Realising the cup-product of local Tate duality

Rachel Newton

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 order 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.

Introduction

Let K be any field and let M be a G_K-module of prime cardinality p, where p is not equal to $\mathrm{char}(K)$. In this paper, we give an explicit description of the following cup-product which occurs in the statement of local Tate duality:

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

The main result is Theorem 1.6 where, given elements $0 \neq f \in H^1(G_K, M)$ and $0 \neq g \in H^1(G_K, M^\vee)$, we construct a central simple algebra $\mathcal{D}$ such that

1. The class of $\mathcal{D}$ in $\mathrm{Br}(K)$ 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 $f \cup g \neq 0$.

In the prime order case, 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) more amenable to explicit computation.

1   The Artin-Wedderburn theorem and local Tate duality

Let K be a field. We will consider K to be fixed throughout the paper and will use the following notation:

K_s a fixed separable closure of K

G_K the absolute Galois group of K, $G_K = \mathrm{Gal}(K_s/K)$

M a G_K-module of cardinality p prime and not divisible by $\mathrm{char}(K)$

μ_p the group of pth roots of unity in K_s

$M^\vee$ the Tate dual of M, $M^\vee = \mathrm{Hom}(M, \mu_p)$.

For elements $f, g, \varphi, \ldots$ of cohomology groups, we often employ the notation $f_0, g_0, \varphi_0, \ldots$ to refer to a choice of representative cocycles. From now on, we fix $0 \neq f \in H^1(G_K, M)$ and $0 \neq g \in H^1(G_K, M^\vee)$. 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 $G_K \to \mathrm{Aut}(M)$. Let H_M denote the kernel of this map and consider the inflation-restriction exact sequence

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

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

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

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

Therefore, the restriction map gives an isomorphism

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

Let N_f denote the kernel of the restriction of f to H_M. Then the isomorphism above shows that $N_f \triangleleft G_K$. 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.

Lemma 1.1. *If $N_f = N_g$, then M and $M^\vee$ are isomorphic as G_K-modules.*

Proof. We have isomorphisms of G_K-modules $H_M/N_f \to M$ and $H_{M^\vee}/N_g \to M^\vee$ induced by f and g respectively. So it suffices to show that $H_M/N_f = H_{M^\vee}/N_g$. But H_M/N_f is the unique Sylow p-subgroup of $G_K/N_f \cong H_M/N_f \rtimes G_K/H_M$ and $H_{M^\vee}/N_g$ is also an order p subgroup of $G_K/N_f = G_K/N_g$. $\square$

Corollary 1.2. *If $N_f = N_g$ and $p > 2$, then $f \cup g = 0$.*

Proof. By the lemma above, we know that M and $M^\vee$ are isomorphic as G_K-modules. 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 $\operatorname{Res} : H^1(G_K, M) \to H^1(H_M, M) = \operatorname{Hom}(H_M, M)$ is injective, so it suffices to show that $\operatorname{Res}(g) = n\operatorname{Res}(f)$ for some $n \in \mathbb{Z}$. Now $\operatorname{Res}(f)$ and $\operatorname{Res}(g)$ 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. $\square$

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

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

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 $H^1(G_K/N, M)$, which we will also call g. Now, the properties of the cup-product mean that the following diagram commutes:

$$
\begin{array}{ccc}
H^1(G_K, M) \times H^1(G_K, M^\vee) & \xrightarrow{\cup} & H^2(G_K, \mu_p) \\
\text{Inf} \big\uparrow \qquad\qquad \text{Inf} \big\uparrow & & \text{Inf} \big\uparrow \\
H^1(G_K/N, M) \times H^1(G_K/N, M^\vee) & \xrightarrow{\cup} & H^2(G_K/N, \mu_p)
\end{array}
$$

Therefore, we can reduce to studying the cup-product

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

Let $L = K_s^N$ 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 $s \in G_K$ and all $m \in M$. Hence, μ_p is fixed by all elements in $H_M \cap H_{M^\vee}$, so $\mu_p \subset L^*$. We have the following commutative diagram:

$$
\begin{array}{ccc}
H^2(G_K, \mu_p) \hookrightarrow H^2(G_K, K_s^*) & \xrightarrow{\cong} & \mathrm{Br}(K) \\
\text{Inf} \big\uparrow & & \big\uparrow \\
H^2(\mathrm{Gal}(L/K), \mu_p) \longrightarrow H^2(\mathrm{Gal}(L/K), L^*) & \xrightarrow{\cong} & \mathrm{Br}(L/K)
\end{array}
$$

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 ϑ to the central simple algebra A_ϑ as defined below.

Definition 1.3. Let L/K be a finite Galois extension and let $\vartheta \in Z^2(\mathrm{Gal}(L/K), L^*)$ be a 2-cocycle. Define the K-algebra A_ϑ 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_ϑ is a central simple algebra of dimension $[L : K]^2$ over K. See, for example, [3], where this is Theorem 29.12.

Definition 1.4. Let $\varphi = f \cup g$. Fix representative cocycles f_0, g_0 for f, g respectively. The formula given in the remark at the end of §2.4 of [2] tells us that a representative 2-cocycle for φ is $\varphi_0 : \mathrm{Gal}(L/K) \times \mathrm{Gal}(L/K) \to \mu_p$, given by

$$\varphi_0(s, t) = (s \cdot g_0(t))(f_0(s)). \tag{3}$$

Lemma 1.5. *If $N_f = N_g$ and $p = 2$, then $f \cup g$ corresponds to a quaternion algebra generated by x, y such that $K(x) \cong K_s^{N_f}$, $x^2 \in K^*$, $y^2 = -1$ and $yx = -xy$. Consequently, $f \cup g = 0$ if and only if $-1 \in N_{K_s^{N_f}/K}(K_s^{N_f})$.*

Proof. This follows from the explicit construction of a central simple algebra given above. By [1], Theorem 8.14, the quaternion algebra A_{φ_0} is a division ring if and only if $y^2 \notin N_{K(x)/K}(K(x))$. $\square$

Having dealt with the case $N_f = N_g$ for all p, henceforth we assume that $N_f \neq N_g$. Below, we state the main result which will be proved in this paper.

Theorem 1.6. *Write $K_s^{\ker(f_0)} = K(\alpha)$, $K_s^{\ker(g_0)} = K(\beta)$ with $\mathrm{Tr}_{K(\alpha)/K}(\alpha) = 0 = \mathrm{Tr}_{K(\beta)/K}(\beta)$. Let $\sigma \in G_K$ be such that σ fixes 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 β. 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 $m_{ij} \in K_s^{H_{M^\vee}}$. 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 α, 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 $\mathrm{Br}(K)$.

Corollary 1.7. *Suppose that $p = 2$. Then $f \cup g$ corresponds to a quaternion algebra over K, generated by two elements x and y such that $K(x) \cong K_s^{\ker(g_0)}$ and $K(y) \cong K_s^{\ker(f_0)}$, 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 the Theorem 1.6. 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 [1], Theorem 8.14. $\qquad\square$

The algebra A_{φ_0} has dimension at most $p^4(p-1)^4$ over K. 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. The quantity $\sqrt{\dim_K(D)}$ is called the *index* of A_{φ_0}.

Lemma 1.8. $K_s^{\ker(f_0)}/K$ *and* $K_s^{\ker(g_0)}/K$ *are degree p subextensions of L which split A_{φ_0}.*

Proof. First, note 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, $K_s^{\ker(f_0)}/K$ is a degree p extension. Since $N \subset N_f \subset \ker(f_0)$, we have $K_s^{\ker(f_0)} \subset L$. The following diagram commutes:

$$
\begin{array}{ccc}
H^2(\mathrm{Gal}(L/K), L^*) & \overset{\cong}{\longrightarrow} & \mathrm{Br}(L/K) \\
\big\downarrow{\scriptstyle\mathrm{Res}} & & \big\downarrow \\
H^2(\mathrm{Gal}(L/K_s^{\ker(f_0)}), L^*) & \overset{\cong}{\longrightarrow} & \mathrm{Br}\big(L/K_s^{\ker(f_0)}\big)
\end{array}
\qquad(4)
$$

where the map $\mathrm{Br}(L/K) \to \mathrm{Br}\big(L/K_s^{\ker(f_0)}\big)$ is induced by $A \mapsto A \otimes_K K_s^{\ker(f_0)}$. The restriction of f to $\ker(f_0)$ is trivial in $H^1(\ker(f_0), M)$, 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 (4) shows that $A_{\varphi_0} \otimes_K K_s^{\ker(f_0)}$ is trivial in $\operatorname{Br}(L/K_s^{\ker(f_0)})$. In other words, $K_s^{\ker(f_0)}$ splits A_{φ_0}. The argument for $K_s^{\ker(g_0)}$ is analogous.

$\square$

Remark 1.9. 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 $K_s^{\ker(f_0)}$ in L is changed. But the K-isomorphism class of the field $K_s^{\ker(f_0)}$ only depends on f.

Corollary 1.10. *Suppose that the class of A_{φ_0} in $\operatorname{Br}(K)$ is non-trivial. Then A_{φ_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_{φ_0} is equal to its period, p. Moreover, $K_s^{\ker(f_0)}$ and $K_s^{\ker(g_0)}$ embed into D as maximal commutative subalgebras.*

Proof. The index of A_{φ_0} is the greatest common divisor of the degrees of finite separable extensions which split A_{φ_0}. The extension $K_s^{\ker(f_0)}/K$ splits A_{φ_0}. Since $K_s^{\ker(f_0)}/K$ has degree p, the index of A_{φ} 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 $K_s^{\ker(f_0)}$. Likewise, $K_s^{\ker(g_0)}$ also embeds into D as a maximal commutative subalgebra. Moreover, A_{φ_0} has K-dimension $[L : K]^2 = n^2[D : K] = n^2 p^2$. Therefore, $n = p^{-1}[L : K]$. $\square$

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

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

Definition 1.11. Let $\theta = \sum_{t \in \operatorname{Gal}(L/K_s^{\ker(g_0)})} e_t$ and let $\mathcal{S}$ be the left ideal of A_{φ_0} generated by θ.

Proposition 1.12. *We have $\mathcal{S} = \{xe_s\theta \mid x \in L, s \in R\}$, where R is a set of left coset representatives for $\mathrm{Gal}(L/K_s^{\mathrm{ker}(g_0)})$ in $\mathrm{Gal}(L/K)$. Moreover, the dimension of $\mathcal{S}$ as a K-vector space satisfies the following equality:*

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

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 $s \in \mathrm{Gal}(L/K)$, we have

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

where the last equality holds because $\varphi_0(s,t) = 1$ for all $t \in \mathrm{Gal}(L/K_s^{\mathrm{ker}(g_0)})$, by definition of φ_0. In particular, if $s \in \mathrm{Gal}(L/K_s^{\mathrm{ker}(g_0)})$, we have $e_s\theta = \theta$. So if R is a set of left coset representatives for $\mathrm{Gal}(L/K_s^{\mathrm{ker}(g_0)})$ 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 we have

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

But the elements $\{e_r\}_{r \in \mathrm{Gal}(L/K)}$ form a left L-basis for A_{φ_0}. Therefore, we must have $x_s = 0$ 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 is

$$\frac{|\mathrm{Gal}(L/K)|}{|\mathrm{Gal}(L/K_s^{\mathrm{ker}(g_0)})|} = [K_s^{\mathrm{ker}(g_0)} : K] = p,$$

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

Corollary 1.13. *If the class of A_{φ_0} in $\mathrm{Br}(K)$ is non-trivial, then $\mathcal{S}$ is a minimal left ideal of A_{φ_0}.*

Proof. The proof of the Artin-Wedderburn Theorem shows that a left ideal in A_{φ_0} is minimal if and only if its dimension over K is equal to $n[D:K]$, where $A_{\varphi_0} \cong M_n(D)$. If the class of A_{φ_0} in $\mathrm{Br}(K)$ is non-trivial, then we have

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

Thus, a left ideal in A_{φ_0} is minimal if and only if its dimension over K is equal to $np^2 = p[L:K]$. $\qquad\square$

Corollary 1.14. *If $D \neq K$, then $D \cong \mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{opp}$.*

Proof. By definition, the class of A_{φ_0} in $\mathrm{Br}(K)$ is trivial if and only if $D = K$. The proof of the Artin-Wedderburn Theorem shows that $D \cong \mathrm{End}_{A_{\varphi_0}}(S)^{\mathrm{opp}}$ for any minimal left ideal S of A_{φ_0}. Thus, the result follows from Corollary 1.13. $\qquad\square$

Remark 1.15. If the class of A_{φ_0} in $\mathrm{Br}(K)$ is trivial, then $\mathcal{S}$ is no longer a minimal left ideal of A_{φ_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_{φ_0}. We will prove that $\mathcal{D} = \mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$ is as described in Theorem 1.6.

2   Computing the endomorphism ring

Let R be a set of left coset representatives for $\mathrm{Gal}(L/K_s^{\ker(g_0)})$ in $\mathrm{Gal}(L/K)$ and let $B = \{xe_s \mid x \in L, s \in R\}$. Proposition 1.12 tells us that $\mathcal{S} = A_{\varphi_0}\theta = B\theta$. We would like B to be a subalgebra of A_{φ_0}, so we want to choose R so that it is a subgroup of $\mathrm{Gal}(L/K)$.

Lemma 2.1. *Let $\rho \in H_{M^\vee}/N$ be such that its image generates $H_{M^\vee}/N_g$. Then $R = \{\rho^i\}_{0 \leq i \leq p-1}$ is a set of left coset representatives for $\mathrm{Gal}(L/K_s^{\ker(g_0)})$ in $\mathrm{Gal}(L/K)$.*

Proof. We have $\#R = [K_s^{\ker(g_0)} : K] = p$. Thus, it is enough to show that $\rho^r \in \mathrm{Gal}(L/K_s^{\ker(g_0)}) = \ker(g_0)/N$ if and only if p divides r. But $\rho \in H_{M^\vee}/N$ and $N_g/N = H_{M^\vee}/N \cap \ker(g_0)/N$. Hence, $\rho^r \in \ker(g_0)/N$ if and only if $\rho^r \in N_g/N$. But the image of ρ 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. $\qquad\square$

From now on, we fix $R = \{\rho^i\}_{0 \leq i \leq p-1}$, so B is a subalgebra of A_{φ_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 θ, 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 χ 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 any element of $\mathcal{S}$ can be written as $c\theta$ for a *unique* $c \in B$. But it may not be an A_{φ_0}-endomorphism. We see that χ 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, when we allow multiplication by the whole of A_{φ_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 χ to give a well-defined element of $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})$, we would also need $a_1 b\theta = a_2 b\theta$ in this case. Equivalently, χ 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 $\theta = \sum_{t \in \mathrm{Gal}(L/K_s^{\mathrm{ker}(g_0)})} e_t$. Hence, it suffices for b to commute with e_t for every $t \in \mathrm{Gal}(L/K_s^{\mathrm{ker}(g_0)})$. The multiplication on $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})$ is the opposite of the multiplication on B inherited from A_{φ_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

$$B \supset \mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}} \supset \{b \in B \mid e_t b = b e_t \quad \forall t \in \mathrm{Gal}(L/K_s^{\mathrm{ker}(g_0)})\}. \quad (5)$$

Remark 2.2. In fact, a careful analysis of the left-annihilator of θ 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 (5) leads us to ask the following question. Which elements of B commute with e_t for all $t \in \mathrm{Gal}(L/K_s^{\mathrm{ker}(g_0)})$? Recall that

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

where $\rho \in H_{M^\vee}/N \le G_K/N = \mathrm{Gal}(L/K)$ is such that its image generates $H_{M^\vee}/N_g$. Therefore, there is an obvious subalgebra of B whose elements commute with e_t for every $t \in \mathrm{Gal}(L/K_s^{\mathrm{ker}(g_0)})$; namely the field $K_s^{\mathrm{ker}(g_0)}$. This is by definition of the multiplication in A_{φ_0}; recall that

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

Thus, $x \in L$ commutes with e_s if and only if $s(x) = x$.

Lemma 2.3. $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{opp}$ *is generated as a K-algebra by the elements of* $K_s^{\mathrm{ker}(g_0)}$ *and any element* $d \in \mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{opp} \setminus K_s^{\mathrm{ker}(g_0)}$.

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

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

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

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

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

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

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

Therefore, V is a simple $K_s^{\ker(g_0)}$-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 $K_s^{\ker(g_0)}$ 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 $T = \operatorname{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$, as required. $\qquad\square$

Proposition 2.4. $\operatorname{End}_{A_{\varphi_0}}(\mathcal{S})^{opp}$ *contains a maximal commutative subalgebra isomorphic to* $K_s^{\ker(f_0)}$.

Proof. Let $\mathcal{T} = A_{\varphi_0}\vartheta$ with $\vartheta = \sum_{t \in \mathrm{Gal}(L/K_s^{\mathrm{ker}(f_0)})} e_t$. A similar argument to that of Proposition 1.12 shows that $\dim_K(\mathcal{T}) = p[L : K] = \dim_K(\mathcal{S})$. A_{φ_0} is a central simple algebra, so any two A_{φ_0}-modules with the same finite dimension are isomorphic. Hence, $\mathcal{T}$ is isomorphic to $\mathcal{S}$ as an A_{φ_0}-module. In analogy with Lemma 2.1, choose $\mathcal{R} = \{\sigma^i\}_{0 \leq i \leq p-1}$ where $\sigma \in H_M/N$ is such that its image generates H_M/N_f. Replacing $\mathcal{S}$ by $\mathcal{T}$ and following the arguments leading up to Lemma 2.3, we find $K_s^{\mathrm{ker}(f_0)}$ as a subalgebra of $\mathrm{End}_{A_{\varphi_0}}(\mathcal{T})^{\mathrm{opp}} \cong \mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$. $\qquad\square$

Previously, we found $K_s^{\mathrm{ker}(g_0)}$ as a maximal commutative subalgebra of $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$, because the elements of $K_s^{\mathrm{ker}(g_0)}$ commute with e_t for all $t \in \mathrm{Gal}(L/K_s^{\mathrm{ker}(g_0)})$. In view of Proposition 2.4 above, we see that $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$ contains a maximal commutative subalgebra isomorphic to $K_s^{\mathrm{ker}(f_0)}$. Therefore, if these two subalgebras are distinct, then together they generate the whole of $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$. In this case, in Lemma 2.3 we could choose $d \in \mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}} \setminus K_s^{\mathrm{ker}(g_0)}$ such that $K(d) \cong K_s^{\mathrm{ker}(f_0)}$.

3 Finding generators

In light of (5) and Lemma 2.3, we seek an element $d \in B \setminus K_s^{\mathrm{ker}(g_0)}$ such that d commutes with e_t for all $t \in \mathrm{Gal}(L/K_s^{\mathrm{ker}(g_0)})$. Recall that

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

where $\rho \in H_{M^\vee}/N \leq G_K/N = \mathrm{Gal}(L/K)$ is such that its image generates $H_{M^\vee}/N_g$. Thus, we can write d in the form

$$d = \sum_{i=0}^{p-1} a_i e_{\rho^i} \text{ with } a_i \in L. \tag{6}$$

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 $t \in \mathrm{Gal}(L/K_s^{\mathrm{ker}(g_0)})$.

Lemma 3.1. *We have $N_f N_g/N = H_M H_{M^\vee}/N$ and therefore*

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

and

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

Proof. Clearly, $N_f N_g/N \leq H_M H_{M^\vee}/N$, so it remains to show the reverse inclusion. We will show that $H_M/N \leq N_f N_g/N$; the argument for $H_{M^\vee}/N$ is identical. Observe that $G_K/N_f \cong H_M/N_f \rtimes G_K/H_M$, where $H_M/N_f \cong M$ has order p and $G_K/H_M \hookrightarrow \text{Aut}(M)$ has order prime to p. Thus, any non-trivial normal subgroup of G_K/N_f contains H_M/N_f. Since $N_g \lhd G_K$, the subgroup $N_f N_g/N_f$ is normal in G_K/N_f and $N_f N_g/N_f$ is non-trivial since we are assuming that $N_f \neq N_g$. Therefore, $H_M/N_f \leq N_f N_g/N_f$ and hence $H_M/N \leq N_f N_g/N$, as required. The last part follows by observing that

$$\frac{H_M \cap N_g}{N} \cong \frac{N_f(H_M \cap N_g)}{N_f} = \frac{N_f N_g}{N_f} \cap \frac{H_M}{N_f}$$

and noting that $N_f N_g/N = H_M H_{M^\vee}/N$ implies that $N_f N_g/N_f = H_M H_{M^\vee}/N_f$. $\square$

Lemma 3.2. *We have*

$$\text{Gal}(L/K_s^{\ker(g_0)}) = \frac{\ker(g_0)}{N} \cong \frac{H_M \cap N_g}{N} \rtimes \frac{\ker(g_0) \cap \ker(f_0)}{N}.$$

Proof. Clearly, $\frac{H_M \cap N_g}{N} \cap \frac{\ker(g_0) \cap \ker(f_0)}{N} = 0$. It remains to show that

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

Lemma 3.1 shows that $\frac{H_M \cap N_g}{N} \cong \frac{H_M}{N_f}$. The cocycle f_0 gives an isomorphism $\frac{H_M}{N_f} \to M$. So, if $s \in \ker(g_0)$, 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 $h^{-1}s \in \ker(g_0) \cap \ker(f_0)$. $\square$

We require that

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

for all $s \in \mathrm{Gal}(L/K_s^{\ker(g_0)}) = \ker(g_0)/N$. Lemma 3.2 allows us to look sepa-
rately 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 3.3. *For all $t \in (\ker(f_0) \cap \ker(g_0))/N$, 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 (3) 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 $t \in (\ker(f_0) \cap \ker(g_0))/N$, we have $e_t^{-1} = e_{t^{-1}}$ and $e_t e_{\rho^i} e_t^{-1} = e_t e_{\rho^i} e_{t^{-1}} = e_{t\rho^i t^{-1}}$. $\square$

Lemma 3.1 shows that $(H_M \cap N_g)/N \cong H_M/N_f$ is a cyclic group of order
p. Let σ be a generator of $(H_M \cap N_g)/N$. Lemma 3.1 allows us to assume
that $\rho \in (N_f \cap H_{M^\vee})/N$, which we will do from now on. In particular, σ and
ρ act trivially on both M and $M^\vee$. Now we consider conjugation by e_σ.

Lemma 3.4. *We have $e_\sigma e_{\rho^i} e_\sigma^{-1} = \zeta^i e_{\rho^i}$, where $\zeta = g(\rho)(f(\sigma)) \in K_s$ is a
primitive pth root of unity.*

Proof. Recall that $\sigma \in (H_M \cap N_g)/N$, so $g(\sigma) = 0$. Hence, (3) gives

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

In particular, $e_\sigma^{-1} = e_{\sigma^{-1}}$ and 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 σ and ρ commute in G_K/N, since their commutator is in the intersection of the normal subgroups $(N_g \cap H_M)/N$ and $(N_f \cap H_{M^\vee})/N$, which is trivial. Now,

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

Therefore, it suffices to show that $\zeta = g(\rho)(f(\sigma))$ is a primitive pth 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 μ_p as an abelian group. $\qquad\square$

Combining the results of Lemmas 3.3 and 3.4, we see that $d = \sum_{i=0}^{p-1} a_i e_{\rho^i}$ commutes with e_t for all $t \in \mathrm{Gal}(L/K_s^{\mathrm{ker}(g_0)})$ if and only if

- $\sigma(a_i) = \zeta^{-i} a_i \quad \forall\, 0 \le i \le p-1$, and

- if $t \in (\mathrm{ker}(f_0) \cap \mathrm{ker}(g_0))/N$ is such that $t\rho t^{-1} = \rho^\ell$, then

$$
t(a_i) = a_{\ell i} \quad \forall\, 0 \le i \le p-1.
$$

Proposition 3.5. *Let $\alpha \in K_s^{\mathrm{ker}(f_0)}$ be such that $K_s^{\mathrm{ker}(f_0)} = K(\alpha)$. For each $0 \le i \le p-1$, 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 $t \in \mathrm{Gal}(L/K_s^{\mathrm{ker}(g_0)})$.*

Proof. In order to show that $\sigma(a_i) = \zeta^{-i} a_i$, it suffices to show that σ fixes $\zeta \in \mu_p$. But σ acts trivially on both M and $M^\vee = \mathrm{Hom}(M, \mu_p)$, so σ must also act trivially on μ_p. Now, let $t \in (\mathrm{ker}(f_0) \cap \mathrm{ker}(g_0))/N$ and suppose that

$t\rho t^{-1} = \rho^\ell$. It suffices to show that $t(a_i) = a_{\ell i}$. We have

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

$$= \sum_{j=0}^{p-1} t(\zeta)^{ij}(t\sigma t^{-1})^j(\alpha) \qquad \text{since } t \text{ fixes } \alpha \in K_s^{\text{ker}(f_0)}.$$

Suppose that t acts as multiplication by k on M. Then t acts as multiplication by $k\ell$ on μ_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,

$$t(a_i) = \sum_{j=0}^{p-1} t(\zeta)^{ij}(t\sigma t^{-1})^j(\alpha) = \sum_{j=0}^{p-1} \zeta^{ijk\ell} \sigma^{jk}(\alpha)$$

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

as required. □

So we have demonstrated a candidate for d. It remains to check that this element is not in $K_s^{\text{ker}(g_0)}$. It suffices to show that some a_i with $i \geq 1$ is nonzero.

Proposition 3.6. *Let α be such that $K_s^{\text{ker}(f_0)} = K(\alpha)$ and $\text{Tr}_{K_s^{\text{ker}(f_0)}/K}(\alpha) = 0$. Then there exists $i \geq 1$ with $a_i = \sum_{j=0}^{p-1} \zeta^{ij} \sigma^j(\alpha)$ nonzero. 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 ith 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

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

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

Since we assumed from the start that the characteristic of K is not p, we can always arrange that $\mathrm{Tr}_{K_s^{\mathrm{ker}(f_0)}/K}(\alpha) = 0$, by subtracting $p^{-1}\,\mathrm{Tr}_{K_s^{\mathrm{ker}(f_0)}/K}(\alpha)$ from α. Thus, by Lemma 2.3 $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$ is generated as a K-algebra by d together with the elements of $K_s^{\mathrm{ker}(g_0)}$.

4 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 $K(\alpha) = K_s^{\mathrm{ker}(f_0)}$. We will do this by showing that d and $p\alpha$ satisfy the same minimal polynomial over K. Let σ be a generator for $(N_g \cap H_M)/N$ and let ρ be a generator for $(N_f \cap H_{M^\vee})/N$. Recall that $\alpha \in L$ is such that $K_s^{\mathrm{ker}(f_0)} = K(\alpha)$ and $\mathrm{Tr}_{K_s^{\mathrm{ker}(f_0)}/K}(\alpha) = 0$. We have $d = \sum_{i=0}^{p-1} a_i e_{\rho^i}$, where $a_i = \sum_{j=0}^{p-1} \zeta^{ij} \sigma^j(\alpha)$ and $\zeta = \varphi_0(\sigma, \rho) = g(\rho)(f(\sigma))$. Similarly, let β be such that $K_s^{\mathrm{ker}(g_0)} = K(\beta)$ and $\mathrm{Tr}_{K_s^{\mathrm{ker}(g_0)}/K}(\beta) = 0$. Let $b_i = \sum_{j=0}^{p-1} \zeta^{ij} \rho^j(\beta)$. In the proof of Proposition 3.6, 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 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 4.1. *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

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

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

$\square$

Lemma 4.2. *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 $\rho \in (N_f \cap H_{M^\vee})/N$, clearly ρ fixes $\sigma^k(a_j) = \sum_{\ell=0}^{p-1} \zeta^{j\ell} \sigma^{\ell+k}(\alpha)$. Moreover, $f(\rho) = 0$ and so (3) gives $\varphi_0(\rho^i, \rho^j) = 1$ for all $i, j \in \mathbb{Z}$. Hence,

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

$\square$

Corollary 4.3. *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 4.1, 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 4.2, this is equal to

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

$\square$

Proposition 4.4. *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_{φ_0}, it suffices to show that the coefficients of P commute with every element of A_{φ_0}. As a K-algebra, A_{φ_0} is generated by the elements of L and $\{e_s\}_{s \in \mathrm{Gal}(L/K)}$. We prove Proposition 4.4 in three steps.

Lemma 4.5. *The coefficients of P commute with x for every $x \in L$.*

Proof. We know that ρ generates $(N_f \cap H_{M^\vee})/N \cong H_{M^\vee}/N_g \cong M^\vee$, which has cardinality p. Therefore, $[L : L^{\langle \rho \rangle}] = p$ and $L = L^{\langle \rho \rangle}(x)$ for any $x \in L \setminus L^{\langle \rho \rangle}$. Since $\mathcal{B} = b_m$ for some $1 \leq m \leq p-1$, 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. $\qquad\square$

Lemma 4.6. *The coefficients of P commute with e_t for all t in $\mathrm{Gal}(L/K_s^{\mathrm{ker}(g_0)})$.*

Proof. By construction, d commutes with e_t for all $t \in \mathrm{Gal}(L/K_s^{\mathrm{ker}(g_0)})$. Suppose $t \in \mathrm{Gal}(L/K_s^{\mathrm{ker}(g_0)})$ is such that t acts as multiplication by k on M and t acts as multiplication by ℓ 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, $t\rho t^{-1} = \rho^\ell$. By definition of the action on $M^\vee = \mathrm{Hom}(M, \mu_p)$, we have $t(\zeta) = \zeta^{k\ell}$. Therefore,

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

$$= \sum_{j=0}^{p-1} \zeta^{mjk}\rho^j t(\beta) = \sum_{j=0}^{p-1} \zeta^{mjk}\rho^j(\beta)$$

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

$$e_t \mathcal{B} d \mathcal{B}^{-1} e_t^{-1} = t(\mathcal{B})dt(\mathcal{B})^{-1} = t(\mathcal{B})\sum_{i=0}^{p-1} a_i e_{\rho^i} t(\mathcal{B})^{-1} = \sum_{i=0}^{p-1} t(\mathcal{B})a_i \rho^i(t(\mathcal{B}))^{-1}e_{\rho^i}$$

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

by Lemma 4.1. Thus, we see that conjugation by e_t for $t \in \mathrm{Gal}(L/K_s^{\mathrm{ker}(g_0)})$ permutes the roots of P. Consequently, the coefficients of P commute with e_t for all $t \in \mathrm{Gal}(L/K_s^{\mathrm{ker}(g_0)})$. $\qquad\square$

Lemma 4.7. *The coefficients of P commute with e_t for every t in $\mathrm{Gal}(L/K)$.*

Proof. By Lemma 4.6, the coefficients of P commute with e_t for all $t \in \mathrm{Gal}(L/K_s^{\mathrm{ker}(g_0)})$. 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 $\mathrm{Gal}(L/K_s^{\mathrm{ker}(g_0)})$ in $\mathrm{Gal}(L/K)$. By Lemma 2.1, R can be taken to be $\{\rho^i\}_{0 \le i \le p-1}$. Since $f(\rho) = 0$, (3) gives $\varphi(\rho^i, t) = 1$ for all $t \in G_K/N$ and all $i \in \mathbb{Z}$. Hence, $e_{\rho^i} = e_\rho^i$ and it suffices to show that the coefficients of P commute with e_ρ. By Lemma 4.1,

$$e_\rho \mathcal{B}^k d \mathcal{B}^{-k} e_\rho^{-1} = e_\rho \sum_{i=0}^{p-1} \zeta^{ikm} a_i e_{\rho^i} e_\rho^{-1} = \sum_{i=0}^{p-1} \zeta^{ikm} e_\rho a_i e_{\rho^i} e_\rho^{-1} \tag{7}$$

because ζ is fixed by $\rho \in (N_f \cap H_{M^\vee})/N$. By Lemma 4.2, we have

$$\sum_{i=0}^{p-1} \zeta^{ikm} e_\rho a_i e_{\rho^i} e_\rho^{-1} = \sum_{i=0}^{p-1} \zeta^{ikm} a_i e_{\rho^{i+1}} e_\rho^{-1}. \tag{8}$$

We have $\rho \in (N_f \cap H_{M^\vee})/N \subset \mathrm{ker}(f_0)/N$, whereby for all $j \in \mathbb{Z}$ and all $s \in G_K/N$ we have $\varphi_0(\rho^j, s) = (\rho^j \cdot g_0(s))(f_0(\rho^j)) = 1$. Hence, $e_{\rho^{-1}} = e_\rho^{-1}$ and

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

Therefore, equations (7) and (8) give $e_\rho \mathcal{B}^k d \mathcal{B}^{-k} e_\rho^{-1} = \mathcal{B}^k d \mathcal{B}^{-k}$ for all $0 \le k \le p-1$. Hence, the coefficients of P commute with e_ρ.

$\qquad\square$

Combining Lemma 4.5 and Lemma 4.7, we see that the coefficients of P lie in the centre of A_{φ_0}, which is K. Thus, we have proved Proposition 4.4.

Definition 4.8. 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 4.9. We define $R(X, Y) = \prod_{k=0}^{p-1} (X - \sum_{i=0}^{p-1} \sigma^k(a_i)Y^i)$.

Lemma 4.10. *We have $P(X) = R(X, e_\rho)$ and $Q(X) = R(X, 1)$.*

Proof. Since $\rho \in (N_f \cap H_{M^\vee})/N$, we have $f_0(\rho) = 0$ and $\varphi_0(\rho^i, \rho^j) = 1 \quad \forall i, j \in \mathbb{Z}$. Therefore, $e_\rho^i = e_{\rho^i} \quad \forall i \in \mathbb{Z}$. Thus, the equality $P(X) = R(X, e_\rho)$ follows from Lemma 4.1. Regarding the second claim, we have

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

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 completes the proof that $R(X, 1) = Q(X)$. $\square$

Proposition 4.11. *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 $0 \leq j \leq N$. 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 ρ 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 4.4, the coefficients of P lie in K. Therefore,

$$\sum_{j \equiv k \pmod p} c_{ij} = 0, \quad \text{unless k=0}.$$

Whereby

$$R(X,Y) = \sum_{i=0}^{p-1} X^i \sum_{j \equiv 0 \pmod p} c_{ij} Y^j. \tag{9}$$

Since $e_\rho^p = 1$, (9) gives $P(X) = R(X, e_\rho) = R(X, 1) = Q(X)$. $\square$

Corollary 4.12. *P is the minimal polynomial of d over K and $K(d) \cong K(\alpha) = K_s^{\mathrm{ker}(f_0)}$.*

Proof. Proposition 4.11 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 $K(d) \cong K(p\alpha) = K(\alpha)$. $\square$

5 The multiplication rule

Recall that $\alpha \in K_s$ is such that $K_s^{\mathrm{ker}(f_0)} = K(\alpha)$ and $\mathrm{Tr}_{K_s^{\mathrm{ker}(f_0)}/K}(\alpha) = 0$. Similarly, $\beta \in K_s$ is such that $K_s^{\mathrm{ker}(g_0)} = K(\beta)$ and $\mathrm{Tr}_{K_s^{\mathrm{ker}(g_0)}/K}(\beta) = 0$.

Definition 5.1. 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 4.11, the minimal polynomial of z over K is the same as that of α.

Lemma 2.3 along with the work done in Section 3 tells us that $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$ is generated as a K-algebra by β and z. The elements $\beta^i z^j$ for $0 \le i, j \le p-1$

form a basis for $\text{End}_{A_{\varphi_0}}(\mathcal{S})^{\text{opp}}$ as a K-vector space. To specify the multiplication on $\text{End}_{A_{\varphi_0}}(\mathcal{S})^{\text{opp}}$, it is enough to specify structure constants $c_{ij} \in K$ such that

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

Lemma 5.2. *For all $0 \le j \le p-1$, we have*

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

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

Proof. It is easily seen that $h_{0k} = 0$ for all $1 \le k \le p-1$ 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 $0 \le k \le p-1$. We proceed by induction on j. Suppose that

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

for some $0 \le m \le p-2$. Then,

$$z^{m+1} = z^m z = \left(p^{-1}\sum_{k=0}^{p-1} h_{mk}e_{\rho^k}\right)\left(p^{-1}\sum_{i=0}^{p-1} a_i e_{\rho^i}\right)$$

$$= p^{-2}\sum_{i,k=0}^{p-1} h_{mk}a_i e_{\rho^{k+i}} \qquad \text{by Lemma 4.2}$$

$$= p^{-2}\sum_{n,k=0}^{p-1} h_{mk}a_{n-k}e_{\rho^n}.$$

Hence, it suffices to prove that

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

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. $\square$

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

$$z\beta = \sum_{0 \leq i,j \leq p-1} c_{ij} \beta^i z^j. \tag{10}$$

By the definition of z,

$$z\beta = p^{-1} \sum_{i=0}^{p-1} a_i e_{\rho^i} \beta = p^{-1} \sum_{i=0}^{p-1} a_i \rho^i(\beta) e_{\rho^i}. \tag{11}$$

Using Lemma 5.2, we expand the right-hand side of (10) as

$$\sum_{i,j=0}^{p-1} c_{ij} \beta^i z^j = p^{-1} \sum_{i,j=0}^{p-1} c_{ij} \beta^i \sum_{k=0}^{p-1} h_{jk} e_{\rho^k}. \tag{12}$$

Hence, equating (11) and (12), we obtain for every $0 \leq k \leq p-1$

$$a_k \rho^k(\beta) = \sum_{i,j=0}^{p-1} c_{ij} \beta^i h_{jk}. \tag{13}$$

Recall that $\ker(g_0) \cap H_{M^\vee} = N_g \lhd G_K$. So $K_s^{N_g} = K_s^{H_{M^\vee}}(\beta)$ is Galois over K and we write

$$\rho^k(\beta) = \sum_{i=0}^{p-1} m_{ik} \beta^i \tag{14}$$

for $m_{ik} \in K_s^{H_{M^\vee}} \subset L^{\langle \rho \rangle}$. We know that $L/L^{\langle \rho \rangle}$ has degree p and is generated by β. Thus, the elements $1, \beta, \dots \beta^{p-1}$ form a basis for L as a vector space over $L^{\langle \rho \rangle}$. Therefore, combining (13) and (14) gives

$$a_k m_{ik} = \sum_{j=0}^{p-1} c_{ij} h_{jk} \tag{15}$$

for all $0 \leq i, k \leq p - 1$.

Definition 5.3. 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, (15) 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 $0 \leq i, j \leq p - 1$ form a basis for $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$.

Lemma 5.4. *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. $\square$

Therefore, $\mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$ 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 α, 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 5.3. Thus, $\mathcal{D} = \mathrm{End}_{A_{\varphi_0}}(\mathcal{S})^{\mathrm{opp}}$ is as described in Theorem 1.6.

6   An example

We apply Theorem 1.6 to the case $K_s^{H_M} = K(\mu_p)$. In this case, any 1-cocycle f_0 which represents a non-trivial element $f \in H^1(G_K, M)$ has $K_s^{\ker(f_0)} = K(\alpha)$ where $\alpha^p \in K$. Since $K_s^{H_M} = K(\mu_p)$, the action of G_K on $M^\vee$ is trivial. Thus, $H^1(G_K, M^\vee) = \mathrm{Hom}(G_K, M^\vee)$ and any non-trivial $g \in \mathrm{Hom}(G_K, M^\vee)$

corresponds to a degree p Galois extension $K_s^{\ker(g)}/K$. Let $K_s^{\ker(g)} = K_s(\beta)$ with $\mathrm{Tr}_{K(\beta)/K}(\beta) = 0$. Let $\sigma \in G_K$ be such that σ fixes $K(\beta, \mu_p)$ and $\sigma(\alpha)/\alpha = \zeta_p$ for some primitive pth root of unity ζ_p. Choose $\rho \in G_K$ such that ρ fixes $K(\alpha, \mu_p)$ and $(g(\rho))(f_0(\sigma)) = \zeta_p$. 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

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

Now Theorem 1.6 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.

References

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

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

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