = h \in H\). When one changes \(Kg(K)\) to \(h(Kg(K))\), this is equivalent to changing from \(g\) to \(hg\) in \(HgH\), and in the original description of \(K[g] = K_i = K[x]/(f_i)\), choosing a different root in \(L\) of \(f_i\). Note that \(h(Kg(K)) \neq Kg(K)\) in general. That is, adding the extra structure of fixing \(K \subset K[g]\) still does not uniquely define \(K[g]\) as a subfield of \(L\).

There are many bimodule surjections \(K \otimes K \rightarrow K[g]\), namely, one for every generator of \(K[g]\), though they all have the same kernel. However, there is a unique such surjection which is a ring homomorphism, namely, the one sending \(1\) to \(1\). We call this map \(\pi[g] : K \otimes K \rightarrow K[g]\). This map is hard to work with because we do
not have a fixed instantiation for $K_{[g]}$. Once we fix an embedding $K_{[g]} \subset L$ (which is the identity on $K$) we have the composition $K \otimes K \to L$, defined by $\theta \otimes 1 \mapsto \theta$ and $1 \otimes \theta \mapsto g(\theta)$, which depends on the choice of $gH \subset HgH$ (because the embedding $K_{[g]} \to L$ depends on $gH$) and so we write this composition as $\pi_{gH}$. When we need to make it clear, we set $K_{gH} = K\hat{g}(K)$ to be the specific intermediate subfield of $L/K$ isomorphic to $K_{[g]}$. Thus it makes sense to write $\pi_{[g]} : K \otimes K \to K_{[g]}$ but $\pi_{gH} : K \otimes K \to K_{gH}$. Since $K \otimes K$ is semisimple, $\pi_{[g]}$ splits. That is, there is a unique idempotent $e_{[g]} \in K \otimes K$ such that $K_{[g]} \cong (K \otimes K)e_{[g]}$ as a bimodule; clearly $\pi_{[g]}(e_{[g]}) = 1$ and $\pi_{[g]}$ restricts to an isomorphism on $(K \otimes K)e_{[g]}$. The description of $\pi_{gH}$ can be summarized by the diagram:

$$
\begin{array}{ccc}
K \otimes_F K & \overset{\iota \otimes g}{\longrightarrow} & L \otimes_F L \\
\downarrow {\pi_{gH}} & & \downarrow m \\
K_{gH} & \longrightarrow & L
\end{array}
$$

where $\iota : K \to L$ is the embedding, and $m : L \otimes L \to L$ is the multiplication map.

4. Multiplication in $A$

Our goal is to understand how to multiply, in $A$, the simple summands of $A$ as a $K-K$ bimodule. We approach this by extending scalars to split $K$ and $A$.

4.1. Splitting the extension $K/F$. More precisely, we form $\bar{K} = L \otimes_F K$ which is naturally a subalgebra of $\bar{A} = L \otimes_F A \cong M_n(L)$. By definition,

$$
\bar{K} = L \otimes_F K \cong L[x]/L[x]f(x) \cong \bigoplus_{gH \in G/H} L.
$$

Note that $L \otimes_F (K \otimes K) \cong (L \otimes_F K) \otimes_L (L \otimes_F K) = \bar{K} \otimes_L \bar{K}$. Thus $K-K$-sub-bimodules of $A$ become, after extending scalars to $L$, $\bar{K-\bar{K}}$-sub-bimodules of $\bar{A}$.

Rewriting (3) we have

$$
\bar{K} = \sum_{gH \in G/H} L_{gH}
$$

where the $e_{gH}$ are the respective idempotents. Since

$$\text{Ker}(\pi_{gH}) = \text{span}_L \{ g(k) \otimes 1 - 1 \otimes k \mid k \in K \},$$

the components can be characterized as

$$
L_{gH} = \left\{ \sum a_i \otimes b_i : \sum g(k)a_i \otimes b_i = \sum a_i \otimes b_i k \text{ for all } k \in K \right\};
$$

noting that $g(\theta)^{1} \otimes 1 - 1 \otimes \theta^{1}$ is divisible by $g(\theta) \otimes 1 - 1 \otimes \theta$, we arrive at the convenient description

$$
L_{gH} = \left\{ \sum a_i \otimes b_i : \sum g(\theta)a_i \otimes b_i = \sum a_i \otimes b_i \theta \right\}.
$$

Remark 12. In the spirit of Corollary 9 but simpler, there is a correspondence between $\bar{K}$ submodules of $\bar{K}$ and unions of cosets $S \subseteq G$, given by $S \mapsto \sum_{gH \subseteq S} L_{gH}$. 
Note that, since the idempotent \( e_{gH} \) is minimal, equation (5) uniquely defines \( e_{gH} \) among all idempotents. Unlike the idempotents \( e_{[g]} \in K \otimes K \), \( e_{gH} \) varies according to the representative in the double coset. In fact, as in [Jac4 Section 2.3], one easily verifies that for each \( g \),

\[
e_{gH} = \prod_{g'H : g'H \neq gH} \frac{(g(\theta) \otimes 1 - g'(\theta) \otimes 1)^{-1} \cdot \prod_{g'H \neq gH} (1 \otimes \theta - g'(\theta) \otimes 1)}{.}
\]

Letting \( G \) act on the \( L \) in \( \bar{K} = L \otimes_F K \), we immediately observe from equation (6) that

\[
e_{g'H} = (g'(\otimes 1)(e_{gH})) , \quad \forall g' \in G.
\]

It will be useful to view \( \bar{K} = L \otimes_F K \subset L \otimes_F L \). Now, \( L \otimes_F L = \oplus_{g \in G} L e_g \) for idempotents \( e_g \), and since \( gH \) are exactly the elements of \( G \) that agree with \( g \) on \( K \),

\[
e_{gH} = \sum_{h \in H} e_{gh}
\]

as an element of \( L \otimes_F L \). Clearly, \( (g'(\otimes 1)(e_g)) = e_{g'H} \). Moreover, from the equation

\[
(g(t) \otimes 1 - 1 \otimes t)e_g = 0 \quad \text{for all} \quad t \in K,
\]

it also follows that

\[
(1 \otimes g')(e_g) = e_{gg'}^{-1}.
\]

We now have three layers of idempotents: \( e_{[g]} \in K \otimes K \), \( e_{gH} \in L \otimes K \) and \( e_g \in L \otimes L \), where \( e_{[g]} = \sum_{g'H \subseteq H \otimes H} e_{gH} \) and \( e_{gH} = \sum_{g \in H} e_{gH} \).

4.2. **Example.** To get an example, suppose that \( K / F \) contains an intermediate field \( K' \). Let \( H' \) be the Galois group of \( L / K' \), a subgroup of \( G \) containing \( H \). Of course, \( H' \) is a union of double cosets of \( H \). We ask, “What is the sub-bimodule of \( K \otimes K \), i.e., of \( A \), corresponding to \( H' \)?”

The answer provided by Corollary 8 in terms of the components \( K_{[g]} \), is unsatisfactory, being non-explicit as a subset of \( K \otimes_F K \) or \( A \). Instead, we will state the right answer and proceed to prove it.

In order to utilize idempotents, we note that the isomorphism \( K \otimes K \cong A \) as \( K \otimes K \)-modules extends to an isomorphism of \( L \otimes_F K = L \otimes K(K \otimes K) \) and \( L \otimes K A \) as \( L \otimes K \)-modules. The advantage is that now we have a concrete decomposition of the module, in terms of idempotents and annihilators. Indeed, let \( T_{gH} = \ker(\pi_{gH}) \), which is given in (3). Viewing \( T_{gH} \) as an ideal of the base ring \( L \otimes K \), we have that \( L e_{gH} = \text{Ann}(T_{gH}) \) by (4). Now, let \( S \subseteq G \) be a subset closed under multiplication by \( H \) from the right; the correspondence of Remark 12 takes \( S \) to

\[
\sum_{gH \subseteq S} L e_{gH} = \text{Ann} \left( \bigcap_{gH \subseteq S} T_{gH} \right),
\]

which is isomorphic (as \( L \)-\( K \)-bimodules) to the annihilator of \( \bigcap_{gH \subseteq S} T_{gH} \) in its action on \( L \otimes K A \). By Corollary 11 the dimension of this module over \( L \) is \( |S|/|H| \).

Let us now describe the submodule of \( A \) associated to the subgroup \( H' \). Let \( T' \) be the ideal (of \( L \otimes K \)) generated by the elements \( k' \otimes 1 - 1 \otimes k' \), ranging over \( k' \in K' \). Clearly, \( T' \subseteq T_{gH} \) for any \( g \in H' \), since \( g(k') = k' \) for \( g \in H' \). Now, the annihilator of \( T' \) in its action on \( L \otimes K A \) is composed of the elements commuting with \( K' \), so is equal to \( L \otimes K C_A(K') \). The dimension is \( [C_A(K') : K] = |K : K'| = |H'|/|H| \), noting that \( K \) is a maximal subfield of \( C_A(K') \). To summarize, the annihilator
Similarly, the action of \( G/G/H \) on \( \pi \) corresponds to the pairs of idempotents of the form \( e \) denoting its \( L \) isomorphism \( K \). Since we are going to apply this \( \pi \), we will record the precise definition, via a commutative diagram built on (2), where \( m \) denotes the multiplication of \( L \) in the right-most vertical arrow and the multiplication of \( L \) in the right-most diagonal arrow. All the undecorated tensor products

\[
\sum_{gH \subseteq H} T_g H \text{ is contained in the annihilator of } T', \text{ and they have the same dimension, so they are equal.}
\]

By descent from \( L \otimes K \) to \( K \otimes K \), we have proved:

**Lemma 13.** \( H' \) corresponds to the \( K \)- \( K \) submodule of \( A \) which is the centralizer, \( C_A(K') \), of \( K' \) in \( A \).

More generally, suppose there is an intermediate field \( K''/F \) where \( K' \subset K'' \subset K \) and \( K''/K' \) is cyclic Galois with Galois group generated by \( \sigma \). Let \( N \) be the Galois group of \( K'' \) in \( L \). We have that \( H \subset N \subset H' \), and \( N \) is normal in \( H' \), and \( H'/N \) is generated by \( \sigma \). Since \( \sigma \) normalizes \( N \), \( N \sigma \) is a union of \( H \) double cosets. Arguing as above with \( T'' \) generated by \( \{ \sigma(\ell) \otimes 1 - 1 \otimes \ell : \ell \in L \} \), we have:

**Proposition 14.** \( N \sigma \) corresponds to the submodule

\[
C_A(K'', \sigma) = \{ a \in A | \sigma(\ell)a = a\ell \text{ for all } \ell \in K'' \}.
\]

In particular \( C_A(K'', \sigma) \) is non-zero, and as we will show (Lemma 23), it contains an invertible element. Thus Lemma 4 is actually a generalization of the Skolem-Noether Theorem.

### 4.3. Splitting \( K \otimes K \)

Next, we consider the tensor product \( L \otimes_F (K \otimes_F K) = \bar{K} \otimes_L \bar{K} \). Taking the tensor product of (4) with itself, we obtain a direct sum decomposition

\[
L \otimes_F (K \otimes_F K) = \sum_{g' H, g'' H \in G/H} L(e_{g' H} \otimes e_{g'' H}).
\]  

In Subsection 4.1, we observed that \( L \otimes_F K = L \otimes_K (K \otimes_F K) \) decomposes as \( \sum L e_{gH} \). The action of \( H \) on \( L \) translates to the action of \( H \) on the set of idempotents corresponding to \( G/H \), so the orbits correspond to the double cosets \( H \backslash G/H \). Similarly, the action of \( G \) on \( L \) in \( L \otimes_F (K \otimes_F K) \) translates to the natural action on the pairs \( e_{g' H} \otimes e_{g'' H} \), which correspond to \( G/H \times G/H \). We observe that the invariant space is \( K \otimes_F K \) in both cases, while the actions on idempotents demonstrate the set isomorphism \( G \backslash (G/H \times G/H) \cong H \backslash G/H \) given by

\[
G \cdot (xH, yH) \mapsto H y^{-1} x H.
\]

### 4.4. Description of \( L \otimes K_{[g]} \)

Let \( K_{[g]} \subset K \otimes_F K \) be the direct summand corresponding to the double coset \( HgH \) with idempotent \( e_{[g]} \). Thus \( e_{[g]} \) is, after tensoring over \( F \) by \( L \), the sum of idempotents of the form \( e_{g'H} \otimes e_{g''H} \) and we need to determine which ones appear. We defined a projection \( \pi_{gH} : \tilde{K} \otimes_F K \to \tilde{K}_{gH} \cong \tilde{K}_{[g]} \), and we also use \( \pi_{gH} \) to denote its \( L \)-linear extension \( L \otimes_F (K \otimes_F K) \to L \otimes_F K_{gH} \). We have an induced morphism (also called \( \pi_{gH} \)):

\[
\pi_{gH} : \tilde{K} \otimes_L \tilde{K} = L \otimes_F (K \otimes_F K) \to L \otimes_F K_{gH} \subset L \otimes_F L.
\]

Since we are going to apply this \( \pi_{gH} \) to idempotents of the form \( e_{g'H} \otimes e_{g''H} \) let us record the precise definition, via a commutative diagram built on (2), where \( m \) denotes the multiplication of \( L \) in the right-most vertical arrow and the multiplication of \( L \otimes L \) in the right-most diagonal arrow. All the undecorated tensor products
are over $F$.

\[
(\bar{K}) \otimes_L (\bar{K}) \xrightarrow{(1 \otimes 1) \otimes (1 \otimes g)} (L \otimes L) \otimes_L (L \otimes L)
\]  

(12)

\[
\pi_{gH} \quad \pi_{gH} \quad 1 \otimes \pi_m
\]

\[
L \otimes (K \otimes K) \xrightarrow{1 \otimes (1 \otimes g)} L \otimes (L \otimes L) \xrightarrow{m} L \otimes L
\]

Let $H(g) = H \cap gHg^{-1}$ which we saw was the Galois group of $L$ over $KgH$. Exactly as in (3) and (4),

\[
L \otimes K_{gH} = \bigoplus_{fH(g) \subseteq G/H(g)} L e'_{fH(g)} \simeq \sum_{fH(g) \subseteq G/H(g)} L
\]

for idempotents $e'_{fH(g)}$. (The $e'_{fH(g)}$ are components of the $e_{fH} \in L \otimes K$, in the sense that $e_{fH} = \sum fH(g) \subseteq H e'_{fH(g)}$; in analogy to (9).)

**Proposition 15.** Let $g', g'' \in G$. The image $\pi_{gH}(e_{g'\bar{H}} \otimes e_{g''\bar{H}})$ is the primitive idempotent $e'_{fH(g)1}$, if $f \in G$ restricts to $g'$ on $K$ and to $g''g^{-1}$ on $g(K)$. If there is no such $f$, then $\pi_{gH}(e_{g'\bar{H}} \otimes e_{g''\bar{H}}) = 0$.

**Proof.** We apply $\pi_{gH}$ to $e_{g'\bar{H}} \otimes e_{g''\bar{H}}$ using diagram (12), taking the route to the right and then down. The first step takes us to $e_{g'\bar{H}} \otimes (1 \otimes g)(e_{g''\bar{H}})$, where each entry is now an element of $\bar{K} \otimes \bar{K}$, where we can apply (10) to get the sum

\[
\sum_{h', h'' \in H} e_{g' h' \otimes (1 \otimes g)}(e_{g'' h''}).
\]

Applying (10), this is equal to

\[
\sum_{h', h'' \in H} e_{g' h' \otimes e_{g'' h''} g^{-1}}.
\]

Multiplication in $L \otimes L$ takes us now to

\[
\sum_{h', h'' \in H} e_{g' h'} e_{g'' h''} g^{-1} = \sum_{h', h'' \in H} \delta_{g' h', g'' h''} g^{-1} e_{g' h'},
\]

where $\delta$ is the Kronecker delta. Thus, the image is nonzero iff there are $h', h'' \in H$ such that $g' h' = g'' h'' g^{-1}$.

Assume that $f = g' h' = g'' h'' g^{-1} = g'' g^{-1} (g h'' g^{-1})$. Note that $f \in g' H$ is equivalent to $f$ restricting to $g'$ on $K$; and $f \in g'' g^{-1} (g H g^{-1})$ is equivalent to $f$ restricting to $g'' g^{-1}$ on $g(K)$.

If this happens for one pair $g' h'$ and $g'' g^{-1} g h'' g^{-1}$ the same is true for $g' h' h$ and $g'' g^{-1} g h'' g^{-1} h$ for any $h \in H \cap g H g^{-1} = H(g)$, and so when such a pair exists we have $\pi_{g}(e_{g' \bar{H}} \otimes e_{g'' \bar{H}}) = e_{fH(g)}$ as needed.

**Corollary 16.** The idempotent $e_{g'\bar{H}} \otimes e_{g''\bar{H}}$ appears in $L \otimes_F K_{gH}$ if and only if $g^{-1} g'' \in H g H$. In other words, as a subalgebra of (11),

\[
L \otimes K_{gH} = \sum_{g^{-1} g'' \in H g H} L(e_{g'\bar{H}} \otimes e_{g''\bar{H}}).
\]
Proof: We proved in the proposition that the idempotent appears in $L \otimes K_{gH}$ iff $g'H \cap g''Hg^{-1} = g'H \cap g''g^{-1}(gHg^{-1})$ is nonempty. This is equivalent to the second statement because if $gh' = g''h''g^{-1}$ then $g^{-1}g'' = h'gh''^{-1}$.

Remark 17. Note that the decomposition of $A$ into submodules isomorphic to the $K_{[g]}$'s (associated with double cosets) is a generalized grading of $A$, and has as a special case the known gradings when $H = 1$. When combined with Theorem 19 to come, the $K$-$K$ bimodule decomposition of $A$ will be seen to be a generalized grading as well.

4.5. The matrix representation of $A$.

Our next step is to understand the product of sub-bimodules of $A$, which are all of the form $KaK$ for $a \in A$, as subsets of $A$. One might think we have to specify and understand $A$. However, the fact that isomorphic $K$-$K$ sub-bimodules are equal implies we can multiply the sets inside $L \otimes A = M_n(L)$, and the Brauer class of $A$ does not matter.

As we stated above, $L \otimes A$ is the matrix algebra $M_n(L)$, but we want to be more specific. Since $L \otimes K$ is a direct sum of copies of $L$, we may assume that

$$\bar{K} = L \otimes L \subset A$$

are diagonal matrices. More specifically, the idempotents $e_{gH}$ of (4) are then diagonal idempotents. Moreover, we can choose matrix units $e_{gH,g'H}$ for $\bar{A}$, such that the embedding (13) sends $e_{gH}$ to the diagonal matrix unit $e_{gH,gH}$. In addition, we can be very free to choose $v \in \bar{A}$ such that $(\bar{K})v(\bar{K}) = \bar{A}$, subject only to the condition that all the matrix entries of $v$ are nonzero. Furthermore, taking $v$ to be the all-1 matrix, the bimodule isomorphism $(\bar{K}) \otimes (\bar{K}) \rightarrow \bar{A}$ defined by $x \otimes y \mapsto xvy$, maps $e_{gH} \otimes e_{g'H}$ to $e_{gH,g'H}$.

Recall that our starting point is the isomorphism of $K$-$K$-bimodules $K \otimes K \rightarrow A$, as in the bottom row of Figure 1 (see below). However, since we adjust the isomorphism on the upper row to send $e_{gH} \otimes e_{g'H}$ to $e_{gH,g'H}$, the diagram does not commute when the side arrows are the natural embeddings (since the all-1 matrix is not an element of $A$). Our strategy still works, because a submodule of $K \otimes K$ has the same image in $\bar{K} \otimes A$ under both routes of the diagram, since the images are isomorphic as bimodules.

Following Corollary 11, we thus have a one to one correspondence between $H$-bisets $S \subseteq G$ and $K$-$K$-sub-bimodules of $A$, given by

$$\Phi : S \mapsto \sum_{HgH \subseteq S} \varphi_v(K_{[g]}),$$

where $\varphi_v(x \otimes y) = xvy$ and $v \in A$ is any element for which $KvK = A$.

\begin{figure}[h]
\centering
\begin{tikzpicture}
    \node (A) at (0,0) {$A$};
    \node (B) at (0,2) {$\bar{K} \otimes A$};
    \node (C) at (-1,1) {$\bar{K} \otimes (K \otimes K)$};
    \node (D) at (-1,2) {$\bar{K} \otimes K$};

    \draw[->] (C) -- (D);
    \draw[->] (C) -- (B);
    \draw[->] (D) -- (A);
    \draw[->] (B) -- (A);
\end{tikzpicture}
\caption{The diagram does not commute on elements when the upper arrow sends $e_{gH} \otimes e_{g'H} \mapsto e_{gH,g'H}$, but does commute on sub-bimodules}
\end{figure}
From Corollary\[16\] we have:

**Proposition 18.** With $\bar{A}$ and $e_{gH,g'H}$ as above, if $KaK \subset A$ is the simple bimodule associated to the double coset $HgH$, then $L \otimes_F (KaK) \subset \bar{A}$ is spanned by all $e_{gH,g'H}$ such that $g^{-1}g' \in HgH$.

From this we get our main theorem on products of bimodules. Notice that the set of $H$-biset in $G$ is a semiring with respect to the operations of union and multiplication (with the empty set as a zero element and $H$ as a multiplicative unit).

Similarly, the sum of bimodules and the product of bimodules in $A$ are bimodules, and moreover the product is distributive with respect to the sum. The induces a semi-ring structure on the $K$-$K$ sub-bimodules of $A$ (where the zero module is a zero element and $K$ is a multiplicative unit).

**Theorem 19.** Let $A/F$ be a central simple algebra with maximal separable sub-field $K$. The map $\Phi$ of \[14\] is an isomorphism of semirings, from the semiring of $H$-bisets in $G$ to the semiring of $K$-$K$ sub-bimodules of $A$.

**Proof.** Suppose that $KaK$, $Ka'$ are $K$-$K$ sub-bimodules associated to the $H$-biset $S, S' \subseteq G$, respectively. Because isomorphism and equality of sub-bimodules are equivalent, it suffices to prove this result after extension of scalars to $\bar{A} = \bar{K} \otimes FA$. Then $(\bar{K} \otimes_F (KaK))((\bar{K} \otimes_F (Ka'K)))$ is spanned by all products $e_{g_1H,g_2H}e_{g_2H,g_3H} = e_{g_1H,g_3H}$ where $g_1^{-1}g_2 \in S$ and $g_2^{-1}g_3 \in S'$. But $(g_1^{-1}g_2)(g_2^{-1}g_3) = g_1^{-1}g_3$ is the general element of $SS'$.

In fact our semirings are idempotent semirings ($x + x = x$ for every $x$), and they come with some extra structure. The additive atoms are double cosets on one hand, and irreducible sub-bimodule on the other hand. There is also an involution, defined by inversion on bisets, and by $\varphi_v(K_{g'}) \mapsto \varphi_v(K_{g^{-1}})$ on irreducible sub-bimodules.

**Corollary 20.** Let $S$ be an $H$-biset in $G$. Then $\Phi(S)$ is a subalgebra if and only if $S$ is a subgroup.

It will be useful to observe a property of $KaK$ relating to the trace.

**Lemma 21.** Let $KaK \subseteq A$ be a sub-bimodule corresponding to a biset $S$. If $K \not\subseteq KaK$ then $tr(KaK) = 0$.

**Proof.** Let $S$ be the biset corresponding to $KaK$. After passing to $\bar{K} \otimes_F A$, we note by Proposition\[18\] that matrix units from the principal diagonal are in $L \otimes_F KaK$ iff $H \subseteq S$, iff $K = \Phi(H) \subseteq \Phi(S) = KaK$.

5. **Powers of indecomposable modules**

In this section, we consider the series $(KaK)^m$ as $m$ increases. By Theorem\[19\] we have:

**Corollary 22.** Let $KaK$ be the sub-bimodule associated to the $H$-biset $S \subseteq G$. Then $(KaK)^m$ is the bimodule associated to $S^m = \{s_1 \ldots s_m : s_1, \ldots, s_m \in S\}$.

Before going any further, let us settle a technical point.

**Lemma 23.** Suppose that $F$ is a field of order $> 2$, and $A$, $K$ are as usual. If $KaK$ is a sub-bimodule, we can choose $a$ to be invertible.
Proof. We begin with the case $F$ infinite. Associated to $K\alpha K$ is a set of idempotents $e_{gH,g'H} \in \bar{K}$. Form the generic element $T = \sum x_{gH,g'H}e_{gH,g'H}$ where the coefficients are indeterminates. Viewing $T$ as a matrix, let $t$ be the determinant. Then $t$ is a polynomial in the $x_{gH,g'H}$ whose coefficients are $\pm 1$. Since the $F$ points of $K\alpha K$ are Zariski dense, it suffices to show that $t$ is nonzero. However, there is a field extension $F' > F$, and a division algebra $D'$ over $F'$ such that $K' = K \otimes_F F'$ is a maximal subfield of $D'$ and $\bar{K} = \bar{K} \otimes_F F'$ is a field, with $G, H$ the corresponding Galois groups of $K'$. Now $D'$ has a $K'-K'$ sub-bimodule corresponding to the same set of double cosets, which has the form $K'dK'$ where $d'$ is obviously invertible. But this shows that $t$ is nonzero.

Next suppose $F$ has finite order $q > 2$. Then $K/F$ must be cyclic Galois and $A$ is the cyclic algebra $(K/F, \sigma, 1)$ where $\sigma : K \to K$ is defined by $\sigma(k) = k^q$. Write $A = \sum_{i=0}^{n} K u^i$ where $uk = k^q u$ and $u^n = 1$. Viewing $A = \text{End}_F(K)$, then $k \in K$ acts by left multiplication and $u(x) = x^q$. Then any bimodule is of the form $\sum_{i \in I} K u^i$ where $I \subset \{1, \ldots, n-1\}$. It suffices to show that for any such $I$ there are nonzero $k_i$ such that $\sum_{i \in I} k_i u^i$ is nonsingular.

We proceed by induction on the order of $I$. Multiplying by a power of $u$, we can always assume that $0 \in I$. If $|I| = 1$, then 1 is nonsingular. The induction step is covered by the following lemma.

Lemma 24. Assume that $|F| > 2$. Suppose that $B : K \to K$ is $F$-linear and nonsingular. Then there is an element $k \in K^*$ such that $k + B$ is nonsingular.

Proof. If $F$ is infinite one can take $k \in F$ since there are finitely many eigenvalues. Assume that $F$ is finite. If $(k + B)x = 0$ for nonzero $x \in K$ then $k = -B(x)/x$. It suffices to show that $x \mapsto B(x)/x$ as a function $K^* \to K^*$ is not surjective. But if $a \in F^*$ then $B(ax)/(ax) = B(x)/x$ so when $|F| > 2$, this map is not injective. □

Remark 25. Note that the above result is false if $F$ has order 2. In the notation of the above proof, $u(x) = x^2$. Thus $k+u$ is always singular because $kx+x^2 = (k+x)x$ and for any $k$, $x = -k$ is a kernel element.

From now on, for simplicity, we assume that $K\alpha K$ is a simple sub-bimodule associated via $\Phi$ to the single double coset $S = HgH$. We also assume throughout that $a$ is invertible. Define

$$K(a, m) = (K\alpha K)^m a^{-m} = K(1 - aK^{-1})(a^2 K^{-2}) \cdots (a^m K^{-m}).$$

Lemma 26. If $K(a, m) = K(a, m+1)$ then $K(a, m) = K(a, m+s)$ for all $s \geq 0$. Moreover,

$$K = K(a, 0) \subseteq K(a, 1) \subseteq K(a, 2) \subseteq \cdots$$

stabilizes at some $m \leq n$. Thus, $\dim_K(K\alpha K)^m$ stabilizes at the same $m$.

Similarly

$$H(g, m) = (HgH)^m g^{-m} = H(gH^{-1})g^{-2} \cdots (g^m H^{-m}),$$

is an ascending chain of subsets

$$H = H(g, 0) \subseteq H(g, 1) \subseteq H(g, 2) \subseteq \cdots,$$

so $|(HgH)^m|$ stabilizes.
Proof. To prove the first statement, assume that \( K(a, m) = K(a, m + 1) \). It suffices to show that \( K(a, m + 1) = K(a, m + 2) \). But \((KaK)^m a^{-m} = (KaK)^{m+1} a^{-(m+1)}\) implies \((KaK)^m a = (KaK)^{m+1}\) and so
\[
(KaK)^{m+1} a^{-(m+1)} = (KaK)(KaK)^m a(a^{-(m+2)})
\]
\[
= (KaK)(KaK)^{m+1} a^{-(m+2)} = K(a, m + 2).
\]

As for the second statement, since \( \dim_K A = n \) this ascending series must repeat for \( m \leq n \) and the result follows. \( \square \)

Definition 27. The height of \( a \) is the minimal \( m_0 \) such that
\[
K(a, m_0) = K(a, m_0 + 1);
\]
we denote \( h(a) = m_0 \).

Notice that the height \( m_0 \) only depends on the bimodule \( KaK \) and we are really talking about the height of \( KaK \). Similarly, we can talk about the height of \( g \) or \( HgH \). Of course, if \( KaK \) is associated to \( HgH \) then they have the same height.

The obvious question concerns the possible asymptote for the sequence
\[
H(g, m) = (HgH)^m g^{-m} = H(gH g^{-1})(g^2 H g^{-2}) \cdots (g^m H g^{-m}).
\]
When this sequence stabilizes, it has the following properties:

Lemma 28. Let \( m_0 \) be the height of \( a \). Let \( N = H(g, m_0) \) and let \( G' \) be the subgroup of \( G \) generated by \( H \) and \( g \).

Then \( N \) is a normal subgroup of \( G' \), \( G'/N \) is generated by the image of \( g \), and \( N \) is the smallest subgroup of \( G' \) containing \( H \) and normal in \( G' \).

Proof. Let \( m_1 \geq m_0 \) be such that \( g^{m_1} = 1 \). Then
\[
N = H(g, m_1) = (HgH)^{m_1} g^{-m_1} = (HgH)^{m_1},
\]
so
\[
N^2 = (HgH)^{2m_1} = (HgH)^{2m_1} g^{-2m_1} = H(g, 2m_1) = N,
\]
proving that \( N \) is a subgroup. As such, it is obviously the subgroup generated by all the conjugates \( g^i H g^{-i} \) and the rest is clear. \( \square \)

Let \( N \) and \( G' \) be as in the above lemma. Recall that \( L \) is the Galois closure of \( K/F \), \( G = \text{Gal}(L/F) \) and \( H = \text{Gal}(L/K) \). The groups
\[
G \supseteq G' \supseteq N \supseteq H \supseteq 1
\]
define fields
\[
F \subseteq K' \subseteq E \subseteq K \subseteq L,
\]
where \( G' \) is the Galois group of \( L/K' \) and \( N \) is the Galois group of \( L/E \). Clearly \( E/K' \) is a cyclic Galois extension. In fact \( E = \bigcap_i g^i(K) \) by the Galois correspondence, so \( E \) is the maximal subfield of \( K \) that is stable under \( g \).

Lemma 29. \((KaK)^m \) is stable under conjugation by \( a \) if and only if \( m \geq m_0 \).

Proof. Indeed, \( K(a, m + 1) = K(a, m) \) iff \((KaK)^{m+1} a^{-1} = (KaK)^m \) by multiplication by \( a^m \) from the right, but the left-hand side is \( Ka(KaK)^m a^{-1} \), so we have an equality iff \( a(KaK)^m a^{-1} \subseteq (KaK)^m \). \( \square \)

But \((KaK)^{m_0} \) need not be a subalgebra. Accordingly, we must go a bit further. Let \( m_1 \geq m_0 \) be such that \( g^{m_1} = 1 \).
Lemma 30. \((KaK)^{m_1}\) is a subalgebra of \(A\).

Proof. As in Lemma 25 let \(N = (HgH)^{m_1}\) which is a subgroup of \(G\). By Corollary 20 \(\Phi(N) = (KaK)^{m_1}\) is a subalgebra. \(\Box\)

Let \(m \geq \text{ht}(a)\). Then \((HgH)^m = N g^m\). By Lemma 14 we obtain:

Proposition 31. Let \(KaK \subset A\) be a simple sub-bimodule corresponding to \(HgH\). Then for \(m \geq \text{ht}(a)\), \((KaK)^m = \{x \in A \mid x \ell = g^m(\ell)x\ \text{for all} \ \ell \in L\}\).

Notice that the double coset \(HgH\) determines \(G' = \langle H, HgH \rangle\) and therefore determines \(N\) (as the minimal normal subgroup of \(G'\) containing \(H\)) and \(L = K^N\). The proposition shows that \(HgH\) provides explicit information on \(a\):

Corollary 32. Let \(m_1\) and \(g \in G\) be as in Lemma 30. Let \(a \in A\) be any element such that \(KaK\) is the simple bimodule corresponding to \(HgH\). Then

(1) Let \(C = (KaK)^{m_1}\). Then \(C = C_A(L)\).
(2) \(a\ell = g(\ell)a\) for every \(\ell \in L\).

Proof. By Proposition 31 \((KaK)^{m_1} = C_A(L)\). Taking \(m_1 + 1\) gives

\[ a \in C_A(L)a \subseteq C_A(L)KaK = (KaK)^{m_1+1} = \{x \in A \mid x \ell = g(\ell)x\ \text{for all} \ \ell \in L\}\]. \(\Box\)

Corollary 33. \(K' = \text{Cent}(A')\), where \(A'\) is the subalgebra of \(A\) generated by \(K\) and \(a\).

Proof. Since \(C \subseteq A'\), the centralizer of \(A'\) is contained in \(C_A(C) = L\), so \(C_A(A')\) is the subfield of \(L\) fixed by conjugation by \(a\):

\[ C_A(A') = L^{(g)} = \tilde{K}^{(H,g)} = \tilde{K}^{G'} \]. \(\Box\)

In the special case where \(g\) normalizes \(H\), we have that \(N = H\) so \(L = K\), and in particular \(g\) is an automorphism of \(K\). In this case, the condition \(a\ell = g(\ell)a\) (for all \(\ell \in K\)) implies that the coset \(Ka = KaK\) is well defined by \(g\).

Note that the property that \(E/K'\) was cyclic arose from the assumption that \(KaK\) was simple. One could obviously formulate a more general result for more general \(KaK\).

6. Examples for \(A\) cyclic

We consider situations when the algebra \(A\) is cyclic, although the subfield \(K\) need not be cyclic.

6.1. \(K\) cyclic.

Assume that \(F\) contains a primitive \(n\)-th root \(\omega\) of 1. Throughout, \((K, \sigma, \beta)\) denotes the cyclic algebra with maximal subfield \(K\) cyclic over \(F\) with Galois group \(\langle \sigma \rangle\) and element \(y\) such that \(y^n = \beta\) and \(\gamma y \gamma^{-1} = \sigma(\gamma)\) for all \(\gamma \in K\). In particular, when \(K = F[x]\) with \(x^n = \alpha\), we write \((K, \sigma, \beta)\) as the symbol algebra \((\alpha, \beta)\).

Proposition 34. Suppose that \(A = (K/F, \sigma, b)\) is a cyclic algebra, \(yk = \sigma(k)y\) for all \(k \in K\), and \(a \in A\). Then any subalgebra of the form \(KaK\) must have the form \(K[y^d]\) for some \(d \mid n\).
Proof. Here $H$ is trivial so sets of double cosets are just sets of elements. We identify $S$ with this subset of $\mathbb{Z}/n\mathbb{Z}$ (the Galois group). However, by Theorem 19 $S$ is closed under addition. \hfill \Box

6.2. $K$ cyclic after adjoining roots of unity.

Let $E/F$ be a Galois extension of dimension 4, with $\text{Gal}(E/F) = \{1, \eta, \eta^2, \eta^3\}$. A cyclic algebra of degree 4 over $F$ which is split by $E$ has the form $A = E[\theta]$ where conjugation by $\theta$ induces $\eta$, and $\theta^4 \in F^\times$. For a maximal subfield which is not Galois over $F$, we take $K = F[\theta]$, and assume that $i = \sqrt{-1} \not\in F$. Our goal is to decompose $A$ as a $K$-$K$ bimodule. The Galois closure of $K$ is $L = K[i]$, with $G = \text{Gal}(L/F) = \langle \sigma, \tau \rangle$, where $\sigma : \theta \to i\theta$, $i \mapsto i$; $\tau : \theta \to \theta$, $i \mapsto -i$. We calculate that $\tau \sigma = \sigma^{-1} \tau$ so $G$ is dihedral. The Galois group of $L$ over $K$ is $H = \langle \tau \rangle$. Also, $E' = E[i]$ is cyclic over $F' = F[i]$, so there is a Kummer generator $u \in E'$ for which $\theta u \theta^{-1} = iu$. In particular $\theta u^2 \theta^{-1} = -u^2$ and $u^2 \in E'[u]$. As before, we extend scalars to obtain explicit idempotents. Extending the bimodule isomorphism $K \otimes_F K \cong A$, we have $L \otimes_K (K \otimes K) \cong L \otimes_K A$. In general this would not have a relevant structure as an algebra. However, taking $F' = F[i]$, we have that $L = F' \otimes_F K$, and therefore $L \otimes_K A = (F' \otimes_F K) \otimes_K A = F' \otimes_F A$, which conveniently is an algebra. The component of $L \otimes_K A$ corresponding to the coset $gH \in G/H$ is defined in (7), which can be rewritten as $\{ \alpha : g(\theta) \alpha = \alpha \theta \}$. There are four cosets. Over $F'$, the component corresponding to the coset $\sigma^j H$ is $\{ \alpha \in F'A : \sigma^j \theta \alpha = \alpha \theta \} = \bar{K} u^{-j}$. In $A$ itself, the components corresponding to $H$ and $\sigma^2 H$, which are in fact double cosets, are $K$ and $Ku^2$ respectively. Note that together $H' = H \cup \sigma^2 H$ is a subgroup of $G$ containing $H$, which stabilizes the subfield $K' = E^2$. As shown in the example above, $H'$ corresponds to the sum of the components $K + Ku^2 = K[u^2] = C_A(K')$. The final component corresponds to the double coset $H \sigma H$; over $F'$, this component decomposes as $F'Ku + F'Ku^3$; but $u \not\in A$, so over $F$ we only have the single component $Ku + Ku^2$. To summarize, the bimodule decomposition of $A$ over $F$ is $A = K \oplus Ku^2 \oplus (Ku + Ku^3)$.

7. Characteristic coefficients and trace of powers

Let $F$ be a field of arbitrary characteristic, and $A$ an $F$-algebra which is contained in $n \times n$ matrices over some extension of $F$. Define $\rho_i : A \to F$ to be the polynomial functions such that $(-1)^i \rho_i(a)$ is the coefficient of $t^{n-i}$ in the Cayley Hamilton polynomial $p_n(t)$ of $a$.

The well known Newton’s identities are, for $k = 1, \ldots, n$, 

$$k \rho_k(a) = \sum_{i=1}^{k} (-1)^{i-1} \rho_{k-i}(a) \text{tr}(a^i).$$

Fix an $F$-vector subspace $V \subseteq A$.

Proposition 35. Fix some $r \leq n$. Consider the conditions

1. $\rho_k(a) = 0$ for $1 \leq k \leq r$ and every $a \in V$;
2. $\text{tr}(a^k) = 0$ for $1 \leq k \leq r$ and every $a \in V$.

Then (1) $\implies$ (2) (and in characteristic zero, (1)$\iff$ (2)).

Proof. Since $\rho_0(a) = 1$, (15) expresses $\text{tr}(a^r)$ as a linear combination of $r \rho_k(a)$ and the products $\rho_{r-k}(a) \text{tr}(a^k)$.
Because of the presence of the integer $k$ at the left hand side of the above identity, we cannot obtain the converse statement, that if $\text{tr}(a^i) = 0$ for $i \leq k$ then $\rho_k(a) = 0$ as well, unless we assume char $F = 0$. Instead, we prove a characteristic-free multilinear version. For any $\rho \in \text{End}_F(V)$, the coefficient of $t\rho$ in $\sum_{i,j,s} t^i a_i^j s$ is taken in the extension $F[t_1, \ldots, t_k] \otimes_F A$. For $k = 1$ the newly defined $\text{tr}(a_1)$ and $\rho_1(a_1)$ coincide with the usual definitions.

**Theorem 36.** Fix $r \leq n$. The following two conditions are equivalent:

1. $\rho_k(a_1, \ldots, a_k) = 0$ for all $1 \leq k \leq r$ and every $a_1, \ldots, a_k \in V$;
2. $\text{tr}(a_1, \ldots, a_k) = 0$ for all $1 \leq k \leq r$ and every $a_1, \ldots, a_k \in V$.

**Remark 37.** (1) $\implies$ (1') when $F$ is infinite. Indeed, consider $V[t] = V \otimes_F F[t_1, \ldots, t_k]$ and note that $\rho_k(a) = 0$ for all $a \in V[t]$ since $F$ is infinite. Applying this to $a = t_1 a_1 + \ldots + t_k a_k$ we have that $\rho_k(a_1, \ldots, a_k) = 0$.

In order to prove Theorem 36 we need a version of (1) where $k$ cancels. Consider the polynomial ring $R_0 = \mathbb{Z}[x_{i,j,s} \mid 1 \leq s \leq r, 1 \leq i, j \leq n]$ in $rn^2$ variables, and $R = R_0[t_1, \ldots, t_r]$. In $M_n(R)$, form the generic matrix $X_s$ with $i,j$ entry $x_{i,j,s}$. Next form the generic sum $X = \sum_s t_s X_s$. Let $T$ be the set $\{1, \ldots, r\}$ and let $S \subseteq T$ (nonempty). Define $t^S$ to be the product of the $t_s$ where $s \in S$, so $t^T = t_1 \cdots t_r$. Define $X_S = \sum_{s \in S} t_s X_s$. We adopt the following notation from [W]: $[t^S]p$ is the coefficient of the monomial $t^S$ in a polynomial $p \in R$. Note that if $k = |S|$ then $[t^S] \rho_k(X_S) = [t^S] \rho_k(X)$.

For $S = \{s_1, \ldots, s_k\}$, let $\text{tr}_S = \text{tr}(X_{s_1}, \ldots, X_{s_k})$, as defined above. Clearly, $[t^S] \text{tr}(X_S^k) = k \text{tr}_S$, where we use the fact that $\text{tr}(x_1 \cdots x_k)$ remains invariant under cyclic shifts of the variables. Once again we have that $k \text{tr}_S = [t^S] \text{tr}(X^k)$. Note that, as a special case, $[t^T] \text{tr}(X^T) = r \text{tr}_T$.

We are interested in an identity for the multilinearization of $\rho_r(X_T)$. To this end we multilinearize $\rho_{r-k}(x) \text{tr}(x^k)$. Notice that for any two polynomials $p$ and $p'$,

$$[t^T](pp') = \sum_S [t^S]p \cdot [t^{T-S}]p',$$

where the sum is over all subsets $S \subseteq T$. In particular

$$[t^T] \rho_{r-k}(X) \text{tr}(X^k) = \sum_S [t^S] \text{tr}(X^k) \cdot [t^{T-S}] \rho_{r-k}(X)$$

$$= \sum_S k \text{tr}_S \cdot [t^{T-S}] \rho_{r-k}(X_{T-S}),$$

where the sum being over all $S \subseteq T$ with $|S| = k$, because $\text{tr}(X^k)$ is homogeneous of degree $k$. 
Assume the result for all \( k < r \). We prove this by induction on \( r \).

**Proof.**

\( T \) of Theorem 38. \( \rho \) substitute the expressions we have for \( \rho \) is a partition of \( T \). Theorem 38 presents \( \text{tr}(X) \rho \).

Remark 39. In characteristic zero the conditions (1), (1*), (2), (2*) are equivalent. More precisely, we have:

1. if \((r-1)!\) is invertible then \((2*) \implies (2)\);
2. if \(r!\) is invertible then \((2) \implies (1)\) and the four conditions coincide.

Let \( \Delta = S_1 \cup \ldots \cup S_m \) be a partition of \( T \) into nonempty parts. Set \((-1)^\Delta = (-1)^{\sum (|S|-1)} \). For this \( \Delta \) we define \( \text{tr}_\Delta = \prod_i \text{tr}_{S_i} \). We claim:

**Theorem 38.** \( \rho_r(X_1, \ldots, X_r) = \sum_\Delta (-1)^\Delta \text{tr}_\Delta \), where the sum is over all partitions of \( T \).

**Proof.** We prove this by induction on \( r \). If \( r = 1 \) this just says that \( \rho_1(X_1) = \text{tr}(X_1) \).

Assume the result for all \( k < r \). We start with the formula (19) for \( \rho_r(X_T) \) and substitute the expressions we have for \( \rho_{r-|S|}(X_{T-S}) \) by induction. Note that if \( \Delta' \) is a partition of \( T-S \), and \( \Delta \) is \( \Delta' \) with \( S \) adjoined, then \( (-1)^\Delta = (-1)^\Delta' (-1)^{|S|-1} \).

We can thus compute:

\[
[t^T]\rho_r(X_T) = \sum_{S \neq \emptyset} (-1)^{|S|} |S| \text{tr}_S \cdot [t^{T-S}] \rho_{r-|S|}(X_{T-S})
\]

\[
= \sum_{S \neq \emptyset} (-1)^{|S|} |S| \text{tr}_S \sum_{\Delta' T-S} (-1)^{\Delta'} \text{tr}_{\Delta'}
\]

\[
= \sum_{S \neq \emptyset} \sum_{\Delta' T-S} (-1)^{|S|} (-1)^{\Delta'} |S| \text{tr}_S \text{tr}_{\Delta'}
\]

\[
= \sum_{\Delta' T S \in \Delta} (-1)^{\Delta} |S| \text{tr}_S \text{tr}_{\Delta-S}
\]

\[
= \sum_{\Delta' T \Delta \in \Delta} (-1)^{\Delta} \text{tr}_\Delta \cdot \sum_{S \in \Delta} |S|
\]

and the \( r \)'s cancel. \( \square \)

**Proof of Theorem 38 (2*) \implies (1*):** Fix a specialization of \( M_s(R_0) \) by sending \( X_s \) to arbitrary elements of \( V \). By assumption we have that \( \text{tr}_S = 0 \) for every subset \( S \subseteq T \), so \( \text{tr}_\Delta = 0 \) for any partition \( \Delta \) or \( T \). By Theorem 38 we obtain \( \rho_r(X_1, \ldots, X_r) = 0 \). \( (1^*) \implies (2^*) \): same argument by induction on \( r \), since Theorem 35 presents \( \text{tr}(X_1, \ldots, X_r) \) as a linear combination of \( \rho_r(X_1, \ldots, X_r) \) and products of values of the form \( \text{tr}_S \) for \( |S| < r \).

**Remark 39.** In characteristic zero the conditions (1), (1*), (2), (2*) are equivalent. More precisely, we have:

1. if \((r-1)!\) is invertible then \((2*) \implies (2)\);
2. if \(r!\) is invertible then \((2) \implies (1)\) and the four conditions coincide.
Indeed, if $k$ is invertible then $\text{tr}(a^k) = 0$ implies $\rho_k(a) = 0$ by Newton’s formula. If $(k-1)!$ is invertible then $\text{tr}(a_1, \ldots, a_k) = 0$ implies $\text{tr}(a^k) = 0$ by taking $a_1 = \cdots = a_k = a$. The claim follows by ranging over all $1 \leq k \leq r$.

**Example 40.** We show that the conditions (2) and $(2^*)$ are independent when $\text{char} \, F = 2$ and $r = 3$. We take $V$ to be a space of diagonal matrices in $M_6(F)$. Notice that $\text{tr}(a_1, a_2) = \text{tr}(a_1a_2)$ and $\text{tr}(a_1, a_2, a_3) = \text{tr}(a_1a_2a_3) + \text{tr}(a_1a_3a_2)$. Since elements of $V$ commute, $\text{tr}(a_1, a_2, a_3) = 0$ automatically.

$(2^*) \iff (2)$: Fix some $\alpha \neq 0, 1$ in $F$, and let $\alpha' = \alpha + 1$. Let $V$ be spanned by the matrices with diagonals $(1, 0, 0, 0, \alpha, \alpha'), (0, 1, 0, 0, \alpha', \alpha)$, and $(0, 0, 1, 1, 0, 0)$. Then $\text{tr}(a_1) = 0$ and $\text{tr}(a_1a_2) = 0$ for every $a_1, a_2 \in V$, so $(2^*)$ holds. However $1 + \alpha^3 + \alpha^3 = a\alpha' \neq 0$, so $(2)$ fails.

$(2) \iff (2^*)$: For the converse, assume $\rho \in F$ is a primitive third root of unity. Let $V$ be spanned by the matrices with diagonals $(1, 0, 0, 1, \rho, \rho)$, $(0, 1, 0, 1, \rho, \rho)$ and $(0, 0, 1, \rho, \rho, 1)$. Then $\text{tr}(a_1) = 0$ for every $a_1 \in V$, which implies $\text{tr}(a_1^2) = \text{tr}(a_1a_2) = 0$; $\text{tr}(a_1^3) = 0$ holds by computation, which confirms (2). However the identity $\text{tr}(a_1a_2) = 0$ fails, and so does $(2^*)$.

8. Criteria for $KaK$ to be a Kummer space

As assumed throughout this paper, $K \subset A$ is a maximal separable subfield, and $G \supset H$ are the Galois groups of $L/F$ and $L/K$ respectively, where $L/F$ is the Galois closure of $K/F$. We set $n = [K:F]$. An $F$-vector space $V \subset A$ is Kummer if for every $v \in V$, $\rho_1(v) = 0$ for $i \in \{1, \ldots, n-1\}$, so in particular $v^n \in F$.

If $aKa^{-1} = K$, and $a$ induces an automorphism $\sigma \neq 1$ on $K$ which generates the Galois group of $K/F$, then $a^\sigma \in C_A(K)^\sigma = K^n = F$ but $a^d \notin F$ for a proper divisor $d | n$, implying $\rho_1(a) = 0$ for each $1 \leq i \leq n-1$. Since we may replace $a$ by any element of $Ka$, it then follows that $Ka$ is a Kummer subspace. We seek to prove a converse.

We first consider the question when is $V = KaK$ a Kummer subspace (i.e. (1) of Proposition 35 for $r = n$). Let $H$ be the $H-H$ biset of $G$ associated to $KaK$. For convenience, we write the coset $gH$ as $g$ when it appears in a subscript.

**Proposition 41.** The following are equivalent.

a) For all $x \in KaK$ and all $1 \leq k \leq r$, $\rho_k(x) = 0$.

b) For all $1 \leq k \leq r$ there are no $g_1, \ldots, g_k \in H$ such that $g_1g_2 \cdots g_k = 1$.

**Proof.** Assume a). By way of contradiction, suppose such $g_1, \ldots, g_k$ exist. By induction we can assume that b) holds for all $k < r$. Since $F$ is infinite, it is also true that $\text{tr}(x^k) = 0$ for all $x \in KaK$, where, as always $K = L \otimes K$ and $L$ is the Galois closure of $K/F$. Choose any $\tau \in G$ and set $v_i = e_{\tau g_1g_2 \cdots g_{i-1}g_i}$. Of course $(\tau g_1g_2 \cdots g_{i-1})^{-1}(\tau g_1g_2 \cdots g_{i-1}g_i) = g_i \in H$ so $v_i \in KaK$. Also, $v_1 = e_{\tau g_1}$ and $v_k = e_{\tau g_1 \cdots g_{k-1} \tau}$. Then $v_1 \cdots v_k = e_{\tau \tau}$. Since $g_1 \cdots g_j = 1$ for $i \leq j$ can only hold when $i = 1$ and $j = k$ by assumption, the elements $\tau g_1 \cdots g_{i-1} (i = 1, \ldots, k)$ are distinct. Therefore, the only non-zero product $v_1v_2 \cdots v_{\eta(k)} \neq 0$, for a permutation $\eta \in S_{\{2, \ldots, k\}}$, is obtained when $\eta$ is the identity. Thus $\text{tr}(v_1, \ldots, v_k) = 1$, contrary to the condition $(2^*)$ of Theorem 35 which follows from (1) by that theorem and Remark 77 a contradiction.

Conversely, assume b). Let $R = \mathbb{Z}[g, g'] | g, g' \in G/H]$ be the polynomial ring in $n^2$ variables. We write $X$ to be the matrix with $x_{g, g'}$ in the $(g, g')$ entry when $g^{-1}g' \in H$ and 0 otherwise. In effect, $X$ is a generic element of $KaK$ but over $\mathbb{Z}$. It
suffices to show $\rho_k(X) = 0$ because $X$ specializes to all elements of $\bar{K}a\bar{K}$. Thus we reduce to the case $F$ has characteristic 0. (The reader may object that there is no $K$ etc. over $\mathbb{Z}$. There are two answers, one being that all the essential properties of $K\bar{a}\bar{K}$ are present over $\mathbb{Z}$, or alternatively we can embed $M_n(\mathbb{Z})$ into some $\bar{A}$ so that the matrix idempotents are preserved.)

In characteristic 0 it suffices to prove that $\text{tr}(x^k) = 0$ for all $1 \leq k \leq r$. By induction it suffices to prove $\text{tr}(x^r) = 0$. Write

$$x = \sum_{\tau \in G, g \in H} d_{\tau, g} e_{\tau, \tau g}$$

where $d_{\tau, g} \in \bar{K}$. Then expanding $x^r$ there is no term of the form $Ke_{\tau, \tau}$ by the assumption on $H$.

\[\square\]

**Remark 42.** By the above we see that $\text{tr}(v) = 0$ for all $v \in V$ if and only if $H \not\subseteq H$. Thus zeroing out the characteristic coefficients corresponds to avoiding having $H$ in the powers of the associated $H$-biset $H$.

For example,

1. Assume that $G = \langle \sigma \rangle$ is cyclic, namely $H = \{1\}$. Then the bimodule $V$ corresponding to the $H$-biset $\{\sigma\}$ satisfies, $\rho_k(v) = 0$ for all $1 \leq k \leq n - 1$; indeed, $\{\sigma\}^k \cap H = \emptyset$ for all the relevant cases.

2. Assume that $G = \langle \sigma \rangle \rtimes \langle \tau \rangle \cong C_n \rtimes C_2$ is dihedral, namely $H = \langle \tau \rangle$. Then the bimodule $V$ corresponding to the $H$-biset $H\sigma H$ satisfies $\rho_k(v) = 0$ for all odd $k$, $1 \leq k \leq n - 1$; indeed, $\{\sigma\}^k \cap H = \emptyset$ for all the relevant cases. This was used in [RS] to prove that dihedral algebras of odd degree are cyclic.

We are interested in saying something about elements in $K\bar{a}$, where again we may pass to $\bar{K}a$. Notice that in $\bar{K}a$ we can choose elements of the form $x = \sum_{\tau^{-1} \in H} x_{\tau} e_{\tau, \sigma}$ for a fixed $\sigma$. Fixing $\tau$ with $\tau^{-1} \sigma \in H$, we can always choose $x$ with $x_{\tau} = 1$ because $e_{\tau, \sigma} \in \bar{K}a\bar{K}$ and so $e_{\tau, \sigma} = e_{\tau, \tau} x$ for $x \in a\bar{K}$. We claim:

**Theorem 43.** Suppose that $\rho_k(x) = 0$ for all $1 \leq k \leq r$ and all $x \in K\bar{a}$. Then the same is true for all $x \in Ka\bar{K}$.

**Proof.** We proceed by induction on $r$. If $\rho_1(ak) = \text{tr}(a\bar{K}) = 0$ for all $k \in K$ then $\text{tr}(k'ak) = \text{tr}(akk') = 0$ for all $k', k \in K$ and any element of $K\bar{a}\bar{K}$ is a sum of $k'ak$'s.

For $r > 1$ the result is harder but we know by induction that $\rho_1(x) = 0$ for all $i < r$ and all $x \in K\bar{a}$. In particular, for all $i < r$ there are no $g_1, \ldots, g_i \in H$ with $g_1 \cdots g_i = 1$ by Proposition 41.

Again by Proposition 41 it suffices to show that there are no $g_1, \ldots, g_r$ with $g_1 \cdots g_r = 1$. Assume otherwise. Choose $\tau$ arbitrary, define $\tau_0 = \tau$ and set $\tau_i = \tau g_i \cdots g_1$ for $i = 1, \ldots, r$. Choose $v_i = \sum_{\tau'} x_i, \tau e_{\tau', \tau} \in \bar{K}e_{\tau, \tau}, \tau$ such that $x_i, \tau e_{\tau, \tau}, \tau$ = 1, then $v_1 \cdots v_r$ has a unique diagonal element $e_{\tau, \tau}$. By Proposition 39 there is a $1 \neq \eta \in S_{r - 1}$ such that $v_1 v_{j(2)} \cdots v_{j(r)}$ has a nonzero diagonal component $ye_{\tau, \tau}$. If $1 \neq j = \eta(1)$, then $j > 1$ and in $v_j = \sum_{\tau} x_j, \tau e_{\tau, \tau}$ we must have $x_j, \tau \neq 0$. This implies $\tau^{-1} \tau_j = g_1 \cdots g_j \in H$ which implies $(g_1 \cdots g_j)g_{j + 1} \cdots g_r = 1$ which contradicts the induction assumption. Thus $\eta(j) = 1$. If we redefine $j = \eta(2)$ and assume that $j > 2$, then arguing similarly we have $x_{\tau_1, \tau_j} \neq 0$ and so $\tau_2 \cdots \tau_j \in H$. This again contradicts the induction
assumption and so, by an inner induction that proceeds now in the obvious way, we have \( \eta \) is the identity, proving the theorem.

\[ \square \]

**Corollary 44.** Ka is Kummer iff KaK is Kummer.

**Theorem 45.** Suppose that Ka is Kummer. Then \( H = \{1\} \), \( G \) is cyclic of order \( n \) with generator \( g \), and KaK = Ku for invertible \( u \in KaK \) satisfying \( uku^{-1} = g(k) \) for all \( k \in K \). If \( a \) is invertible we may assume \( u = a \).

**Proof.** By Corollary 44 KaK is Kummer. Let \( H \) be the H-biset associated to KaK. By Proposition 41 there are no \( g_i \in H \) such that \( g_1 g_2 \ldots g_s = 1 \) for any \( 1 \leq s < n \). Equivalently, \( H \) is not contained in \( H^s \) for any \( 1 \leq s < n \). Fix some \( g \in H \). If \( g^i H = g^j H \) for \( i < j \), then \( g^{j-i} H \) implies \( j - i \geq n \). Thus \( H, gH, \ldots, g^{n-1} H \) are all distinct. This implies that their union is \( G \) and hence \( g^s H = H \) or \( g^s \notin H \) for \( 1 \leq s < n \).

We show that \( H = gH \). Indeed, assume \( g^s H \subseteq H \); then \( g^n = g^{n-s} g^s \in H^{-s} H = H^{-s+1} \). Hence \( s = 1 \). But now \( gH \) is an \( H \)-biset, so \( H g = gH \) and \( H \wr G \) since \( (H, g) = G \).

Since \( L/F \) was the Galois closure of \( K/F \), this implies \( H = \{1\} \) and now clearly \( G \) is cyclic of order \( n \), and KaK is associated to the double coset \( H g H = \{g\} \) for \( g \) a generator of \( G \). But this implies KaK = uK where \( u k u^{-1} = g(k) \) for all \( k \in K \). \[ \square \]

9. **Algebras of prime degree**

Assume that the degree of \( A \) over \( F \) is a prime \( p \). We observe that the dimensions of the irreducible components, other than \( K \), are all equal.

**Proposition 46.** Suppose that \( A/F \) has prime degree \( p \). There are two possibilities:

1. For every \( a \notin K \), \( \dim_K(\text{KaK}) = p - 1 \). In this case \( G \) is doubly transitive.
2. All irreducible sub-\( K \)-\( K \)-bimodules of \( A \) other than \( K \) have the same dimension \( r \); and \( L/F \) has Galois group \( C_p \rtimes C_r \) where \( C_r \) acts faithfully on \( C_p \), so \( r \) (strictly) divides \( p - 1 \).

**Proof.** If (1) fails, the group \( G \) is transitive, but not doubly transitive by Remark 16. By a theorem of Burnside [11, Theorem I.7.3], \( G \) then is solvable and hence of the form \( C_p \rtimes C_r \). \( H \) is now a conjugate of \( C_r \) and its double cosets correspond to the orbits of \( C_r \) on \( C_p \).

Notice that the case \( r = 1 \) is when \( K \) is cyclic. It is interesting to consider the “next best” case where (some) \( KaK \) has dimension exactly 2 over \( K \). If \( K/F \) is not cyclic, then there is a double coset \( H g H \) which has order \( 2|H| \). By the proposition this forces \( L/F \) to have dihedral Galois group – which means \( A \) is cyclic by [15] (although not with respect to \( K \)).

In the situation (1), \( A = K \oplus KaK \) for some \( a \notin K \), and \( (KaK)^2 = A \). Let us look more closely at the situation (2) in the above proposition. That is, assume that \( n = p \) is prime, and \( G \) is transitive but not doubly transitive. Again by Burnside's theorem, \( G \) is contained in the affine group of the field \( \mathbb{F}_p \), and contains the element \( \sigma(i) = i + 1 \). In the earlier notation, we may assume \( H \) is the stabilizer of 0, which is cyclic of some order \( r \) strictly dividing \( p - 1 \). We present

\[ G = C_p \rtimes C_r = \langle \sigma, \tau \mid \sigma^p = \tau^r = 1, \tau \sigma \tau^{-1} = \sigma^i \rangle; \]
thus $H = \langle \tau \rangle$, which we identify with the subgroup $\langle t \rangle \subseteq \mathbb{F}_p^\times$ where we fix an element $t \in \mathbb{F}_p^\times$ of order $r$.

For $c \in \mathbb{F}_p$, let us denote

$$\sigma^cH = \{ \tau' \sigma^c \tau'^{-1} \mid \tau' \in H \} = \{ \sigma^c \tau^i \mid i = 0, \ldots, r - 1 \};$$

thus $\sigma^cH = H \sigma^cH$. Any double coset of $H$ in $G$ has the form $H \sigma^c \tau^d H = \{ \tau^d \sigma^c \tau^{-1} \mid \tau^d \in H \} = \sigma^cH H$. The double cosets correspond to the orbits of $\mathbb{F}_p$ under the action of $H = \langle t \rangle$ by multiplication. The inverse of this double coset is $(\sigma^cH)^{-1} = H \sigma^{-c}H = \sigma^{-c}H H$, and the product (in $G$) of two double cosets $\sigma^cH, \sigma^{c'}H$ is $\sigma^{c+c'}H H$, which is a union of all the $\sigma^{c''}H H$ for which $c''H \subseteq cH + c'H$. Thus, the semiring of double cosets with union and multiplication is isomorphic to the semiring of subsets of the quotient group $\mathbb{F}_p^\times/\langle t \rangle$ with union and addition of subsets.

We may identify $A = L \otimes \mathbb{A}$ with $M_p(\mathbb{F})$, with $e_{ii}$ the idempotent corresponding to $\sigma^iH$. The irreducible bimodule corresponding to a double coset $\sigma^{c}H$ is $K \sum_{i \neq j \in cH} e_{ij} K$.

References

[AlM] Albert, A.A.; Muckenhoupt. On matrices of trace 0, Michigan Math. J. 1 (1957), 1–3.
[Al] A.A. Albert, Two element generation of a separable algebra, Bull. Amer. Math. Soc. 50 (1944), 786-788.
[G] Guralnick, R. Some applications of subgroup structure to probabilistic generation and covers of curves, Algebraic groups and their representations, NATO Adv. Sci. Inst. Ser. C. Math. Phys. Sci. 517 (1996), 301–320.
[Jac1] N. Jacobson, Structure of Rings, Amer. Math. Soc. Colloq. Pub. 37, 1956.
[Jac2] N. Jacobson, Generation of separable and central simple algebras, J. Math. Pures Appl. 36 (1957), 217–227.
[Jac3] N. Jacobson, Brauer factor sets, Noether factor sets, and crossed products, Emmy Noether in Bryn Marr 1–19, Springer-Verlag, New York.
[Jac4] N. Jacobson, Finite-Dimensional Division Algebras over Fields, Springer, 1996.
[P] D.S. Passman, “Permutation Groups”, Dover, 2012.
[R1] L.H. Rowen, Polynomial identities in ring theory, Academic Press Pure and Applied Mathematics 84, 1980.
[RS] L.H. Rowen, and D. Saltman, Dihedral algebras are cyclic, Proc. Amer. Math. Soc. 84 (1982), 162–164.
[S] D. Saltman, Lectures in Division algebras, CBMS 94, Amer. Math. Soc., 1999.
[W] H. Wilf, Generating functionology, Academic Press, 1994.