JOURNAL
de Théorie des Nombres
de BORDEAUX

*anciennement Séminaire de Théorie des Nombres de Bordeaux*

Rachel NEWTON

**Realising the cup product of local Tate duality**

Tome 27, nº 1 (2015), p. 219-244.

<http://jtnb.cedram.org/item?id=JTNB_2015__27_1_219_0>

*Journal de Théorie des Nombres*
*de Bordeaux* **27** (2015), 219–244

# Realising the cup product of local Tate duality

par Rachel NEWTON

Résumé. Nous présentons une description explicite, en termes d'algèbres centrales simples, d'un cup-produit intervenant dans l'énoncé de la dualité de Tate locale pour les modules galoisiens d'ordre premier $p$. Étant donnés deux cocycles $f$ et $g$, nous construisons une algèbre centrale simple de dimension $p^2$ dont la classe dans le groupe de Brauer donne le cup-produit $f \cup g$. Cette algèbre est aussi petite que possible.

Abstract. We present an explicit description, in terms of central simple algebras, of a cup product map which occurs in the statement of local Tate duality for Galois modules of prime cardinality $p$. Given cocycles $f$ and $g$, we construct a central simple algebra of dimension $p^2$ whose class in the Brauer group gives the cup product $f \cup g$. This algebra is as small as possible.

## 1. Introduction

Let $F$ be a non-Archimedean local field with separable closure $F_{\text{sep}}$ and absolute Galois group $G_F = \text{Gal}(F_{\text{sep}}/F)$. Let $A$ be a finite $G_F$-module such that the cardinality of $A$ is not divisible by the characteristic of $F$. Denote by $\mu$ the group of all roots of unity in $F_{\text{sep}}$. Let $A^\vee = \text{Hom}(A, \mu)$. Tate proved the following result in [8].

**Theorem 1.1** (Local Tate duality)**.** *For $i \geq 3$, the group $H^i(G_F, A) = 0$. For $0 \leq i \leq 2$, the group $H^i(G_F, A)$ is finite and the cup product*

$$\cup : H^i(G_F, A) \times H^{2-i}(G_F, A^\vee) \to H^2(G_F, \mu) \cong \text{Br}(F) \cong \mathbb{Q}/\mathbb{Z} \tag{1.1}$$

*gives a duality between $H^i(G_F, A)$ and $H^{2-i}(G_F, A^\vee)$.*

Local Tate duality is a valuable tool for computing the Galois cohomology of local fields. It plays a crucial role in Kolyvagin's work in [3] and [4], where he applies Euler systems to elliptic curves and thereby provides evidence for Birch and Swinnerton-Dyer Conjecture.

In the cases $i = 0$ and $i = 2$, the cup product (1.1) is easily computed, using Lemma 1 of the appendix 'Computations of Cup Products' in [7], for

Manuscrit reçu le 10 juillet 2013, révisé le 18 décembre 2013, accepté le 14 janvier 2014.
*Mathematics Subject Classification.* 16K20, 12G05.

example. In this paper, we focus on the case $i = 1$ for modules of prime cardinality.

**Notation and conventions.** Let $K$ be any field. We will consider $K$ to be fixed throughout the paper and will use the following notation.

| | |
|---|---|
| $K_{\text{sep}}$ | a fixed separable closure of $K$ |
| $G_K$ | the absolute Galois group of $K$, $G_K = \text{Gal}(K_{\text{sep}}/K)$ |
| $M$ | a $G_K$-module of prime cardinality $p$ such that $\text{char}(K) \nmid p$ |
| $\mu_p$ | the group of $p$th roots of unity in $K_{\text{sep}}$ |
| $M^\vee$ | the Tate dual of $M$, $M^\vee = \text{Hom}(M, \mu_p)$ |
| $H_M$ | the kernel of the natural map $G_K \to \text{Aut}(M)$ |
| $H_{M^\vee}$ | the kernel of the natural map $G_K \to \text{Aut}(M^\vee)$. |

For elements $f, g, \varphi, \dots$ of cohomology groups, we often employ the notation $f_0, g_0, \varphi_0, \dots$ to refer to a choice of representative cocycles.

Our aim is to give an explicit description of the following cup product.

$$\cup : H^1(G_K, M) \times H^1(G_K, M^\vee) \longrightarrow H^2(G_K, \mu_p) \cong \text{Br}(K)[p]. \tag{1.2}$$

The main result is Theorem 1.9 where, given non-trivial cocycle classes $f \in H^1(G_K, M)$ and $g \in H^1(G_K, M^\vee)$, we construct a central simple algebra $\mathcal{D}$ with the following properties.

(1) The class of $\mathcal{D}$ in $\text{Br}(K)$ is the class of the cup product $f \cup g$.
(2) $\dim_K(\mathcal{D}) = p^2$. Therefore, $\mathcal{D}$ is a division algebra if and only if $f \cup g \neq 0$.

The usual construction gives a central simple algebra which can have dimension as large as $p^4(p-1)^4$ in general. Our minimisation of the dimension of the central simple algebra makes the cup product (1.2) more amenable to explicit computation.

From now on, we fix two non-trivial cocycle classes: $f \in H^1(G_K, M)$ and $g \in H^1(G_K, M^\vee)$. In order to compute the cup product $f \cup g$ as a central simple algebra, we must replace $G_K$ with a finite Galois group. The action of $G_K$ on $M$ gives a map $G_K \to \text{Aut}(M)$. Let $H_M$ denote the kernel of this map and consider the inflation-restriction exact sequence

$$0 \longrightarrow H^1(G_K/H_M, M) \xrightarrow{\text{Inf}} H^1(G_K, M) \xrightarrow{\text{Res}} H^1(H_M, M)^{G_K/H_M}$$

$$\longrightarrow H^2(G_K/H_M, M).$$

Observe that $G_K/H_M$ injects into $\text{Aut}(M)$, which has order $p-1$. Hence, $G_K/H_M$ has order coprime to $\#M = p$ and consequently

$$H^1(G_K/H_M, M) = H^2(G_K/H_M, M) = 0.$$

Therefore, the restriction map gives an isomorphism

$$H^1(G_K, M) \cong H^1(H_M, M)^{G_K/H_M} = \mathrm{Hom}_{G_K}(H_M, M).$$

The restriction of $f$ to $H_M$ is a homomorphism from $H_M$ to $M$. Let $N_f$ denote the kernel of the restriction of $f$ to $H_M$. Then $N_f$ is a normal subgroup of $G_K$. Because $f \neq 0$, the injective $G_K$-homomorphism $H_M/N_f \to M$ induced by $f$ is also surjective. So $H_M/N_f$ has order $p$. In the same way, we define $H_{M^\vee}$ and $N_g$. Let $N = N_f \cap N_g$. The lattice of subgroups is as follows.

$$\begin{tikzcd}
& G_K \arrow[dl, dash] \arrow[dr, dash] & \\
H_M \arrow[d, dash] & & H_{M^\vee} \arrow[d, dash] \\
N_f \arrow[dr, dash] & & N_g \arrow[dl, dash] \\
& N &
\end{tikzcd}$$

**Lemma 1.2.** *If $N_f = N_g$, then $M$ and $M^\vee$ are isomorphic as $G_K$-modules.*

*Proof.* We have isomorphisms of $G_K$-modules $H_M/N_f \to M$, induced by $f$, and $H_{M^\vee}/N_g \to M^\vee$, induced by $g$. So it suffices to show that

$$H_M/N_f = H_{M^\vee}/N_g.$$

Observe that $G_K/N_f \cong H_M/N_f \rtimes G_K/H_M$ and therefore $H_M/N_f$ is the unique Sylow $p$-subgroup of $G_K/N_f$. But $H_{M^\vee}/N_g$ is also an order $p$ subgroup of $G_K/N_f = G_K/N_g$. □

**Corollary 1.3.** *If $N_f = N_g$ and $p > 2$, then $f \cup g = 0$.*

*Proof.* By Lemma 1.2, $M$ and $M^\vee$ are isomorphic as $G_K$-modules. By fixing such an isomorphism, we identify $M$ with $M^\vee$. The cup product map is anti-symmetric and $p > 2$ so anti-symmetric implies alternating. Thus, it is enough to show that $g = nf$ for some $n \in \mathbb{Z}$. The restriction map

$$\mathrm{Res} : H^1(G_K, M) \to H^1(H_M, M) = \mathrm{Hom}(H_M, M)$$

is injective, so it suffices to show that $\mathrm{Res}(g) = n\mathrm{Res}(f)$ for some $n \in \mathbb{Z}$. Now $\mathrm{Res}(f)$ and $\mathrm{Res}(g)$ both have kernel $N_f$, so they both arise from isomorphisms $H_M/N_f \to M$. But $M$ has order $p$, so any two such isomorphisms differ by a scalar multiple. □

**Lemma 1.4.** *If $N_f \subset N_g$ or $N_g \subset N_f$, then $N_f = N_g$.*

*Proof.* Suppose that $N_f \subset N_g$. We will show that $N_f = N_g$. The other argument is identical. Let $\pi : G_K/N_f \twoheadrightarrow G_K/N_g$ be the natural projection. Recall that $G_K/N_f \cong H_M/N_f \rtimes G_K/H_M$, where $H_M/N_f$ has order $p$ and $G_K/H_M$ has order coprime to $p$. Similarly, $G_K/N_g \cong H_{M^\vee}/N_g \rtimes G_K/H_{M^\vee}$. Since $H_{M^\vee}/N_g$ has order $p$ and $\pi$ is surjective, the order of $\pi^{-1}(H_{M^\vee}/N_g)$ is divisible by $p$. Therefore, $\pi^{-1}(H_{M^\vee}/N_g)$ contains the unique Sylow $p$-subgroup of $G_K/N_f$, namely $H_M/N_f$. Suppose for contradiction that $\pi(H_M/N_f) = 0$. This implies that $\mathrm{Im}(\pi) = \pi(G_K/H_M)$. But this contradicts the surjectivity of $\pi$ because the order of $G_K/H_M$ is coprime to $p$, whereas $p$ divides the order of $G_K/N_g$. Therefore, $\pi$ defines an isomorphism of $G_K$-modules $\pi : H_M/N_f \to H_{M^\vee}/N_g$. Moreover, $f$ and $g$ define $G_K$-module isomorphisms $f : H_M/N_f \to M$ and $g : H_{M^\vee}/N_g \to M^\vee$ respectively. Hence, $M$ and $M^\vee$ are isomorphic as $G_K$-modules. But then $H_M = H_{M^\vee}$ by definition. This, combined with the fact that the natural projection gives an isomorphism $\pi : H_M/N_f \to H_{M^\vee}/N_g$, is enough to complete the proof that $N_f = N_g$. □

Recall that $N = N_f \cap N_g$. Consider the inflation-restriction exact sequence

$$0 \longrightarrow H^1(G_K/N, M) \xrightarrow{\mathrm{Inf}} H^1(G_K, M) \xrightarrow{\mathrm{Res}} H^1(N, M).$$

By definition of $N$, the element $f$ is in the kernel of restriction to $N$. So $f$ comes from an element of $H^1(G_K/N, M)$, which we will also call $f$. Similarly, $g$ comes from an element of $H^1(G_K/N, M^\vee)$, which we will also call $g$. The properties of the cup product mean that the following diagram commutes.

$$\begin{tikzcd}
H^1(G_K, M) \times H^1(G_K, M^\vee) \arrow[r, "\cup"] & H^2(G_K, \mu_p) \\
H^1(G_K/N, M) \times H^1(G_K/N, M^\vee) \arrow[u, "\mathrm{Inf}"] \arrow[r, "\cup"] & H^2(G_K/N, \mu_p) \arrow[u, "\mathrm{Inf}"]
\end{tikzcd}$$

Therefore, we can reduce to studying the cup product

$$\cup : H^1(G_K/N, M) \times H^1(G_K/N, M^\vee) \longrightarrow H^2(G_K/N, \mu_p). \tag{1.3}$$

Let $L = K_{\mathrm{sep}}^N$ so that $\mathrm{Gal}(L/K) = G_K/N$. Thus, $L/K$ is a finite Galois extension of degree dividing $p^2(p-1)^2$. Note that the action of $G_K$ on $M^\vee = \mathrm{Hom}(M, \mu_p)$ is given by $(s \cdot \phi)(m) = s \cdot \phi(s^{-1} \cdot m)$ for all $\phi \in M^\vee$, all $s \in G_K$ and all $m \in M$. Hence, $\mu_p$ is fixed by all elements in $H_M \cap H_{M^\vee}$, so $\mu_p \subset L^*$. We have the following commutative diagram:

$$\begin{tikzcd}
H^2(G_K, \mu_p) \arrow[r, hook] & H^2(G_K, K_{\mathrm{sep}}^*) \arrow[r, "\cong"] & \mathrm{Br}(K) \\
H^2(\mathrm{Gal}(L/K), \mu_p) \arrow[r] \arrow[u, "\mathrm{Inf}"] & H^2(\mathrm{Gal}(L/K), L^*) \arrow[r, "\cong"] & \mathrm{Br}(L/K) \arrow[u, hook]
\end{tikzcd}$$

where $\mathrm{Br}(L/K)$ denotes the subgroup of $\mathrm{Br}(K)$ consisting of the classes of central simple algebras over $K$ which are split by $L/K$. The isomorphism $H^2(\mathrm{Gal}(L/K), L^*) \to \mathrm{Br}(L/K)$ is induced by the map sending a 2-cocycle $\vartheta$ to the central simple algebra $A_\vartheta$ as defined below.

**Definition 1.5.** Let $L/K$ be a finite Galois extension and let $\vartheta$ be a 2-cocycle representing an element of $H^2(\mathrm{Gal}(L/K), L^*)$. The $K$-algebra $A_\vartheta$ is defined to be the left $L$-vector space with basis $\{e_s\}_{s \in \mathrm{Gal}(L/K)}$ and multiplication given by

$$e_s x = s(x) e_s \quad \forall\ s \in \mathrm{Gal}(L/K), \quad \forall\ x \in L$$
$$e_s e_t = \vartheta(s,t) e_{st} \quad \forall\ s, t \in \mathrm{Gal}(L/K).$$

$A_\vartheta$ is a central simple algebra of dimension $[L:K]^2$ over $K$. See, for example, [6], where this is Theorem 29.12.

From now on, fix representative cocycles $f_0, g_0$ for $f$ and $g$ respectively.

**Definition 1.6.** Let $\varphi = f \cup g$. The formula given in the remark at the end of §2.4 of [5] tells us that a representative 2-cocycle for $\varphi$ is

$$\varphi_0 : \mathrm{Gal}(L/K) \times \mathrm{Gal}(L/K) \to \mu_p$$

given by

$$\varphi_0(s,t) = (s \cdot g_0(t))(f_0(s)). \tag{1.4}$$

**Lemma 1.7.** *If $N_f = N_g$ and $p = 2$, then $f \cup g$ corresponds to a quaternion algebra over $K$, generated by two elements $x$ and $y$ such that $K(x) \cong K_{\mathrm{sep}}^{N_f}$, $x^2 \in K^*$, $y^2 = -1$ and $yx = -xy$. Consequently, $f \cup g = 0$ if and only if $-1 \in N_{K_{\mathrm{sep}}^{N_f}/K}(K_{\mathrm{sep}}^{N_f})$.*

*Proof.* This follows from the explicit construction of a central simple algebra given above. By [2], Theorem 8.14, the quaternion algebra $A_{\varphi_0}$ is a division ring if and only if $y^2 \notin N_{K(x)/K}(K(x))$. □

Having dealt with the case $N_f = N_g$ for all $p$, henceforth we assume that $N_f \neq N_g$.

**Definition 1.8.** Define $\ker(f_0) = \{s \in G_K \mid f_0(s) = 0\}$. Since $f_0$ is a 1-cocycle, $\ker(f_0)$ is a subgroup of $G_K$. Likewise, we define the subgroup $\ker(g_0)$ of $G_K$ by $\ker(g_0) = \{s \in G_K \mid g_0(s) = 0\}$.

The Galois correspondence gives the following diagram of subfields.

$$\begin{tikzcd}
 & & & L = K_{\text{sep}}^{N} \arrow[dlll, dash] \arrow[drrr, dash] & & & \\
K_{\text{sep}}^{N_f} \arrow[dr, dash] \arrow[dd, dash] & & & & & & K_{\text{sep}}^{N_g} \arrow[dl, dash] \arrow[dd, dash] \\
 & K_{\text{sep}}^{\ker(f_0)} \arrow[ddrr, dash] & & & & K_{\text{sep}}^{\ker(g_0)} \arrow[ddll, dash] & \\
K_{\text{sep}}^{H_M} \arrow[drrr, dash] & & & & & & K_{\text{sep}}^{H_{M^\vee}} \arrow[dlll, dash] \\
 & & & K & & &
\end{tikzcd}$$

Below, we state the main result which will be proved in this paper.

**Theorem 1.9.** *Write $K_{\text{sep}}^{\ker(f_0)} = K(\alpha)$ with $\operatorname{Tr}_{K(\alpha)/K}(\alpha) = 0$. Similarly, write $K_{\text{sep}}^{\ker(g_0)} = K(\beta)$ with $\operatorname{Tr}_{K(\beta)/K}(\beta) = 0$. Let $\sigma \in G_K$ be such that $\sigma$ acts trivially on the normal closure of $K(\beta, \mu_p)$ and $\sigma(\alpha) \neq \alpha$. Likewise, let $\rho \in G_K$ act trivially on the normal closure of $K(\alpha, \mu_p)$ but non-trivially on $\beta$. Let $\zeta = (g_0(\rho))(f_0(\sigma)) \in \mu_p$. Let $h_{ij} = \sum_{\ell=0}^{p-1} \zeta^{j\ell} \sigma^\ell(\alpha^i)$. Write $\rho^j(\beta) = \sum_{i=0}^{p-1} m_{ij}\beta^i$ for $m_{ij} \in K_{\text{sep}}^{H_{M^\vee}}$. Let $\mathcal{D}$ be the left $K(\beta)$-vector space with basis $\{z^j\}_{0 \leq j \leq p-1}$, where $z$ satisfies the same minimal polynomial over $K$ as $\alpha$, with multiplication*

$$z\beta = \sum_{i,j=0}^{p-1} c_{ij}\beta^i z^j$$

*where the matrix $(c_{ij})_{i,j} = (h_{1j}m_{ij})_{i,j}(h_{ij})_{i,j}^{-1}$. Then $\mathcal{D}$ is a central simple algebra of dimension $p^2$ over $K$ which gives the class of $f \cup g$ in $\operatorname{Br}(K)$.*

**Corollary 1.10.** *Suppose that $p = 2$. Then $f \cup g$ is represented by a quaternion algebra over $K$, generated by two elements $x$ and $y$ such that $K(x) \cong K_{\text{sep}}^{\ker(g_0)}$ and $K(y) \cong K_{\text{sep}}^{\ker(f_0)}$, with $x^2, y^2 \in K^*$ and $yx = -xy$. Consequently, $f \cup g$ is trivial if and only if $x^2 \in N_{K(y)/K}(K(y))$, if and only if $y^2 \in N_{K(x)/K}(K(x))$.*

*Proof.* This follows immediately from Theorem 1.9. The quaternion algebra is a division ring if and only if $x^2 \notin N_{K(y)/K}(K(y))$, if and only if $y^2 \notin N_{K(x)/K}(K(x))$ by [2], Theorem 8.14. □

The algebra $A_{\varphi_0}$, constructed as in Definition 1.5, is a representative in $\operatorname{Br}(K)$ of $f \cup g$. The dimension of $A_{\varphi_0}$ over $K$ can be as large as

$p^4(p-1)^4$. In Section 2, we find a minimal left ideal $\mathcal{S}$ of $A_{\varphi_0}$. The Artin-Wedderburn Theorem shows that $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$ represents the same class in $\mathrm{Br}(K)$ as $A_{\varphi_0}$. Moreover, the dimension of $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$ over $K$ is just $p^2$. In Section 3, we show that $K_{\mathrm{sep}}^{\ker(f_0)}$ and $K_{\mathrm{sep}}^{\ker(g_0)}$ are maximal commutative subalgebras of $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$, and that $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$ is generated by $K_{\mathrm{sep}}^{\ker(g_0)}$ together with any element $d \in \mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}} \setminus K_{\mathrm{sep}}^{\ker(g_0)}$. In Section 4, we find such an element $d \in \mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}} \setminus K_{\mathrm{sep}}^{\ker(g_0)}$ and in Section 5 we calculate its minimal polynomial over $K$ and deduce that $K(d) \cong K_{\mathrm{sep}}^{\ker(f_0)}$. In Section 6, we describe the multiplicative structure of the algebra $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$ in terms of structure constants. In Section 7, we apply Theorem 1.9 to a specific example.

## 2. Applying the Artin-Wedderburn theorem

Recall the construction given in Definition 1.5 of the algebra $A_{\varphi_0}$ from the 2-cocycle $\varphi_0$ representing $f \cup g$. The dimension of $A_{\varphi_0}$ over $K$ is equal to $[L : K]^2$ and is therefore at most $p^4(p-1)^4$. The Artin-Wedderburn Theorem tells us that $A_{\varphi_0} \cong M_n(D)$ for some $n \in \mathbb{N}$ and some division algebra $D$. It is the division algebra $D$ which gives the class of $A_{\varphi_0}$ in $\mathrm{Br}(K)$. We will show that if $D \neq K$ then the dimension of $D$ over $K$ is $p^2$ and we will describe $D$ in terms of an endomorphism ring.

**Definition 2.1.** Let $A$ be a central simple algebra over a field $K$. Write $A \cong M_n(D)$ for $n \in \mathbb{N}$ and a division algebra $D$.

(1) The *period* of $A$ is the order of the class of $A$ in $\mathrm{Br}(K)$.
(2) The quantity $\sqrt{\dim_K(D)}$ is called the *index* of $A$. The index of $A$ is known to be equal to the greatest common divisor of the degrees of finite separable field extensions which split $A$. See Proposition 4.5.8 of [1], for example.

**Lemma 2.2.** *$K_{\mathrm{sep}}^{\ker(f_0)}/K$ and $K_{\mathrm{sep}}^{\ker(g_0)}/K$ are degree $p$ subextensions of $L$ which split $A_{\varphi_0}$.*

*Proof.* Recall that $\ker(f_0)$ is a subgroup of $G_K$ because $f_0$ is a 1-cocycle. Also, $f_0$ defines an injection from the left cosets of $\ker(f_0)$ in $G_K$ to $M$. This injection is also a surjection because the restriction of $f$ to $H_M$ surjects onto $M$. Thus, $K_{\mathrm{sep}}^{\ker(f_0)}/K$ is a degree $p$ extension. Since $N \subset N_f \subset \ker(f_0)$, we have $K_{\mathrm{sep}}^{\ker(f_0)} \subset L$. The following diagram commutes.

(2.1)
$$\begin{tikzcd}
H^2(\mathrm{Gal}(L/K), L^*) \arrow[r, "\cong"] \arrow[d, "\mathrm{Res}"] & \mathrm{Br}(L/K) \arrow[d] \\
H^2(\mathrm{Gal}(L/K_{\mathrm{sep}}^{\ker(f_0)}), L^*) \arrow[r, "\cong"] & \mathrm{Br}(L/K_{\mathrm{sep}}^{\ker(f_0)})
\end{tikzcd}$$

where the map $\mathrm{Br}(L/K) \to \mathrm{Br}(L/K_{\mathrm{sep}}^{\ker(f_0)})$ is induced by

$$A \mapsto A \otimes_K K_{\mathrm{sep}}^{\ker(f_0)}.$$

Recall that $\mathrm{Gal}(L/K_{\mathrm{sep}}^{\ker(f_0)}) = \ker(f_0)/N$. The restriction of $f$ to $\ker(f_0)/N$ is trivial in $H^1(\ker(f_0)/N, M)$, and the cup product commutes with the restriction homomorphism. So we have

$$\mathrm{Res}(f \cup g) = \mathrm{Res}(f) \cup \mathrm{Res}(g) = 0 \cup \mathrm{Res}(g) = 0.$$

Therefore, diagram (2.1) shows that $A_{\varphi_0} \otimes_K K_{\mathrm{sep}}^{\ker(f_0)}$ represents the trivial class in $\mathrm{Br}(L/K_{\mathrm{sep}}^{\ker(f_0)})$. In other words, $K_{\mathrm{sep}}^{\ker(f_0)}$ splits $A_{\varphi_0}$. The argument for $K_{\mathrm{sep}}^{\ker(g_0)}$ is analogous. □

**Remark 2.3.** If $f_0$ is modified by a coboundary, the subgroup $\ker(f_0)$ is conjugated by an element of $G_K$. Thus, the embedding of $K_{\mathrm{sep}}^{\ker(f_0)}$ in $L$ is changed. But the $K$-isomorphism class of the field $K_{\mathrm{sep}}^{\ker(f_0)}$ only depends on $f$. Therefore, the fact that $K_{\mathrm{sep}}^{\ker(f_0)}$ splits $A_{\varphi_0}$ only depends on $f$ and not on the choice of cocycle representative $f_0$.

**Corollary 2.4.** *Suppose that the class of $A_{\varphi_0}$ in $\mathrm{Br}(K)$ is non-trivial. Then $A_{\varphi_0}$ is isomorphic to $M_n(D)$, where $D$ is a central division algebra over $K$ of dimension $p^2$ and $n = p^{-1}[L : K]$. Thus, the index of $A_{\varphi_0}$ is equal to its period, $p$. Moreover, $K_{\mathrm{sep}}^{\ker(f_0)}$ and $K_{\mathrm{sep}}^{\ker(g_0)}$ embed into $D$ as maximal commutative subalgebras.*

*Proof.* Recall that the index of $A_{\varphi_0}$ is the greatest common divisor of the degrees of finite separable extensions which split $A_{\varphi_0}$. Lemma 2.2 states that $K_{\mathrm{sep}}^{\ker(f_0)}/K$ is a degree $p$ extension which splits $A_{\varphi_0}$. Since $p$ is prime, the index of $A_{\varphi_0}$ is $p$. Consequently, $A_{\varphi_0} \cong M_n(D)$, where $D$ is a central division algebra of dimension $p^2$ over $K$, and $D$ has a maximal commutative subalgebra isomorphic to $K_{\mathrm{sep}}^{\ker(f_0)}$. Likewise, $K_{\mathrm{sep}}^{\ker(g_0)}$ also embeds into $D$ as a maximal commutative subalgebra. Moreover,

$$[L : K]^2 = \dim_K(A_{\varphi_0}) = \dim_K(M_n(D)) = n^2[D : K] = n^2p^2.$$

Therefore, $n = p^{-1}[L : K]$. □

We know that $A_{\varphi_0}$ is isomorphic to $M_n(D)$ for a division algebra $D$. We want to compute $D$ explicitly and relate its generators to the splitting fields $K_{\mathrm{sep}}^{\ker(f_0)}$ and $K_{\mathrm{sep}}^{\ker(g_0)}$. The proof of the Artin-Wedderburn Theorem shows that $D \cong \mathrm{End}_{A_{\varphi_0}}(S)^{\mathrm{opp}}$ for any minimal left ideal $S$. The same proof also shows that a left ideal $I$ of $A_{\varphi_0}$ is minimal if and only if

$$\dim_K(I) = n[D : K].$$

**Definition 2.5.** Let $\theta = \sum_{t\in\mathrm{Gal}(L/K_{\mathrm{sep}}^{\ker(g_0)})} e_t$ and let $\mathcal{S}$ be the left ideal of $A_{\varphi_0}$ generated by $\theta$.

**Proposition 2.6.** *Let $R$ be a set of left coset representatives for the subgroup $\mathrm{Gal}(L/K_{\mathrm{sep}}^{\ker(g_0)})$ in $\mathrm{Gal}(L/K)$. Then the elements $\{e_s\theta\}_{s\in R}$ form a basis for $\mathcal{S}$ as a left $L$-vector space. Consequently, the dimension of $\mathcal{S}$ as a $K$-vector space satisfies the following equality.*

$$\dim_K(\mathcal{S}) = [K_{\mathrm{sep}}^{\ker(g_0)} : K][L : K] = p[L : K].$$

*Proof.* The elements $\{e_s\theta\}_{s\in\mathrm{Gal}(L/K)}$ span the left $L$-vector space $\mathcal{S} = A_{\varphi_0}\theta$. For any $s \in \mathrm{Gal}(L/K)$,

$$e_s\theta = \sum_{t\in\mathrm{Gal}(L/K_{\mathrm{sep}}^{\ker(g_0)})} e_s e_t = \sum_{t\in\mathrm{Gal}(L/K_{\mathrm{sep}}^{\ker(g_0)})} \varphi_0(s,t)e_{st} = \sum_{t\in\mathrm{Gal}(L/K_{\mathrm{sep}}^{\ker(g_0)})} e_{st}$$

where the last equality holds because $\varphi_0(s,t) = 1$ for all $t \in \mathrm{Gal}(L/K_{\mathrm{sep}}^{\ker(g_0)})$, by definition of $\varphi_0$. In particular, if $s \in \mathrm{Gal}(L/K_{\mathrm{sep}}^{\ker(g_0)})$, then $e_s\theta = \theta$. So, since $R$ is a set of left coset representatives for $\mathrm{Gal}(L/K_{\mathrm{sep}}^{\ker(g_0)})$ in $\mathrm{Gal}(L/K)$, the elements $\{e_s\theta\}_{s\in R}$ span the left $L$-vector space $\mathcal{S}$. In fact, these elements form a left $L$-basis for $\mathcal{S}$. To show linear independence, suppose that

$$\sum_{s\in R} x_s e_s \theta = 0$$

for some coefficients $x_s \in L$. Then

$$0 = \sum_{s\in R} x_s e_s\theta = \sum_{s\in R} x_s \sum_{t\in\mathrm{Gal}(L/K_{\mathrm{sep}}^{\ker(g_0)})} e_{st} = \sum_{r\in\mathrm{Gal}(L/K)} x_r e_r$$

where the coefficients $x_r$ for $r \in \mathrm{Gal}(L/K)$ are given by $x_r = x_s$ where $s \in R$ is the coset representative for the left coset of $\mathrm{Gal}(L/K_{\mathrm{sep}}^{\ker(g_0)})$ in $\mathrm{Gal}(L/K)$ containing $r$. But the elements $\{e_r\}_{r\in\mathrm{Gal}(L/K)}$ form a left $L$-basis for $A_{\varphi_0}$. Therefore, $x_s = 0$ for all $s \in R$. Hence, the elements $\{e_s\theta\}_{s\in R}$ form a left $L$-basis for $\mathcal{S}$, with $\#R$ distinct elements. The cardinality of $R$ satisfies

$$\#R = \frac{\#\,\mathrm{Gal}(L/K)}{\#\,\mathrm{Gal}(L/K_{\mathrm{sep}}^{\ker(g_0)})} = [K_{\mathrm{sep}}^{\ker(g_0)} : K] = p,$$

whereby the dimension of $\mathcal{S}$ as a $K$-vector space is $p[L : K]$, as required. □

**Corollary 2.7.** *If the class of $A_{\varphi_0}$ in $\mathrm{Br}(K)$ is non-trivial, then $\mathcal{S}$ is a minimal left ideal of $A_{\varphi_0}$.*

*Proof.* The proof of the Artin-Wedderburn Theorem shows that a left ideal in $A_{\varphi_0}$ is minimal if and only if its dimension over $K$ is equal to $n[D : K]$, where $A_{\varphi_0} \cong M_n(D)$. By Corollary 2.4, $[D : K] = p^2$ and therefore

$$[L : K]^2 = \dim_K(A_{\varphi_0}) = \dim_K(M_n(D)) = n^2[D : K] = n^2p^2.$$

Thus, a left ideal in $A_{\varphi_0}$ is minimal if and only if its dimension over $K$ is equal to $np^2 = p[L:K]$. □

**Corollary 2.8.** *If $D \neq K$, then $D \cong \mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{opp}$.*

*Proof.* By definition, the class of $A_{\varphi_0}$ in $\mathrm{Br}(K)$ is trivial if and only if $D = K$. The proof of the Artin-Wedderburn Theorem shows that

$$D \cong \mathrm{End}_{A_{\varphi_0}}(I)^{\mathrm{opp}}$$

for any minimal left ideal $I$ of $A_{\varphi_0}$. Therefore, the result follows from Corollary 2.7. □

**Remark 2.9.** If the class of $A_{\varphi_0}$ in $\mathrm{Br}(K)$ is trivial, then $\mathcal{S}$ is no longer a minimal left ideal of $A_{\varphi_0}$. But $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$ is still a central simple algebra over $K$ of dimension $p^2$ with the same class in $\mathrm{Br}(K)$ as $A_{\varphi_0}$. We will prove that $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$ is the algebra $\mathcal{D}$ described in Theorem 1.9.

## 3. Computing the endomorphism ring

We have seen that $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$ gives the class of $A_{\varphi_0}$ in $\mathrm{Br}(K)$. We want to give an explicit description of $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$ in terms of generators and relations. The first step will be to find a maximal commutative subalgebra of dimension $p$ inside $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$.

Recall that $\mathcal{S} = A_{\varphi_0}\theta$, where $\theta = \sum_{t \in \mathrm{Gal}(L/K_{\mathrm{sep}}^{\ker(g_0)})} e_t$. Let $R$ be a set of left coset representatives for $\mathrm{Gal}(L/K_{\mathrm{sep}}^{\ker(g_0)})$ in $\mathrm{Gal}(L/K)$ and let

$$B = \{xe_s \mid x \in L, s \in R\}.$$

Proposition 2.6 tells us that $\mathcal{S} = B\theta$. We would like $B$ to be a subalgebra of $A_{\varphi_0}$, so we want to choose $R$ so that it is a subgroup of $\mathrm{Gal}(L/K)$.

**Lemma 3.1.** *Let $\rho \in H_{M^\vee}/N$ be such that the image of $\rho$ in $H_{M^\vee}/N_g$ generates $H_{M^\vee}/N_g$. Then $R = \{\rho^i\}_{0 \leq i \leq p-1}$ is a set of left coset representatives for $\mathrm{Gal}(L/K_{\mathrm{sep}}^{\ker(g_0)})$ in $\mathrm{Gal}(L/K)$.*

*Proof.* Recall that $\mathrm{Gal}(L/K) = G_K/N$ and $\mathrm{Gal}(L/K_{\mathrm{sep}}^{\ker(g_0)}) = \ker(g_0)/N$. We have $\#R = [K_{\mathrm{sep}}^{\ker(g_0)} : K]$. By Lemma 2.2, $[K_{\mathrm{sep}}^{\ker(g_0)} : K] = p$. Thus, it is enough to show that $\rho^r \in \ker(g_0)/N$ if and only if $p$ divides $r$. We have

$$N_g/N = (H_{M^\vee}/N) \cap (\ker(g_0)/N).$$

By construction, $\rho \in H_{M^\vee}/N$. Hence, $\rho^r \in \ker(g_0)/N$ if and only if $\rho^r \in N_g/N$. But the image of $\rho$ generates $H_{M^\vee}/N_g$ and $[H_{M^\vee} : N_g] = p$, so $\rho^r \in N_g/N$ if and only if $p$ divides $r$. □

From now on, we fix $R = \{\rho^i\}_{0 \leq i \leq p-1}$, so $B$ is a subalgebra of $A_{\varphi_0}$. We want to compute $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$. We know that $\mathcal{S}$ is a principal left ideal generated by $\theta$, so any $\chi \in \mathrm{End}_{A_{\varphi_0}}(\mathcal{S})$ is completely determined by $\chi(\theta)$.

Since $\chi(\theta) \in \mathcal{S} = B\theta$, we have $\chi(\theta) = b\theta$ for some $b \in B$. The question is, which $b$ can occur? In other words, for which $b \in B$ does $\chi : \theta \mapsto b\theta$ extend to a well-defined element of $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})$? The extension of $\chi$ to the whole of $\mathcal{S}$ is given by

$$\chi(c\theta) = c\chi(\theta) \quad \forall\ c \in B.$$

This is well defined because it follows from Proposition 2.6 that any element of $\mathcal{S}$ can be written as $c\theta$ for a *unique* $c \in B$. But it may not be an $A_{\varphi_0}$-endomorphism. We see that $\chi$ gives a well-defined element of $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})$ if and only if

$$\chi(a\theta) = a\chi(\theta) = ab\theta \qquad \forall\ a \in A_{\varphi_0}.$$

The point is that, when we allow multiplication by the whole of $A_{\varphi_0}$ (rather than just the subalgebra $B$), it is possible to have $a_1\theta = a_2\theta$ with $a_1, a_2 \in A_{\varphi_0}$ and $a_1 \neq a_2$. For $\chi$ to give a well-defined element of $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})$, we would also need $a_1b\theta = a_2b\theta$ in this case. Equivalently, $\chi$ extends to a well-defined element of $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})$ if and only if

$$ab\theta = 0 \text{ for all } a \in A_{\varphi_0} \text{ such that } a\theta = 0.$$

Clearly, it suffices for $b$ to commute with $\theta = \sum_{t \in \mathrm{Gal}(L/K_{\mathrm{sep}}^{\ker(g_0)})} e_t$. Hence, it suffices for $b$ to commute with $e_t$ for every $t \in \mathrm{Gal}(L/K_{\mathrm{sep}}^{\ker(g_0)})$. The multiplication on $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})$ is the opposite of the multiplication on $B$ inherited from $A_{\varphi_0}$. Therefore, we can view $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$ as a subalgebra of $B$. We will make this identification from now on. Thus, we have

$$(3.1) \quad B \supset \mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}} \supset \{b \in B \mid e_t b = b e_t \quad \forall t \in \mathrm{Gal}(L/K_{\mathrm{sep}}^{\ker(g_0)})\}.$$

**Remark 3.2.** In fact, a careful analysis of the left annihilator of $\theta$ may be used to show that the rightmost inclusion is an equality. We omit the details of this rather involved calculation and instead demonstrate the equality simply by finding enough elements in the right-hand side and comparing dimensions.

The rightmost inclusion in (3.1) leads us to ask the following question. Which elements of $B$ commute with $e_t$ for every $t \in \mathrm{Gal}(L/K_{\mathrm{sep}}^{\ker(g_0)})$?

**Lemma 3.3.** *The field $K_{\mathrm{sep}}^{\ker(g_0)}$ is a subalgebra of $B$ and every element of $K_{\mathrm{sep}}^{\ker(g_0)}$ commutes with $e_t$ for every $t \in \mathrm{Gal}(L/K_{\mathrm{sep}}^{\ker(g_0)})$. Therefore, $K_{\mathrm{sep}}^{\ker(g_0)}$ is a maximal commutative subalgebra of $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{opp}$.*

*Proof.* Recall that

$$B = \{x e_{\rho^i} \mid x \in L,\ 0 \le i \le p-1\},$$

where $\rho \in H_{M^\vee}/N$ is such that its image generates $H_{M^\vee}/N_g$. Recall the definition of the multiplication in $A_{\varphi_0}$. We have

$$e_s x = s(x) e_s \quad \forall s \in \mathrm{Gal}(L/K), \quad \forall x \in L.$$

Thus, $x \in L$ commutes with $e_s$ if and only if $s(x) = x$. By (3.1), we conclude that $K_{\mathrm{sep}}^{\ker(g_0)} \subset \mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}} \subset B$. Now $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$ is a central simple algebra of dimension $p^2$ over $K$ and $[K_{\mathrm{sep}}^{\ker(g_0)} : K] = p$. Therefore, $K_{\mathrm{sep}}^{\ker(g_0)}$ is a maximal commutative subalgebra of $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$. □

**Lemma 3.4.** $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{opp}$ *is generated as a* $K$*-algebra by the elements of* $K_{\mathrm{sep}}^{\ker(g_0)}$ *together with any element* $d \in \mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{opp} \setminus K_{\mathrm{sep}}^{\ker(g_0)}$*.*

*Proof.* We know that the algebra $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$ has dimension $p^2$ over $K$. Let $d \in \mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}} \setminus K_{\mathrm{sep}}^{\ker(g_0)}$ and let $T$ be the subalgebra of $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$ generated over $K$ by $K_{\mathrm{sep}}^{\ker(g_0)}$ and $d$. Then,

$$K \subset K_{\mathrm{sep}}^{\ker(g_0)} \subsetneq T \subset \mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}.$$

First, suppose that $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$ is a division ring. Then $T$ is also a division ring and we can view $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$ as a left $T$-vector space. We have

$$p^2 = \dim_K \mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}} = (\dim_T \mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}})(\dim_K T).$$

But $\dim_K T > [K_{\mathrm{sep}}^{\ker(g_0)} : K] = p$, whereby $\dim_K T = p^2$ and therefore $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}} = T$.

Now suppose that $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$ is not a division ring. Since it is a central simple algebra of dimension $p^2$ over $K$, the Artin-Wedderburn Theorem tells us that $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}} \cong M_p(K)$. In other words, $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$ is isomorphic to $\mathrm{End}_K(V)$, where $V$ is a $K$-vector space of dimension $p$. Note that $V$ is a faithful $T$-module. Moreover,

$$\dim_{K_{\mathrm{sep}}^{\ker(g_0)}} V = \frac{\dim_K V}{[K_{\mathrm{sep}}^{\ker(g_0)} : K]} = 1.$$

Therefore, $V$ is a simple $K_{\mathrm{sep}}^{\ker(g_0)}$-module, and hence a simple $T$-module. So $T$ has a non-zero faithful simple module, whereby the Jacobson radical of $T$ is zero. Therefore, $T$ is a semisimple $K$-algebra, since $T$ is finite-dimensional over $K$. Now the Artin-Wedderburn Theorem tells us that $T \cong M_m(E)$ for some division ring $E$ over $K$ and some $m \in \mathbb{N}$. Furthermore, any nonzero simple module for $M_m(E)$ is isomorphic to the left ideal $I$ of $M_m(E)$ consisting of matrices with all entries zero except in the first column. In particular,

$$p = \dim_K V = \dim_K I = m[E : K].$$

If $m = 1$ and $[E : K] = p$ then $T \cong E$ and we get a contradiction because $K_{\mathrm{sep}}^{\ker(g_0)}$ is a proper subalgebra of $T$ of dimension $p$ over $K$. Therefore, we must have $m = p$ and $E = K$, whereby $T \cong M_p(K)$. So $T = \mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$, as required. □

**Proposition 3.5.** $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{opp}$ *contains a maximal commutative subalgebra isomorphic to* $K_{\mathrm{sep}}^{\ker(f_0)}$.

*Proof.* Let $\mathcal{T} = A_{\varphi_0} J$ where $J = \sum_{t \in \mathrm{Gal}(L/K_{\mathrm{sep}}^{\ker(f_0)})} e_t$. A similar argument to that of Proposition 2.6 shows that $\dim_K(\mathcal{T}) = p[L : K] = \dim_K(\mathcal{S})$. The algebra $A_{\varphi_0}$ is a central simple algebra, so any two $A_{\varphi_0}$-modules with the same finite dimension are isomorphic. Hence, $\mathcal{T}$ is isomorphic to $\mathcal{S}$ as an $A_{\varphi_0}$-module. Write $\mathcal{T} = \{x e_{\sigma^i} J \mid x \in L,\ 0 \leq i \leq p-1\}$, where $\sigma \in H_M/N$ is such that its image generates $H_M/N_f$. Replacing $\mathcal{S}$ by $\mathcal{T}$ and imitating the proof of Lemma 3.3, we find $K_{\mathrm{sep}}^{\ker(f_0)}$ as a maximal commutative subalgebra of $\mathrm{End}_{A_{\varphi_0}}(\mathcal{T})^{\mathrm{opp}}$. Moreover, $\mathrm{End}_{A_{\varphi_0}}(\mathcal{T})^{\mathrm{opp}} \cong \mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$. □

**Remark 3.6.** In Lemma 3.3, we found $K_{\mathrm{sep}}^{\ker(g_0)}$ as a maximal commutative subalgebra of $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$. Proposition 3.5 tells us that $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$ contains a maximal commutative subalgebra isomorphic to $K_{\mathrm{sep}}^{\ker(f_0)}$. If these two subalgebras are distinct, then together they generate $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$. In this case, in Lemma 3.4 we could choose $d \in \mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}} \setminus K_{\mathrm{sep}}^{\ker(g_0)}$ such that $K(d) \cong K_{\mathrm{sep}}^{\ker(f_0)}$. In fact, in the next two sections we show that we can always choose $d \in \mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}} \setminus K_{\mathrm{sep}}^{\ker(g_0)}$ such that $K(d) \cong K_{\mathrm{sep}}^{\ker(f_0)}$.

## 4. Finding generators

Lemma 3.4 states that $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$ is generated as a $K$-algebra by the elements of $K_{\mathrm{sep}}^{\ker(g_0)}$ together with any element $d \in \mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}} \setminus K_{\mathrm{sep}}^{\ker(g_0)}$. Recall that

$$B = \{x e_{\rho^i} \mid x \in L,\ 0 \leq i \leq p-1\} \subset A_{\varphi_0},$$

where $\rho \in H_{M^\vee}/N$ is such that its image generates $H_{M^\vee}/N_g$. In light of (3.1), we seek an element $d \in B \setminus K_{\mathrm{sep}}^{\ker(g_0)}$ such that $d$ commutes with $e_t$ for all $t \in \mathrm{Gal}(L/K_{\mathrm{sep}}^{\ker(g_0)})$. We can write $d$ in the following way.

$$d = \sum_{i=0}^{p-1} a_i e_{\rho^i} \quad \text{for some } a_i \in L. \tag{4.1}$$

We want to find suitable coefficients $a_i$. We will determine the precise conditions on the $a_i$ which must be satisfied if $d$ is to commute with $e_t$ for all $t \in \mathrm{Gal}(L/K_{\mathrm{sep}}^{\ker(g_0)})$.

**Lemma 4.1.** *We have* $N_f N_g/N = H_M H_{M^\vee}/N$ *as subgroups of* $G_K/N$, *and therefore*

$$\frac{H_M \cap N_g}{N} \cong \frac{H_M}{N_f} \tag{4.2}$$

*and*

$$\frac{H_{M^\vee}\cap N_f}{N}\cong\frac{H_{M^\vee}}{N_g}. \tag{4.3}$$

*Proof.* Clearly, $N_fN_g/N\le H_MH_{M^\vee}/N$, so it remains to show the reverse inclusion. We will show that $H_M/N\le N_fN_g/N$; the argument for $H_{M^\vee}/N$ is identical. Recall that $G_K/N_f\cong H_M/N_f\rtimes G_K/H_M$, where $H_M/N_f$ has order $p$ and $G_K/H_M$ has order coprime to $p$. Thus, any non-trivial normal subgroup of $G_K/N_f$ contains $H_M/N_f$. Since $N_g$ is a normal subgroup of $G_K$, the subgroup $N_fN_g/N_f$ is normal in $G_K/N_f$. Since we are assuming that $N_f\neq N_g$, Lemma 1.4 tells us that $N_fN_g/N_f$ is non-trivial. Therefore, $H_M/N_f\le N_fN_g/N_f$ and hence $H_M/N\le N_fN_g/N$, as required.

To prove the existence of the isomorphism (4.2), we observe that

$$\frac{H_M\cap N_g}{N}\cong\frac{N_f(H_M\cap N_g)}{N_f}=\left(\frac{H_M}{N_f}\right)\cap\left(\frac{N_fN_g}{N_f}\right) \tag{4.4}$$

where the final intersection takes place in $G_K/N_f$. Above, we showed that $N_fN_g/N=H_MH_{M^\vee}/N$. Consequently, $N_fN_g/N_f=H_MH_{M^\vee}/N_f$. Thus, the isomorphism (4.2) follows from (4.4). The argument regarding the isomorphism (4.3) is identical. □

**Lemma 4.2.** *We have*

$$\mathrm{Gal}(L/K_{\mathrm{sep}}^{\ker(g_0)})=\frac{\ker(g_0)}{N}\cong\left(\frac{H_M\cap N_g}{N}\right)\rtimes\left(\frac{\ker(g_0)\cap\ker(f_0)}{N}\right).$$

*Proof.* Recall that $L=K_{\mathrm{sep}}^N$, so $\mathrm{Gal}(L/K_{\mathrm{sep}}^{\ker(g_0)})=\ker(g_0)/N$. By definition, $N=N_f\cap N_g$ and $N_f=H_M\cap\ker(f_0)$. Therefore,

$$\left(\frac{H_M\cap N_g}{N}\right)\cap\left(\frac{\ker(g_0)\cap\ker(f_0)}{N}\right)=0.$$

It remains to show that

$$\Big(\frac{H_M\cap N_g}{N}\Big)\Big(\frac{\ker(g_0)\cap\ker(f_0)}{N}\Big)=\frac{\ker(g_0)}{N}.$$

Lemma 4.1 shows that

$$\frac{H_M\cap N_g}{N}\cong\frac{H_M}{N_f}.$$

Let $s\in\ker(g_0)$. The cocycle $f_0$ gives an isomorphism $H_M/N_f\to M$. So there exists some $h\in H_M\cap N_g$ such that $f_0(h)=f_0(s)$. But then $s=hh^{-1}s$ and $h^{-1}s\in\ker(g_0)\cap\ker(f_0)$. □

We require that $d=e_sde_s^{-1}$ for all $s\in\mathrm{Gal}(L/K_{\mathrm{sep}}^{\ker(g_0)})$. Writing

$$d=\sum_{i=0}^{p-1}a_ie_{\rho^i}$$

with $a_i \in L$, this requirement gives

$$\sum_{i=0}^{p-1} a_i e_{\rho^i} = \sum_{i=0}^{p-1} s(a_i) e_s e_{\rho^i} e_s^{-1}.$$

for all $s \in \mathrm{Gal}(L/K_{\mathrm{sep}}^{\ker(g_0)})$. Recall that $\mathrm{Gal}(L/K_{\mathrm{sep}}^{\ker(g_0)}) = \ker(g_0)/N$. Lemma 4.2 allows us to look separately at conjugation by elements in $(H_M \cap N_g)/N$ and $(\ker(f_0) \cap \ker(g_0))/N$. First, we look at conjugation by $e_t$ for $t \in (\ker(f_0) \cap \ker(g_0))/N$.

**Lemma 4.3.** *For all $t \in (\ker(f_0) \cap \ker(g_0))/N$ and all $i \in \mathbb{Z}$, we have*

$$e_t e_{\rho^i} e_t^{-1} = e_{t\rho^i t^{-1}}.$$

*Proof.* If either $s$ or $t$ is in $(\ker(f_0) \cap \ker(g_0))/N$, then (1.4) gives

$$\varphi_0(s,t) = (s \cdot g_0(t))(f_0(s)) = 1$$

and hence $e_s e_t = e_{st}$. Thus, for all $t \in (\ker(f_0) \cap \ker(g_0))/N$ and for all $i \in \mathbb{Z}$ we have $e_t^{-1} = e_{t^{-1}}$ and $e_t e_{\rho^i} e_t^{-1} = e_t e_{\rho^i} e_{t^{-1}} = e_{t\rho^i t^{-1}}$. □

Lemma 4.1 allows us to assume that $\rho \in (H_{M^\vee} \cap N_f)/N$, which we will do from now on. Lemma 4.1 also shows that $(H_M \cap N_g)/N$ is isomorphic to $H_M/N_f$. Thus, $(H_M \cap N_g)/N$ is a cyclic group of order $p$. Let $\sigma$ be a generator of $(H_M \cap N_g)/N$. In particular, $\sigma$ and $\rho$ act trivially on both $M$ and $M^\vee$. Now we consider conjugation by $e_\sigma$.

**Lemma 4.4.** *For all $i \in \mathbb{Z}$, we have $e_\sigma e_{\rho^i} e_\sigma^{-1} = \zeta^i e_{\rho^i}$, where $\zeta = g(\rho)(f(\sigma))$ is a primitive pth root of unity in $K_{\mathrm{sep}}$.*

*Proof.* Recall that $\sigma \in (H_M \cap N_g)/N$, so $g_0(\sigma) = 0$. Hence, (1.4) gives

$$\varphi_0(t, \sigma^j) = 1 \quad \forall t \in G_K/N,\ \forall j \in \mathbb{Z}.$$

In particular, $e_\sigma^{-1} = e_{\sigma^{-1}}$ and for all $i \in \mathbb{Z}$ we have

$$e_\sigma e_{\rho^i} e_\sigma^{-1} = e_\sigma e_{\rho^i} e_{\sigma^{-1}} = e_\sigma \varphi_0(\rho^i, \sigma^{-1}) e_{\rho^i \sigma^{-1}} = e_\sigma e_{\rho^i \sigma^{-1}} = \varphi_0(\sigma, \rho^i \sigma^{-1}) e_{\rho^i}.$$

The last line holds because $\sigma$ and $\rho$ commute in $G_K/N$, since their commutator is in the intersection of the normal subgroups $(N_g \cap H_M)/N$ and $(N_f \cap H_{M^\vee})/N$, and this intersection is trivial. Now,

$$\begin{array}{rcll} \varphi_0(\sigma, \rho^i \sigma^{-1}) & = & (\sigma \cdot g_0(\rho^i \sigma^{-1}))(f_0(\sigma)) & \\ & = & (\sigma \cdot g_0(\rho^i))(f_0(\sigma)) & \text{since } g_0(\sigma^{-1}) = 0 \\ & = & g(\rho^i)(f(\sigma)) & \text{since } \sigma \text{ acts trivially on } M^\vee \\ & = & (g(\rho)(f(\sigma)))^i & \text{since } g \text{ gives a homomorphism} \\ & & & \text{on } H_{M^\vee}. \end{array}$$

Therefore, it suffices to show that $\zeta = g(\rho)(f(\sigma))$ is a primitive $p$th root of unity. We know that $f$ induces an isomorphism $H_M/N_f \xrightarrow{\sim} M$ and $f(\sigma)$ generates $M$ as an abelian group. Likewise, $g$ induces an isomorphism

$H_{M^\vee}/N_g \xrightarrow{\sim} M^\vee$ and $g(\rho)$ generates $M^\vee = \mathrm{Hom}(M, \mu_p)$ as an abelian group. Thus, $\zeta = g(\rho)(f(\sigma))$ generates $\mu_p$ as an abelian group. □

Let $\zeta = g(\rho)(f(\sigma))$. Combining the results of Lemmas 4.3 and 4.4, we see that $d = \sum_{i=0}^{p-1} a_i e_{\rho^i}$ commutes with $e_t$ for all $t \in \mathrm{Gal}(L/K_{\mathrm{sep}}^{\ker(g_0)})$ if and only if

- $\sigma(a_i) = \zeta^{-i} a_i \quad \forall\, i \in \mathbb{Z}$ with $0 \le i \le p-1$, and
- if $t \in (\ker(f_0) \cap \ker(g_0))/N$ is such that $t\rho t^{-1} = \rho^\ell$, then
$$t(a_i) = a_{\ell i} \quad \forall\, i \in \mathbb{Z} \text{ with } 0 \le i \le p-1.$$

**Proposition 4.5.** *Let $\alpha \in K_{\mathrm{sep}}$ be such that $K_{\mathrm{sep}}^{\ker(f_0)} = K(\alpha)$. For each $i \in \mathbb{Z}$ with $0 \le i \le p-1$, let $a_i = \sum_{j=0}^{p-1} \zeta^{ij} \sigma^j(\alpha)$. Then $d = \sum_{i=0}^{p-1} a_i e_{\rho^i}$ commutes with $e_t$ for all $t \in \mathrm{Gal}(L/K_{\mathrm{sep}}^{\ker(g_0)})$.*

*Proof.* In order to show that $\sigma(a_i) = \zeta^{-i} a_i$, it suffices to show that $\sigma$ fixes $\zeta \in \mu_p$. Recall that $\sigma$ acts trivially on both $M$ and $M^\vee$. By definition, $M^\vee = \mathrm{Hom}(M, \mu_p)$ and therefore the action of $\sigma$ on $\mu_p$ is trivial. Now, let $t \in (\ker(f_0) \cap \ker(g_0))/N$ and suppose that $t\rho t^{-1} = \rho^\ell$. It suffices to show that $t(a_i) = a_{\ell i}$. We have

$$\begin{aligned} t(a_i) &= \sum_{j=0}^{p-1} t(\zeta)^{ij} t\sigma^j(\alpha) = \sum_{j=0}^{p-1} t(\zeta)^{ij} (t\sigma t^{-1})^j t(\alpha) \\ &= \sum_{j=0}^{p-1} t(\zeta)^{ij} (t\sigma t^{-1})^j(\alpha) \end{aligned}$$

since $t$ fixes $\alpha$, because $\alpha \in K_{\mathrm{sep}}^{\ker(f_0)}$. Suppose that $t$ acts as multiplication by $k$ on $M$. Then $t$ acts as multiplication by $k\ell$ on $\mu_p$. We have isomorphisms of $G_K$-modules $H_M/N_f \cong M$ and $H_{M^\vee}/N_g \cong M^\vee$ induced by $f$ and $g$ respectively. Hence,

$$\begin{aligned} t(a_i) &= \sum_{j=0}^{p-1} t(\zeta)^{ij} (t\sigma t^{-1})^j(\alpha) = \sum_{j=0}^{p-1} \zeta^{ijk\ell} \sigma^{jk}(\alpha) \\ &= \sum_{j=0}^{p-1} t(\zeta)^{ij\ell} \sigma^j(\alpha) = a_{\ell i} \end{aligned}$$

as required. □

So we have found an element $d = \sum_{i=0}^{p-1} a_i e_{\rho^i} \in B$ such that $d$ commutes with $e_t$ for all $t \in \mathrm{Gal}(L/K_{\mathrm{sep}}^{\ker(g_0)})$. By (3.1), this means that $d \in \mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$. We want to show that the $K$-algebra $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$ is generated by $d$ together with the elements of $K_{\mathrm{sep}}^{\ker(g_0)}$. By Lemma 3.4, it only remains to check that $d \notin K_{\mathrm{sep}}^{\ker(g_0)}$. It suffices to show that some $a_i$ with $i \geq 1$ is nonzero.

**Proposition 4.6.** *Write* $K_{\mathrm{sep}}^{\ker(f_0)} = K(\alpha)$ *with* $\mathrm{Tr}_{K_{\mathrm{sep}}^{\ker(f_0)}/K}(\alpha) = 0$. *For each* $i \in \mathbb{Z}$ *with* $0 \leq i \leq p-1$, *let* $a_i = \sum_{j=0}^{p-1} \zeta^{ij}\sigma^j(\alpha)$. *Then there exists* $i \geq 1$ *with* $a_i \neq 0$. *Consequently,* $d = \sum_{i=0}^{p-1} a_i e_{\rho^i}$ *is not in* $L$.

*Proof.* Let $V$ denote the Vandermonde matrix $(\zeta^{ij})_{0 \leq i,j \leq p-1}$. Then $a_i$ is the $i$th row of $V(\alpha, \sigma(\alpha), \ldots, \sigma^{p-1}(\alpha))^T$. Also,

$$\det(V) = \prod_{0 \leq i < j \leq p-1} (\zeta^j - \zeta^i) \neq 0.$$

Thus, $V(\alpha, \sigma(\alpha), \ldots, \sigma^{p-1}(\alpha))^T$ is nonzero, so it has at least one nonzero row. In other words, at least one of the $a_i$'s is nonzero. But

$$a_0 = \alpha + \sigma(\alpha) + \cdots + \sigma^{p-1}(\alpha) = \mathrm{Tr}_{K_{\mathrm{sep}}^{\ker(f_0)}/K}(\alpha) = 0.$$

Hence, there exists $i \geq 1$ with $a_i \neq 0$, as required. □

**Remark 4.7.** Since we assumed from the start that the characteristic of $K$ is not $p$, we can subtract $p^{-1}\,\mathrm{Tr}_{K_{\mathrm{sep}}^{\ker(f_0)}/K}(\alpha)$ from any generator $\alpha$ of $K_{\mathrm{sep}}^{\ker(f_0)}/K$ to ensure that $\mathrm{Tr}_{K_{\mathrm{sep}}^{\ker(f_0)}/K}(\alpha) = 0$.

**Corollary 4.8.** $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{opp}$ *is generated as a* $K$*-algebra by the elements of* $K_{\mathrm{sep}}^{\ker(g_0)}$ *together with the element* $d$ *described in Proposition 4.6.*

*Proof.* Lemma 3.4 states that $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$ is generated as a $K$-algebra by the elements of $K_{\mathrm{sep}}^{\ker(g_0)}$ together with any $d \in \mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}} \setminus K_{\mathrm{sep}}^{\ker(g_0)}$. By (3.1) and Proposition 4.5 the $d$ of Proposition 4.6 satisfies $d \in \mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$. By Proposition 4.6, this $d$ also satisfies $d \notin K_{\mathrm{sep}}^{\ker(g_0)}$. □

## 5. A minimal polynomial

Our next aim is to show that the $K$-subalgebra of $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$ generated by $d$ is isomorphic to $K(\alpha) = K_{\mathrm{sep}}^{\ker(f_0)}$. We will do this by showing that $d$ and $p\alpha$ satisfy the same minimal polynomial over $K$. Recall that $\sigma$ is a generator for $(H_M \cap N_g)/N$ and $\rho$ is a generator for $(H_{M^\vee} \cap N_f)/N$. Recall that $\alpha \in K_{\mathrm{sep}}$ is such that $K_{\mathrm{sep}}^{\ker(f_0)} = K(\alpha)$ and $\mathrm{Tr}_{K_{\mathrm{sep}}^{\ker(f_0)}/K}(\alpha) = 0$. Let $\zeta = \varphi_0(\sigma, \rho) = g(\rho)(f(\sigma))$ and for $i \in \mathbb{Z}$ with $0 \leq i \leq p-1$ let $a_i = \sum_{j=0}^{p-1} \zeta^{ij}\sigma^j(\alpha)$. We have $d = \sum_{i=0}^{p-1} a_i e_{\rho^i}$. Similarly, let $\beta \in K_{\mathrm{sep}}$ be such that $K_{\mathrm{sep}}^{\ker(g_0)} = K(\beta)$ and $\mathrm{Tr}_{K_{\mathrm{sep}}^{\ker(g_0)}/K}(\beta) = 0$. For $i \in \mathbb{Z}$ with $0 \leq i \leq p-1$, let $b_i = \sum_{j=0}^{p-1} \zeta^{ij}\rho^j(\beta)$. In the proof of Proposition 4.6, we showed that $a_i \neq 0$ for some $i \geq 1$. The same argument shows that $b_m \neq 0$ for some $m \geq 1$. Choose such a $b_m$ and denote it by $\mathcal{B}$. We would like to define a polynomial with roots $\mathcal{B}^k d\mathcal{B}^{-k}$ for $0 \leq k \leq p-1$. We will show that $\mathcal{B}^k d\mathcal{B}^{-k}$ commutes with $\mathcal{B}^\ell d\mathcal{B}^{-\ell}$ for every $k, \ell \in \mathbb{Z}$, so that $P(X) = \prod_{k=0}^{p-1}(X - \mathcal{B}^k d\mathcal{B}^{-k})$ is the desired polynomial. First, we prove two auxiliary lemmas.

**Lemma 5.1.** *For all $k \in \mathbb{Z}$, we have*

$$\mathcal{B}^k d\mathcal{B}^{-k} = \sum_{i=0}^{p-1} \zeta^{ikm} a_i e_{\rho^i} = \sum_{i=0}^{p-1} \sigma^{-km}(a_i) e_{\rho^i},$$

*where $\mathcal{B} = b_m = \sum_{j=0}^{p-1} \zeta^{mj} \rho^j(\beta) \neq 0$.*

*Proof.* We have

$$\begin{aligned} \mathcal{B}^k d\mathcal{B}^{-k} = &\quad \mathcal{B}^k \sum_{i=0}^{p-1} a_i e_{\rho^i} \mathcal{B}^{-k} = \sum_{i=0}^{p-1} a_i \mathcal{B}^k e_{\rho^i} \mathcal{B}^{-k} = \sum_{i=0}^{p-1} a_i \mathcal{B}^k \rho^i(\mathcal{B}^{-k}) e_{\rho^i} \\ = &\quad \sum_{i=0}^{p-1} a_i \mathcal{B}^k \zeta^{ikm} \mathcal{B}^{-k} e_{\rho^i} = \sum_{i=0}^{p-1} \zeta^{ikm} a_i e_{\rho^i} = \sum_{i=0}^{p-1} \sigma^{-km}(a_i) e_{\rho^i}. \end{aligned}$$

□

**Lemma 5.2.** *For all $i, j, k \in \mathbb{Z}$, we have $e_{\rho^i} \sigma^k(a_j) e_{\rho^j} = \sigma^k(a_j) e_{\rho^{i+j}}$.*

*Proof.* Since $\rho \in (H_{M^\vee} \cap N_f)/N$, clearly $\rho$ fixes $\zeta$ and $\alpha$. Therefore, $\rho$ fixes $\sigma^k(a_j) = \sum_{\ell=0}^{p-1} \zeta^{j\ell} \sigma^{\ell+k}(\alpha)$. Moreover, $f(\rho) = 0$ and so (1.4) gives $\varphi_0(\rho^i, \rho^j) = 1$ for all $i, j \in \mathbb{Z}$. Hence,

$$e_{\rho^i} \sigma^k(a_j) e_{\rho^j} = \rho^i \sigma^k(a_j) e_{\rho^i} e_{\rho^j} = \sigma^k(a_j) \varphi_0(\rho^i, \rho^j) e_{\rho^{i+j}} = \sigma^k(a_j) e_{\rho^{i+j}}.$$

□

**Corollary 5.3.** *For all $k, \ell \in \mathbb{Z}$, $\mathcal{B}^k d\mathcal{B}^{-k}$ commutes with $\mathcal{B}^\ell d\mathcal{B}^{-\ell}$.*

*Proof.* By Lemma 5.1, we have

$$\mathcal{B}^k d\mathcal{B}^{-k} \mathcal{B}^\ell d\mathcal{B}^{-\ell} = \sum_{0 \leq i, j \leq p-1} \sigma^{-km}(a_i) e_{\rho^i} \sigma^{-\ell m}(a_j) e_{\rho^j}.$$

By Lemma 5.2, this is equal to

$$\sum_{0 \leq i, j \leq p-1} \sigma^{-km}(a_i) \sigma^{-\ell m}(a_j) e_{\rho^{i+j}} = \mathcal{B}^\ell d\mathcal{B}^{-\ell} \mathcal{B}^k d\mathcal{B}^{-k}.$$

□

**Proposition 5.4.** *Let $P(X) = \prod_{k=0}^{p-1}(X - \mathcal{B}^k d\mathcal{B}^{-k})$. Then the coefficients of $P$ lie in $K$.*

Since $K$ is the centre of $A_{\varphi_0}$, it suffices to show that the coefficients of $P$ commute with every element of $A_{\varphi_0}$. As a $K$-algebra, $A_{\varphi_0}$ is generated by the elements of $L$ and $\{e_s\}_{s\in\mathrm{Gal}(L/K)}$. We prove Proposition 5.4 in three steps.

**Lemma 5.5.** *The coefficients of $P$ commute with $x$ for every $x \in L$.*

*Proof.* We chose $\rho$ to be a generator of $(H_{M^\vee} \cap N_f)/N$. By Lemma 4.1, $(H_{M^\vee} \cap N_f)/N$ is isomorphic to $H_{M^\vee}/N_g$. Now $H_{M^\vee}/N_g$ is isomorphic to $M^\vee$ and therefore has cardinality $p$. Hence, $[L : L^{\langle\rho\rangle}] = p$ and consequently $L = L^{\langle\rho\rangle}(x)$ for any $x \in L \setminus L^{\langle\rho\rangle}$. Since $\mathcal{B} = b_m$ for some $m \in \mathbb{Z}$ with $1 \le m \le p-1$, we have $\rho(\mathcal{B}) = \zeta^{-m}\mathcal{B} \neq \mathcal{B}$. Therefore, $L = L^{\langle\rho\rangle}(\mathcal{B})$. Observe that conjugation by $\mathcal{B}$ permutes the roots of $P$. For any $x \in L^{\langle\rho\rangle}$, we have $xdx^{-1} = d$, since $\rho^i(x) = x$ for such $x$. Hence, conjugation by $x \in L^{\langle\rho\rangle}$ fixes the roots of $P$. Therefore, conjugation by any element of $L$ fixes the coefficients of $P$. □

**Lemma 5.6.** *The coefficients of $P$ commute with $e_t$ $\forall t \in \mathrm{Gal}(L/K_{\mathrm{sep}}^{\ker(g_0)})$.*

*Proof.* By construction, $d$ commutes with $e_t$ for all $t \in \mathrm{Gal}(L/K_{\mathrm{sep}}^{\ker(g_0)})$. Suppose $t \in \mathrm{Gal}(L/K_{\mathrm{sep}}^{\ker(g_0)})$ is such that $t$ acts as multiplication by $k$ on $M$ and $t$ acts as multiplication by $\ell$ on $M^\vee$. Then $t\sigma t^{-1} = \sigma^k$, because $f$ induces an isomorphism of $G_K$-modules $H_M/N_f \cong M$. Similarly, we have $t\rho t^{-1} = \rho^\ell$. By definition of the action on $M^\vee = \mathrm{Hom}(M, \mu_p)$, we have $t(\zeta) = \zeta^{k\ell}$. Therefore,

$$\begin{aligned} e_t\mathcal{B}e_t^{-1} = t(\mathcal{B}) &= \sum_{j=0}^{p-1} t(\zeta)^{mj}(t\rho t^{-1})^j t(\beta) = \sum_{j=0}^{p-1} \zeta^{mjk\ell}\rho^{j\ell}t(\beta) \\ &= \sum_{j=0}^{p-1} \zeta^{mjk}\rho^j t(\beta) = \sum_{j=0}^{p-1} \zeta^{mjk}\rho^j(\beta) \end{aligned}$$

because $\beta \in K_{\mathrm{sep}}^{\ker(g_0)}$ and $t \in \mathrm{Gal}(L/K_{\mathrm{sep}}^{\ker(g_0)})$. Hence,

$$\begin{aligned} e_t\mathcal{B}d\mathcal{B}^{-1}e_t^{-1} = t(\mathcal{B})dt(\mathcal{B})^{-1} &= t(\mathcal{B})\sum_{i=0}^{p-1} a_i e_{\rho^i} t(\mathcal{B})^{-1} \\ &= \sum_{i=0}^{p-1} t(\mathcal{B})a_i\rho^i(t(\mathcal{B}))^{-1}e_{\rho^i} = \sum_{i=0}^{p-1} t(\mathcal{B})(\zeta^{-ikm}t(\mathcal{B}))^{-1}a_i e_{\rho^i} \\ &= \sum_{i=0}^{p-1} \zeta^{ikm}a_i e_{\rho^i} = \mathcal{B}^k d\mathcal{B}^{-k} \end{aligned}$$

by Lemma 5.1. Thus, we see that conjugation by $e_t$ for $t \in \mathrm{Gal}(L/K_{\mathrm{sep}}^{\ker(g_0)})$ permutes the roots of $P$. Consequently, the coefficients of $P$ commute with $e_t$ for all $t \in \mathrm{Gal}(L/K_{\mathrm{sep}}^{\ker(g_0)})$. □

**Lemma 5.7.** *The coefficients of $P$ commute with $e_t$ $\forall t \in \mathrm{Gal}(L/K)$.*

*Proof.* By Lemma 5.6, the coefficients of $P$ commute with $e_t$ for all $t$ in $\mathrm{Gal}(L/K_{\mathrm{sep}}^{\ker(g_0)})$. Thus, it suffices to prove that the coefficients of $P$ commute with $e_t$ for all $t$ in some set $R$ of left coset representatives for $\mathrm{Gal}(L/K_{\mathrm{sep}}^{\ker(g_0)})$ in $\mathrm{Gal}(L/K)$.
By Lemma 3.1, $R$ can be taken to be $\{\rho^i\}_{0\leq i\leq p-1}$. Since $f_0(\rho) = 0$, (1.4) gives $\varphi_0(\rho^i, t) = 1$ for all $t \in \mathrm{Gal}(L/K)$ and all $i \in \mathbb{Z}$. Hence, $e_{\rho^i} = e_\rho^i$ for all $i \in \mathbb{Z}$ and it suffices to show that the coefficients of $P$ commute with $e_\rho$. By Lemma 5.1,

$$e_\rho \mathcal{B}^k d\mathcal{B}^{-k} e_\rho^{-1} = e_\rho \sum_{i=0}^{p-1} \zeta^{ikm} a_i e_{\rho^i} e_\rho^{-1} = \sum_{i=0}^{p-1} \zeta^{ikm} e_\rho a_i e_{\rho^i} e_\rho^{-1} \tag{5.1}$$

because $\zeta$ is fixed by $\rho$, since $\rho \in (H_{M^\vee} \cap N_f)/N$. By Lemma 5.2, we have

$$\sum_{i=0}^{p-1} \zeta^{ikm} e_\rho a_i e_{\rho^i} e_\rho^{-1} = \sum_{i=0}^{p-1} \zeta^{ikm} a_i e_{\rho^{i+1}} e_\rho^{-1} = \sum_{i=0}^{p-1} \zeta^{ikm} a_i e_{\rho^i}. \tag{5.2}$$

Thus, equations (5.1) and (5.2) give $e_\rho \mathcal{B}^k d\mathcal{B}^{-k} e_\rho^{-1} = \mathcal{B}^k d \mathcal{B}^{-k}$ for all $k \in \mathbb{Z}$ with $0 \leq k \leq p-1$. Hence, the coefficients of $P$ commute with $e_\rho$. □

Combining Lemma 5.5 and Lemma 5.7, we see that the coefficients of $P$ lie in the centre of $A_{\varphi_0}$, which is $K$. Thus, we have proved Proposition 5.4.

**Definition 5.8.** Let $Q(X)$ be the minimal polynomial of $p\alpha$ over $K$,

$$Q(X) = \prod_{i=0}^{p-1} (X - \sigma^i(p\alpha)).$$

We will show that $P = Q$ and thus conclude that $P$ is irreducible and $K(d) \cong K(\alpha)$.

**Definition 5.9.** We define $R(X,Y) = \prod_{k=0}^{p-1} (X - \sum_{i=0}^{p-1} \sigma^k(a_i) Y^i)$.

**Lemma 5.10.** *We have $P(X) = R(X, e_\rho)$ and $Q(X) = R(X, 1)$.*

*Proof.* Since $\rho \in (H_{M^\vee} \cap N_f)/N$, we have $f_0(\rho) = 0$ and consequently $\varphi_0(\rho^i, \rho^j) = 1$ for all $i, j \in \mathbb{Z}$. Therefore, $e_\rho^i = e_{\rho^i}$ for all $i \in \mathbb{Z}$. Thus, the equality $P(X) = R(X, e_\rho)$ follows from Lemma 5.1. Regarding the second claim, we have

$$R(X,1) = \prod_{k=0}^{p-1} (X - \sum_{i=0}^{p-1} \sigma^k(a_i)) = \prod_{k=0}^{p-1} (X - \sigma^k\Big(\sum_{i=0}^{p-1} a_i\Big)).$$

Observe that

$$\sum_{i=0}^{p-1} a_i = \sum_{i=0}^{p-1}\sum_{j=0}^{p-1} \zeta^{ij}\sigma^j(\alpha) = \sum_{j=0}^{p-1} \sigma^j(\alpha) \sum_{i=0}^{p-1} \zeta^{ij} = p\alpha$$

because $\sum_{i=0}^{p-1} \zeta^{ij} = 0$ unless $j = 0$. This proves that $R(X, 1) = Q(X)$. □

**Proposition 5.11.** *We have $P(X) = Q(X)$.*

*Proof.* Write $R(X,Y) = \sum_{i=0}^{p-1}\sum_{j=0}^{N} c_{ij} X^i Y^j$, where $N = (p-1)^2$ and $c_{ij} \in L$. Then

$$R(X,Y) = \sum_{i=0}^{p-1} X^i \sum_{k=0}^{p-1} \sum_{j \equiv k \pmod p} c_{ij} Y^j$$

where the innermost sum runs over $j \in \mathbb{Z}$ with $0 \le j \le N$. Therefore,

$$P(X) = R(X, e_\rho) = \sum_{i=0}^{p-1} X^i \sum_{k=0}^{p-1} e_\rho^k \sum_{j \equiv k \pmod p} c_{ij}$$

because $\rho$ has order $p$ in $\mathrm{Gal}(L/K)$, so $e_\rho^p = 1$. Hence, the coefficient of $X^i$ is $\sum_{k=0}^{p-1} e_\rho^k \sum_{j\equiv k \pmod p} c_{ij}$. By Lemma 5.4, the coefficients of $P$ lie in $K$. Therefore,

$$\sum_{j \equiv k \pmod p} c_{ij} = 0,$$

unless $k = 0$. Consequently,

$$R(X,Y) = \sum_{i=0}^{p-1} X^i \sum_{j \equiv 0 \pmod p} c_{ij} Y^j. \tag{5.3}$$

Since $e_\rho^p = 1$, (5.3) gives $P(X) = R(X, e_\rho) = R(X, 1) = Q(X)$. □

**Corollary 5.12.** *The minimal polynomial of $d$ over $K$ is $P$ and therefore $K(d)$ is isomorphic to $K(\alpha) = K_{\mathrm{sep}}^{\ker(f_0)}$.*

*Proof.* Proposition 5.11 shows that $d$ and $p\alpha$ are roots of the same polynomial over $K$. This polynomial is irreducible because it is the minimal polynomial of $p\alpha$. The characteristic of $K$ is not $p$, so $p$ is invertible and $K(d) \cong K(p\alpha) = K(\alpha)$. □

## 6. The multiplicative structure

Now that we have found generators for the $K$-algebra $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$, it remains to describe its multiplicative structure. Recall that $\alpha \in K_{\mathrm{sep}}$ is such that $K_{\mathrm{sep}}^{\ker(f_0)} = K(\alpha)$ and $\mathrm{Tr}_{K_{\mathrm{sep}}^{\ker(f_0)}/K}(\alpha) = 0$. Similarly, $\beta \in K_{\mathrm{sep}}$ is such that $K_{\mathrm{sep}}^{\ker(g_0)} = K(\beta)$ and $\mathrm{Tr}_{K_{\mathrm{sep}}^{\ker(g_0)}/K}(\beta) = 0$.

**Definition 6.1.** Let

$$z = p^{-1}d = p^{-1}\sum_{i=0}^{p-1} a_i e_{\rho^i},$$

where $a_i = \sum_{j=0}^{p-1}\zeta^{ij}\sigma^j(\alpha)$. Thus, by Proposition 5.11, the minimal polynomial of $z$ over $K$ is the same as that of $\alpha$.

Corollary 4.8 tells us that the algebra $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$ is generated over $K$ by $\beta$ and $z$. The elements $\beta^i z^j$ for $i, j \in \mathbb{Z}$ with $0 \leq i, j \leq p-1$ form a basis for $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$ as a $K$-vector space. To specify the multiplication on $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$, it is enough to specify structure constants $c_{ij} \in K$ such that

$$z\beta = \sum_{0\leq i,j\leq p-1} c_{ij}\beta^i z^j.$$

**Lemma 6.2.** *For all $j \in \mathbb{Z}$ with $0 \leq j \leq p-1$, we have*

$$z^j = p^{-1}\sum_{k=0}^{p-1} h_{jk} e_{\rho^k}$$

*where $h_{jk} = \sum_{\ell=0}^{p-1}\zeta^{k\ell}\sigma^\ell(\alpha^j) \in L^{\langle\rho\rangle} = K_{\mathrm{sep}}^{N_f\cap H_{M^\vee}}$.*

*Proof.* It is easily seen that $h_{0k} = 0$ for all $k \in \mathbb{Z}$ with $1 \leq k \leq p-1$, and $h_{00} = p$. Thus, the statement holds for $j = 0$. The statement for $j = 1$ follows immediately from the definition of $z$, upon observing that $h_{1k} = a_k$ for all $k \in \mathbb{Z}$ with $0 \leq k \leq p-1$. We proceed by induction on $j$. Suppose that

$$z^m = p^{-1}\sum_{k=0}^{p-1} h_{mk} e_{\rho^k}$$

for some $m \in \mathbb{Z}$ with $0 \leq m \leq p-2$. Then,

$$\begin{aligned} z^{m+1} = z^m z &= \Big(p^{-1}\sum_{k=0}^{p-1} h_{mk} e_{\rho^k}\Big)\Big(p^{-1}\sum_{i=0}^{p-1} a_i e_{\rho^i}\Big) \\ &= p^{-2}\sum_{i,k=0}^{p-1} h_{mk} a_i e_{\rho^{k+i}} \qquad \text{by Lemma 5.2} \\ &= p^{-2}\sum_{n,k=0}^{p-1} h_{mk} a_{n-k} e_{\rho^n}. \end{aligned}$$

Hence, it suffices to prove that

$$\sum_{k=0}^{p-1} h_{mk} a_{n-k} = p h_{(m+1)n}.$$

We have

$$\sum_{k=0}^{p-1} h_{mk}a_{n-k} = \sum_{k,\ell,j=0}^{p-1} \zeta^{k\ell}\sigma^{\ell}(\alpha^m)\zeta^{(n-k)j}\sigma^j(\alpha)$$
$$= \sum_{\ell,j=0}^{p-1} \zeta^{nj}\sigma^{\ell}(\alpha^m)\sigma^j(\alpha)\sum_{k=0}^{p-1}\zeta^{k(\ell-j)}.$$

Now observe that $\sum_{k=0}^{p-1}\zeta^{k(\ell-j)}$ equals zero when $\ell \neq j$, and equals $p$ when $\ell = j$. This concludes the proof. □

We want to find structure constants $c_{ij} \in K$ for all integers $i$ and $j$ with $0 \le i, j \le p-1$ such that

$$z\beta = \sum_{0\le i,j\le p-1} c_{ij}\beta^i z^j. \tag{6.1}$$

By the definition of $z$,

$$z\beta = p^{-1}\sum_{i=0}^{p-1} a_i e_{\rho^i}\beta = p^{-1}\sum_{i=0}^{p-1} a_i\rho^i(\beta)e_{\rho^i}. \tag{6.2}$$

Using Lemma 6.2, we expand the right-hand side of (6.1) as

$$\sum_{i,j=0}^{p-1} c_{ij}\beta^i z^j = p^{-1}\sum_{i,j=0}^{p-1} c_{ij}\beta^i\sum_{k=0}^{p-1} h_{jk}e_{\rho^k}. \tag{6.3}$$

Equating (6.2) and (6.3), we obtain for every integer $k$ with $0 \le k \le p-1$

$$a_k\rho^k(\beta) = \sum_{i,j=0}^{p-1} c_{ij}\beta^i h_{jk}. \tag{6.4}$$

Recall that $N_g = \ker(g_0) \cap H_{M^\vee}$, so $K_{\mathrm{sep}}^{N_g} = K_{\mathrm{sep}}^{H_{M^\vee}}(\beta)$. Moreover, $N_g$ is a normal subgroup of $G_K$, so $K_{\mathrm{sep}}^{H_{M^\vee}}(\beta)$ is Galois over $K$. Write

$$\rho^k(\beta) = \sum_{i=0}^{p-1} m_{ik}\beta^i \tag{6.5}$$

for $m_{ik} \in K_{\mathrm{sep}}^{H_{M^\vee}} \subset L^{\langle\rho\rangle}$. We know that $L/L^{\langle\rho\rangle}$ has degree $p$ and is generated by $\beta$. Thus, the elements $1, \beta, \ldots \beta^{p-1}$ form a basis for $L$ as a vector space over $L^{\langle\rho\rangle}$. Therefore, combining (6.4) and (6.5) gives

$$a_k m_{ik} = \sum_{j=0}^{p-1} c_{ij}h_{jk} \tag{6.6}$$

for all $i, k \in \mathbb{Z}$ with $0 \le i, k \le p-1$.

**Definition 6.3.** We define three $p$-by-$p$ matrices $X$, $Y$ and $Z$.

$$X=(a_k m_{ik})_{i,k}, \quad Y=(c_{ik})_{i,k}, \quad Z=(h_{ik})_{i,k}.$$

In all three cases, the indices $i$ and $k$ run from 0 to $p-1$.

In terms of these matrices, (6.6) becomes $X=YZ$, where $Y$ is to be found. We know that such a $Y$ exists and is unique because the elements $\beta^i z^j$ for $i,j\in\mathbb{Z}$ with $0\leq i,j\leq p-1$ form a basis for $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$.

**Lemma 6.4.** *The matrix $Z$ is invertible. Thus, $Y=XZ^{-1}$.*

*Proof.* Suppose for contradiction that $Z$ is not invertible. Then $Z$ has a nontrivial kernel and there exists a nonzero matrix $T$ such that $TZ=0$. But then $(Y+T)Z=YZ=X$. This contradicts the fact that $Y$ is unique. □

**Corollary 6.5.** *The algebra $\mathcal{D}$ described in Theorem 1.9 is $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{opp}$.*

*Proof.* The algebra $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$ has a basis $\{\beta^i z^j\}_{0\leq i,j\leq p-1}$ as a $K$-vector space, where $z$ satisfies the same minimal polynomial over $K$ as $\alpha$, and the multiplication satisfies

$$z\beta=\sum_{i,j=0}^{p-1} c_{ij}\beta^i z^j$$

where $(c_{ij})_{i,j}=XZ^{-1}$ for $X$ and $Z$ as defined in Definition 6.3. Recall that $G_K/N_f\cong H_M/N_f\rtimes G_K/H_M$, where $H_M/N_f$ has order $p$ and $G_K/H_M$ has order coprime to $p$. Thus, any non-trivial normal subgroup of $G_K/N_f$ contains $H_M/N_f$. Therefore, the normal closure of $K_{\mathrm{sep}}^{\ker(f_0)}$ in $K_{\mathrm{sep}}$ is equal to $K_{\mathrm{sep}}^{N_f}$. Since $\rho$ is a generator for $(H_{M^\vee}\cap N_f)/N$, $\rho$ acts trivially on the normal closure of $K_{\mathrm{sep}}^{\ker(f_0)}(\mu_p)$ and non-trivially on $\beta$. Likewise, $\sigma$ acts trivially on the normal closure of $K_{\mathrm{sep}}^{\ker(g_0)}(\mu_p)$ and non-trivially on $\alpha$. Therefore, $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$ is the algebra $\mathcal{D}$ described in Theorem 1.9. □

## 7. An example

We apply Theorem 1.9 to the case $M=\mu_p$. In this case, any 1-cocycle $f_0$ which represents a non-trivial element $f\in H^1(G_K,M)$ has $K_{\mathrm{sep}}^{\ker(f_0)}=K(\alpha)$, where $\alpha^p\in K^*$. By definition of the Tate dual, $G_K$ acts trivially on $M^\vee$. Thus, $H^1(G_K,M^\vee)=\mathrm{Hom}(G_K,\mathbb{Z}/p\mathbb{Z})$ and any non-trivial $g\in H^1(G_K,M^\vee)$ corresponds to a degree $p$ Galois extension $K_{\mathrm{sep}}^{\ker(g)}/K$. Let $K_{\mathrm{sep}}^{\ker(g)}=K_{\mathrm{sep}}(\beta)$ with $\mathrm{Tr}_{K(\beta)/K}(\beta)=0$. Let $\sigma\in G_K$ be such that $\sigma$ fixes $K(\beta,\mu_p)$ and $\sigma(\alpha)/\alpha=\zeta$ for some primitive $p$th root of unity $\zeta$. Choose $\rho\in G_K$ such that $\rho$ fixes $K(\alpha,\mu_p)$ and $(g(\rho))(f_0(\sigma))=\zeta$. We calculate

$$h_{ij}=\sum_{\ell=0}^{p-1}\zeta^{j\ell}\sigma^\ell(\alpha^i)=\sum_{\ell=0}^{p-1}\zeta^{(i+j)\ell}\alpha^i.$$

Hence, $h_{ij} = 0$ unless $i + j \equiv 0 \pmod p$. Write $\rho^j(\beta) = \sum_{i=0}^{p-1} m_{ij}\beta^i$ for $m_{ij} \in K$. An easy matrix calculation shows that

$$(h_{1j}m_{ij})_{i,j}(h_{ij})_{i,j}^{-1} = \begin{pmatrix} 0 & m_{0(p-1)} & 0 & \dots & 0 \\ 0 & m_{1(p-1)} & 0 & \dots & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & m_{(p-1)(p-1)} & 0 & \dots & 0 \end{pmatrix}.$$

Now Theorem 1.9 tells us that the class of $f \cup g$ in $\mathrm{Br}(K)$ is given by the algebra $\mathcal{D}$ with $K$-basis $\{\beta^i z^j\}_{0 \le i,j \le p-1}$, where $z^p = \alpha^p \in K$, and we have

$$z\beta z^{-1} = \sum_{i=0}^{p-1} m_{i(p-1)}\beta^i = \rho^{-1}(\beta).$$

So in this case $\mathcal{D}$ is a cyclic algebra of dimension $p^2$ over $K$.

**Acknowledgements.** I would like to thank my Ph.D. supervisor Tim Dokchitser for suggesting this problem and for his excellent support and guidance throughout my Ph.D. I am grateful to Hendrik Lenstra for a very detailed discussion of my work and for many suggestions for its improvement, in particular for pointing out a gap in the proof of Lemma 3.4 and providing the rest of the argument. I would like to thank Vladimir Dokchitser, Charles Vial, Rishi Vyas and James Newton for several useful discussions. I am grateful to the referee of this paper for many helpful comments and suggestions which have improved the exposition. I was supported by an EPSRC scholarship for the duration of this research.

## References

[1] P. Gille and T. Szamuely, *Central simple algebras and Galois cohomology*, Cambridge University Press, (2006).

[2] N. Jacobson, *Basic Algebra II*, W. H. Freeman and Co., San Francisco, Calif., USA, (1980).

[3] V. A. Kolyvagin, *Finiteness of* $E(\mathbb{Q})$ *and* $Ш(E, \mathbb{Q})$ *for a subclass of Weil curves*, Izv. Akad. Nauk SSSR Ser. Mat. **52**, 3 (1988), 522–540.

[4] V. A. Kolyvagin, *On the Mordell-Weil and Shafarevich-Tate groups for Weil elliptic curves*, Izv. Akad. Nauk SSSR Ser. Mat. **52**, 6 (1988), 1154–1180.

[5] A. Pillons, *Exposé 7. – Cup-produit* in *Cohomologie Galoisienne des Modules Finis*, Ed. G. Poitou, Travaux et Recherches Mathématiques, Dunod Paris, (1967).

[6] I. Reiner, *Maximal Orders*, London Mathematical Society Monographs New Series, Clarendon Press, Oxford, UK, (2003).

[7] J.-P. Serre, *Local Fields*, Graduate Texts in Mathematics 67, Springer-Verlag New York, Inc., New York, (1979).

[8] J. Tate, *Duality theorems in Galois cohomology over number fields*, Proc. Int. Congress Math. Stockholm (1962), 288–295.

Rachel Newton
Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany
*E-mail*: rachel@mpim-bonn.mpg.de
*URL*: http://quests.mpim-bonn.mpq.de/rachel/