Extensions of representations of division algebras over non-Archimedean local fields

Andrew Keisling
Dylan Pentland
Mentored by Tasho Kaletha and Karol Koziol

July 30, 2021

Abstract. Let F be a local field of ramification degree e over $\mathbf{Q}_p$ or $\mathbf{F}_p((t))$, and let D be a central simple division algebra over F of degree d so $p > de + 1$.

For the pro-p Iwahori subgroup $K = 1 + \varpi_D \mathcal{O}_D$ of $D^\times$ we determine information about the structure of $\mathrm{H}^1(K, \overline{\mathbf{F}}_p)$ and $\mathrm{H}^2(K, \overline{\mathbf{F}}_p)$ as modules over the Hecke algebra $\mathcal{H}_K$. The computation of $\mathrm{H}^1(K, \overline{\mathbf{F}}_p)$, as a byproduct, gives a method of constructing almost all elements of $[K, K]K^p$. In the p-adic case, we show Poincaré duality respects the $\mathcal{H}_K$-module structure and higher cohomology groups. For $\mathrm{GL}_2(D)$, we compute $\mathrm{H}^1(I_1, \overline{\mathbf{F}}_p)$ as a module over the Hecke algebra $\mathcal{H}_{I_1}$ where I_1 is a pro-p Iwahori subgroup of $\mathrm{GL}_2(D)$.

For $D^\times$, we use this cohomological information to compute the groups $\mathrm{Ext}^1_{D^\times}(\rho, \rho')$ for all pairs ρ, ρ' of smooth irreducible representations of $D^\times$ over $\overline{\mathbf{F}}_p$. We then obtain a partial description of $\mathrm{Ext}^2_{D^\times}(\rho, \rho')$, and in the p-adic case use Poincaré duality to describe higher extensions.

Contents

1. Introduction

Let F be a p-adic field, and let C be $\mathbf{C}$ or $\mathbf{Q}_\ell$ for $\ell \neq p$. In the characteristic 0 case, the local Langlands correspondence yields an injection

$$\left\{\begin{matrix}\text{continuous representations}\\ \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_n(C)\end{matrix}\right\} / \simeq \longrightarrow \left\{\begin{matrix}\text{irreducible smooth}\\ \text{representations}\\ \text{of } \mathrm{GL}_n(F) \text{ over } C\end{matrix}\right\} / \simeq$$

which satisfies certain nice properties. There exists a precise way to enlarge the left side to make this a true bijection. Thus, we can translate difficult questions about field extensions of F to questions about $\mathrm{GL}_n(F)$ which are often easier to answer. In the case of $n = 1$, this is local class theory. Division algebras also play an important role, because for a division algebra D of invariant $1/n$ there is a Jacquet-Langlands correspondence yielding an injection

$$\left\{\begin{matrix}\text{irreducible smooth}\\ \text{representations}\\ \text{of } D^\times \text{ over } C\end{matrix}\right\} / \simeq \longrightarrow \left\{\begin{matrix}\text{irreducible smooth}\\ \text{representations}\\ \text{of } \mathrm{GL}_n(F) \text{ over } C\end{matrix}\right\} / \simeq$$

where one can describe the image. Putting these two correspondences together, we can translate information about the smooth characteristic 0 representations of $D^\times$ to information about field extensions of F.

When we use coefficients in $\overline{\mathbf{F}}_p$ instead of C, these correspondences no longer work. There has been some progress towards giving a characteristic p local Langlands correspondence, such as in [Bre10], but in general it is not clear how to formulate correspondences like the Jacquet-Langlands correspondence or the local Langlands correspondence given above. In [Sch15], for a division algebra of invariant $1/n$ over F, Scholze constructs a functor

$$\left\{\begin{matrix}\text{smooth admissible}\\ \text{representations}\\ \text{of } \mathrm{GL}_n(F) \text{ over } \mathbf{F}_p\end{matrix}\right\} \xrightarrow{\ \mathcal{F}\ } \left\{\begin{matrix}\text{smooth admissible}\\ \text{representations}\\ \text{of } D^\times \text{ over } \mathbf{F}_p\end{matrix}\right\}$$

where $\mathcal{F}(\rho)$ also carries an action of $\mathrm{Gal}(\overline{F}/F)$. This gives some evidence for a mod p analogue of the Jacquet-Langlands correspondence. Because of this, understanding the representation theory of $D^\times$ with $\overline{\mathbf{F}}_p$ coefficients can be expected to be of use in the mod p local Langlands program. This is what we seek to do.

In general, for a central simple division algebra D over a local field, we will be looking at the representation theory of $D^\times = \mathrm{GL}_1(D)$ and $\mathrm{GL}_2(D)$. In the case of $D^\times$, because the irreducible representations are already classified, we will be focused on gaining information about extensions of these irreducible representations. Let $K = 1 + \varpi_D \mathcal{O}_D$ denote the pro-p Iwahori subgroup of $D^\times$. Here, ϖ_D and $\mathcal{O}_D$ denote a uniformizer and the ring of integers of D respectively. Most of the work will be in computing the $D^\times/K$ representation structure, or equivalently $\mathcal{H}_K$-module structure, of $\mathrm{H}^i(K, \overline{\mathbf{F}}_p)$ and applying the Hochschild-Serre spectral sequence to deduce information about extensions. For $\mathrm{GL}_2(D)$, it is not as simple to obtain information directly about representations such as extensions, since we do not even have a classification of irreducible representations at hand. However, we do calculate the $\mathcal{H}_{I_1}$-module structure of $\mathrm{H}^1(I_1, \overline{\mathbf{F}}_p)$ where I_1 is a pro-p Iwahori subgroup of $\mathrm{GL}_2(D)$. As explained in [Koz17], an understanding of $\mathrm{H}^\bullet(I_1, \overline{\mathbf{F}}_p)$ as a module over the Hecke algebra $\mathcal{H}_{I_1}$ can give insight about the derived category of smooth $\mathrm{GL}_2(D)$ representations.

This paper is organized as follows: In §2, we review necessary background on local fields, division algebras, and the representation theory of the unit groups of division algebras. Theorem 5 reviews the classification of all smooth irreducible representations, while Lemma 6 translates the problem of computing extensions of smooth characters to computing certain continuous cohomology groups. In §3, we turn to computing the most difficult cohomology group that we use in order to compute $\mathrm{Ext}^1_{D^\times}(\rho, \rho')$, namely $\mathrm{H}^1(K, \overline{\mathbf{F}}_p)$ with K acting trivially, where $K = 1 + \varpi_D \mathcal{O}_D$ as given above. A basis of this $\overline{\mathbf{F}}_p$ vector space is presented in Theorem 17. We do this by constructing almost all elements of $[K, K]K^p$. In §4, we use this basis to compute the dimension of $\mathrm{Ext}^1_{D^\times}(\rho, \rho')$ for any irreducible representations ρ and ρ' of $D^\times$ by computing $\mathrm{H}^1(K, \overline{\mathbf{F}}_p)$ as a representation of $D^\times/K$, or equivalently as a module over the Hecke algebra $\mathcal{H}_K$. Theorem 20 reduces the computation of $\mathrm{Ext}^n_{D^\times}(\rho, \rho')$ to computing extensions of certain characters, and Theorem 24 explicitly says how to compute these extension groups for $n = 1$.

In §5, we compute some information about $\mathrm{Ext}^n_{D^\times}(\rho, \rho')$ for $n > 1$. For $n = 2$, we find a lower bound on the dimension. Namely, we may again reduce to extensions of characters, and Proposition 26 places the corresponding extension group in an exact sequence with a cohomology group we compute in Lemma 27 and the cohomology group $\mathrm{H}^2(K, \overline{\mathbf{F}}_p)$. Theorem 34 gives information about each component of a Kunneth decomposition of $\mathrm{H}^2(K, \overline{\mathbf{F}}_p)$, where for two of the components we have complete information. In the case of a division algebra over a p-adic field, Proposition 37 uses Poincaré duality to allow us to apply knowledge of low cohomology groups to compute the highest cohomology groups.

Finally, in §6 we focus on the group $\mathrm{GL}_2(D)$. We compute $\mathrm{H}^1(I_1, \overline{\mathbf{F}}_p)$ in Theorem 43, where I_1 is now a pro-p Iwahori subgroup of $\mathrm{GL}_2(D)$. While we cannot easily extract concrete information about extensions, we do compute the $\mathcal{H}_{I_1}$-module structure of this group in Theorem 53, with the specific action given in Corollaries 51 and 52.

1.1. **Notation.** Throughout, we will fix the following notations:

- $\mathbf{N} \subset \mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$ are the positive integers, integers, rational numbers, real numbers, and complex numbers
- p is an odd prime integer
- $\mathbf{Z}_p$ is the ring of p-adic integers
- $\mathbf{Q}_p$ is the field of p-adic numbers
- $\mathbf{F}_{p^n}$ is the finite field with p^n elements for positive integer n
- $\overline{\mathbf{F}}_p = \bigcup_{n \in \mathbf{N}} \mathbf{F}_{p^n}$ is the algebraic closure of $\mathbf{F}_p$
- $\mathbf{F}_p((t))$ is the field of Laurent series over $\mathbf{F}_p$
- F is a non-Archimedean local field
- e is the ramification degree of F over $\mathbf{F}_p((t))$ or $\mathbf{Q}_p$
- k_F is the residue field of F, of order q
- f is the residue field degree of F over $\mathbf{F}_p((t))$ or $\mathbf{Q}_p$, so $q = p^f$
- $\mathcal{O}_F$ is the ring of integers of F
- π_F is a uniformizer of F
- ν_F is the discrete valuation on F, normalized so that $\nu_F(\pi_F) = 1$
- D is a degree d division algebra over F ($d \geq 2$, so D is not a field)
- $\mathrm{Nrd} : D \to F$ is the reduced norm on D
- $\nu_D = \frac{1}{d}\nu_F \circ \mathrm{Nrd}$ is the valuation on D extending ν_F
- k_D is the residue field of D, so $k_D \simeq \mathbf{F}_{q^d}$
- $[x]$ is the Teichmuller lift of $x \in k_D$ (or k_F) into D (or F)
- $\mathcal{O}_D$ is the ring of integers of D
- ϖ_D is a uniformizer of D which satisfies $\varpi_D^d = \pi_F$
- σ is a generator of $\mathrm{Gal}(k_D/k_F)$ such that $\varpi_D [x] \varpi_D^{-1} = [\sigma(x)]$ for all $x \in k_D$. Explicitly, $\sigma : x \mapsto x^{q^r}$ for some r coprime to d

· K is the pro-p Iwahori subgroup $1 + \varpi_D \mathcal{O}_D$ of $D^\times$
· For $a|d$, $D_a^\times$ is the subgroup $F^\times \mathcal{O}_D^\times \langle \varpi_D^a \rangle$ of $D^\times$
· For a field extension E/F, $\mathrm{Nm}_{E/F}$ and $\mathrm{Tr}_{E/F}$ are the field norm and field trace
· For a group G and $g, h \in G$, the commutator $[g, h]$ is the product $ghg^{-1}h^{-1}$ and the commutator subgroup $[G, G]$ is the subgroup generated by all commutators
· For a compact open subgroup H of a locally profinite group G, the Hecke algebra $\mathcal{H}_H$ is the algebra $\overline{\mathbf{F}}_p[H \setminus G / H]$ of bi-H-invariant continuous functions of compact support under convolution
· For a topological group G and G-module A, $\mathrm{H}^n(G, A)$ is the degree-n continuous group cohomology, meaning cocycles are continuous in the topology of G and discrete topology on A
· For G-representations ρ and ρ', $\mathrm{Hom}_G(\rho, \rho')$ is the space of G-equivariant linear maps from ρ to ρ', and $\mathrm{Ext}_G^n(\rho, -)$ is the nth derived functor of $\mathrm{Hom}_G(\rho, -)$
· $I_1 \rhd I_2 \rhd I_3 \rhd \cdots$ are the subgroups

$$\begin{pmatrix} 1 + \varpi_D \mathcal{O}_D & \mathcal{O}_D \\ \varpi_D \mathcal{O}_D & 1 + \varpi_D \mathcal{O}_D \end{pmatrix} \rhd \begin{pmatrix} 1 + \varpi_D \mathcal{O}_D & \varpi_D \mathcal{O}_D \\ \varpi_D^2 \mathcal{O}_D & 1 + \varpi_D \mathcal{O}_D \end{pmatrix} \rhd \begin{pmatrix} 1 + \varpi_D^2 \mathcal{O}_D & \varpi_D \mathcal{O}_D \\ \varpi_D^2 \mathcal{O}_D & 1 + \varpi_D^2 \mathcal{O}_D \end{pmatrix} \rhd \cdots$$

of the chosen Iwahori subgroup $I = \begin{pmatrix} \mathcal{O}_D^\times & \mathcal{O}_D \\ \varpi_D \mathcal{O}_D & \mathcal{O}_D^\times \end{pmatrix}$ of $\mathrm{GL}_2(D)$
· T is the subgroup $\begin{pmatrix} 1 + \varpi_D \mathcal{O}_D & 0 \\ 0 & 1 + \varpi_D \mathcal{O}_D \end{pmatrix}$ of diagonal matrices in I_1
· U^+ and U^- are the subgroups $\begin{pmatrix} 1 & \mathcal{O}_D \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ \varpi_D \mathcal{O}_D & 1 \end{pmatrix}$ of upper and lower unipotent matrices in I_1

2. Background

2.1. **Local fields.** The idea behind a local field can be seen from the usual construction of $\mathbf{R}$: we begin with $\mathbf{Q}$, and then take the completion with respect to the usual absolute value $|\cdot|$ on $\mathbf{Q}$. This means we add in all limits of Cauchy sequences, where distance is defined using the given absolute value.

However, there are more general absolute values we can consider.

Definition. Let F be a field. An absolute value on F is a map $|\cdot| : F \to \mathbf{R}$ satisfying:
· $|x| \geq 0$, with equality if and only if $x = 0$,
· $|xy| = |x| \cdot |y|$,
· $|x + y| \leq |x| + |y|$.

An absolute value is *non-Archimedean* if the strong triangle inequality $|x + y| \leq \max(|x|, |y|)$ holds - otherwise, it is *Archimedean.* Given an absolute value on F, it becomes a topological field by making it into a metric space. We say $|\cdot|$ and $|\cdot|'$ are equivalent absolute values when $|x| < 1$ implies that $|x|' < 1$ for all $x \in F$. These will induce the same metric space topology.

On $\mathbf{Q}$, another type of absolute value we can produce is the *p-adic absolute value* $|\cdot|_p$, where p is some fixed prime number.

Definition. Define the p-adic valuation $\nu_p : \mathbf{Q} \to \mathbf{Z} \cup \{\infty\}$ as $\nu_p(\pm \prod_q q^{e_q}) = e_p$, where $\nu_p(0) = \infty$. Then we define $|x|_p := p^{-\nu_p(x)}$, where we define $p^{-\infty} = 0$.

Completing $\mathbf{Q}$ with respect to this absolute value gives the field $\mathbf{Q}_p$ of p-adic numbers. The following theorem tells us that these are all the absolute values we can produce on $\mathbf{Q}$, up to equivalence.

Theorem (Ostrowski)**.** Up to equivalence, the only nontrivial absolute values on $\mathbf{Q}$ are the usual absolute value, denoted $|\cdot|_\infty$, and the p-adic absolute values $|\cdot|_p$.

A common property that $\mathbf{R}$ and $\mathbf{Q}_p$ have, although their topologies are very different and the absolute value $|\cdot|_p$ is actually non-Archimedean, is that they are locally compact, or that every point has a compact neighborhood. This also holds when we complete any algebraic extension $F/\mathbf{Q}$ with respect to some absolute value. In general, this is precisely the property that we want to capture, and is the definition of a local field.

Definition. A local field is a field F equipped with a nontrivial absolute value $|\cdot|_F$ so that it is locally compact under the induced topology of $|\cdot|_F$.

It is not too difficult to classify the local fields from this definition.

Proposition. Let F be a local field. If the absolute value is Archimedean, it is isomorphic to $\mathbf{R}$ or $\mathbf{C}$. If it is non-Archimedean, it is isomorphic to a finite extension of $\mathbf{Q}_p$ or $\mathbf{F}_p((t))$.

In this paper, we will be focused on finite extensions extensions of $\mathbf{Q}_p$ and $\mathbf{F}_p((t))$. We will now explore the structure of these local fields in more detail.

Definition. Let F be a non-Archimedean local field with absolute value $|x|_F$. We define the ring of integers to be $\mathcal{O}_F := \{x \in F : |x|_F \leq 1\}$.

As defined, $\mathcal{O}_F$ is not only a ring but a complete DVR. Here, complete is meant in the topological sense (so that it contains its limit points). A DVR, or discrete valuation ring, is a local principal ideal domain which is not a field.

By virtue of being a DVR, there is a unique maximal ideal $\mathfrak{m} \subset \mathcal{O}_F$. This is also a principal ideal, and so we can pick a generator π_F know as a *uniformizer.*

Definition. The residue field of $\mathcal{O}_F$ is $k_F := \mathcal{O}_F/\mathfrak{m} = \mathcal{O}_F/\pi_F\mathcal{O}_F$.

We will use q to denote the order of the residue field. In direct analogy with how we defined the p-adic valuation ν_p, we can also define a valuation $\nu_F : F \to \mathbf{Z} \cup \{\infty\}$ on F mapping $\nu_F(\pi_F^n u) = n$ for $u \in \mathcal{O}_F^\times$ and $\nu_F(0) = \infty$. Then the absolute values $|\cdot|_F$ and $x \mapsto q^{-\nu_F(x)}$ are equivalent.

The residue field of F will allow us to write down elements of F easily, using Teichmuller lifts. This is enabled by the following lemma.

Lemma (Hensel's Lemma)**.** Let A be a complete DVR, with maximal ideal $\mathfrak{m}$ and residue field $k = A/\mathfrak{m}$. Then if $f \in A[x]$ is a polynomial with reduction $\overline{f} \in k[x]$ having a simple root, this root can be lifted to a root of f in A.

Corollary. Let F be a non-Archimedean local field. There is an injective homomorphism $[\cdot] : k_F^\times \to \mathcal{O}_F^\times$.

Proof. Consider the roots of $x^{|k_F^\times|} - 1 \in k_F[x]$. These are all distinct and simple, and are precisely the elements of $k_F^\times$. By Hensel's lemma, there is then a map of sets $[\cdot] : k_F^\times \to \mathcal{O}_F^\times$ provided by Hensel lifting. The lifts are $|k_F^\times|$th roots of unity in $\mathcal{O}_F^\times$, and hence a product of them is also such a root of unity. Because reduction to the residue field is a homomorphism, we see the reduction of $[x]\cdot[y]$ is xy, which lifts to $[xy]$. Hence, we obtain a homomorphism - it is easily seen to be injective. ☐

This map is known as the Teichmuller lift. A consequence of this map is that we can write any element of F as

$$x = \sum_{i \geq n} [x_i]\pi_F^i$$

for some $n \in \mathbf{Z}$, $x_n \in k_F^\times$, and $x_i \in k_F$ for $i > n$ (where we define $[0] = 0$). Using Teichmuller representatives to write elements, we can then decompose $F^\times$ as

$$F^\times \simeq \pi_F^{\mathbf{Z}} \times k_F^\times \times (1 + \pi_F \mathcal{O}_F).$$

The field $k_F = \mathbf{F}_q$ is a finite extension of $\mathbf{F}_p = k_{\mathbf{Q}_p} = k_{\mathbf{F}_p((t))}$, so we can write $k_F = \mathbf{F}_{p^f}$ for some positive integer f, which we call the *residue field degree* of F. We can similarly define the residue field degree relative to any extension.

Definition. Let E/F be a finite extension of F. Then $f_{E/F} = [k_E : k_F]$, and $e_{E/F} = \nu_E(\pi_F)$. These are the residue field degree and ramification degree respectively.

Given some E/F with ramification degree $e_{E/F}$, it follows from this definition that $\pi_E^{e_{E/F}} \mathcal{O}_E = \pi_F \mathcal{O}_E$, so $\pi_E^{e_{E/F}}$ and π_F are unit multiples of each other. In particular, if F is an extension of $\mathbf{Q}_p$, then $\pi_F^e = pu$ for some unit $u \in \mathcal{O}_F^\times$.

For our field F, over the base field $\mathbf{Q}_p$ or $\mathbf{F}_p((t))$, we denote the ramification degree and residue field degree by e and f. We call F an *unramified extension* of $\mathbf{Q}_p$ or $\mathbf{F}_p((t))$ if $e = 1$, and a *ramified extension* if $e > 1$.

Given any $F/\mathbf{Q}_p$ there is a unique subfield F' such that we have the tower of fields

$$\begin{array}{c} F \\ | \\ F' \\ | \\ \mathbf{Q}_p \end{array}$$

The extension F' is unramified, and contains all unramified extensions of $\mathbf{Q}_p$ in F. It satisfies $[F' : \mathbf{Q}_p] = f_{F/\mathbf{Q}_p} = f$. The extension F/F' is *totally ramified* - that is, $[F : F'] = e_{F/\mathbf{Q}_p} = e$, and $f_{F/F'} = 1$. The situation is identical for $F/\mathbf{F}_p((t))$.

The unramified extensions of any non-Archimedean local field F are easy to describe: there is one for each finite field extension of k_F. Moreover, this is an equivalence

$$\mathcal{C}_F^{\mathrm{unr}} \simeq \mathcal{C}_{k_F}^{\mathrm{sep}},$$

where $\mathcal{C}_F^{\mathrm{unr}}$ is the category of unramified extensions and the maps are F-algebra homomorphisms. On the other side, we have the category of separable extensions of k_F with k_F-algebra homomorphisms.

2.2. **Division algebras.** In this section we provide a brief overview of division algebras. For a more comprehensive survey, see [PY96, II].

Let F be a non-Archimedean local field. We will be studying central simple division algebras over F, which are a type of central simple algebra.

Definition. A central simple algebra (CSA) over F is a simple, not necessarily commutative ring A with center F.

A central simple division algebra D over F is a CSA over F where every nonzero element has a unique inverse. Throughout, we assume D is also not a field. It is always the case for a CSA A that $\dim_F A = d^2$ for some d. We call d the *degree* of A.

Any such D can always be written as a cyclic algebra.

Definition. Let E/F be a degree d cyclic extension of F, and let σ be a generator of $\mathrm{Gal}(E/F)$. Letting $\alpha \in F^\times$ there exists a central simple algebra (E, σ, α) defined as follows: let $E[t]_\sigma$ be the polynomials $\sum_i a_i t^i$ as an algebra over E with multiplication

$t \cdot \lambda = \sigma(\lambda) \cdot t$ for $\lambda \in E$. Then $(t^d - \alpha)$ is a two-sided ideal in $E[t]_\sigma$, so we can define $(E, \sigma, \alpha) := E[t]_\sigma/(t^d - \alpha)$.

By Theorem 5' in [Has32], this is a division algebra precisely when α^d is the least power of α which is in the image of the norm map $\mathrm{Nm}_{E/F}$. Thus, we already have an explicit description of division algebras over F. In particular, this allows us to write elements of a division algebra D uniquely using the decomposition

$$D = E \oplus E\varpi \oplus \cdots \oplus E\varpi^{d-1}$$

where E/F is a degree d unramified extension and ϖ is some choice of an element so $\varpi^d = \pi_F$. For all $\lambda \in E$, we also have $\varpi\lambda\varpi^{-1} = \sigma(\lambda)$ for some generator σ of $\mathrm{Gal}(E/F) \simeq \mathrm{Gal}(k_E/k_F)$. We then see D can be written as a matrix algebra over E. An element $x = \sum_{0 \le i \le d-1} x_i \varpi^i$ for $x_i \in E$ is uniquely represented by the matrix

$$\begin{pmatrix} x_0 & x_1 & \cdots & x_{d-1} \\ \sigma(x_{d-1})\pi_F & \sigma(x_0) & \cdots & \sigma(x_{d-2}) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma^{d-1}(x_1)\pi_F & \sigma^{d-1}(x_2)\pi_F & \cdots & \sigma^{d-1}(x_0) \end{pmatrix}.$$

Given a central simple division algebra D over F, we can extend ν_F to D in a natural way. To do this, we must first define the reduced norm $\mathrm{Nrd} : D \to F$.

Definition. Let D be a division algebra over F of degree d, and let E/F be the degree d unramified extension used to define D. Then we define the reduced norm Nrd to be the determinant map on D with elements of D viewed as matrices over E.

It is a fact that the image of Nrd is contained in F. Now we can define a valuation on D.

Lemma. Let D be a degree d central simple division algebra over F. Then $\nu_D(x) := \frac{1}{d}\nu_F(\mathrm{Nrd}(x))$ is the unique valuation on D extending ν_F.

Given this, we can define $\mathcal{O}_D$ and a uniformizer ϖ_D precisely as with F. For any choice of uniformizers ϖ_D and π_F, we again have $\varpi_D^d = \pi_F u$ for some $u \in \mathcal{O}_D^\times$. We can also define a residue field k_D/k_F as a quotient by the maximal ideal - note that in this setting D need not be commutative, however it remains the case that the maximal ideal is a principal two-sided ideal $\langle \varpi_D \rangle$. It is a fact that $[k_D : k_F] = d$, so $[k_D : \mathbf{F}_p] = fd$ with f the residue field degree of F. The Teichmuller representative representation of elements can also be extended.

Lemma. Let D be a central simple division algebra over F. There is a map $[\cdot] : k_D \to \mathcal{O}_D$, such that we have a unique representation of any $x \in D$ as

$$x = \sum_{i \ge n} [x_i]\varpi_D^i.$$

We will make use of this representation frequently - it is far easier to use in our situation than the cyclic algebra representation of D. The following lemma will make it easier to use Teichmuller representatives, since we will know they work almost additively with some error term.

Lemma (Witt vectors)**.** For Teichmuller representatives, we have $[x] + [y] = [x + y] + O(p)$. This means when $F/\mathbf{F}_p((t))$, the error is equal to zero, and when $F/\mathbf{Q}_p$, the error is $O(\varpi_D^{de})$.

By choosing a certain uniformizer ϖ_D, we can recover, in terms of Teichmuller representatives, the degree d unramified extension E/F used in defining D as a cyclic algebra.

Lemma. There is a choice of uniformizer ϖ_D such that $\varpi_D^d = \pi_F$. When we use this ϖ_D, the field E consists of series of the form $E = \left\{\sum_{i \geq n} [x_{id}] \varpi_D^{id} : x_{id} \in k_D\right\}$.

Henceforth, we will assume that we are using this uniformizer ϖ_D. The reduced norm Nrd is easy to understand on E.

Lemma. The restriction $\mathrm{Nrd}\,|_E$ is equal to $\mathrm{Nm}_{E/F}$.

Thus, we can apply our understanding of $\mathrm{Nm}_{E/F}$ to get many results about Nrd. For example, the following result is well known.

Lemma. Let E/F be an unramified extension of non-Archimedean local fields. Then the norm map $\mathrm{Nm}_{E/F} : E \to F$ restricts to a surjection $\mathrm{Nm}_{E/F} : \mathcal{O}_E^\times \to \mathcal{O}_F^\times$.

Proof. See [Ser13b], Chapter V §2. $\square$

Corollary. The reduced norm $\mathrm{Nrd} : D \to F$ is surjective.

Proof. It is clear that $\mathrm{Nrd}(0) = 0$, so it suffices to show that Nrd surjects onto $F^\times$. From $F^\times \simeq \pi_F^{\mathbf{Z}} \times \mathcal{O}_F^\times$, for some n we have $x \in \pi_F^n \mathcal{O}_F^\times$. Note that $\mathrm{Nrd}(\varpi_D^n) \in \pi_F^n \mathcal{O}_F^\times$ as well. Then by the previous lemma, we get

$$\mathrm{Nrd}(\varpi_D^n \mathcal{O}_E^\times) = \mathrm{Nrd}(\varpi_D^n) \cdot \mathcal{O}_F^\times = \pi_F^n \mathcal{O}_F^\times,$$

and so there is a preimage of x under Nrd. $\square$

The final thing that is important to remember is that D will not be commutative. To actually make commutations using the Teichmuller representative representation of an element, we will need to understand $\varpi_D [x] \varpi_D^{-1}$ in terms of $[x]$. This will always equal $[\sigma(x)]$ for some generator $\sigma \in \mathrm{Gal}(k_D/k_F)$. Once such a σ has been specified, we can decompose $D^\times$ as

$$D^\times \simeq \varpi_D^{\mathbf{Z}} \ltimes (k_D^\times \ltimes (1 + \varpi_D \mathcal{O}_D)),$$

where the first coordinate gives the smallest power n of ϖ_D to appear in the Teichmuller representative representation, and the second coordinate gives the coefficient of ϖ_D^n.

As it turns out, the commutation relation and the degree of a division algebra suffice to describe the isomorphism classes of all division algebras over F. To classify division algebras, we return to the larger context of central simple algebras over F.

Definition. Two CSAs A and B over F are Brauer equivalent if the division algebras in the isomorphisms $A \simeq \mathrm{Mat}_n(D)$ and $B \simeq \mathrm{Mat}_m(D')$ provided by the Artin-Wedderburn structure theorem are isomorphic.

Equivalently, A and B are stably isomorphic: for some n, m we have $\mathrm{Mat}_n(A) \simeq \mathrm{Mat}_m(B)$. We let $[A]$ denote the equivalence class of A. Under the tensor product $- \otimes_F -$, the set of Brauer equivalence classes form a group $\mathrm{Br}(F)$.

Theorem. Let F be any field. There is an isomorphism

$$\mathrm{Br}(F) \xrightarrow{\simeq} \mathrm{H}^2(\mathrm{Gal}(F^{\mathrm{sep}}/F), (F^{\mathrm{sep}})^\times).$$

Here, F^{sep} denotes the separable closure and the absolute Galois group $\mathrm{Gal}(F^{\mathrm{sep}}/F)$ acts in the natural way on $(F^{\mathrm{sep}})^\times$.

Local class field theory gives us, through the cohomological interpretation of the Galois group, a better description of $\mathrm{Br}(F)$.

Theorem. Let F be a non-Archimedean local field. There is an isomorphism

$$\mathrm{H}^2(\mathrm{Gal}(F^{\mathrm{sep}}/F), (F^{\mathrm{sep}})^\times) \xrightarrow{\mathrm{inv}_F} \mathbf{Q}/\mathbf{Z}.$$

Under this isomorphism, the classes $[D]$ of central simple division algebras of degree d are obtained as preimages of $\frac{r}{d}$ where $\gcd(r, d) = 1$.

Corollary. The central simple division algebras D over F are classified up to isomorphism by the preimages $\mathrm{inv}_F^{-1}(\frac{r}{d})$ where $\gcd(r, d) = 1$. The preimage of $\frac{r}{d}$ is the degree d division algebra with commutation relation $\varpi_D[x]\varpi_D^{-1} = [x^{q^r}]$.

Note that correspondence between $\frac{r}{d} \in \mathbf{Q}/\mathbf{Z}$ and the degree d division algebra with this commutation relation is well defined precisely because $[k_D : \mathbf{F}_q] = d$, so $[x^{q^{r+dn}}] = [x^{q^r}]$ for all $n \in \mathbf{Z}$. Thus, we specify a division algebra by its degree and the automorphism that conjugation by ϖ_D induces on a Teichmuller lift.

For our purposes, we will want to assume $p > de + 1$. This will mainly arise when computing $(1 + \varpi_D\mathcal{O}_D)^p$, but will appear in other situations as well. One major reason is the following proposition.

Proposition. If $p > de + 1$ over a p-adic field, then $1 + \varpi_D\mathcal{O}_D$ has no p-torsion.

Combining this fact with the logarithm map gives the following useful isomorphism.

Corollary. If F is a p-adic field with $p > e + 1$, then $1 + \pi_F\mathcal{O}_F \simeq \mathbf{Z}_p^{[F:\mathbf{Q}_p]}$ where we view the first as a group under multiplication and the second as a group under coordinate-wise addition.

If F is a local function field, then a similar isomorphism holds: we have $1 + \pi_F\mathcal{O}_F \simeq \mathbf{Z}_p^{\mathbf{N}}$. This is a direct product of countably many copies of $\mathbf{Z}_p$.

2.3. **Smooth representations of $D^\times$.** If F is a non-Archimedean local field, then $G(F)$ is what is known as an ℓ-group for any algebraic group G over $\mathrm{Spec}\, F$.

Definition. An ℓ-group is a Hausdorff topological group in which the identity has a basis of neighborhoods which are open compact subgroups.

For such groups, we consider *smooth* representations. This is a representation (ρ, V) of the group $G(F)$ such that $\mathrm{Stab}_{G(F)}(v)$ is an open subgroup of of $G(F)$ for each $v \in V$. The group $D^\times = \mathrm{GL}_1(D)$ is such a group. We can realize $\mathrm{GL}_n(D)$ as an algebraic group.

Lemma. Let D be a degree d division algebra over F. There is an algebraic group $\mathrm{GL}_n(D)$ over $\mathrm{Spec}\, F$ whose F points agree with the group $\mathrm{GL}_n(D)$.

Let us now focus on representations of the ℓ-group $D^\times$.

Lemma. The group $D^\times$ is compact modulo its center $F^\times$.

Proof. The subgroup $\mathcal{O}_D^\times$ is compact, and the subgroup $F^\times\mathcal{O}_D^\times$ has index d in $D^\times$. □

Proposition 1. Let G be an ℓ-group which is compact modulo its center Z, and further assume that the center modulo any compact open subgroup is finitely generated as a topological group. Then the smooth irreducible representations with coefficients in any field L are finite dimensional.

Proof. Let V be a smooth irreducible representation. Then if v is a nonzero vector in V, we see $\langle G \cdot v\rangle = V$ by irreducibility. By smoothness of V, we can pick an open subgroup K which stabilizes v.

Denote the center of G by Z. Because G/Z is assumed to be compact and K is open, the image of K in G/Z is of finite index. Then KZ is of finite index in G. We may replace K by $\bigcap_{g\in G/(KZ)} gKg^{-1}$ so that we can assume K is normal, and KZ has finite index in G. Now since K stabilizes v we have $\langle G\cdot v\rangle = \langle G/K\cdot v\rangle$. We can then replace G by G/K and Z by its image in G/K.

We then reduce to the case where G and Z are discrete and G/Z is finite, and V is some smooth irreducible representation. It is known in this situation that $V|_Z$ is semisimple of finite length. It then suffices to show any irreducible representation of Z is finite dimensional. These are the simple $L[Z]$-modules - that is, quotients $L[Z]/\mathfrak{m}$ where $\mathfrak{m}$ is a maximal ideal. It suffices to show this is a finite extension of L. As Z is finitely generated as an abelian group, we conclude $L[Z]$ is a finitely generated L-algebra and by Zariski's lemma the claim follows. ☐

We note that the center must be finitely generated, which rules out some groups, such as $\mathbf{Q}$ with the discrete topology. However, the assumptions will be satisfied for $D^\times$ over a non-Archimedean local field.

Definition. A group G is pro-p if it is profinite and for any open normal subgroup N the quotient G/N is a p group.

Note that a profinite group is automatically compact; it follows that these open subgroups are also closed subgroups of finite index, and hence the quotients are discrete. The following lemma will be useful in classifying irreducible representations of $D^\times$, allowing us to reduce this to classifying representations of a discrete group.

Lemma 2. Let G be a pro-p group. Then any smooth $\overline{\mathbf{F}}_p$-representation V has $V^G \neq 0$.

Proof. Take $v\in V$, and set $K = \mathrm{Stab}_G(v)$. Then $\langle G\cdot v\rangle = \langle G/K\cdot v\rangle$, and we can replace V with $\langle G/K\cdot v\rangle$. We see G/K is finite because K is a compact open subgroup, and we may also assume K is normal by replacing it with $\bigcap_{g\in G/K} gKg^{-1}$.

Now we see G/K is a finite p-group acting on the finite dimensional vector space V. Any finite dimensional $\overline{\mathbf{F}}_p$-representation of a finite group can be reduced to being over a finite dimensional extension $\mathbf{F}_q/\mathbf{F}_p$, as G/K is finite so there are finitely many coefficients c_i in the matrices $\rho(g)$, and we can let $\mathbf{F}_q = \mathbf{F}_p(c_i)$. Now we use that G/K is a finite p-group, with a representation on $\mathbf{F}_q^n$. Each G-orbit has order p^i, and 0 is a fixed point of the G-action. The orbits partition $\mathbf{F}_q^n$, and hence there are at least p fixed points. In particular, $V^G\neq 0$. ☐

Hence, the only smooth irreducible $\overline{\mathbf{F}}_p$-representation of a pro-p group is the trivial representation. With these more general results in mind, we turn to understanding smooth representations of $D^\times$. Although $D^\times$ is not pro-p, the normal subgroup $1+\varpi_D\mathcal{O}_D$ is, which will allow us to make frequent use of the previous lemma. Henceforth, we will use the shorthand $K = 1+\varpi_D\mathcal{O}_D$.

To begin, we would like to understand the characters of $D^\times$. There is an exact sequence

$$1 \longrightarrow D^\times_{\mathrm{Nrd}=1} \longrightarrow D^\times \xrightarrow{\mathrm{Nrd}} F^\times \longrightarrow 1,$$

where exactness follows immediately from the definitions as we have already shown that Nrd is surjective. We then claim that $D^\times_{\mathrm{Nrd}=1} = [D^\times, D^\times]$. Here the notation $[G,G]$ for a group G denotes the commutator subgroup, the subgroup generated by all commutators $[g,h] = ghg^{-1}h^{-1}$ with $g,h\in G$. Once this is established, we will know that any character $D^\times \to \overline{\mathbf{F}}_p^\times$ arises as

$$\chi : D^\times \xrightarrow{\mathrm{Nrd}} F^\times \xrightarrow{\kappa} \overline{\mathbf{F}}_p^\times$$

because $\overline{\mathbf{F}}_p^\times$ is abelian, so any homomorphism into this group must factor through the abelianization. We can easily classify the characters κ of $F^\times$ via $F^\times \simeq \pi_F^{\mathbf{Z}} \times k_F^\times \times (1+\pi_F\mathcal{O}_F)$, where the final component is pro-p and hence we only need to compute characters of $\pi_F^{\mathbf{Z}} \times k_F^\times$ by the previous lemma. These are both cyclic groups, so the characters are then determined by where we send the generators of each component.

Thus, to understand characters of $D^\times$ it suffices to show $D^\times_{\mathrm{Nrd}=1} = [D^\times, D^\times]$. This is somewhat tricky in general to prove.

Lemma 3 ([Wan50])**.** *Let D be a division algebra over a non-Archimedean local field F, and let $\mathrm{Nrd} : D^\times \to F^\times$ be the reduced norm map. Then $D^\times_{\mathrm{Nrd}=1} = [D^\times, D^\times]$.*

Proof. Because $F^\times$ is abelian, we have $[D^\times, D^\times] \subset \ker \mathrm{Nrd}$. We want to show this is actually an equality.

We claim every norm one element is a product of two commutators. Let $\mathrm{Nrd}(x) = 1$. Recall that the division algebra D contains a maximal unramified extension E/F of degree d, where we have the decomposition

$$D = E \oplus E\varpi_D \oplus \cdots \oplus E\varpi_D^{d-1}.$$

Let x have coefficients $x_0, \ldots, x_{d-1} \in E$ in this representation. Reducing modulo π_F, we have $x_0 \equiv \zeta \pmod{\pi_F}$ where ζ is a q^d-1th root of unity in E. Modulo π_F, we have $\mathrm{Nrd}(x) \equiv \mathrm{Nrd}(x_0) \equiv \mathrm{Nrd}(\zeta) \equiv 1 \pmod{\pi_F}$. But ζ was a q^d-1th root of unity, so this congruence means $\mathrm{Nrd}(\zeta) = 1$ and it is actually a $\frac{q^d-1}{q-1}$th root of unity.

Now suppose that ζ is a primitive $\frac{q^d-1}{q-1}$th root of unity. Then it is not a q^i-1th root of unity for any $i < d$, and therefore generates the residue field in its image. It follows that x also generates the residue field. Consequently, x generates a maximal unramified (hence cyclic) subfield E' in D. Because conjugation by ϖ_D can replicate the action of $\mathrm{Gal}(E'/F)$ sending $\xi \mapsto \sigma(\xi)$ for $\xi \in E'$, Hilbert's theorem 90 says if $\mathrm{Nrd}(x) = 1$ then we have for some ξ that $x = \frac{\sigma(\xi)}{\xi}$. Thus, $\varpi_D\xi\varpi_D^{-1} = \sigma(\xi) = x\xi$, so x is indeed a commutator.

Otherwise, if we do not obtain a primitive root of unity, let $\zeta \in E$ be a primitive $\frac{q^d-1}{q-1}$th root of unity. Then by the above reasoning ζ and $\zeta^{-1}x$ are both commutators, so the result follows. ∎

For the purposes of writing down irreducible representations through inductions, we define $D_a^\times$ for $a|d$ as $F^\times\mathcal{O}_D^\times\langle\varpi_D^a\rangle$. Let $\chi : k_D^\times \to \overline{\mathbf{F}}_p^\times$ be a character. As $\mathcal{O}_D^\times = k_D^\times \ltimes (1+\varpi_D\mathcal{O}_D)$, we may extend χ trivially to $\mathcal{O}_D^\times$. Because $F^\times$ is the center of $D^\times$, we may extend trivially to $F^\times\mathcal{O}_D^\times$ as well. Supposing ϖ_D has a conjugation action by $\sigma \in \mathrm{Gal}(k_D/k_F)$, if $\chi(x) = \chi(\sigma^a(x))$ then we may extend to $D_a^\times$ by setting $\chi(\varpi_D^a) = 1$. We say the character has order a in this case if this a is minimal.

The general characters of $D_a^\times$ are not too difficult to classify. We have a decomposition

$$D_a^\times \simeq \varpi_D^{a\mathbf{Z}} \ltimes (k_D^\times \ltimes (1+\varpi_D\mathcal{O}_D)),$$

similar to the decomposition of $D^\times$. As $1+\varpi_D\mathcal{O}_D$ is a pro-p group, we need only compute characters of $\varpi_D^{a\mathbf{Z}} \ltimes k_D^\times$. Identifying $\varpi_D^{a\mathbf{Z}} \simeq \mathbf{Z}$, the action of some integer n on $x \in k_D^\times$ is to send $x \mapsto \sigma^{na}(x)$.

Any character of $\varpi_D^{a\mathbf{Z}} \ltimes k_D^\times$ is determined by where it sends generators of each cyclic group in the semidirect product. Thus, any character χ is of the form $(\varpi_D^n, x, \bullet) \mapsto \alpha^n x^m$ for some $\alpha \in \overline{\mathbf{F}}_p^\times$ and $n, m \in \mathbf{Z}$, where $a|n$. Here the triple $(\varpi_D^n, x, \bullet)$ denotes components in the decomposition $\varpi_D^{a\mathbf{Z}} \ltimes (k_D^\times \ltimes (1+\varpi_D \mathcal{O}_D)$, in the same order. What remains is to check which m and n actually give well-defined characters.

Let $\chi : D_a^\times \to \overline{\mathbf{F}}_p^\times$ be a character acting as described in the previous paragraph. For $x \in k_D^\times$, it is necessary that $\chi([x]) = \chi(\varpi_D^a[x]\varpi_D^{-a}) = \chi([\sigma^a(x)])$, since χ maps into $\overline{\mathbf{F}}_p^\times$, which is abelian. This means that when writing χ as $(n, x, \bullet) \mapsto \alpha^n x^m$ we must have $x^m = \sigma^a(x^m)$, and this must also hold for every element of the subgroup $\langle \sigma^a \rangle$ generated by σ^a. Thus, x^m must be a power of $\prod_{\sigma' \in \langle \sigma^a \rangle} \sigma'(x)$. For fixed $\alpha \in \overline{\mathbf{F}}_p^\times$, it can be checked that

$$\chi_{a,\alpha,m} : (n, x, \bullet) \mapsto \alpha^n \prod_{\sigma' \in \langle \sigma^a \rangle} \sigma'(x)^m$$

is a well-defined character, and thus gives all characters. When $a = 1$, this also recovers the fact that $\chi = \kappa \circ \mathrm{Nrd}$ because the product becomes $\mathrm{Nm}_{k_D/k_F}(x)^m$. We also obtain the following corollary.

Corollary 4. Suppose $a|a'$ are divisors of d. Let $\chi = \chi_{a,\alpha,m}$, and let $k_{D,a}$ and $k_{D,a'}$ be the index a and a' subfields of k_D. Then

$$\mathrm{Res}^{D_a^\times}_{D_{a'}^\times} \chi = \chi_{a',\alpha^{a'/a},m'}$$

where m' is the exponent after applying $\mathrm{Nm}_{k_{D,a}/k_{D,a'}}$.

In particular, we see that we can obtain all characters $\chi_{a,\alpha,0}$ from restrictions of characters $\chi_{1,\alpha',0} = \kappa \circ \mathrm{Nrd}$ of $D^\times$. We will now show that all irreducible representations can be obtained from inductions of characters of $D_a^\times$.

Theorem 5 ([Ly13]). The smooth irreducible mod p representations V of $D^\times$ are given by

$$V \simeq \mathrm{Ind}^{D^\times}_{D_a^\times} \left(\chi \otimes \mathrm{Res}^{D^\times}_{D_a^\times}(\kappa \circ \mathrm{Nrd}) \right) \simeq (\mathrm{Ind}^{D^\times}_{D_a^\times} \chi) \otimes (\kappa \circ \mathrm{Nrd}).$$

Here, $\kappa : F^\times \simeq \pi_F^{\mathbf{Z}} \times k_F^\times \times (1+\pi_F \mathcal{O}_F) \to \overline{\mathbf{F}}_p^\times$ is a character and χ is extended from an order a character $k_D^\times \to \overline{\mathbf{F}}_p^\times$. This covers all irreducibles even when we assume κ to be trivial on the $k_F^\times$ component.

Proof. Let V be an irreducible representation of $D^\times$ over $\overline{\mathbf{F}}_p$. Then by Lemma 2, we know V^K is nonzero. For all $g \in D^\times$, we have $g \cdot V^K = V^{gKg^{-1}} = V^K$ because K is normal, so V^K is a subrepresentation. Because V is irreducible, we must have $V^K = V$. It follows that irreducible representations of $D^\times$ are in bijection with those of

$$D^\times/K \simeq \varpi_D^{\mathbf{Z}} \ltimes k_D^\times.$$

For ease of notation, we denote this by $\mathbf{Z} \ltimes k_D^\times$. Because irreducible representations of $D^\times$ are finite dimensional, so are irreducible representations of $\mathbf{Z} \ltimes k_D^\times$.

As $|k_D^\times|$ is prime to p and the group is abelian, we know that $\mathsf{Rep}(k_D^\times)$ is semisimple and all irreducible representations are characters. The irreducible characters $\mathrm{X} = \mathrm{Hom}(k_D^\times, \overline{\mathbf{F}}_p^\times)$ form a group, which is acted upon by $D^\times/K$ via conjugation: $s \cdot \chi(x) = \chi(s^{-1}xs)$. We have a subgroup $D_a^\times/K \simeq a\mathbf{Z} \ltimes k_D^\times$, generated by the elements in $\mathbf{Z}$ which stabilize the order a characters.

Consider an irreducible representation of $a\mathbf{Z}$, namely a character $\kappa : a\mathbf{Z} \to \overline{\mathbf{F}}_p^\times$. Then upon composition with the projection $D_a^\times/K \simeq a\mathbf{Z} \ltimes k_D^\times \to a\mathbf{Z}$ we may view it as a character of $D_a^\times/K$. We may tensor with some character χ of $D_a^\times/K$ of order a which is extended trivially from a character of $k_D^\times$. We claim that the a-dimensional representation $\mathrm{Ind}^{D^\times/K}_{D_a^\times/K}(\chi \otimes \kappa)$ is an irreducible representation. This follows from the

Mackey criterion for irreducibility: we may extend the conjugation action of $D^\times/K$ on X to all of $\mathrm{Hom}(D_a^\times/K, \overline{\mathbf{F}}_p)$, then check for $s \in (D^\times/K)\backslash(D_a^\times/K)$ that the representations $s\cdot(\chi\otimes\kappa)$ and $\chi\otimes\kappa$ are non-isomorphic. This follows by looking at the restriction to $k_D^\times$, as χ has order a but s is not in $D_a^\times/K$.

Now we show that all irreducible representations V must take the form

$$V = \mathrm{Ind}_{D_a^\times/K}^{D^\times/K}(\chi\otimes\kappa).$$

Letting $\rho : D^\times/K \to \mathrm{GL}(V)$ be some irreducible representation of $D^\times/K$, we consider $\mathrm{Res}_{k_D^\times}^{D^\times/K} V$. As previously mentioned, this is a direct sum of characters, so we have a decomposition $\mathrm{Res}_{k_D^\times}^{D^\times/K} V = \bigoplus_{\chi\in \mathrm{X}} V_\chi$ where V_χ is the eigenspace of χ when we restrict to $k_D^\times$. There exists some χ such that V_χ is nonzero. Let a be the order of χ, so that $a\mathbf{Z}$ maps V_χ to itself because $\rho(s)\cdot V_\chi = V_{s\cdot\chi}$. There is then an irreducible $a\mathbf{Z}$-subrepresentation of V_χ, which must be a character κ of $a\mathbf{Z}$ because $a\mathbf{Z}$ stabilizes χ under conjugation. The corresponding representation of $D_a^\times/K$ inside V_χ must then be $\chi\otimes\kappa$, when both are extended as before. Then $\mathrm{Res}_{D_a^\times/K}^{D^\times/K} V$ contains $\chi\otimes\kappa$ at least once. But then

$$\mathrm{Hom}_{D_a^\times/K}(\chi\otimes\kappa, \mathrm{Res}_{D_a^\times/K}^{D^\times/K} V) \simeq \mathrm{Hom}_{D^\times/K}(\mathrm{Ind}_{D_a^\times/K}^{D^\times/K}(\chi\otimes\kappa), V)$$

is nontrivial, and as V and $\mathrm{Ind}_{D_a^\times/K}^{D^\times/K}(\chi\otimes\kappa)$ are both irreducible, we must have from Schur's lemma that

$$V \simeq \mathrm{Ind}_{D_a^\times/K}^{D^\times/K}(\chi\otimes\kappa).$$

Under the correspondence $V \mapsto V^K$ from $\mathrm{Irr}(D^\times)$ to $\mathrm{Irr}(D^\times/K)$, irreducible representations we have just classified allow us to write any irreducible representation V of $D^\times$ as $\mathrm{Ind}_{D_a^\times}^{D^\times}(\chi\otimes\chi_{a,\alpha,0})$, with χ as in the statement of the theorem. The character $\chi_{a,\alpha,0}$ can be written as $\mathrm{Res}_{D_a^\times}^{D^\times}(\kappa\circ\mathrm{Nrd})$ for some κ as in the statement of the theorem by the previous corollary. Finally, the push-pull formula gives the second desired isomorphism. ☐

One can show additionally that two irreducibles V in the theorem are isomorphic precisely when they have the same value of a the characters χ of $k_D^\times$ are in the same orbit under the action of $D^\times/K$.

Our goal will be to understand $\mathrm{Ext}^n_{D^\times}(\rho,\rho')$ for irreducible representations ρ and ρ'. In general, we will later show that you can reduce this to understanding $\mathrm{Ext}^n_{D_a^\times}(\chi,\chi') \simeq \mathrm{Ext}^n_{D_a^\times}(\mathbf{1}, \chi'\otimes\chi^*)$ where χ and χ' are characters of $D_a^\times$, χ^* denotes the dual character, and $\mathbf{1}$ denotes the trivial character. For this problem, group cohomology is useful due to the following lemma. Note that we use cohomology with continuous cocycles in the topology of the group - this will be the assumption throughout.

Lemma 6. There is an isomorphism $\mathrm{H}^n(D_a^\times,\chi) \simeq \mathrm{Ext}^n_{D_a^\times}(\mathbf{1},\chi)$, where χ denotes the $D_a^\times$-module $\overline{\mathbf{F}}_p$ with the action by the character χ.

Proof. These are computing the same thing, just in different contexts. Let $\mathsf{Rep}(D_a^\times)$ denote the category of smooth representations. The group cohomology functors can be restricted to $\mathrm{H}^n(D_a^\times,-) : \mathsf{Rep}(D_a^\times) \to \overline{\mathbf{F}}_p - \mathsf{Vect}$ as any representation is a $D_a^\times$-module, since there is an action of $D_a^\times$ and the underlying group of the vector space is abelian. These can be computed as the derived functors of $\mathrm{H}^0(D_a^\times,-) = \mathrm{Hom}_{D_a^\times}(\mathbf{1},-) : \mathsf{Rep}(D_a^\times) \to \overline{\mathbf{F}}_p{-}\mathsf{Vect}$. On the other hand, we define $\mathrm{Ext}^n_{D_a^\times}(\mathbf{1},-) : \mathsf{Rep}(D_a^\times) \to \overline{\mathbf{F}}_p{-}\mathsf{Vect}$

as derived functors of $\mathrm{Ext}^0_{D_a^\times}(\mathbf{1},-) = \mathrm{Hom}_{D_a^\times}(\mathbf{1},-)$. These are the same functor at 0, and so the claim follows. ☐

We note briefly that these derived functors make sense, since for any ℓ-group G the category $\mathsf{Rep}(G)$ has enough injectives, for example as shown in [Eme10] Proposition 2.1.1. Unlike the complex case, it is not actually true that there are enough projectives.

Consider the case of Lemma 6 where we inspect $\mathrm{H}^1(D_a^\times,\chi)$. In this case, we can write down $\mathrm{Ext}^1_{D_a^\times}(\mathbf{1},\chi)$ and see explicitly how the correspondence goes. For an extension V fitting in an exact sequence

$$0 \longrightarrow \chi \longrightarrow V \longrightarrow \mathbf{1} \longrightarrow 0,$$

a $D_a^\times$ representation structure extending the two characters is given by a matrix

$$\begin{bmatrix}\chi(g) & \Psi(g)\\ 0 & 1\end{bmatrix}$$

where $\Psi(gh) = \Psi(g) + \chi(g)\Psi(h)$. This is a crossed homomorphism $\Psi \in Z^1(D_a^\times,\overline{\mathbf{F}}_p)$, where $D^\times$ acts by $\chi(g)$ on $\overline{\mathbf{F}}_p$. Two different extensions are isomorphic precisely when these crossed homomorphisms Ψ,Ψ' differ by a principal crossed homomorphism $(\Psi-\Psi')(g) = \chi(g)c - c$ for fixed $c \in \overline{\mathbf{F}}_p$. Thus, $\mathrm{H}^1(D_a^\times,\chi) \simeq \mathrm{Ext}^1_{D^\times}(\mathbf{1},\chi)$.

We can now employ all the tools of group cohomology to solve our problem. In particular, continuing to take $K = 1+\varpi_D\mathcal{O}_D$ of $D^\times$, we have the five term inflation-restriction sequence obtained from the Hochschild-Serre spectral sequence:

$$0 \longrightarrow \mathrm{H}^1(D_a^\times/K,\chi) \xrightarrow{\text{inf}} \mathrm{Ext}^1_{D_a^\times}(\mathbf{1},\chi) \xrightarrow{\text{res}} (\mathrm{Hom}(K,\overline{\mathbf{F}}_p)\otimes\chi)^{D_a^\times/K} \longrightarrow \mathrm{H}^2(D_a^\times/K,\chi) \xrightarrow{\text{inf}} \mathrm{Ext}^2_{D_a^\times}(\mathbf{1},\chi)$$

Here we have replaced $\mathrm{H}^i(D_a^\times,\chi)$ by the extension group in the second and fifth terms via Lemma 6. We also have $K \subset \ker\chi$ because K is a pro-p group so we may apply Lemma 2. In the first and fourth terms this means we may consider $\mathrm{H}^i(D_a^\times/K,\chi)$ rather than $\mathrm{H}^i(D_a^\times/K,\chi^K)$. It also implies that in the third term, as a $D^\times/K$-module, we have $\mathrm{H}^1(K,\chi) = \mathrm{H}^1(K,\overline{\mathbf{F}}_p)\otimes\chi = \mathrm{Hom}(K,\overline{\mathbf{F}}_p)\otimes\chi$.

Some computation will be required here. Almost all of the nontrivial work needed in determining $\mathrm{Ext}^1_{D_a^\times}(\mathbf{1},\chi)$ is in the computation of $\mathrm{Hom}(K,\overline{\mathbf{F}}_p)$, and the $D^\times/K$ action on it. We compute the $\overline{\mathbf{F}}_p$-vector space structure of $\mathrm{Hom}(K,\overline{\mathbf{F}}_p)$ in the next section, and we compute the $D^\times/K$ representation structure in Proposition 23.

Remark. For a general reductive group G over a local field and a G-representation V, a pro-p Iwahori subgroup I_1 will only allow V^{I_1} to have the structure of a module over the Hecke algebra $\mathcal{H}_{I_1}$. In the case of $D^\times$, we have $\mathcal{H}_K \simeq \overline{\mathbf{F}}_p[D^\times/K]$. Thus, our work computing the $D^\times/K$ representation structure can be viewed as a special case of computing these modules over Hecke algebras, as we do in §6 for the group $\mathrm{GL}_2(D)$.

3. Determining $\mathrm{Hom}(1+\varpi_D\mathcal{O}_D,\overline{\mathbf{F}}_p)$

Recall that we use K to denote the normal subgroup $1+\varpi_D\mathcal{O}_D$ of $D^\times$. A key step in computing all extensions of irreducible representations of $D^\times$ is to understand the space $\mathrm{H}^1(K,\overline{\mathbf{F}}_p)$, which is equal to $\mathrm{Hom}(K,\overline{\mathbf{F}}_p)$ because the action of K is trivial. In this section we compute an explicit basis for this vector space over $\overline{\mathbf{F}}_p$, which will have dimension $df+ef$ when F is an extension of $\mathbf{Q}_p$ and countable dimension when F is an extension of $\mathbf{F}_p(\!(t)\!)$. Recall also that we only consider primes $p > de+1$.

Because the additive group $\overline{\mathbf{F}}_p$ is abelian and every element is p-torsion, any homomorphism $\varphi : K \to \overline{\mathbf{F}}_p$ will factor through the following diagram:

$$\begin{array}{ccc} K & \xrightarrow{\ \varphi\ } & \overline{\mathbf{F}}_p \\ \big\downarrow & \overset{\varphi'}{\nearrow} & \\ \frac{K}{[K,K]K^p} & & \end{array}$$

The homomorphism φ' is unique given φ. The subgroup $[K,K]K^p \lhd K$ generated by commutators and pth powers is called the Frattini subgroup of K.

Hence, we can reduce our problem of computing $\mathrm{Hom}(K, \overline{\mathbf{F}}_p)$ to that of computing $\mathrm{Hom}(K/[K,K]K^p, \overline{\mathbf{F}}_p)$. We first compute the subgroup K^p.

Proposition 7. If F is an extension of $\mathbf{Q}_p$, then $K^p = 1 + \varpi_D^{de+1}\mathcal{O}_D$.

Proof. Let $1 + x \in K$ for $x \in \varpi_D \mathcal{O}_D$. Then we have $(1 + x)^p = \sum_{0 \le i \le p} \binom{p}{i} x^i = 1 + px \sum_{1 \le i \le p-1} \left(\binom{p}{i}/p\right) x^{i-1} + x^p$. Recall that $\varpi_D^{de} = \pi_F^e = pu$ for some unit $u \in \mathcal{O}_F^\times$, so because $\varpi_D | x$, px is divisible by ϖ_D^{de+1} in $\mathcal{O}_D$. Moreover, because $p > de + 1$, we have that x^p is divisible by ϖ_D^{de+1}, so $(1 + x)^p$ is in $1 + \varpi_D^{de+1}\mathcal{O}_D$. Thus, $K^p \subset 1 + \varpi_D^{de+1}\mathcal{O}_D$.

Conversely, let $1 + y \in 1 + \varpi_D^{de+1}\mathcal{O}_D$ for some $y \in \varpi_D^{de+1}\mathcal{O}_D$. As a formal power series, we know that

$$\left(\sum_{n=0}^{\infty} \binom{1/p}{n} y^n \right)^p = 1 + y,$$

so to prove that $1 + y \in K^p$ it suffices to show that $\sum_{n=0}^{\infty} \binom{1/p}{n} y^n$ converges in K. Note that it suffices to prove convergence in D: if $x \in D$ satisfies $x^p = 1 + y$, then we have $p\nu_D(x) = \nu_D(1 + y) = 0$ so $x \in \mathcal{O}_D$. Writing $x = [x_0] + O(\varpi_D)$ we see that $x_0^p = 1$, so $x_0 = 1$ because the Frobenius map is an automorphism. Therefore, $x \in K$ if it exists.

To show that $\sum_{n=0}^{\infty} \binom{1/p}{n} y^n$ converges in D, it suffices to show that $\nu_D\left(\binom{1/p}{n} y^n\right) \to \infty$ as $n \to \infty$. We have the identity

$$\binom{1/p}{n} = \frac{(-1)^n}{n!} \prod_{0 \le i \le n-1} \left(\frac{ip - 1}{p} \right).$$

Because $\nu_D = \nu_F = e\nu_p$ on $\mathbf{Q}_p$, we compute $\nu_D\left(\binom{1/p}{n} y^n\right) = \nu_D(y^n) - (e\nu_p(n!) + e\nu_p(p^n)) = n\nu_D(y) - e(\nu_p(n!) + n)$. We also have $d\nu_D(\varpi_D) = \nu_D(\varpi_D^d) = \nu_F(\pi_F) = 1$, so because $y \in \varpi_D^{de+1}\mathcal{O}_D$, we have $\nu_D(y) \ge \nu_D(\varpi_D^{de+1}) = (de + 1)\frac{1}{d} = e\left(1 + \frac{1}{de}\right)$. By Legendre's formula, $\nu_p(n!)$ is bounded above by $\frac{n}{p-1}$. Therefore,

$$\nu_D\left(\binom{1/p}{n} y^n\right) \ge ne\left(1 + \frac{1}{de}\right) - ne\left(\frac{1}{p-1} + 1\right),$$

and because $p - 1 > de$ this will approach ∞ as $n \to \infty$. Thus, the series converges and $K^p \supset 1 + \varpi_D^{de+1}\mathcal{O}_D$. ☐

Corollary 8. If $F/\mathbf{Q}_p$, then $K^{p^k} = 1 + \varpi_D^{kde+1}\mathcal{O}_D$.

Proof. We can prove this with the exact same method as in Proposition 7. We need only change to using the identity

$$\binom{1/p^k}{n} = \frac{(-1)^n}{n!} \prod_{0 \le i \le n-1} \left(\frac{ip^k - 1}{p^k} \right),$$

and from there the analysis is identical. ☐

When F is an extension of $\mathbf{F}_p((t))$, this computation is much simpler: we work in characteristic p. In particular, we now have

$$(1+x)^p = 1 + x^p,$$

so we have $K^p = 1 + (\varpi_D \mathcal{O}_D)^p$.

The strategy we will use is to construct a large number of elements of $[K,K]K^p$ to put an upper bound on $\dim_{\overline{\mathbf{F}}_p} \mathrm{Hom}(K, \overline{\mathbf{F}}_p)$. Then, by writing down enough linearly independent maps in $\mathrm{Hom}(K, \overline{\mathbf{F}}_p)$, we can determine it completely.

Before constructing the commutators, we will need several preliminary results. The general idea is to first gain a strong understanding of how many ways the coefficient of ϖ_D^2 in a commutator $[a,b] \in [K,K]$ can be obtained - this only depends on the coefficients of ϖ_D in a and b. We then use this to inductively approximate a and b which produce the desired commutator. Throughout, we let $\sigma \in \mathrm{Gal}(k_D/k_F)$ be such that $\varpi_D[x]\varpi_D^{-1} = [\sigma(x)]$ for any $x \in k_D$.

We will use the following lemma in constructing commutators, as it is related to the expression for the coefficient of ϖ_D^{i+1} in a commutator $[a,b]$ of K for $i \geq 2$.

Lemma 9. Let $i \geq 0$, and for $y \in k_D$ let $\varphi_{i,y} \in \mathrm{End}_{k_F}(k_D)$ denote the map

$$\varphi_{i,y} : x \mapsto \sigma(x)y - x\sigma^i(y).$$

The image of $\varphi_{i,y}$ is the subspace

$$V = \ker(\mathrm{Tr}_{k_D/k_F}) \cdot \prod_{0 \leq j \leq i} \sigma^j(y),$$

which has codimension one for $y \in k_D^\times$.

Proof. Since σ is an automorphism, the k_F-linearity of this map follows immediately. When $y = 0$, the result is clear, so suppose now that $y \in k_D^\times$.

We first compute the kernel of this map. We have $\varphi_{i,y}(x) = 0$ if and only if $\sigma(x)y = x\sigma^i(y)$. For $x \neq 0$, this is equivalent to $x/\sigma(x) = y/\sigma^i(y)$, which is always solvable by the multiplicative version of Hilbert's theorem 90 as

$$\mathrm{Nm}_{k_D/k_F}(y/\sigma^i(y)) = 1$$

and σ is a generator of the Galois group. Again since σ is a generator, the solution set is one-dimensional, being the k_F-multiples of a particular solution: Supposing for nonzero x' we have $\frac{x'}{\sigma(x')} = \frac{x}{\sigma(x)}$, then $\sigma(x'/x) = x'/x$ so the ratio lies in $k_F^\times$. Thus, $V = \mathrm{im}\,\varphi_{i,y}$ is a codimension one subspace. Noting that

$$\frac{\varphi_{i,y}(x)}{\prod_{0 \leq j \leq i} \sigma^j(y)} = \frac{\sigma(x)}{\prod_{0 < j \leq i} \sigma^j(y)} - \frac{x}{\prod_{0 \leq j < i} \sigma^j(y)},$$

applying σ to the second term yields the first. Then since Tr_{k_D/k_F} is Galois-invariant, the subspace V is contained in $\ker(\mathrm{Tr}_{k_D/k_F}) \cdot \prod_{0 \leq j \leq i} \sigma^j(y)$. The additive version of Hilbert's theorem 90 says $\ker \mathrm{Tr}_{k_D/k_F} = \mathrm{im}(\sigma(x) - x) = \mathrm{im}\,\varphi_{i,1}$, which was shown to also have codimension one. Hence, we have equality. □

The following lemma is used in Proposition 11, where we reduce to studying the curve $\sigma(x)y - x\sigma(y) = \alpha$. This curve appears as a formula the coefficient of ϖ_D^2 in a commutator $[a,b]$ of K, which is why we study it. One of the main tools we will use is the fact that the automorphism group of this curve is $\mathrm{SL}_2(k_F) \times \mu_{q+1}(k_D)$, and these can be extended to $\mathrm{GL}_2(k_F)$ and $k_D^{\times(q+1)}$ to act on the entire family of curves for $\alpha \in k_D$.

Lemma 10. Let d be even, and let $\alpha \in k_D$. The curve $X_\alpha : \sigma(x)y - x\sigma(y) = \alpha$ is isomorphic to $Y_{\alpha'} : \sigma(x)x + \sigma(y)y = \alpha'$ over k_D. Here, we choose $\zeta \neq 0$ so that $\sigma(\zeta) = -\zeta$ and set $\alpha' = \zeta\alpha$.

Proof. The isomorphism can be divided into several smaller maps. Namely, we break it up into the simpler isomorphisms

$$X_\alpha \xrightarrow{\phi_X} \tilde{X}_{\alpha'} \xleftarrow{\phi_{\tilde{X},\omega}} \tilde{X}_{(\omega+\sigma(\omega))\alpha'} \xleftarrow{\phi_Y} Y_{\alpha'}.$$

In the above, we let X_α and $Y_{\alpha'}$ be as in the theorem, and we define intermediate curves $\tilde{X}_{\alpha'}$ and $\tilde{X}_\omega$. Set $\tilde{X}_{\alpha'} : \sigma(x)y + x\sigma(y) = \zeta \cdot \alpha = \alpha'$ as the first. As d is even there exists an ω so $\sigma(\omega)\omega = -1$, and for any such root we have $\omega + \sigma(\omega) \in k_F^\times$. We then let $\tilde{X}_{(\omega+\sigma(\omega))\alpha'} : \sigma(x)y + x\sigma(y) = (\omega + \sigma(\omega))\alpha'$ be the other curve.

Now we construct the isomorphisms. First, we consider ϕ_X. There exists a nonzero element ζ so that $\sigma(\zeta) = -\zeta$. Then sending $y \mapsto \zeta y$ is an isomorphism, such that the image lies in $\tilde{X}_{\alpha'}$.

For ϕ_Y, this sends a point $(x, y) \in Y_{\alpha'}$ to $(x + \omega y, \omega x + y) \in \tilde{X}_{(\omega+\sigma(\omega))\alpha'}$. The result obtained by making this substitution in $\sigma(x)y + x\sigma(y)$ is

$$(\omega + \sigma(\omega))(\sigma(x)x + \sigma(y)y) + (\sigma(\omega)\omega + 1)(x\sigma(y) + y\sigma(x)) = (\omega + \sigma(\omega))\alpha'.$$

By construction of ω, this equals $(\omega + \sigma(\omega))\alpha'$ as $x^{q+1} + y^{q+1} = \alpha'$ on $Y_{\alpha'}$. We then obtain a point on $\tilde{X}_\omega$. This is an isomorphism, as $\det \begin{pmatrix} 1 & \omega \\ \omega & 1 \end{pmatrix}$ is nonzero.

The map $\phi_{\tilde{X},\omega}$ arises from the $\mathrm{GL}_2(k_F)$ action on the entire family of curves $\tilde{X}_\alpha : \sigma(x)y + x\sigma(y) = \alpha$. This restricts applies the natural action of $A \in \mathrm{GL}_2(k_F)$ on $\mathbf{A}^2_{k_D}$ to $(x, y) \in X_\alpha \subset \mathbf{A}^2_{k_D}$ - the result is that we send $\tilde{X}_\alpha$ to $\tilde{X}_{\det A \cdot \alpha}$. Then choosing any element $A \in \mathrm{GL}_2(k_F)$ so $\det(A) = (\omega + \sigma(\omega))^{-1} \in k_F^\times$, the action of A provides the map $\phi_{\tilde{X},\omega} : \tilde{X}_{(\omega+\sigma(\omega))\alpha'} \to \tilde{X}_{\alpha'}$. □

In Proposition 11, we actually obtain a stronger result than is needed by determining the exact number of preimages in $\Phi^{-1}(\alpha)$. However, all we will need for the construction of commutators is the stated bound.

Proposition 11. The map

$$\Phi : k_D^\times \times k_D^\times \longrightarrow k_D$$

sending $(x, y) \mapsto \sigma(x)y - x\sigma(y)$ is surjective for $[k_D : k_F] \geq 3$, and for $[k_D : k_F] = 2$ the image is $\ker \mathrm{Tr}_{k_D/k_F}$. Moreover, $|\Phi^{-1}(\alpha)| \geq (q + 1)\sqrt{|k_D|}$ for $d \geq 3$, with the exception of $d = 4$ where this is true for a fraction $\frac{q}{q+1}$ of nonzero values and for zero.

Proof. When $[k_D : k_F] = 2$, if we fix y the image is determined by Lemma 9. In particular, it is $\operatorname{im} \varphi_{1,y} = y^{q+1} \ker \mathrm{Tr}_{k_D/k_F}$. But this is $\mathrm{Nm}_{k_D/k_F}(y) \cdot \ker \mathrm{Tr}_{k_D/k_F} = \ker \mathrm{Tr}_{k_D/k_F}$, so the result follows.

Now let $d = [k_D : k_F] \geq 3$. The precise kernel of Φ for given $y \in k_F^\times$ is $c \cdot k_F$ where c is a particular solution to $x/\sigma(x) = y/\sigma(y)$. These do not overlap, so there are precisely $|k_D^\times| \cdot |k_F^\times|$ solutions to $\Phi = 0$. We now restrict ourselves to looking at nonzero elements in the image.

Let $\alpha \in k_D^\times$. We can take the affine curve $\sigma(x)y - x\sigma(y) = \alpha$, and take the projective closure to obtain $\sigma(x)y - x\sigma(y) = \alpha z\sigma(z)$. This will yield additional projective points over k_D corresponding to solutions where $z = 0$ - as σ generates the Galois group, these correspond to $\mathbf{P}^1(k_D^{\langle\sigma\rangle}) = \mathbf{P}^1(k_F)$ which has $q + 1$ points. It also immediately demonstrates we can partition the image of Φ in $k_D^\times$ into corresponding to cosets of $k_D^\times/k_D^{\times(q+1)}$, where elements in the same coset have the same number of solutions. Note that we may use $q+1$ here since σ sends $x \mapsto x^{q^j}$ where $\gcd(j,d) = 1$, so these coincide with the $q+1$th powers.

Let d be odd - then $k_D^\times/k_D^{\times(q+1)} = \mathbf{Z}/2\mathbf{Z}$, since $\gcd(q^d-1, q+1) = 2$. As in Lemma 10, there is a $\mathrm{GL}_2(k_F)$ action on the family of curves $X_\alpha : \sigma(x)y - x\sigma(y) = \alpha$ which scales α by the determinant. In particular, solutions to α and $z \cdot \alpha$ for $z \in k_F$ are in bijection as well. However, there are squares and nonsquares in k_F. In particular, we hit both cosets, so all elements of $k_D^\times$ have the same number of solutions, which will be precisely

$$|\Phi^{-1}(\alpha)| = \frac{|k_D^\times|^2 - |k_D^\times| \cdot |k_F^\times|}{|k_D^\times|} = q^d - q.$$

Now suppose that $d = [k_D : k_F]$ is even - the exact number of solutions in this case is much more complicated. We now have equivalence classes $k_D^\times/k_D^{\times(q+1)} = \mathbf{Z}/(q+1)\mathbf{Z}$ by the same gcd calculation. With the notation as in Lemma 10, we can instead study $\sigma(x)x + \sigma(y)y = \alpha'$. This has several properties which make it possible to compute the exact number of points.

If $\alpha' = -1$, upon taking the projective closure of $\sigma(x)x + \sigma(y)y = \alpha'$ we obtain a curve birational to the smooth hypersurface $C : x^{q+1} + y^{q+1} + z^{q+1} = 0$ defined over $\mathbf{F}_{q^2}$. This is because $x \mapsto x^{q+1}$ and $x \mapsto \sigma(x)x$ have the same image and number of preimages, so we can put solutions into bijection this way. It is possible to compute the explicit Zeta function of this curve. Letting $\overline{C}$ denote the base change of C to $\overline{\mathbf{F}}_{q^2}$, the action of the q^2-Frobenius on $\mathrm{H}^1_c(\overline{C}; \mathbf{Q}_\ell)$ is by a constant, namely $-q$. The Zeta function of C must then take the form

$$Z(C,t) = \frac{(1+qt)^{q(q-1)}}{(1-t)(1-q^2t)}$$

since the genus is $\frac{q(q-1)}{2}$ by the genus-degree formula. From this, we can read off the closed form $q^d + 1 + (-q)^{d/2}\frac{q-q^3}{q+1}$ for the number of projective points, so that the number affine points is

$$N = q^d + 1 + (-q)^{d/2}\frac{q-q^3}{q+1} - (q+1).$$

It is also possible to compute this from [W$^+$49]. See also [SK79] for Zeta functions of more general Fermat varieties.

Over k_D, recall that the curve $\sigma(x)y - x\sigma(y) = \alpha$ will be isomorphic to $\sigma(x)x + \sigma(y)y = \alpha'$, which by similar reasoning has the same number of points as $x^{q+1} + y^{q+1} = \alpha'$. We have obtained an explicit formula for the coset where $\alpha' \in k_D^{\times(q+1)}$. By [W$^+$49], we know the exact number N of affine solutions to any equation of the latter form over k_D. This can be expressed as

$$N = |k_D| + \sum_{1 \le i,j \le q} \chi^{i+j}(\alpha')\mathcal{J}(\chi,\chi)$$

where χ is a multiplicative character of $k_D^\times$ of order $q+1$. The Jacobi sum $\mathcal{J}(\chi,\chi)$ in every case is a constant, so we only need to inspect $\sum_{1\le i,j\le q}\chi^{i+j}(\alpha')$. As the character has order $q+1$, this sum takes two values: one value for α' in the trivial coset of $k_D^\times/k_D^{\times(q+1)}$, and the other for the nontrivial cosets (namely, it becomes 1). By the same reasoning as the odd case, over $k_D^\times$ the average number of solutions is $q^d - q$. In particular, for the trivial coset $k_D^\times/k_D^{\times(q+1)}$, we have the exact formula $q^d + 1 + (-q)^{d/2}\frac{q-q^3}{q+1} - (q+1)$.

The remaining cosets all take on the same value, such that the average is $q^d - q$. This proves the claim, as well as the extra details for the case of $d = 4$. □

Corollary 12. Let $\alpha \in \operatorname{im} \Phi$. Then in $\Phi^{-1}(\alpha)$ for $\alpha \in k_D^\times$, there exists (x, y) so that x/y does not lie in any proper subfield of k_D. When $d = 4$, this is true for $\frac{q}{q+1}|k_D^\times|$ choices of $\alpha \in k_D^\times$.

Proof. The $(q+1)$th roots of unity $\langle\zeta\rangle = \mu_{q+1}(k_D)$ act on $\Phi^{-1}(\alpha)$. In particular, given $(x, y) \in \Phi^{-1}(\alpha)$ we have $(\zeta x, \zeta y)$ as another solution. If we fix the ratio x/y, then the system

$$\sigma(x)y - x\sigma(y) = \alpha, x/y = \beta$$

gives $x = y\beta$, so we solve $y\sigma(y)\sigma(\beta) - y\sigma(y)\beta = \alpha$. This has $|\mu_{q+1}(k_D)|$ solutions as σ is a generator of $\operatorname{Gal}(k_D/k_F)$, unless $\sigma(\beta) - \beta = 0$. This implies that $\alpha = 0$, however, and so we do not consider this case.

Thus, over nonzero values α the number of ratios x/y from $(x, y) \in \Phi^{-1}(\alpha)$ is precisely $|\Phi^{-1}(\alpha)|/|\mu_{q+1}(k_D)|$. This exceeds $\sqrt{|k_D|}$ when $d \neq 4$, and when $d = 4$ is true for $\frac{q}{q+1}$ of the nonzero values by Proposition 11. □

Remark. Unfortunately, Corollary 12 cannot be improved: when $d = 4$, it actually is the case that sometimes x/y always lie in the degree 2 subfield of k_D. Additionally, for $\Phi^{-1}(0)$, the ratios always lie in k_F. Thus, this result is the best possible. It also indicates that the exact number of solutions, or at least a bound, is necessary since there are instances where x/y can lie in a subfield.

We need two more lemmas to be able to put together the previous results and construct a large subset of $[K, K]K^p$.

Lemma 13. Let k_2/k_1 be a finite extension of finite fields. Suppose that for $\alpha \in k_2$ we have $\operatorname{Tr}_{k_2/k_1}(x) = 0$ if and only if $\operatorname{Tr}_{k_2/k_1}(\alpha x) = 0$. Then $\alpha \in k_1^\times$.

Proof. Every k_1-linear map $k_2 \to k_1$ is of the form $M_\alpha(x) = \operatorname{Tr}_{k_2/k_1}(\alpha x)$ for some *unique* α. This follows from the trace pairing being a symmetric non-degenerate bilinear form. Then simply by counting the linear maps with kernel agreeing with that of the trace, we are done. Namely, any linear map in $\operatorname{Hom}_{k_1}(k_2, k_1)$ is of the form $x \mapsto v^T x$, and to have kernel precisely $\ker \operatorname{Tr}_{k_2/k_1}$ determines v up to a scalar in $k_1^\times$ because $\operatorname{codim}_{k_1} \ker \operatorname{Tr}_{k_2/k_1} = 1$. This counts $|k_1^\times|$ maps, which are already given by $\operatorname{Tr}_{k_2/k_1}(\alpha x)$ for $\alpha \in k_1$. □

Lemma 14. The preimage of $k_F = \mathbf{F}_q$ under the map $x \mapsto \prod_{0 \le j < i} \sigma^j(x)$ in $k_D = \mathbf{F}_{q^d}$ is the subfield $\mathbf{F}_{q^{\gcd(i,d)}}$.

Proof. Let $k_i = \mathbf{F}_{q^{\gcd(i,d)}}$, and take some $x \in k_i$. Then $\operatorname{Nm}_{k_i/k_F}(x) \in k_F$. The map $\prod_{0 \le j < i} \sigma^j(x)$ restricts to the $i/\gcd(i, d)$th power of the norm map, since σ restricts to a generator of the Galois group of the subfield k_i over $\mathbf{F}_q$, so k_i is contained in the preimage of k_F.

For the regular norm map $\operatorname{Nm}_{k_i/\mathbf{F}_q}$ viewed as a map on k_D, the preimage of $\mathbf{F}_q$ is precisely k_i - we know the map is surjective, and a gcd calculation counts the exact number of preimages. When we consider the $i/\gcd(i, d)$th power of the norm map, we restrict the image to the $(i/\gcd(i, d))$th powers in $\mathbf{F}_q$, which has index $\gcd(\frac{i}{\gcd(i,d)}, q - 1)$. The number of preimages of each element of $\mathbf{F}_q$, when nonzero, is given by $N = \gcd(\frac{q^{ij}-1}{q^j-1}, q^d - 1) = \gcd(\frac{i}{\gcd(i,d)}, q - 1)\frac{q^{\gcd(i,d)}-1}{q-1}$ where σ sends $x \mapsto x^{q^j}$. To see this, we can use $\gcd(q^j - 1, q^d - 1) = q - 1$ and $\gcd(q^{ij} - 1, q^d - 1) = q^{\gcd(i,d)} - 1$. These are not coprime, however, so we cannot divide them directly to get the result. However, if we account for common factors of $\frac{q^{\gcd(i,d)}-1}{q-1}$ and $q-1$ we can obtain the desired result. We then see that the number of preimages of $\mathbf{F}_q$ is the order of k_i. We conclude the claimed result. ☐

With these results in mind, we can now compute a large subset of the elements of $[K,K]K^p$. Surprisingly, by only producing pure commutators and not products of commutators we can achieve a large enough portion of the commutator subgroup.

Proposition 15. Let D be a division algebra over F of degree $d \geq 2$, and let $K = 1 + \varpi_D \mathcal{O}_D$. Then the subgroup $[K,K]K^p \subset K$ contains products of commutators and pth powers of the form

$$\{1 + \sum_{i \geq 2} [x_i] \varpi_D^i\} \cdot K^p$$

where the $[x_i]$ for $i > 2$ can be any element of k_D when $d \nmid i$ and when $d|i$ can be any element of some additive coset of $V = \ker(\mathrm{Tr}_{k_D/k_F})$ determined by the x_j with $j < i$.

We specify that $[x_2]$ must satisfy $x_2 \in \operatorname{im}\Phi$ (this is true for any commutator $[a,b] = \sum_{i \geq 2}[x_i]\varpi_D^i$), and be an element of $\operatorname{im}\Phi$ which Corollary 12 applies to. This means $x_2 \in k_D^\times$, and when $d = 4$ it can only be one of $\frac{q}{q+1}|k_D^\times|$ nonzero values. For $d = 2$, recall from Proposition 11 that $\operatorname{im}\Phi$ is $\ker \mathrm{Tr}_{k_D/k_F}$ - otherwise, it is all of $k_D^\times$.

Proof. The first important observation we need to make is that $[x]+[y] = [x+y]+O(p)$. This means different things depending on the case we work in. For $F/\mathbf{F}_p((t))$, it means $[x] + [y] = [x + y]$. For $F/\mathbf{Q}_p$, it means that in K/K^p we can ignore the error term because $\varpi_D^{de} u = p$ for $u \in \mathcal{O}_D^\times$ and $K^p = 1 + \varpi_D^{de+1}\mathcal{O}_D$.

In particular, this means to obtain the desired result we can produce commutators of the form $1 + \sum_{i \geq 2}[x_i]\varpi_D^i$ where we ignore the error terms. In the function field case this is never an issue, and in the p-adic case we can absorb them into K^p.

Let $a = 1 + \sum_{i \geq 1}[a_i]\varpi_D^i$, and let $b = 1 + \sum_{i \geq 1}[b_i]\varpi_D^i$. We can write $a^{-1} = 1 + \sum_{i \geq 1}(a-1)^i$ and similarly for b, which allows us to extract some information about the coefficient $[x_i]$ of ϖ_D^i of $[a,b] = 1 + \sum_i [x_i]\varpi_D^i$.

For $i > 2$, there is no term in the coefficient $[x_i]$ of ϖ_D^i of $[a,b] = 1 + \sum_i [x_i]\varpi_D^i$ depending on a_i or b_i (these always cancel). The only term depending on a_{i-1} and b_{i-1} is

$$([\sigma(b_{i-1})a_1] - [b_{i-1}\sigma^{i-1}(a_1)]) - ([\sigma(a_{i-1})b_1] - [a_{i-1}\sigma^{i-1}(b_1)]),$$

and as discussed above we may assume there are no error terms as they are either 0 or can be absorbed into K^p. We can compute this by approximating a^{-1} and b^{-1} up to $1 + (a-1) + (a-1)^2$ and $1 + (b-1) + (b-1)^2$, since after this point the $[a_i], [a_{i-1}]$ and $[b_i], [b_{i-1}]$ coefficients cannot contribute to $[x_i]$. Thus, this term is the same as $\varphi_{i-1,a_1}(b_{i-1}) - \varphi_{i-1,b_1}(a_{i-1})$ in the notation of Lemma 9.

The method of producing commutators is as follows. First, we observe that the coefficient $[x_2]$ of ϖ_D^2 in $[a,b]$ is precisely

$$x_2 = \Phi(a_1, b_1) = \sigma(a_1)b_1 - a_1\sigma(b_1).$$

If $\alpha \in k_D^\times$ and $\Phi^{-1}(\alpha)$ is nonempty then according to Corollary 12 for $d \neq 4$ there exists $(a_1, b_1) \in \Phi^{-1}(\alpha)$ such that a_1/b_1 does not lie in any proper subfield. When $d = 4$, we can do this for $\frac{q}{q+1}|k_D^\times|$ choices.

Now we fix a_j and b_j for $2 \leq j < i-1$, in addition to a_1 and b_1. In terms of the coefficient $[x_i]$ of ϖ_D^i in $[a,b]$, if we ignore the error terms we can achieve the set

$$[C(a_j, b_j)_{j<i-1}] + [\operatorname{im}\varphi_{i-1,a_1} + \operatorname{im}\varphi_{i-1,b_1}],$$

over $(a_{i-1}, b_{i-1}) \in k_D^2$ as possible coefficients $[x_i]$, where $[C(a_j, b_j)_{j<i-1}]$ is a constant depending on lower coefficients in a and b we have already fixed. By Lemma 9, these images are codimension one subspaces. To obtain $k_D = \operatorname{im} \varphi_{i-1,a_1} + \operatorname{im} \varphi_{i-1,b_1}$, we only need to show these are distinct subspaces - otherwise, we get a comdimension one subspace.

Set $V = \ker \operatorname{Tr}_{k_D/k_F}$. By Lemma 9, we wish to compute whether

$$\prod_{j<i} \sigma^j(a_1) \cdot V = \prod_{j<i} \sigma^j(b_1) \cdot V.$$

By Lemma 13, this requires $\prod_{j<i} \sigma^j(a_1/b_1) \in k_F$. By Lemma 14 so long as $\gcd(i,d) < d$ this cannot occur unless a_1/b_1 lies in a proper subfield of k_D. We have already chosen the pair (a_1, b_1) specifically so this is not the case. When $\gcd(i,d) = d$, by Lemma 14 we always have $\prod_{j<i} \sigma^j(a_1/b_1) \in k_F$.

Let us summarize the results for $d \neq 4$. In the p-adic case, we can absorb error terms into K^p so we have produced the desired subset $\{1 + \sum_{i\geq 2}[x_i]\varpi_D^i\} \cdot K^p$ by inductively approximating $a, b \in K$ so $[a,b]$ gives the desired commutator while moving error terms into K^p. In the local function field case, there are no error terms so we produce explicitly a commutator of the form $[a,b] = 1 + \sum_{i\geq 2}[x_i]\varpi_D^i$ through this process. The claim still holds, as $[K,K]K^p$ is a subgroup and contains K^p.

When $d = 4$, we achieve almost the same results. Because Corollary 12 only holds for some values of $x_2 \in \operatorname{im} \Phi$, we must place the additional restriction that it applies to x_2. Because this is still almost all values, this will not present an issue. □

This gives the following corollary.

Corollary 16. Let $F/\mathbf{Q}_p$ be a p-adic field. Then

$$\dim_{\overline{\mathbf{F}}_p} \operatorname{Hom}(K, \overline{\mathbf{F}}_p) \leq df + ef.$$

If $F/\mathbf{F}_p((t))$ is a local function field, then letting $K^{(di+1)} = 1 + \varpi_D^{di+1}\mathcal{O}_D$ we get

$$\dim_{\overline{\mathbf{F}}_p} \operatorname{Hom}(K/K^{(di+1)}, \overline{\mathbf{F}}_p) \leq df + \left(i - \left\lfloor \frac{i}{p} \right\rfloor\right) f.$$

Proof. We consider the p-adic case first. To place a bound on the dimension, we place a bound on $\dim_{\mathbf{F}_p} K/[K,K]K^p$ (this is abelian and p-torsion, hence an $\mathbf{F}_p$-vector space). We have

$$\frac{K}{[K,K]K^p} \simeq \frac{K/K^p}{[K/K^p, K/K^p]}$$

since K^p is normal in K. This is also easily computable, since $K^p = 1 + \varpi_D^{de+1}\mathcal{O}_D$. The commutator construction of Proposition 15 carries over to this quotient by taking the image of the constructed subset under the quotient map. As K/K^p is finite, we just need to compute the number of commutators the construction yields. Explicitly, we may construct at least

$$\left(\frac{q}{q+1}|k_D^\times|\right) \cdot \left(p^{fd}\right)^{ed-2-e} \cdot \left(p^{f(d-1)}\right)^e$$

commutators when $d > 2$, where we respectively have the number of choices for the coefficient of ϖ_D^2, the coefficients of the ϖ_D^i with $i > 2$ and $d \nmid i$, and the coefficients of ϖ_D^i with $d \mid i$ (when $d = 2$, these factors are slightly different but we ultimately get the same bound). As $\frac{q}{q+1}|k_D|^\times \approx p^{df}$ (and in particular is within a factor of p), we can simplify our minimum number of commutators to be within a factor of p of

$$\left(p^{df}\right)^{ed} \cdot p^{-df-ef}.$$

As $|K/K^p| = \left(p^{df}\right)^{ed}$, this gives the desired bound.

In the function field case, the argument is a little different. As there is no error term when adding Teichmuller lifts in characteristic p, we may construct all elements of $[K,K]$ of the form $1+\sum_{i\geq 2}[x_i]\varpi_D^i$ with the conditions of Proposition 15. Similar to before, we wish to bound $\dim_{\mathbf{F}_p} K'/[K',K']K'^p$ where $K' = K/K^{(di+1)}$. Looking at the images of the commutators of Proposition 15 in K', we get a commutator construction for K' of the same form.

Recall that there exists a degree d unramified extension E/F such that E is contained in D as $E = \left\{\sum_{j\geq n}[x_{jd}]\varpi_D^{jd} : x_{jd} \in k_D\right\}$. Then $1+\pi_E\mathcal{O}_E \subset K$. Within this subgroup, pth powers will be commutative because E is a field. As $E/\mathbf{F}_p\left(\!\left(t\right)\!\right)$, we have $(1+\pi_E\mathcal{O}_E)^p = \left\{1+\sum_{j\geq 1}[x_{j(pd)}]\varpi_D^{j(pd)} : x_{j(pd)} \in k_D\right\}$ (there is a pth power in the coefficient, but this is an automorphism of k_D so we may take the coefficients to be arbitrary).

Now we return to K'. The previous observation implies that in the commutator construction under

$$\frac{K'}{[K',K']K^p} \simeq \frac{K'/K'^p}{[K'/K'^p, K'/K'^p]},$$

we may ignore coefficients of $\varpi_D^{j(pd)}$. With similar reasoning as in the p-adic case, from the bound

$$\dim_{\mathbf{F}_p} K'/[K',K']K'^p \leq df + if$$

we may subtract $\lfloor\frac{i}{p}\rfloor f$ due to the coefficients that we ignore. This yields the claimed bound. □

With this corollary in hand, what remains is to produce enough maps to reach these upper bounds. This will allow us to construct a basis of $\mathrm{Hom}(K,\overline{\mathbf{F}}_p)$.

Theorem 17. Let V_ϕ be the subspace of $\mathrm{Hom}(K,\overline{\mathbf{F}}_p)$ consisting of homomorphisms factoring through the quotient $K \to K/(1+\varpi_D^2\mathcal{O}_D) \simeq k_D$, and let V_ψ be the subspace of all homomorphisms factoring through $\mathrm{Nrd} : K \to 1+\pi_F\mathcal{O}_F$. We then have a decomposition

$$\mathrm{H}^1(K,\overline{\mathbf{F}}_p) = \mathrm{Hom}(K,\overline{\mathbf{F}}_p) = V_\psi \oplus V_\phi.$$

Furthermore, we may provide an explicit basis for each. For $\eta_j := (x \mapsto x^{p^j}) \in \mathrm{Aut}_{\mathbf{F}_p}(k_D)$, define the df homomorphisms $\phi^{\eta_j} : K \to \overline{\mathbf{F}}_p$ by

$$\phi^{\eta_j} : 1+[x_1]\varpi_D + O(\varpi_D^2) \mapsto \eta_j(x_1).$$

These form a basis for V_ϕ.

For $\eta \in \mathrm{Hom}(1+\pi_F\mathcal{O}_F,\overline{\mathbf{F}}_p)$, define the homomorphisms $\psi^\eta : K \to \overline{\mathbf{F}}_p$ by

$$\psi^\eta : x \mapsto \eta \circ \mathrm{Nrd}(x).$$

Let $\{\eta_i | i \in I\}$ be a basis of the space of continuous homomorphisms $\mathrm{Hom}(1+\pi_F\mathcal{O}_F,\overline{\mathbf{F}}_p)$ as an $\overline{\mathbf{F}}_p$ vector space, where I is an index set that is countably infinite when F is a local function field and has size ef when F is a p-adic field. The homomorphisms ψ^{η_i} form a basis for V_ψ.

Proof. First we check that these maps are well defined. The only important detail to check is that $\mathrm{Nrd}(K) \subset 1 + \pi_F \mathcal{O}_F$. More generally, by computing the reduction of Nrd in $\mathcal{O}_F^\times$ we can show there is a commutative diagram

$$\begin{array}{ccc} \mathcal{O}_D^\times & \longrightarrow & k_D^\times \\ \big\downarrow \mathrm{Nrd} & & \big\downarrow \mathrm{Nm} \\ \mathcal{O}_F^\times & \longrightarrow & k_F^\times \end{array}$$

and so Nrd must map the kernel K of the upper map to the kernel $1 + \pi_F \mathcal{O}_F$ of the lower map.

Now we check linear independence. First we show that the ϕ^{η_j} are linearly independent. Let $\lambda_0, \dots, \lambda_{df-1} \in \overline{\mathbf{F}}_p$ be such that $\sum_{0=j}^{df-1} \lambda_j \phi^{\eta_j} = 0$. Then for all $x \in k_D$, we have $\sum_{0=j}^{df-1} \lambda_j \phi^{\eta_j}(1 + [x]\varpi_D) = \sum_{0=j}^{df-1} \lambda_j x^{p^j} = 0$. This is a polynomial of degree at most p^{df-1} having p^{df} roots in $k_D = \mathbf{F}_{p^{df}}$, so all the λ_j must be equal to 0 and the ϕ^{η_j} are linearly independent. The subspace $V_\phi \simeq \mathrm{Hom}(k_D, \overline{\mathbf{F}}_p)$ has the same dimension df, and so the V_ϕ has the ϕ^{η_j} as basis elements.

Similarly, the ψ^{η_i} are linearly independent for $i \in I$. Recall that there exists a degree d unramified extension in D defined as $E = \left\{\sum_{i \geq n} [x_{id}]\varpi_D^{id} : x_{id} \in k_D\right\}$. The reduced norm Nrd restricts to $\mathrm{Nm}_{E/F}$ on E. Because $\mathrm{Nm}_{E/F} : 1 + \pi_E \mathcal{O}_E \to 1 + \pi_F \mathcal{O}_F$ is surjective and $1 + \pi_E \mathcal{O}_E \subset K$, we see $\mathrm{Nrd} : K \to 1 + \pi_F \mathcal{O}_F$ is a surjection. The maps ψ^{η_i} then give a basis of V_ψ, since now $V_\psi \simeq \mathrm{Hom}(1 + \pi_F \mathcal{O}_F, \overline{\mathbf{F}}_p)$ and we defined the η_i to be a basis of the latter.

We now claim that V_ϕ and V_ψ have trivial intersection, or equivalently that ψ^η factors as

$$\psi^\eta : K \longrightarrow\!\!\!\!\!\rightarrow k_D \longrightarrow \overline{\mathbf{F}}_p$$

only if η is the trivial homomorphism. As $d \geq 2$, we have $1 + \pi_E \mathcal{O}_E \subset 1 + \varpi_D^2 \mathcal{O}_D$ and so $\mathrm{Nrd} : 1 + \varpi_D^2 \mathcal{O}_D \to 1 + \pi_F \mathcal{O}_F$ is surjective. Therefore, for all $\eta \in \mathrm{Hom}(1 + \pi_F \mathcal{O}_F, \overline{\mathbf{F}}_p)$, we have $\psi^\eta(1 + \varpi_D^2 \mathcal{O}_D) = \eta(1 + \pi_F \mathcal{O}_F) = 0$ only if η is trivial, which is what we wanted. We conclude that $V_\psi \oplus V_\phi \subset \mathrm{Hom}(K, \overline{\mathbf{F}}_p)$ and that as a subspace it has the desired basis. We will now show this is the entire space using Corollary 16.

In the p-adic case, every map in $\mathrm{Hom}(1 + \pi_F \mathcal{O}_F, \overline{\mathbf{F}}_p)$ is 0 on $(1 + \pi_F \mathcal{O}_F)^p = 1 + \pi_F^{e+1} \mathcal{O}_F$. Therefore, $\mathrm{Hom}(1 + \pi_F \mathcal{O}_F, \overline{\mathbf{F}}_p)$ is isomorphic to $\overline{\mathbf{F}}_p^{ef}$, so $|I| = ef$. We conclude that we have produced enough homomorphisms to meet the upper bound of Corollary 16. Therefore, the ϕ^{η_j} and ψ^{η_i} form a basis.

Next, we consider when $F/\mathbf{F}_p((t))$. Here Corollary 16 tells us that when we take a quotient by $K^{(di+1)}$, the dimension of the space of functions is bounded by $df + (i - \lfloor \frac{i}{p} \rfloor) f$. We will show that we already meet this, since the ϕ^{η_j} remain nonzero under this quotient, but the ψ^η which remain nonzero are precisely those for which η reduces to a nonzero map $(1 + \pi_F \mathcal{O}_F)/(1 + \pi_F^{i+1} \mathcal{O}_F) \to \overline{\mathbf{F}}_p$. Note that the reduced norm $\mathrm{Nrd} : 1 + \varpi_D^{di} \mathcal{O}_D \to 1 + \pi_F^i \mathcal{O}_F$ is surjective because the field norm $\mathrm{Nm}_{E/F} : 1 + \pi_E^i \mathcal{O}_E \to 1 + \pi_F^i \mathcal{O}_F$ is surjective, so showing that we have enough linearly independent maps coming from the ψ^η reduces to showing that the dimension of $\mathrm{Hom}\left(\frac{1 + \pi_F \mathcal{O}_F}{1 + \pi_F^{i+1} \mathcal{O}_F}, \overline{\mathbf{F}}_p\right)$ is at least $(i - \lfloor \frac{i}{p} \rfloor) f$. We can again quotient out by the pth powers, which are exactly $1 + (\pi_F \mathcal{O}_F)^p$. This allows us to again ignore the coefficients of the π_F^{pj}, giving the desired dimension. We conclude that if there were some additional basis element, it would need to be 0 modulo $K^{(di+1)}$ for each i. This cannot be the case, since it is then 0 on all of K.

Thus, in either case we have $\mathrm{Hom}(K, \overline{\mathbf{F}}_p) = V_\phi \oplus V_\psi$, and we have computed a basis for each subspace. $\square$

Remark. In the local function field case, we have shown that

$$V_\psi \simeq \mathrm{Hom}(1 + \pi_F \mathcal{O}_F, \overline{\mathbf{F}}_p) \simeq \mathrm{Hom}(\mathbf{Z}_p^{\mathbf{N}}, \overline{\mathbf{F}}_p) \simeq \bigoplus_{i \in \mathbf{N}} \mathrm{Hom}(\mathbf{Z}_p, \overline{\mathbf{F}}_p),$$

which is the decomposition given by the basis ψ^{η_i}. So as a space of homomorphisms, this is a direct sum and not a direct product.

Lemma 18. We have a decomposition

$$K = (1 + \pi_F \mathcal{O}_F) \times K_{\mathrm{Nrd}=1},$$

where $K_{\mathrm{Nrd}=1}$ is the kernel of the reduced norm restricted to K. That is, every $k \in K$ can be written uniquely as $k = k_1 k_2$ for some central element $k_1 \in 1 + \pi_F \mathcal{O}_F$ and $\mathrm{Nrd}(k_2) = 1$.

Proof. We know $\mathrm{Nrd}|_{1+\pi_F\mathcal{O}_F}$ is the map $x \mapsto x^d$, so the kernel is the group of dth roots of unity in $1 + \pi_F \mathcal{O}_F$. Recall that we have the isomorphisms $1 + \pi_F \mathcal{O}_F \simeq \mathbf{Z}_p^{[F:\mathbf{Q}_p]}$ in the p-adic case and $1 + \pi_F \mathcal{O}_F \simeq \mathbf{Z}_p^{\mathbf{N}}$ in the local function field case. Because $p > de + 1$ we know d is coprime to p, so we see that multiplication by d is invertible under this isomorphism. We conclude that every element of $1 + \pi_F \mathcal{O}_F$ is a dth power, and moreover is a dth power in a unique way. It follows that $K = (1 + \pi_F \mathcal{O}_F) \cdot K_{\mathrm{Nrd}=1}$ and also that the intersection is trivial. As $K_{\mathrm{Nrd}=1}$ is normal, we obtain a semidirect product $K = (1 + \pi_F \mathcal{O}_F) \ltimes K_{\mathrm{Nrd}=1}$. This is a direct product since $1 + \pi_F \mathcal{O}_F$ is central, and so its conjugation action is trivial. $\square$

In either case, this decomposition of $\mathrm{H}^1(K, \overline{\mathbf{F}}_p)$ as $V_\phi \oplus V_\psi$ also arises as the Kunneth formula applied to the product decomposition of Lemma 18. With this theorem in hand, we are now able to explicitly compute the extensions $\mathrm{Ext}^1_{D^\times}(\rho, \rho')$ of irreducible representations ρ and ρ'. This decomposition is similar in spirit to the computation of H^1 for pro-p Iwahori subgroups of connected split reductive groups over F done in Corollary 5.4 of [Koz17]. In particular, $1 + \pi_F \mathcal{O}_F$ corresponds to the component $\mathrm{Hom}(\overline{T_1}, \overline{\mathbf{F}}_p)$, and the homomorphisms arising from $K_{\mathrm{Nrd}=1}$ in V_ϕ roughly correspond to those coming from root subgroups. As $D^\times$ is a twist of GL_n which is anisotropic modulo its center, we can only loosely interpret the results this way since the relative root system of $D^\times$ is not very interesting.

We note that $\dim_{\mathbf{F}_p} \mathrm{H}^1(K, \mathbf{F}_p)$ corresponds to a minimal set of topological generators (see [Ser13a]). We can easily construct these as well, as duals to our basis of homomorphisms. Namely, we can take topological generators for $1 + \pi_F \mathcal{O}_F$ as well as norm 1 elements which reduce to an $\mathbf{F}_p$-basis of $K/(1 + \varpi_D^2 \mathcal{O}_D) \simeq k_D$ under the quotient map. We could reprove Corollary 16 by simply showing that this set of generators does topologically generate, although this might seem slightly unmotivated. However, Proposition 15 actually gives us a great deal more than its corollary allowing us to show that Theorem 17 describes all homomorphisms: it gives an explicit method of constructing almost all elements of $[K, K]K^p$ as a product of a commutator and pth power (which can even be carried out in practice), and gives us a very good picture of how to construct elements of $[K, K]K^p$. We may determine this subgroup abstractly as well, as seen by the following corollary.

Corollary 19. We have $[K, K]K^p = K_{\mathrm{Nrd}=1}K^p \cap (1 + \varpi_D^2 \mathcal{O}_D)$.

Proof. We consider the p-adic case first. By Theorem 17, we know $[K:[K,K]K^p] = p^{ef+df}$. The same is true for $K_{\mathrm{Nrd}=1}K^p \cap (1+\varpi_D^2\mathcal{O}_D)$. Furthermore, any $x \in [K,K]$ is sent to 0 by Nrd, and is additionally sent to 0 by reduction modulo $1+\varpi_D^2\mathcal{O}_D$. Hence, $[K,K]K^p \subset K_{\mathrm{Nrd}=1}K^p \cap (1+\varpi_D^2\mathcal{O}_D)$. But these both have the same index in K by Lemma 18 and are therefore equal.

For $F/\mathbf{F}_p((t))$, we can make the same argument but we need to consider the quotient by $K^{(di+1)}$. □

4. Computing $\mathrm{Ext}^1_{D^\times}(\rho,\rho')$

4.1. **Reduction to extensions of characters.** We will begin with explaining how to reduce the computation of $\mathrm{Ext}^n_{D^\times}(\rho,\rho')$ to extensions between characters. There are two main facts used in this reduction: first, that ρ and ρ' are induced from characters. Secondly, the inductions are from *finite index* subgroups, which means that Frobenius reciprocity becomes a two-sided adjunction.

Lemma. For a group G, let $H \leq G$ be such that $[G:H] < \infty$, and let V and W be representations of the groups H and G respectively. Then we have

$$\mathrm{Ext}^n_G(\mathrm{Ind}_H^G V, W) \simeq \mathrm{Ext}^n_H(V, \mathrm{Res}_H^G W).$$

This also holds in the other direction.

Proof. This is a well-known fact from category theory, but we will elaborate here on why it holds. As the index $[G:H]$ is finite, the functors Ind and Res between $\mathsf{Rep}(G)$ and $\mathsf{Rep}(H)$ are both left and right adjoint to each other: this is because the induction functor Ind_H^G agrees with the compact induction functor $c{-}\mathrm{Ind}_H^G$. Because there is a two sided adjunction, both Ind and Res become exact. In particular, an injective resolution

$$0 \longrightarrow V \longrightarrow I^0 \longrightarrow I^1 \longrightarrow \dots$$

in $\mathsf{Rep}(H)$ will then be sent to an injective resolution

$$0 \longrightarrow \mathrm{Ind}_H^G V \longrightarrow \mathrm{Ind}_H^G I^0 \longrightarrow \mathrm{Ind}_H^G I^1 \longrightarrow \dots$$

in $\mathsf{Rep}(G)$ because induction will now be exact and we can check using the adjunction that it also sends injective objects in $\mathsf{Rep}(H)$ to injective objects in $\mathsf{Rep}(G)$. Then applying Hom_H and Hom_G to these resolutions, when we compute derived functors and use the adjunction for Hom we see that the resulting chain complexes we compute Ext^n_H and Ext^n_G from are actually isomorphic. Hence, the adjunction will extend to Ext^n. □

Now we can use this to reduce our problem to computing extensions of characters. Consider, in the notation of Proposition 5, irreducible representations $\rho = (\mathrm{Ind}_{D_a^\times}^{D^\times}\chi)\otimes(\kappa\circ\mathrm{Nrd})$ and $\rho' = (\mathrm{Ind}_{D_{a'}^\times}^{D^\times}\chi')\otimes(\kappa'\circ\mathrm{Nrd})$. We would like to compute the dimension of $\mathrm{Ext}^n_{D^\times}(\rho,\rho')$. Tensoring ρ and ρ' with $(\kappa\circ\mathrm{Nrd})^*$, we can assume $\rho = \mathrm{Ind}_{D_a^\times}^{D^\times}\chi$ and replace $\kappa'\circ\mathrm{Nrd}$ with $(\kappa'\circ\mathrm{Nrd})\otimes(\kappa\circ\mathrm{Nrd})^*$. Using the push-pull formula, we know

$$\rho' = (\mathrm{Ind}_{D_{a'}^\times}^{D^\times}\chi')\otimes(\kappa'\circ\mathrm{Nrd}) \simeq \mathrm{Ind}_{D_{a'}^\times}^{D^\times}(\chi'\otimes\mathrm{Res}_{D_a^\times}^{D^\times}(\kappa'\circ\mathrm{Nrd})).$$

Thus, we have reduced to the case of computing $\mathrm{Ext}^n_{D_a^\times}(\rho,\rho')$ with $\rho = \mathrm{Ind}_{D_a^\times}^{D^\times}\chi$ and $\rho' = \mathrm{Ind}_{D_{a'}^\times}^{D^\times}\chi'$, where χ is extended trivially from a character of $k_D^\times$ but χ' can be any character of $D_{a'}^\times$.

Theorem 20. Let χ, χ', ρ and ρ' be as given above. Then

$$\mathrm{Ext}^n_{D^\times}(\rho, \rho') \simeq \bigoplus_{\overline{s} \in D_a^\times \backslash D^\times / D_{a'}^\times} \mathrm{Ext}^n_{D^\times_{\mathrm{lcm}(a,a')}}(\mathbf{1}, (\mathrm{Res}^{D^\times_{a'}}_{D^\times_{\mathrm{lcm}(a,a')}} \chi') \otimes (\chi^s)^*),$$

where s are coset representatives of the double coset $\overline{s}$. The characters χ^s on $D^\times_{\mathrm{lcm}(a,a')}$ are defined as $\chi^s(x) = \chi(s^{-1}xs)$, and so are conjugated restrictions of χ.

Proof. We first apply Frobenius reciprocity, the first time on the right induced representation. By the previous lemma, we may apply it for Ext^n as the subgroups $D_a^\times$ and $D_{a'}^\times$ have finite index in $D^\times$. We have

$$\mathrm{Ext}^n_{D^\times}(\rho, \rho') = \mathrm{Ext}^n_{D^\times}(\mathrm{Ind}^{D^\times}_{D_a^\times} \chi, \mathrm{Ind}^{D^\times}_{D_{a'}^\times} \chi') \simeq \mathrm{Ext}^n_{D_{a'}^\times}(\mathrm{Res}^{D^\times}_{D_{a'}^\times} \mathrm{Ind}^{D^\times}_{D_a^\times} \chi, \chi').$$

What we need to find is the decomposition of this restriction. The Mackey formula will allow this. In particular, we have

$$\mathrm{Res}^{D^\times}_{D_{a'}^\times} \mathrm{Ind}^{D^\times}_{D_a^\times} \chi \simeq \bigoplus_{\overline{s} \in D_a^\times \backslash D^\times / D_{a'}^\times} \mathrm{Ind}^{D_{a'}^\times}_{sD_a^\times s^{-1} \cap D_{a'}^\times} \chi^s,$$

where s is a representative of the double coset $\overline{s}$. Additionally, both subgroups are normal in $D^\times$ so we can ignore the conjugation by s - the subgroup we induct from is simply $D_a^\times \cap D_{a'}^\times = D^\times_{\mathrm{lcm}(a,a')}$. Note that this is still a subgroup we have studied above, as these are both divisors of d.

We now apply Frobenius reciprocity on the other side. We then obtain

$$\bigoplus_{\overline{s} \in D_a^\times \backslash D^\times / D_{a'}^\times} \mathrm{Ext}^n_{D_{a'}^\times}(\mathrm{Ind}^{D_{a'}^\times}_{D^\times_{\mathrm{lcm}(a,a')}} \chi^s, \chi') \simeq \bigoplus_{\overline{s} \in D_a^\times \backslash D^\times / D_{a'}^\times} \mathrm{Ext}^n_{D^\times_{\mathrm{lcm}(a,a')}}(\chi^s, \mathrm{Res}^{D_{a'}^\times}_{D^\times_{\mathrm{lcm}(a,a')}} \chi').$$

These are now extensions of characters which have been computed, as $\mathrm{lcm}(a, a') | d$. The result then follows after tensoring with $(\chi^s)^*$ on each individual extension group. ☐

Therefore, it suffices to compute $\mathrm{Ext}^n_{D_a^\times}(\mathbf{1}, \chi)$ for all characters χ of $D_a^\times$. We can do this explicitly for $n = 1$.

4.2. **Determining** $\mathrm{Ext}^1_{D_a^\times}(\mathbf{1}, \chi)$**.** We now want to compute $\mathrm{Ext}^1_{D_a^\times}(\mathbf{1}, \chi)$ for an arbitrary character χ. As explained in §2.3, there is a five term exact sequence

$$0 \longrightarrow \mathrm{H}^1(D_a^\times/K, \chi) \xrightarrow{\mathrm{inf}} \mathrm{Ext}^1_{D_a^\times}(\mathbf{1}, \chi) \xrightarrow{\mathrm{res}} (\mathrm{Hom}(K, \overline{\mathbf{F}}_p) \otimes \chi)^{D_a^\times/K} \longrightarrow \mathrm{H}^2(D_a^\times/K, \chi) \xrightarrow{\mathrm{inf}} \mathrm{Ext}^2_{D_a^\times}(\mathbf{1}, \chi)$$

We are now equipped with the tools to compute all terms surrounding the Ext^1 group, since we have computed $\mathrm{Hom}(K, \overline{\mathbf{F}}_p)$.

Proposition 21. We have $\mathrm{H}^i(D_a^\times/K, \chi) = 0$ unless the action by $\chi : D_a^\times \to \overline{\mathbf{F}}_p^\times$ is trivial, in which case $\mathrm{H}^1(D_a^\times/K, \chi) \simeq \overline{\mathbf{F}}_p$ and $\mathrm{H}^i(D_a^\times/K, \chi) = 0$ for $i > 1$.

Proof. Because we have a semidirect product $D_a^\times/K \simeq \varpi_D^{a\mathbf{Z}} \ltimes k_D^\times$, we have a normal subgroup $k_D^\times$ and a quotient $\varpi_D^{a\mathbf{Z}}$ making an exact sequence

$$0 \longrightarrow k_D^\times \longrightarrow D_a^\times/K \longrightarrow \varpi_D^{a\mathbf{Z}} \longrightarrow 0.$$

Then we can again apply the inflation restriction sequence to make our problem easier, namely computing the groups in the exact sequence

$$0 \longrightarrow \mathrm{H}^1(\varpi_D^{a\mathbf{Z}}, \chi^{k_D^\times}) \xrightarrow{\text{inf}} \mathrm{H}^1(\varpi_D^{a\mathbf{Z}} \ltimes k_D^\times, \chi) \xrightarrow{\text{res}} \mathrm{H}^1(k_D^\times, \chi)^{\varpi_D^{a\mathbf{Z}}}$$

We first note that $\mathrm{H}^i(k_D^\times, \chi) = 0$ for any χ and i - we can use Tate cohomology to show this. The norm map $\widehat{N}_{k_D^\times} : \chi_{k_D^\times} \to \chi^{k_D^\times}$ sends $x \mapsto \sum_{g \in k_D^\times} \chi(g)x$. When χ is trivial, this is an isomorphism. When χ is nontrivial the domain and codomain are also zero. In either case, it is then an isomorphism. It follows that $\widehat{\mathrm{H}}^0(k_D^\times, \chi)$ and $\widehat{\mathrm{H}}_0(k_D^\times, \chi)$ are both 0 as these are the cokernel and kernel of this map. By Tate periodicity, these suffice to show that the Tate cohomology is trivial for all i, and in particular so is the regular cohomology.

Thus, we have $\mathrm{H}^1(\varpi_D^{a\mathbf{Z}}, \chi^{k_D^\times}) \simeq \mathrm{H}^1(\varpi_D^{a\mathbf{Z}} \ltimes k_D^\times, \chi)$, where $\mathrm{H}^1(\varpi_D^{a\mathbf{Z}}, \chi^{k_D^\times}) \simeq \mathrm{H}^1(\mathbf{Z}, \chi^{k_D^\times})$. Supposing χ is trivial, this last group becomes $\mathrm{Hom}(\mathbf{Z}, \overline{\mathbf{F}}_p) \simeq \overline{\mathbf{F}}_p$. If instead χ acts nontrivially on $k_D^\times$, then $\chi^{k_D^\times}$ is trivial so this group is 0. Likewise, if χ acts nontrivially on $\mathbf{Z}$ we may compute explicitly that $\mathrm{H}^1(\mathbf{Z}, \chi) = 0$ by showing that all crossed homomorphisms are principal.

Because $\mathrm{H}^i(k_D^\times, \chi) = 0$ are all trivial, we are now in a special case where we have an exact sequence

$$0 \longrightarrow \mathrm{H}^i(\varpi_D^{a\mathbf{Z}}, \chi^{k_D^\times}) \xrightarrow{\text{inf}} \mathrm{H}^i(\varpi_D^{a\mathbf{Z}} \ltimes k_D^\times, \chi) \xrightarrow{\text{res}} \mathrm{H}^i(k_D^\times, \chi)^{\varpi_D^{a\mathbf{Z}}}.$$

The cohomological dimension of $\mathbf{Z}$ with any action is 1. Thus, the leftmost group is 0 regardless of the action since $i \geq 2$ now. The rightmost group has already been shown to be 0. We conclude by exactness that $\mathrm{H}^i(\varpi_D^{a\mathbf{Z}} \ltimes k_D^\times, \chi) = 0$ for $i \geq 2$. ☐

We will also need to understand the $D_a^\times/K$ representation structure on the space $\mathrm{Hom}(K, \overline{\mathbf{F}}_p)$. The action sends a map $f(x)$ to $f(g^{-1}xg)$ for $g \in D_a^\times$ - this is the action which occurs in the inflation-restriction sequence on $\mathrm{H}^1(K, \overline{\mathbf{F}}_p) \otimes \chi$.

Note that the reason we have a $D_a^\times/K$ action is because K acts trivially by this conjugation action: $k \cdot f(x) = f(k^{-1}xk) = f(k^{-1}) + f(x) + f(k) = f(x)$ for all $k \in K$. Because $D_a^\times/K \simeq \varpi_D^{a\mathbf{Z}} \ltimes k_D^\times$, in order to understand the $D_a^\times/K$ action it suffices to understand the action of ϖ_D^a and a generator g of $k_D^\times$. We compute this now.

Lemma 22. As in Theorem 17, let V_ϕ denote the span of the ϕ^{η_j}, and let V_ψ denote the span of the ψ^{η_i} so that $\mathrm{Hom}(K, \overline{\mathbf{F}}_p) = V_\phi \oplus V_\psi$. The action is different on these two subspaces:

- On V_ψ, all elements are fixed by the $D_a^\times/K$ action.
- On V_ϕ, we have $\varpi_D \cdot \phi^{\eta_j} = \phi^{\eta_{j-rf}}$ and $[g] \cdot \phi^{\eta_j} = \left(\frac{\sigma(g)}{g}\right)^{p^j} \phi^{\eta_j}$ for a generator $g \in k_D^\times$,

where r is an integer such that $\sigma(x) = x^{p^{rf}}$.

Proof. Every element of V_ψ is of the form $\eta \circ \mathrm{Nrd}$. Since Nrd maps to $F^\times$, which is abelian, this implies that the conjugation action has no effect.

Next, we consider V_ϕ. The value of ϕ^{η_j} on $x = 1 + \sum_{i \geq 1} [x_i]\varpi_D^i$ in K is $x_1^{p^j} \in \overline{\mathbf{F}}_p$. We then obtain the claimed result by computing $\varpi_D^{-1} x \varpi_D$, as well as $[g]^{-1}x[g]$ and extracting the coefficient of ϖ_D. Explicitly, we have

$$\varpi_D^{-1} x \varpi_D = 1 + \sum_{i \geq 1} [\sigma^{-1}(x_i)]\varpi_D^i = 1 + \sum_{i \geq 1} [x_i^{p^{-rf}}]\varpi_D^i$$

so $\varpi_D \cdot \phi^{\eta_j}(x) = \left(x_1^{p^{-rf}}\right)^{p^j} = \phi^{\eta_{j-rf}}(x)$. We also have

$$[g]^{-1}x[g] = 1 + \sum_{i\geq 1}[g^{-1}x_i\sigma^i(g)]\varpi_D^i$$

so $[g] \cdot \phi^{\eta_j}(x) = (g^{-1}x_1\sigma(g))^{p^j} = \left(\frac{\sigma(g)}{g}\right)^{p^j} \phi^{\eta_j}(x)$. □

For the case of $a = 1$, so that $D_a^\times = D^\times$, we now compute the representation structure of $\mathrm{H}^1(K, \overline{\mathbf{F}}_p)$.

Proposition 23. Let V_ψ be as in Theorem 17. As a representation of $D^\times/K$ via the conjugation action, we have

$$\mathrm{H}^1(K, \overline{\mathbf{F}}_p) \simeq V_\psi \oplus \bigoplus_{j\in\mathbf{Z}/f\mathbf{Z}} \mathrm{Ind}_{F^\times\mathcal{O}_D^\times}^{D^\times} \chi_{\eta_j}$$

where the action on V_ψ is trivial and χ_{η_j} is extended trivially from a character $k_D^\times \to \overline{\mathbf{F}}_p^\times$ given by $x \mapsto \left(\frac{\sigma(x)}{x}\right)^{p^j}$. The choice of a coset representative of j does not matter.

Proof. By Lemma 22, V_ψ and V_ϕ are both invariant under the action of $D^\times/K \simeq \varpi_D^{\mathbf{Z}} \ltimes k_D^\times$. Thus, we have $\mathrm{H}^1(K, \overline{\mathbf{F}}_p) = V_\psi \oplus V_\phi$ as $D^\times/K$ representations, where the subspace V_ψ will be the trivial representation.

Thus, we need only compute the $D^\times/K$-module structure on V_ϕ. For $j \in \mathbf{Z}/f\mathbf{Z}$, let V_j be the subspace of V_ϕ spanned by the ϕ^{η_i} with $i \equiv j \pmod f$. Then from Lemma 22, we see that each of the V_j are $D^\times/K$ invariant, so we have a decomposition

$$\mathrm{H}^1(K, \overline{\mathbf{F}}_p) \simeq V_\psi \oplus \bigoplus_{j\in\mathbf{Z}/f\mathbf{Z}} V_j.$$

We now show that all the V_j are irreducible, so we can use the classification of irreducible representations to understand them. We recall again that $D^\times/K \simeq \varpi_D^{\mathbf{Z}} \ltimes k_D^\times \simeq \mathbf{Z} \ltimes k_D^\times$, so it suffices to show that V_j has no proper subspaces which are both $\mathbf{Z}$ invariant and $k_D^\times$ invariant.

The action of ϖ_D on V_j is by a cyclic shift. As a matrix over V_j, we then have $\det(I - \lambda\varpi_D) = \lambda^d - 1$. Because $p > de + 1$, this has distinct roots over $\overline{\mathbf{F}}_p$, so we conclude that $\varpi_D|_{V_j}$ is diagonalizable and has d distinct eigenvalues. Each V_j then splits into 1-dimensional $\mathbf{Z}$ representations, each spanned by $\sum_{n\in\mathbf{Z}/d\mathbf{Z}} \zeta^n\phi^{\eta_{j-nrf}}$ where ζ is the corresponding eigenvalue which is a dth root of unity.

On the other hand, the action of a generator $g \in k_D^\times$ on any $\phi^{\eta_i} \in V_j$ is simply scaling by $\left(\frac{\sigma(g)}{g}\right)^{p^i}$. Thus, V_j splits into 1-dimensional $k_D^\times$ representations spanned by each of the ϕ^{η_i}. Every nontrivial subrepresentation W of V_j must be both $\mathbf{Z}$-invariant and $k_D^\times$ invariant. The $\mathbf{Z}$-invariance forces W to contain sums of the form $\sum_{n\in\mathbf{Z}/d\mathbf{Z}} \zeta^n\phi^{\eta_{j-nrf}}$ involving non-zero multiples of all the $\phi^{\eta_i} \in V_j$. On the other hand, the restriction $\mathrm{Res}_{k_D^\times}^{D^\times/K} W$ is a direct sum of 1-dimensional representations spanned by the ϕ^{η_i} since $\mathsf{Rep}(k_D^\times)$ is semisimple ($|k_D^\times|$ is prime to p). Thus, we must have $W = V_j$ if it is nontrivial. Hence, each V_j is irreducible.

Note that the V_j have trivial central character because the $D^\times/K$ action is by conjugation. Also, the V_j have dimension d. Therefore, by the classification of irreducible representations of $D^\times$ in Theorem 5, we conclude that $V_j \simeq \mathrm{Ind}_{F^\times \mathcal{O}_D^\times}^{D^\times} \chi_j$ for some character χ_j extended trivially from a character $k_D^\times \to \overline{\mathbf{F}}_p^\times$. We can compute this character from $\mathrm{Res}_{F^\times \mathcal{O}_D^\times}^{D^\times} V_j$, which decomposes into the same 1-dimensional subspaces that it does as a $k_D^\times$-representation as $F^\times$ and K act trivially under conjugation. In particular, we obtain a similar decomposition

$$\mathrm{Res}_{F^\times \mathcal{O}_D^\times}^{D^\times} V_j \simeq \bigoplus_{j'} \chi_{\eta_{j'}}$$

where the characters are extended trivially from $\chi_{\eta_{j'}} : k_D^\times \to \overline{\mathbf{F}}_p^\times$ sending $x \mapsto \left(\frac{\sigma(x)}{x}\right)^{p^{j'}}$, over all $j' \in \mathbf{Z}/(df)\mathbf{Z}$ which reduce to j modulo f. If we choose any two inductions of these characters, say $\mathrm{Ind}_{F^\times \mathcal{O}_D^\times}^{D^\times} \chi_{\eta_{j'}}$ and $\mathrm{Ind}_{F^\times \mathcal{O}_D^\times}^{D^\times} \chi_{\eta_{j''}}$, then after applying Frobenius reciprocity and Schur's lemma we obtain

$$\dim \mathrm{Hom}(\mathrm{Ind}_{F^\times \mathcal{O}_D^\times}^{D^\times} \chi_{\eta_{j'}}, \mathrm{Ind}_{F^\times \mathcal{O}_D^\times}^{D^\times} \chi_{\eta_{j''}}) = 1,$$

and hence the inductions of $\chi_{\eta_{j'}}$ and $\chi_{\eta_{j''}}$ are isomorphic. Thus, the induction of any of these characters $\chi_{\eta_{j'}}$ gives V_j and we recover that

$$\mathrm{H}^1(K, \overline{\mathbf{F}}_p) \simeq V_\psi \oplus \bigoplus_{j \in \mathbf{Z}/f\mathbf{Z}} \mathrm{Ind}_{F^\times \mathcal{O}_D^\times}^{D^\times} \chi_{\eta_j}$$

where χ_{η_j} is extended trivially from the character $x \mapsto \left(\frac{\sigma(x)}{x}\right)^{p^j}$ and the action on V_ψ is trivial. □

For any character χ of $D^\times$, this immediately gives us

$$\mathrm{H}^1(K, \overline{\mathbf{F}}_p) \otimes \chi \simeq (V_\psi \otimes \chi) \oplus \bigoplus_{j \in \mathbf{Z}/f\mathbf{Z}} \mathrm{Ind}_{F^\times \mathcal{O}_D^\times}^{D^\times} (\chi_{\eta_j} \otimes \mathrm{Res}_{F^\times \mathcal{O}_D^\times}^{D^\times} \chi).$$

We have already determined how to compute the restriction of a character of $D^\times$ in general in Corollary 4. We will also want to know the $D_a^\times$-module structure. This is

$$\mathrm{Res}_{D_a^\times}^{D^\times} \mathrm{H}^1(K, \overline{\mathbf{F}}_p) \simeq V_\psi \oplus \bigoplus_{j \in \mathbf{Z}/f\mathbf{Z}} \mathrm{Res}_{D_a^\times}^{D^\times} \mathrm{Ind}_{F^\times \mathcal{O}_D^\times}^{D^\times} \chi_{\eta_j}.$$

The Mackey formula decomposes each term in the direct sum as

$$\bigoplus_{\bar{s} \in D_d^\times \backslash D^\times / D_a^\times} \mathrm{Ind}_{D_d^\times}^{D_a^\times} \chi_{\eta_j}^s.$$

We can similarly compute the tensor product with a character.

Remark. Because the action of K is trivial as it is a pro-p group, we can also conclude $\mathrm{H}^1(K, \rho) \simeq \mathrm{H}^1(K, \overline{\mathbf{F}}_p) \otimes \rho$ as $D_a^\times$-modules for any irreducible representation ρ.

We are now ready to compute $\mathrm{Ext}^1_{D_a^\times}(\mathbf{1}, \chi)$.

Theorem 24. Let D be a degree d division algebra over F. Let χ be a character of $D_a^\times$ where $a|d$. There are two cases where the extensions $\mathrm{Ext}^1_{D_a^\times}(\mathbf{1}, \chi)$ can be nontrivial:

· When χ is trivial, there is an exact sequence

$$0 \longrightarrow \overline{\mathbf{F}}_p \longrightarrow \mathrm{Ext}^1_{D_a^\times}(\mathbf{1}, \chi) \longrightarrow V_\psi \longrightarrow 0$$

where $V_\psi \simeq \mathrm{Hom}(K, \overline{\mathbf{F}}_p)^{D_a^\times / K}$ is as in Theorem 17.

· When $a = d$, and χ is extended trivially from a character $x \mapsto \left(\frac{x}{\sigma(x)}\right)^{p^i}$ of $k_D^\times$ for any i, we have $\dim_{\overline{\mathbf{F}}_p} \operatorname{Ext}^1_{D_a^\times}(\mathbf{1}, \chi) = 1$.

Otherwise, the dimension is 0.

Proof. Suppose first that χ is trivial. Due to Proposition 21, in the inflation-restriction sequence for $D_a^\times$ with the normal subgroup K we obtain

$$0 \longrightarrow \mathrm{H}^1(D_a^\times/K, \chi) \xrightarrow{\text{inf}} \operatorname{Ext}^1_{D_a^\times}(\mathbf{1}, \chi) \xrightarrow{\text{res}} \operatorname{Hom}(K, \overline{\mathbf{F}}_p)^{D_a^\times/K} \longrightarrow 0.$$

From the trivial character case of Proposition 23, we see that $\operatorname{Hom}(K, \overline{\mathbf{F}}_p)^{D_a^\times/K} \simeq V_\psi$ since this is the trivial component of the representation. Additionally, Proposition 21 tells us $\mathrm{H}^1(D_a^\times/K, \overline{\mathbf{F}}_p) \simeq \overline{\mathbf{F}}_p$. We then recover the first case of the theorem statement.

When χ is nontrivial, $\mathrm{H}^1(D_a^\times/K, \chi) = 0$ so we have $\operatorname{Ext}^1_{D_a^\times}(\mathbf{1}, \chi) \simeq (\operatorname{Hom}(K, \overline{\mathbf{F}}_p) \otimes \chi)^{D_a^\times/K}$ via the restriction map. We know this space as a $D_a^\times/K$-module, so we just need to compute the trivial component of the representation.

Recall that as a $D_a^\times/K$-module, we have already shown

$$\mathrm{H}^1(K, \chi) \simeq (V_\psi \otimes \chi) \oplus \bigoplus_{j \in \mathbf{Z}/f\mathbf{Z}} (\operatorname{Res}^{D^\times}_{D_a^\times} \operatorname{Ind}^{D^\times}_{F^\times \mathcal{O}_D^\times} \chi_{\eta_j}) \otimes \chi.$$

As V_ψ is trivial and χ is nontrivial, we know the $(V_\psi \otimes \chi)$ component is nontrivial. By the Mackey formula, the remaining component before tensoring with χ is

$$\bigoplus_{j \in \mathbf{Z}/f\mathbf{Z}} \operatorname{Res}^{D^\times}_{D_a^\times} \operatorname{Ind}^{D^\times}_{F^\times \mathcal{O}_D^\times} \chi_{\eta_j} \simeq \bigoplus_{j \in \mathbf{Z}/f\mathbf{Z}} \bigoplus_{\overline{s} \in F^\times \mathcal{O}_D^\times \backslash D^\times / D_a^\times} \operatorname{Ind}^{D_a^\times}_{F^\times \mathcal{O}_D^\times} \chi^s_{\eta_j}.$$

When we tensor with χ, we can further pull this into the induction via the push-pull formula to obtain a direct sum of inductions of the form

$$\operatorname{Ind}^{D_a^\times}_{F^\times \mathcal{O}_D^\times} (\chi^s_{\eta_j} \otimes \operatorname{Res}^{D_a^\times}_{F^\times \mathcal{O}_D^\times} \chi) =: \operatorname{Ind}^{D_a^\times}_{F^\times \mathcal{O}_D^\times} \chi'.$$

We want to know when $\operatorname{Ind}^{D_a^\times}_{F^\times \mathcal{O}_D^\times} \chi'$ could possibly contain a copy of the trivial representation. By Frobenius reciprocity,

$$\operatorname{Hom}_{D_a^\times}(\mathbf{1}, \operatorname{Ind}^{D_a^\times}_{F^\times \mathcal{O}_D^\times} \chi') \simeq \operatorname{Hom}_{F^\times \mathcal{O}_D^\times}(\mathbf{1}, \chi').$$

As χ' is irreducible and we induct from a finite index subgroup, the induced representation $\operatorname{Ind}^{D_a^\times}_{F^\times \mathcal{O}_D^\times} \chi'$ is semisimple. By Schur's lemma, we conclude there is a copy of the trivial representation precisely when χ' itself is trivial, in which case we have exactly one copy.

Thus, we consider when we can have $\operatorname{Res}^{D_a^\times}_{F^\times \mathcal{O}_D^\times} \chi = (\chi^s_{\eta_j})^*$. Supposing χ satisfies this equality for some choice of a, η_j, and s, we see that the restriction of χ to $F^\times \mathcal{O}_D^\times$ must be extended trivially from a character of $k_D^\times$ because $\chi^s_{\eta_j}$ is. We now show that we must also have $a = d$. Choose coset representatives $1, \varpi_D^2, \ldots, \varpi_D^{a-1}$ for the double coset $F^\times \mathcal{O}_D^\times \setminus D^\times / D_a^\times$. Then the characters $\chi^s_{\eta_j}$ restricted to $k_D^\times$ are given by

$$\chi^s_{\eta_j} : x \mapsto \sigma^{-n} \left(\frac{\sigma(x)}{x}\right)^{p^j}$$

when $s = \varpi_D^n$ so that conjugation by s^{-1} acts by σ^{-n}. The characters of $F^\times \mathcal{O}_D^\times$, also denoted $\chi^s_{\eta_j}$, are extended trivially from these. Note that the character $x \mapsto \frac{\sigma(x)}{x}$ of $k_D^\times$

has order d. This follows because σ generates the Galois group $\mathrm{Gal}(k_D/k_F)$, so $a = d$ is the smallest divisor of d such that $\frac{\sigma(\sigma^a(x))}{\sigma^a(x)} = \frac{\sigma(x)}{x}$ for all x. Applying an automorphism does not change the order, so $\chi^s_{\eta_j}$ also has order d, and the same must be true for χ restricted to $F^\times\mathcal{O}_D^\times$ because they are dual. Hence, we can only have $(\chi^s_{\eta_j})^* = \mathrm{Res}^{D_a^\times}_{F^\times\mathcal{O}_D^\times}\chi$ for $a = d$, or equivalently for $D_a^\times = F^\times\mathcal{O}_D^\times$.

Therefore, the only case where we get a copy of the trivial representation is when χ is a character of $F^\times\mathcal{O}_D^\times$ extended trivially from a character of $k_D^\times$ such that χ is the dual of some $\chi^s_{\eta_j}$. Here, the $\chi^s_{\eta_j}$ are simply the characters extended from $x \mapsto \left(\frac{\sigma(x)}{x}\right)^{p^i}$ over all i in $\mathbf{Z}/(df)\mathbf{Z}$ (with i depending on both j and s), so they are clearly distinct. Thus, we can get exactly one induction containing a copy of the trivial representation by choosing χ to be dual to one of these characters. This shows that the dimension of the extension group is 1 in this case. Otherwise, we get no copies of the trivial representation so the dimension of the extension group is 0. □

By applying the result of Theorem 24 in Theorem 20, we have determined the dimension of $\mathrm{Ext}^1_{D^\times}(\rho, \rho')$ for arbitrary irreducible representations ρ and ρ'. This gives a way to compute any particular extension group. Below, we illustrate what happens for $d = 2$.

Example 25. Suppose that D is a quaternion algebra over F, that is, D has degree $d = 2$. Then let $\rho = \mathrm{Ind}^{D^\times}_{D_a^\times}\chi$ and $\rho' = \mathrm{Ind}^{D^\times}_{D_{a'}^\times}\chi'$ for $a, a' \in \{1, 2\}$ and characters χ and χ' of $D_a^\times$ and $D_{a'}^\times$. Recall that we can apply a tensor product to assume without loss of generality that χ is extended trivially from a character of $k_D^\times$. Then by Theorem 20 we have

$$(1) \qquad \dim \mathrm{Ext}^1_{D^\times}(\rho, \rho') = \sum_{\overline{s} \in D_a^\times\backslash D^\times/D_{a'}^\times} \dim \mathrm{Ext}^1_{D^\times_{\mathrm{lcm}(a,a')}}(\mathbf{1}, \mathrm{Res}^{D_{a'}^\times}_{D^\times_{\mathrm{lcm}(a,a')}}\chi' \otimes (\chi^s)^*).$$

Assume first that we have $a = a' = 1$. Then $D_a^\times = D_{a'}^\times = D^\times$, so equation 1 reduces to

$$\dim \mathrm{Ext}^1_{D^\times}(\rho, \rho') = \dim \mathrm{Ext}^1_{D^\times}(\mathbf{1}, \chi' \otimes \chi^*),$$

where we can apply Theorem 24 to calculate this last dimension. Because $\chi' \otimes \chi^*$ is a character of $D_1^\times$ with $1 \neq d$, the only case where we can get a non-zero dimension is when $\chi' \otimes \chi^* = \mathbf{1}$, in which case we have an exact sequence

$$0 \longrightarrow \overline{\mathbf{F}}_p \longrightarrow \mathrm{Ext}^1_{D_a^\times}(\mathbf{1}, \chi' \otimes \chi^*) \longrightarrow V_\psi \longrightarrow 0.$$

Here, as always, V_ψ has dimension ef if F is a p-adic field and countable dimension if F is a local function field. We therefore recover in the p-adic case that $\dim \mathrm{Ext}^1_{D^\times}(\rho, \rho') = ef + 1$ if $\chi' = \chi$, and otherwise we get a dimension of 0.

Now suppose that $a = 1$ and $a' = 2$, so that $D_a^\times = D^\times$ and $D_{a'}^\times = F^\times\mathcal{O}_D^\times$. Then equation 1 gives

$$\dim \mathrm{Ext}^1_{D^\times}(\rho, \rho') = \dim \mathrm{Ext}^1_{F^\times\mathcal{O}_D^\times}(\mathbf{1}, \chi' \otimes \mathrm{Res}^{D^\times}_{F^\times\mathcal{O}_D^\times}\chi^*).$$

If the restriction of χ to $F^\times\mathcal{O}_D^\times$ is equal to χ', then we again have the exact sequence yielding a dimension of $ef + 1$ in the p-adic case. Moreover, because we are computing an extension of characters of $D_2^\times$ where $2 = d$, we can also have the second outcome of Theorem 24. Namely, if $\chi' \otimes \mathrm{Res}^{D^\times}_{F^\times\mathcal{O}_D^\times}\chi^*$ is extended trivially from a character of $k_D^\times$ of the form $x \mapsto \left(\frac{x}{\sigma(x)}\right)^{p^i}$, then $\dim \mathrm{Ext}^1_{D^\times}(\rho, \rho') = 1$. Using Corollary 4, we have

$\mathrm{Res}^{D^\times}_{F^\times \mathcal{O}_D^\times} \chi_{1,\alpha,m} = \chi_{2,\alpha^2,(q+1)m}$, so one can produce an explicit formula. Otherwise we get a dimension of 0.

Finally, suppose that $a = a' = 2$, so $D_a^\times = D_{a'}^\times = F^\times \mathcal{O}_D^\times$. Then equation 1 becomes

$$\dim \mathrm{Ext}^1_{D^\times}(\rho, \rho') = \dim \mathrm{Ext}^1_{F^\times \mathcal{O}_D^\times}(\mathbf{1}, \chi' \otimes \chi^*) + \dim \mathrm{Ext}^1_{F^\times \mathcal{O}_D^\times}(\mathbf{1}, \chi' \otimes (\chi^{\varpi_D})^*),$$

where $\chi^{\varpi_D}|_{k_D^\times} = \chi|_{k_D^\times} \circ \sigma^{-1}$ and is extended trivially from a character of $k_D^\times$. We can compute these two terms separately just as we did in the previous case. This gives possible dimensions of 0, , 1, 2, $ef+1$, $ef+2$, or $2ef+2$ in the p-adic case.

5. Higher extensions

5.1. **Degree two extensions.** In the first part of this section, we turn our attention to computing information $\mathrm{Ext}^2_{D^\times}(\rho, \rho')$. By Theorem 20, we may again reduce this to computing extensions of characters over $D_a^\times$. Combining this with Lemma 6, we equivalently compute $\mathrm{Ext}^2_{D_a^\times}(\mathbf{1}, \chi) \simeq \mathrm{H}^2(D_a^\times, \chi)$ for $a|d$ and an arbitrary character χ. However, the five-term exact sequence arising from the Hochschild-Serre spectral sequence now only gives us a map into $\mathrm{H}^2(D_a^\times, \chi)$. Because this is a first quadrant spectral sequence, there is also a seven term exact sequence of low degree terms. Using some of our previous results, this will give

$$0 \longrightarrow \ker(\mathrm{Ext}^2_{D_a^\times}(\mathbf{1}, \chi) \to \mathrm{H}^2(K, \chi)) \longrightarrow \mathrm{H}^1(D_a^\times/K, \mathrm{H}^1(K, \chi)) \longrightarrow \ker(\mathrm{H}^3(D_a^\times/K, \chi^K) \to \mathrm{H}^3(D_a^\times, \chi))$$

but the best information we could get out of this is that we have an injection.

Thus, to better understand this cohomology group we will want to use the spectral sequence itself. The spectral sequence is an instance of the Grothendieck spectral sequence. Because K is normal in $D_a^\times$, we can factorize the fixed points functor $\mathrm{H}^0(D_a^\times, -) = (-)^{D_a^\times}$ as

$$\begin{array}{ccc} D_a^\times - \mathsf{Mod} & \xrightarrow{(-)^{D_a^\times}} & \overline{\mathbf{F}}_p - \mathsf{Vect} \\ & {\scriptstyle (-)^K} \searrow \quad \nearrow {\scriptstyle (-)^{D_a^\times/K}} & \\ & D_a^\times/K - \mathsf{Mod} & \end{array}$$

and then use the Grothendieck spectral sequence to analyze the derived functors. This yields a spectral sequence

$$E_2^{p,q} = \mathrm{H}^p(D_a^\times/K, \mathrm{H}^q(K, \chi)) \implies \mathrm{H}^{p+q}(D_a^\times, \chi).$$

However, many of the terms on the E_2 page are already zero. This is why we can expect to get more out of the spectral sequence than what the exact sequence of low degree terms can give us.

Proposition 26. *For any character χ of $D_a^\times$, there is an exact sequence*

$$0 \longrightarrow \mathrm{H}^1(D_a^\times/K, \mathrm{H}^1(K, \chi)) \longrightarrow \mathrm{Ext}^2_{D_a^\times}(\mathbf{1}, \chi) \longrightarrow \mathrm{H}^2(K, \chi)^{D_a^\times/K} \longrightarrow 0$$

arising from the Hochschild-Serre spectral sequence. In particular, the E_2 page has $E_2^{\geq 2, \bullet} = 0$ so the spectral sequence collapses at the E_2 page.

Proof. On the E_2 page of the spectral sequence, we have

$$\begin{array}{c|ccc}
2 & \mathrm{H}^2(K,\chi)^{D_a^\times/K} & \mathrm{H}^1(D_a^\times/K,\mathrm{H}^2(K,\chi)) & \mathrm{H}^2(D_a^\times/K,\mathrm{H}^2(K,\chi)) \\
1 & \mathrm{H}^1(K,\chi)^{D_a^\times/K} & \mathrm{H}^1(D_a^\times/K,\mathrm{H}^1(K,\chi)) & \mathrm{H}^2(D_a^\times/K,\mathrm{H}^1(K,\chi)) \\
0 & \chi^{D_a^\times} & \mathrm{H}^1(D_a^\times/K,\chi^K) & \mathrm{H}^2(D_a^\times/K,\chi^K) \\
\hline
 & 0 & 1 & 2
\end{array}$$

First, we show that $E_2^{\geq 2,\bullet} = 0$, so this is a two column spectral sequence. In Proposition 21, we shown that $E_2^{\geq 2,1} = 0$ for any character χ. This fact extends to arbitrary representations V. Recall we have an exact sequence

$$0 \longrightarrow k_D^\times \longrightarrow D_a^\times/K \longrightarrow \varpi_D^{a\mathbf{Z}} \longrightarrow 0.$$

so we may apply the very same spectral sequence. We note that $\mathrm{H}^i(k_D^\times, V)$ is trivial for any mod p representation V and any i: the $k_D^\times$-module structure on V makes it decompose as $V = \bigoplus_i \chi_i$, since $\mathsf{Rep}(k_D^\times)$ is semisimple ($|k_D^\times|$ is prime to p) and all irreducible representations are 1-dimensional because $k_D^\times$ is abelian. Since we know already that $\mathrm{H}^i(k_D^\times,\chi) = 0$ for any character χ of $k_D^\times$, it follows that $\mathrm{H}^i(k_D^\times, V) = 0$ for any representation V of $k_D^\times$. This allows us to use the higher inflation-restriction sequence as in Proposition 21, and in particular we obtain an isomorphism $\mathrm{H}^i(\varpi_D^{a\mathbf{Z}}, V^{k_D^\times}) \simeq \mathrm{H}^i(D_a^\times/K, V)$. But the cohomological dimension of $\mathbf{Z}$ is 1, so for $i \geq 2$ we have $\mathrm{H}^i(D_a^\times/K, V) = 0$ for any V (and in particular for $V = \mathrm{H}^j(K,\chi)$). We then have $E_2^{\geq 2,\bullet} = 0$.

Because we have a two column spectral sequence on the E_2 page, we conclude that $\mathrm{Ext}^2_{D_a^\times}(\mathbf{1},\chi) \simeq \mathrm{H}^2(D_a^\times,\chi)$ has a filtration $0 = F_0 \subset F_1 \subset F_2 = \mathrm{H}^2(D_a^\times,\chi)$ where $F_1 = \mathrm{H}^1(D_a^\times/K,\mathrm{H}^1(K,\chi))$ and $F_2/F_1 = \mathrm{H}^2(K,\chi)^{D_a^\times/K}$ by looking at the E_∞ page. Applying Lemma 6 gives the exact sequence. □

Now we turn to $\mathrm{H}^1(D_a^\times/K,\mathrm{H}^1(K,\chi))$. From Proposition 23, we know as a $D_a^\times$-module we have

$$\mathrm{H}^1(K,\chi) \simeq (V_\psi \otimes \chi) \oplus \bigoplus_{j \in \mathbf{Z}/f\mathbf{Z}} (\mathrm{Res}^{D^\times}_{D_a^\times} \mathrm{Ind}^{D^\times}_{F^\times \mathcal{O}_D^\times} \chi_{\eta_j}) \otimes \chi.$$

For any V, we have already shown $\mathrm{H}^1(\varpi_D^{a\mathbf{Z}}, V^{k_D^\times}) \simeq \mathrm{H}^1(D_a^\times/K, V)$. However, there is a chance that this group is nontrivial when $V = \mathrm{H}^1(K,\chi)$.

Lemma 27. We have $\mathrm{H}^1(D_a^\times/K,\mathrm{H}^1(K,\chi)) \simeq V_\psi$ if χ is trivial. It can also be nonzero if $a = d$ and χ is extended trivially from a character $x \mapsto \left(\frac{x}{\sigma(x)}\right)^{p^i}$ of $k_D^\times$, in which case it is $\overline{\mathbf{F}}_p$. It is 0 otherwise.

Proof. Let $V = \mathrm{H}^1(K,\chi)$ with the $D_a^\times$-module structure as given above, so that

$$\mathrm{H}^1(\varpi_D^{a\mathbf{Z}}, V^{k_D^\times}) \simeq \mathrm{H}^1(D_a^\times/K, V).$$

Thus, our first task is to describe $V^{k_D^\times}$ as a $\varpi_D^{a\mathbf{Z}}$-module. As a representation of $k_D^\times$, it again splits into a direct sum characters by semisimplicity of $\mathsf{Rep}(k_D^\times)$. The subrepresentation $V^{k_D^\times}$ is simply a collection of all of the trivial characters.

Consider $\chi|_{k_D^\times}$. If this is trivial, then $V^{k_D^\times} = V_\psi$. The only other case in which it can be nontrivial is if $\chi|_{k_D^\times}$ is the dual of one of the characters $x \mapsto \left(\frac{\sigma(x)}{x}\right)^{p^i}$ appearing in V_ϕ, in which case we get precisely one copy of the trivial $k_D^\times$-representation.

In the first case where $\chi|_{k_D^\times}$ is trivial, $V^{k_D^\times} = V_\psi \otimes \chi$ is simply a direct sum of copies of χ. Then for an index set I as in Theorem 17 we obtain

$$\mathrm{H}^1(\varpi_D^{a\mathbf{Z}}, V^{k_D^\times}) \simeq \bigoplus_{i \in I} \mathrm{H}^1(\varpi_D^{a\mathbf{Z}}, \chi^{k_D^\times}).$$

As each H^1 group vanishes for any nontrivial action, this is 0 unless $\chi = \mathbf{1}$ in which case it is isomorphic to V_ψ as a vector space.

In the second case, $\chi|_{k_D^\times}$ is the dual of one of the characters $x \mapsto \left(\frac{\sigma(x)}{x}\right)^{p^i}$ appearing in V_ϕ. This means $a = d$, and so the $\varpi_D^{d\mathbf{Z}}$-module structure on $V^{k_D^\times}$ is trivial. Then $\mathrm{H}^1(D_d^\times/K, \mathrm{H}^1(K, \chi)) \simeq \mathrm{H}^1(\varpi_D^{d\mathbf{Z}}, \overline{\mathbf{F}}_p) \simeq \overline{\mathbf{F}}_p$. □

The most difficult component to understand in the exact sequence of Proposition 26 is $\mathrm{H}^2(K, \chi)^{D_a^\times/K}$. As with $\mathrm{H}^1(K, \chi)$, the action of K is trivial so we equivalently compute $\mathrm{H}^2(K, \overline{\mathbf{F}}_p) \otimes \chi$, and then extract the multiplicity of the trivial representation when regarded as a representation of $D^\times/K$ via the conjugation action. This then determines $\mathrm{H}^2(K, \chi)^{D^\times/K}$.

Although we will be unable to produce a complete description of $\mathrm{H}^2(K, \overline{\mathbf{F}}_p)$, we can use the Kunneth formula to decompose this space into simpler spaces that we can extract information from using various methods.

Lemma 28. Let V_ϕ and V_ψ be as in Theorem 17. The homomorphisms in $\mathrm{H}^1(1 + \pi_F \mathcal{O}_F, \overline{\mathbf{F}}_p)$ are the restrictions to $1 + \pi_F\mathcal{O}_F$ of the homomorphisms in V_ψ. The homomorphisms in $\mathrm{H}^1(K_{\mathrm{Nrd}=1}, \overline{\mathbf{F}}_p)$ are the restrictions to $K_{\mathrm{Nrd}=1}$ of the homomorphisms in V_ϕ. Both of these restrictions have trivial kernel.

Proof. From the decomposition in Lemma 18 we have

$$\mathrm{H}^1(K, \overline{\mathbf{F}}_p) \simeq \mathrm{H}^1(1 + \pi_F\mathcal{O}_F, \overline{\mathbf{F}}_p) \oplus \mathrm{H}^1(K_{\mathrm{Nrd}=1}, \overline{\mathbf{F}}_p).$$

Any homomorphism $\varphi \in \mathrm{H}^1(1 + \pi_F\mathcal{O}_F, \overline{\mathbf{F}}_p)$ can thus be extended trivially to $K_{\mathrm{Nrd}=1}$, giving a homomorphism $\overline{\varphi}$ on all of K. Writing $\overline{\varphi} = \phi + \psi$ for some $\phi \in V_\phi$ and $\psi \in V_\psi$, we can restrict back to $1 + \pi_F\mathcal{O}_F$ to get $\varphi = \psi|_{1+\pi_F\mathcal{O}_F}$ because ϕ restricts to 0 on $1 + \pi_F\mathcal{O}_F$. The restriction $\psi|_{1+\pi_F\mathcal{O}_F}$ is 0 if and only if $\psi = 0$ because the $\mathrm{Nrd}_{1+\pi_F\mathcal{O}_F}$ still surjects onto $1 + \pi_F\mathcal{O}_F$. The argument for $\mathrm{H}^1(K_{\mathrm{Nrd}=1}, \overline{\mathbf{F}}_p)$ is identical because every element of V_ψ restricts to 0 in $K_{\mathrm{Nrd}=1}$ and the only map in V_ϕ that restricts to 0 in $K_{\mathrm{Nrd}=1}$ is 0. □

Using Lemma 18, the Kunneth formula for profinite groups with coefficients in a field and a trivial action then gives

$$\mathrm{H}^2(K, \overline{\mathbf{F}}_p) \simeq \bigoplus_{i+j=2} \mathrm{H}^i(1 + \pi_F\mathcal{O}_F, \overline{\mathbf{F}}_p) \otimes \mathrm{H}^j(K_{\mathrm{Nrd}=1}, \overline{\mathbf{F}}_p).$$

We note that $K_{\mathrm{Nrd}=1}$ is profinite because it is a closed normal subgroup of a profinite group. Additionally, as $K_{\mathrm{Nrd}=1} = \ker \mathrm{Nrd} \cap K$ and $1 + \pi_F\mathcal{O}_F$ is central, both subgroups are normal in $D^\times$ - this means each cohomology group appearing in the decomposition is a $D_a^\times/K$ representation.

We first make some computations of the $(i, j) = (0, 2)$ term $\mathrm{H}^0(1 + \pi_F\mathcal{O}_F, \overline{\mathbf{F}}_p) \otimes \mathrm{H}^2(K_{\mathrm{Nrd}=1}, \overline{\mathbf{F}}_p)$ using the Bockstein homomorphism. The Bockstein map will only provide enough information to put a lower bound on the dimension of this term.

This will require us to make some observations about the elements of $\mathrm{H}^1(K, \mathbf{F}_p)$ and $\mathrm{H}^1(K, \mathbf{Z}/p^2\mathbf{Z})$ with the trivial action that are analogous to our computations of $\mathrm{H}^1(K, \overline{\mathbf{F}}_p)$ in §3.

Lemma 29. We have a decomposition

$$\mathrm{H}^1(K, \mathbf{F}_p) \simeq V'_\psi \oplus V'_\phi,$$

where these subspaces are defined in the same way as V_ψ and V_ϕ in Theorem 17 except as homomorphisms to $\mathbf{F}_p$.

- The space V'_ϕ is isomorphic to $\mathrm{Hom}(k_D, \mathbf{F}_p)$, which has dimension df and a basis given by any dual basis to a basis of k_D over $\mathbf{F}_p$.
- A basis of V'_ψ are the maps $\psi^{\eta_i} = \eta_i \circ \mathrm{Nrd}$ where the η_i are a basis of $\mathrm{Hom}(1+\pi_F\mathcal{O}_F, \mathbf{F}_p)$ and the i are in some index set I with size ef when F is a p-adic field and $I = \mathbf{N}$ when F is a local function field.

Proof. This is entirely analogous to the proof of Theorem 17. In particular, we get the same upper bound in the dimension that we had in Corollary 16 by factoring homomorphisms through the quotient by $[K, K]K^p$. The only part of the proof that is different is showing that a basis of η_j of $\mathrm{Hom}(k_D, \mathbf{F}_p)$ gives a basis ϕ^{η_j} by precomposing with the quotient map $K \to K/(1 + \varpi_D^2 \mathcal{O}_D)$. This follows from the surjectivity of this quotient map. □

Lemma 30. We have a decomposition

$$\mathrm{H}^1(K, \mathbf{Z}/p^2\mathbf{Z}) \simeq V''_\psi \oplus V''_\phi$$

where the subspaces are defined analogously to the subspaces in Lemma 29 except that they now map into $\mathbf{Z}/p^2\mathbf{Z}$.

- The space V''_ϕ is isomorphic to $\mathrm{Hom}(k_D, \mathbf{Z}/p^2\mathbf{Z}) \simeq (p\mathbf{Z}/p^2\mathbf{Z})^{df} \simeq (\mathbf{Z}/p\mathbf{Z})^{df}$.
- The space V''_ψ is isomorphic to $\mathrm{Hom}(1 + \pi_F\mathcal{O}_F, \mathbf{Z}/p^2\mathbf{Z}) \simeq \bigoplus_{i\in I}(\mathbf{Z}/p^2\mathbf{Z})$, where I is an index set of order ef when F is a p-adic field, and $I = \mathbf{N}$ when F is a local function field.

Proof. By Corollary 8, we can compute that $K^{p^2} = 1 + \varpi_D^{2de+1}\mathcal{O}_D$ in the p-adic case, while in the local function field case we have $K^{p^2} = 1 + (\varpi_D\mathcal{O}_D)^{p^2}$. Any map to $\mathbf{Z}/p^2\mathbf{Z}$ factors through the quotient $\frac{K}{[K,K]K^{p^2}}$. Using Proposition 15, we obtain an analogous version of Corollary 16 to bound the number of homomorphisms overall or those which are nontrivial on $K/K^{(di+1)}$ in the local function field case. Then entirely analogously to Theorem 17, we can show that the subspaces V''_ψ and V''_ϕ meet this upper bound and have the desired descriptions. The only significant change is that we need to modify our computation of V''_ψ and V''_ϕ somewhat.

For V''_ϕ, we again recover that this is isomorphic to $\mathrm{Hom}(k_D, \mathbf{Z}/p^2\mathbf{Z})$. As a group, k_D consists of all p-torsion elements, so this is $(p\mathbf{Z}/p^2\mathbf{Z})^{df}$. As for V''_ψ, in the p-adic case because there is no p-torsion in K we have

$$1 + \pi_F\mathcal{O}_F \simeq \mathbf{Z}_p^{[F:\mathbf{Q}_p]}$$

as a topological group and hence we have an isomorphism $\mathrm{Hom}(1 + \pi_F\mathcal{O}_F, \mathbf{Z}/p^2\mathbf{Z}) \simeq \bigoplus_{1\leq i\leq ef} \mathbf{Z}_p/p^2\mathbf{Z}_p$ which is the same as the claim. In the local function field case, $1 + \pi_F\mathcal{O}_F \simeq \mathbf{Z}_p^{\mathbf{N}}$ and similar reasoning gives the claim. □

Proposition 31. With V_ϕ as in Theorem 17, we have $\mathrm{H}^1(K_{\mathrm{Nrd}=1}, \overline{\mathbf{F}}_p) \simeq V_\phi$ and there is a $D_a^\times/K$-equivariant Bockstein homomorphism β_p so that the composition

$$\mathrm{H}^1(K_{\mathrm{Nrd}=1}, \overline{\mathbf{F}}_p) \xrightarrow{\beta_p} \mathrm{H}^2(K_{\mathrm{Nrd}=1}, \overline{\mathbf{F}}_p) \xrightarrow{\simeq} \mathrm{H}^0(1 + \pi_F\mathcal{O}_F, \overline{\mathbf{F}}_p) \otimes \mathrm{H}^2(K_{\mathrm{Nrd}=1}, \overline{\mathbf{F}}_p)$$

is an injection.

Proof. The isomorphism $\mathrm{H}^1(K_{\mathrm{Nrd}=1}, \overline{\mathbf{F}}_p) \simeq V_\phi$ follows from Lemma 28. We can repeat the same argument with homomorphisms into $\mathbf{Z}/p^2\mathbf{Z}$ and $\mathbf{F}_p$ to conclude that $\mathrm{H}^1(K_{\mathrm{Nrd}=1}, \mathbf{Z}/p^2\mathbf{Z}) \simeq V''_\phi$ (as in Lemma 30) and $\mathrm{H}^1(K_{\mathrm{Nrd}=1}, \mathbf{F}_p) \simeq V'_\phi$ (as in Lemma 29). Because we have the isomorphisms $V''_\phi \simeq (\mathbf{Z}/p\mathbf{Z})^{df} \simeq V'_\phi$, the reduction map $\mathrm{H}^1(K_{\mathrm{Nrd}=1}, \mathbf{Z}/p^2\mathbf{Z}) \to \mathrm{H}^1(K_{\mathrm{Nrd}=1}, \mathbf{F}_p)$ in the long exact sequence arising from the short exact sequence

$$0 \longrightarrow \mathbf{F}_p \longrightarrow \mathbf{Z}/p^2\mathbf{Z} \longrightarrow \mathbf{F}_p \longrightarrow 0$$

is the 0 map. By exactness, we see that the Bockstein map $\beta_p : \mathrm{H}^1(K_{\mathrm{Nrd}=1}, \mathbf{F}_p) \to \mathrm{H}^2(K_{\mathrm{Nrd}=1}, \mathbf{F}_p)$ is an injection. The map β_p is also $D_a^\times/K$-equivariant because is arises from a long exact sequence of $D_a^\times/K$ representations. Upon tensoring with $\overline{\mathbf{F}}_p$ to change to the desired coefficient field, we get the injective Bockstein map described in the proposition. To get the map that we compose with β_p, note that $\mathrm{H}^0(1+\pi_F\mathcal{O}_F, \overline{\mathbf{F}}_p) \simeq \overline{\mathbf{F}}_p$, so the cup product $\mathrm{H}^0(1+\pi_F\mathcal{O}_F, \overline{\mathbf{F}}_p) \otimes \mathrm{H}^2(K_{\mathrm{Nrd}=1}, \overline{\mathbf{F}}_p) \to \mathrm{H}^2(K_{\mathrm{Nrd}=1}, \overline{\mathbf{F}}_p)$ is a $D_a^\times/K$-equivariant isomorphism. □

We now compute the term $\mathrm{H}^1(1+\pi_F\mathcal{O}_F, \overline{\mathbf{F}}_p) \otimes \mathrm{H}^1(K_{\mathrm{Nrd}=1}, \overline{\mathbf{F}}_p)$ in the Kunneth formula. Lemma 28 essentially gives this term because it tells us both of these cohomology groups, but we still need to compute the action of $D_a^\times/K$.

Proposition 32. As $D_a^\times/K$ representations, we have

$$\mathrm{H}^1(1+\pi_F\mathcal{O}_F, \overline{\mathbf{F}}_p) \otimes \mathrm{H}^1(K_{\mathrm{Nrd}=1}, \overline{\mathbf{F}}_p) \simeq V_\psi \otimes V_\phi.$$

Proof. The map in the Kunneth formula embedding the product $\mathrm{H}^1(1+\pi_F\mathcal{O}_F, \overline{\mathbf{F}}_p) \otimes \mathrm{H}^1(K_{\mathrm{Nrd}=1}, \overline{\mathbf{F}}_p)$ into $\mathrm{H}^2(K, \overline{\mathbf{F}}_p)$ as a $D_a^\times/K$ module is given by computing the cup product $\alpha \otimes \beta \mapsto p_1^*(\alpha) \smile p_2^*(\beta)$, where p_i are the projection maps from K onto $K_{\mathrm{Nrd}=1}$ and $1+\pi_F\mathcal{O}_F$. Because the cup product respects the action of $D^\times$, namely

$$d \cdot (\alpha \smile \beta) = (d \cdot \alpha) \smile (d \cdot \beta),$$

the map respects the $D_a^\times/K$ representation structure on the tensor product $\mathrm{H}^1(1+\pi_F\mathcal{O}_F, \overline{\mathbf{F}}_p) \otimes \mathrm{H}^1(K_{\mathrm{Nrd}=1}, \overline{\mathbf{F}}_p)$. By Lemma 28, these may be identified with V_ψ and V_ϕ respectively; since the identification is via restriction from $\mathrm{H}^1(K, \overline{\mathbf{F}}_p)$ the $D_a^\times/K$ module structure is preserved. □

Remark. We may also verify explicitly that these cup products are nontrivial. In the notation of Theorem 17, consider $\psi^{\eta_{i_0}} \smile \phi^{\eta_{j_0}}$. Suppose that this is trivial in $\mathrm{H}^2(K, \overline{\mathbf{F}}_p)$, or that

$$\psi^{\eta_{i_0}}(k)\phi^{\eta_{j_0}}(k') = h(kk') - h(k) - h(k')$$

for some function $h : K \to \overline{\mathbf{F}}_p$. Because $K = K_{\mathrm{Nrd}=1} \times (1+\pi_F\mathcal{O}_F)$, we can write any $k \in K$ uniquely as $k = k_1k_2$ for $k_1 \in 1+\pi_F\mathcal{O}_F$ and $k_2 \in K_{\mathrm{Nrd}=1}$. As $\phi^{\eta_{j_0}}(k_1)\psi^{\eta_{i_0}}(k_2) = 0 \cdot 0 = 0$, we then obtain

$$h(k) = h(k_1k_2) = h(k_1) + h(k_2) = \sum_i \alpha_i \psi^{\eta_i}(k_1) + \sum_j \beta_j \phi^{\eta_j}(k_2)$$

for $\alpha_i, \beta_j \in \overline{\mathbf{F}}_p$. This follows because the restriction of h to $1+\pi_F\mathcal{O}_F$ or $K_{\mathrm{Nrd}=1}$ must be a homomorphism, so we can apply Lemma 28. But this function is actually a homomorphism on K, because writing $k' = k'_1k'_2$ for the same decomposition we have $h(kk') = h((k_1k'_1)(k_2k'_2))$ as $1+\pi_F\mathcal{O}_F$ is central. Then applying the above formula and using that ψ^{η_i} and ϕ^{η_j} are homomorphisms, we see $h(kk') = h(k) + h(k')$. As

$\psi^{\eta_{i_0}}(k)\phi^{\eta_{j_0}}(k')$ is not identically 0 but $h(kk') - h(k) - h(k')$ is, we have a contradiction and the claim follows.

We now tackle the final component of the Kunneth decomposition of $\mathrm{H}^2(K, \overline{\mathbf{F}}_p)$.

Proposition 33. We have $\mathrm{H}^2(1 + \pi_F\mathcal{O}_F, \overline{\mathbf{F}}_p) \otimes \mathrm{H}^0(K_{\mathrm{Nrd}=1}, \overline{\mathbf{F}}_p) \simeq \overline{\mathbf{F}}_p^{\binom{ef}{2}}$ when F is a p-adic field and of countable dimension where F is a local function field. The representation is trivial in either case.

Proof. Because the action of $K_{\mathrm{Nrd}=1}$ is trivial, we have $\mathrm{H}^0(K_{\mathrm{Nrd}=1}, \overline{\mathbf{F}}_p) \simeq \overline{\mathbf{F}}_p$ with a trivial $D_a^\times/K$ action. As for $\mathrm{H}^2(1 + \pi_F\mathcal{O}_F, \overline{\mathbf{F}}_p)$, the action is trivial because $1 + \pi_F\mathcal{O}_F$ is central and $D_a^\times/K$ acts by conjugation.

The dimension itself follows from the Kunneth formula. We have $1 + \pi_F\mathcal{O}_F \simeq \mathbf{Z}_p^{ef}$ in the p-adic case, from which the Kunneth formula gives

$$\mathrm{H}^2(1 + \pi_F\mathcal{O}_F, \overline{\mathbf{F}}_p) \simeq \bigoplus_{\sum_i x_i = 2} \bigotimes_{1 \leq i \leq ef} \mathrm{H}^{x_i}(\mathbf{Z}_p, \overline{\mathbf{F}}_p).$$

As the cohomological dimension of $\mathbf{Z}_p$ is one, we get a copy of $\overline{\mathbf{F}}_p$ for each pair of generators. Similarly, in the local function field case from $1 + \pi_F\mathcal{O}_F \simeq \mathbf{Z}_p^{\mathbf{N}}$ we see the result has countable dimension, as the set of pairs of elements in $\mathbf{N}$ is countable. □

Now we may summarize these results.

Theorem 34. For any character χ of $D_a^\times$, by Proposition 26 we have an exact sequence

$$0 \longrightarrow \mathrm{H}^1(D_a^\times/K, \mathrm{H}^1(K, \chi)) \longrightarrow \mathrm{Ext}^2_{D_a^\times}(\mathbf{1}, \chi) \longrightarrow \mathrm{H}^2(K, \chi)^{D_a^\times/K} \longrightarrow 0.$$

The leftmost term is computed by Lemma 27. The rightmost term is the multiplicity of the trivial representation in $\mathrm{H}^2(K, \overline{\mathbf{F}}_p) \otimes \chi$, where

$$\mathrm{H}^2(K, \overline{\mathbf{F}}_p) \simeq \bigoplus_{i+j=2} \mathrm{H}^i(1 + \pi_F\mathcal{O}_F, \overline{\mathbf{F}}_p) \otimes \mathrm{H}^j(K_{\mathrm{Nrd}=1}, \overline{\mathbf{F}}_p)$$

as $D_a^\times/K$-representations. Among these:

- The component $\mathrm{H}^0(1 + \pi_F\mathcal{O}_F, \overline{\mathbf{F}}_p) \otimes \mathrm{H}^2(K_{\mathrm{Nrd}=1}, \overline{\mathbf{F}}_p)$ contains a subrepresentation isomorphic to V_ϕ by Proposition 31.
- The component $\mathrm{H}^1(1 + \pi_F\mathcal{O}_F, \overline{\mathbf{F}}_p) \otimes \mathrm{H}^1(K_{\mathrm{Nrd}=1}, \overline{\mathbf{F}}_p)$ is isomorphic to $V_\psi \otimes V_\phi$ as a representation by Proposition 32.
- The component $\mathrm{H}^2(1+\pi_F\mathcal{O}_F, \overline{\mathbf{F}}_p) \otimes \mathrm{H}^0(K_{\mathrm{Nrd}=1}, \overline{\mathbf{F}}_p)$ is isomorphic to $\overline{\mathbf{F}}_p^{\binom{ef}{2}}$ with a trivial $D_a^\times/K$ representation structure by Proposition 33.

Here, $V_\psi \oplus V_\phi$ is the $D_a^\times/K$ module obtained by restricting the result of Proposition 23. Entirely analogously to Theorem 24, we know the multiplicity of the trivial representation in each component we know after tensoring with χ. Namely, V_ψ gives no contribution unless χ is trivial, and V_ϕ gives no contribution unless $a = d$ and χ is a character of $F^\times\mathcal{O}_D^\times$ extended trivially from $x \mapsto \left(\frac{x}{\sigma(x)}\right)^{p^i}$ on $k_D^\times$.

This is not a complete answer because in Proposition 31 we only have an injection. The Bockstein homomorphism may only give partial information, so there could be additional copies of the trivial representation that do not get counted. In at least one case, however, this theorem fully answers the question:

Example 35. Let D be a quaternion algebra over $\mathbf{Q}_p$. As we will see in the following section, K is a Poincaré duality group and in this case we have a non-degenerate bilinear form $\mathrm{H}^i(K,\mathbf{F}_p) \times \mathrm{H}^{4-i}(K,\mathbf{F}_p) \to \mathrm{H}^4(K,\mathbf{F}_p)$. The Euler characteristic of K will be 0 using the main result of [Tot99], so we can deduce that $\mathrm{H}^2(K,\overline{\mathbf{F}}_p) = 4$. Then Theorem 34 gives all of $\mathrm{H}^2(K,\overline{\mathbf{F}}_p)$: the Bockstein map gives 2 dimensions, as does the cup product.

We cannot generalize this, because this exploits the fact that $d^2ef = 4$. In any other case, it will be large enough that this no longer bounds the dimension of $\mathrm{H}^2(K,\overline{\mathbf{F}}_p)$. On the other hand, we can always combine the results of Theorem 20, Proposition 26, Lemma 27, and Theorem 34 to place a lower bound on the dimension of $\mathrm{Ext}^2_{D^\times}(\rho,\rho')$ for any irreducible representations ρ and ρ'. Below we demonstrate this for the $d = 2$ case with a p-adic field.

Example 36. Suppose that F is a p-adic field and D is a quaternion algebra over F. As in Example 25, let $\rho = \mathrm{Ind}^{\times}_{D_a^\times} \chi$ and $\rho' = \mathrm{Ind}^{\times}_{D_{a'}^\times} \chi'$, so that Theorem 20 gives a sum for the dimension of the extension group. Just as in Example 25, we have three different cases to consider to evaluate this sum. When $a = a' = 1$, we have

$$\dim \mathrm{Ext}^2_{D^\times}(\rho,\rho') = \dim \mathrm{Ext}^2_{D^\times}(\mathbf{1},\chi'\otimes\chi^*).$$

Recalling from Example 25 that $\mathrm{Res}^{D^\times}_{F^\times\mathcal{O}_D^\times}\chi_{1,n,m} = \chi_{2,n^2,(q+1)m}$, when $a = 1$ and $a' = 2$ we have

$$\dim \mathrm{Ext}^2_{D^\times}(\rho,\rho') = \dim \mathrm{Ext}^2_{F^\times\mathcal{O}_D^\times}(\mathbf{1},\chi'\otimes \mathrm{Res}^{D^\times}_{F^\times\mathcal{O}_D^\times}\chi^*).$$

Finally, when $a = a' = 2$, we have

$$\dim \mathrm{Ext}^2_{D^\times}(\rho,\rho') = \dim \mathrm{Ext}^2_{F^\times\mathcal{O}_D^\times}(\mathbf{1},\chi'\otimes\chi^*) + \dim \mathrm{Ext}^2_{F^\times\mathcal{O}_D^\times}(\mathbf{1},\chi'\otimes(\chi^{\varpi_D})^*).$$

So to compute the dimension of $\mathrm{Ext}^2_{D^\times}(\rho,\rho')$ we must compute at most two dimensions of the form $\dim \mathrm{Ext}^2_{D_a^\times}(\mathbf{1},\tilde\chi)$ for $a = 1,2$ and characters $\tilde\chi$ of $D_a^\times$. By Proposition 26, $\dim \mathrm{Ext}^2_{D_a^\times}(\mathbf{1},\tilde\chi) = \dim \mathrm{H}^1(D_a^\times/K, \mathrm{H}^1(K,\tilde\chi)) + \dim \mathrm{H}^2(K,\tilde\chi)^{D_a^\times/K}$. By Lemma 27, the first term in this sum is either 1, 0, or $\dim V_\psi = ef$.

For the $\dim \mathrm{H}^2(K,\tilde\chi)^{D_a^\times/K}$ term, we consider the decomposition given in Theorem 34 as a $D_a^\times/K$ representation and count the number of copies of the trivial representation. As described at the end of Theorem 34 we have the following cases:

- When $\tilde\chi$ is trivial, we get $\mathbf{F}_p^{\binom{ef}{2}}$ from $\mathrm{H}^2(1+\pi_F\mathcal{O}_F,\overline{\mathbf{F}}_p)\otimes \mathrm{H}^2(K_{\mathrm{Nrd}=1},\overline{\mathbf{F}}_p)$.
- When $a = 2$ and $\tilde\chi$ is extended trivially from $x \mapsto \left(\frac{x}{x^q}\right)^{p^i}$ on $k_D^\times$ we get $\dim V_\phi = ef$ copies of a trivial representation from $V_\phi \otimes V_\psi$ and a single copy from V_ϕ via the Bockstein.

When $F = \mathbf{Q}_p$, by Example 35 this will give the dimension exactly. Otherwise, it will give a lower bound.

5.2. **Poincaré duality.** In [Laz65], many fundamental results about p-adic analytic pro-p groups are shown which will be helpful in understand the structure of the higher cohomology groups in the case where F is a p-adic field. Here, by a p-adic analytic group we mean a group with the structure of an open subgroup of an analytic manifold over $\mathbf{Q}_p$ such that the group multiplication and inversion operations are analytic.

Theorem ([Laz65] §2.5.8)**.** *Let G be a p-adic analytic pro-p group and with no p-torsion, and let $r = \dim_{\mathbf{Q}_p} G$. Then G is a Poincaré duality group of dimension r over $\mathbf{F}_p$. That is,*

- *$\mathrm{H}^n(G,\mathbf{F}_p)$ is finite dimensional for all $n \in \mathbf{N}$.*

· $\dim_{\mathbf{F}_p} \mathrm{H}^r(G, \mathbf{F}_p) = 1$.
· The cup product

$$\mathrm{H}^n(G, \mathbf{F}_p) \times \mathrm{H}^{r-n}(G, \mathbf{F}_p) \to \mathrm{H}^r(G, \mathbf{F}_p)$$

is a non-degenerate bilinear form.

Here, all cohomology taken is continuous.

We will be interested in the case of $K = G$, and we will also want to understand how the bilinear form interacts with the $D_a^\times/K$-representation structure on the cohomology group. We note that K is a p-adic analytic group as it is an open subgroup of $D^\times$, and since $p > de + 1$ it has no p-torsion. Thus, K is a Poincaré duality group. The the most difficult part of the following result is that the $D^\times/K$-module structure on the top cohomology is trivial. This is shown in [Koz20] via Proposition 4.16 (see §5.1) for connected reductive groups. Using the general method of Theorem 7.2 in [Koz17], we can show this by finding a uniform pro-p subgroup and computing explicitly the action on its first cohomology.

Proposition 37. As $D_a^\times/K$-modules, we have $\mathrm{H}^n(K, \overline{\mathbf{F}}_p)^* \simeq \mathrm{H}^{r-n}(G, \overline{\mathbf{F}}_p)$. Here, V^* denotes the dual representation.

Proof. By virtue of being a Poincaré duality group, the cup product

$$\mathrm{H}^n(K, \mathbf{F}_p) \times \mathrm{H}^{r-n}(K, \mathbf{F}_p) \to \mathrm{H}^r(K, \mathbf{F}_p) \simeq \mathbf{F}_p$$

is a non-degenerate bilinear form. However, the cup product also behaves well with respect to the $D_a^\times/K$-action. Let d be an element of $D_a^\times/K$. Then we have for $\alpha \in \mathrm{H}^n(K, \mathbf{F}_p)$ and $\beta \in \mathrm{H}^{r-n}(K, \mathbf{F}_p)$ that

$$d \cdot (\alpha \smile \beta) = (d \cdot \alpha) \smile (d \cdot \beta),$$

which can be easily seen from the definition of the cup product using cocycles. We will show the $D_a^\times/K$-module structure on $\mathrm{H}^r(K, \mathbf{F}_p)$ is trivial. Consider the subgroup $K^{(de+1)} := 1 + \varpi_D^{de+1}\mathcal{O}_D$. Since this is an open subgroup of K, the corestriction map

$$\mathrm{Cor}_{K^{(de+1)}}^K : \mathrm{H}^r(K^{(de+1)}, \mathbf{F}_p) \to \mathrm{H}^r(K, \mathbf{F}_p)$$

is an isomorphism by the proof of Proposition 30 in [Ser13a]. However, one may also check that $K^{(de+1)}$ is a uniform pro-p group - it is clearly pro-p, so we will check that it is uniform. Its Frattini subgroup is in fact $K^{(2de+1)}$, by computing pth powers (which equal this) and observing that $[K^{(de+1)}, K^{(de+1)}] \subset K^{(2de+1)}$. This latter observation is known as being *uniformly powerful*. As $p > de + 1$, this is torsion-free and the group is finitely generated since $\dim_{\mathbf{F}_p} \mathrm{H}^1(K^{(de+1)}, \mathbf{F}_p) = \dim_{\mathbf{F}_p} K^{(de+1)}/K^{(2de+1)} = d^2ef$ is finite and by [Ser13a] §4.2 this dimension equals the number of topological generators. Then by Theorem 4.5 of [DDSMS03], we conclude that this is a uniform pro-p group.

It then follows from results of [Laz65], which are also shown in Theorem 5.1.5 of [SW00], that $\mathrm{H}^r(K^{(de+1)}, \mathbf{F}_p) \simeq \bigwedge^r \mathrm{H}^1(K^{(de+1)}, \mathbf{F}_p)$, as the cohomology ring of a uniform pro-p group is an exterior algebra. It then suffices to compute the conjugation action of on this cohomology group. We wish to show that the action has determinant one - because the Frattini subgroup is $K^{(2de+1)}$, we equivalently compute the determinant on the $\mathbf{F}_p$ vector space $K^{(de+1)}/K^{(2de+1)}$. This computation can be done explicitly, as the space of homomorphisms is isomorphic to $V_\phi^{\oplus de}$ as a $D_a^\times/K$-module - a calculation shows $k_D^\times$ and ϖ_D^a both act with determinant one.

From the non-degeneracy of the bilinear form the claim follows for $\mathbf{F}_p$ coefficients. We have

$$d \cdot \alpha \smile \beta = dd^{-1} \cdot \alpha \smile d^{-1} \cdot \beta = \alpha \smile d^{-1} \cdot \beta$$

since acting by d^{-1} on both arguments does nothing, since this is the same as acting by d^{-1} on $\mathrm{H}^r(K, \mathbf{F}_p)$ which has a trivial action. By definition, the representation is the dual representation since the cup product is a non-degenerate bilinear form. This extends to $\overline{\mathbf{F}}_p$ coefficients once we tensor with $\overline{\mathbf{F}}_p$, and we note that there is no Tor obstruction. □

We will now again use the spectral sequence

$$E_2^{p,q} = \mathrm{H}^p(D_a^\times/K, \mathrm{H}^q(K,\chi)) \implies \mathrm{H}^{p+q}(D_a^\times, \chi) \simeq \mathrm{Ext}^{p+q}_{D_a^\times}(\mathbf{1}, \chi).$$

The main work has already been done in Proposition 26 and the previous proposition.

Lemma 38. Let $r = d^2ef$ and let χ be an arbitrary character of $D_a^\times$. There is an exact sequence

$$0 \to \mathrm{H}^1(D_a^\times/K, \mathrm{H}^{r-i+1}(K,\chi)^*) \to \mathrm{Ext}^i_{D_a^\times}(\mathbf{1}, \chi^*) \to (\mathrm{H}^{r-i}(K,\chi)^*)^{D_a^\times/K} \to 0.$$

Proof. This follows from Proposition 26 combined with the previous proposition. □

For $i = r+1$, we get $\mathrm{Ext}^{r+1}_{D_a^\times}(\mathbf{1}, \chi) \simeq \mathrm{H}^1(D_a^\times/K, (\chi)^*)$, which is trivial unless $\chi = \mathbf{1}$ in which case we get $\overline{\mathbf{F}}_p$. After $r+1$, the extensions are all trivial.

We can make use of this lemma when $i = r$ and $i = r-1$ as well, since we have results about the surrounding terms in the exact sequence. When $i = r$, we get

$$0 \longrightarrow \mathrm{H}^1(D_a^\times/K, \mathrm{H}^1(K,\chi)^*) \longrightarrow \mathrm{Ext}^r_{D_a^\times}(\mathbf{1}, \chi^*) \longrightarrow (\chi^*)^{D_a^\times/K} \longrightarrow 0.$$

By the same methods Lemma 27, we may determine the first group. Just as in Lemma 27, the dimension is the multiplicity of the trivial representation - we take a dual, and so this multiplicity is preserved as $\mathbf{1}^* = \mathbf{1}$.

When $i = r-1$, we have

$$0 \to \mathrm{H}^1(D_a^\times/K, \mathrm{H}^2(K,\chi)^*) \to \mathrm{Ext}^{r-1}_{D_a^\times}(\mathbf{1}, \chi^*) \to (\mathrm{H}^1(K,\chi)^*)^{D_a^\times/K} \to 0.$$

For the rightmost term, above we have already shown that its dimension matches those computed in Theorem 24. Namely, for $\chi = \mathbf{1}$ it has dimension ef as a vector space over $\overline{\mathbf{F}}_p$, and for $a = d$ and χ extended trivially from some character $x \mapsto \left(\frac{x}{\sigma(x)}\right)^{p^i}$ of $k_D^\times$ it is $\overline{\mathbf{F}}_p$. As for the leftmost term, we have partial information given by Theorem 34.

6. Cohomology for $\mathrm{GL}_2(D)$

We now shift our attention from the group $D^\times = \mathrm{GL}_1(D)$, and instead consider analogous computations for the group $\mathrm{GL}_2(D)$. Just as we computed the $D^\times/K$-representation structure $\mathrm{H}^1(K, \overline{\mathbf{F}}_p) = \mathrm{Hom}(K, \overline{\mathbf{F}}_p)$ in the GL_1 case, where K was the pro-p Iwahori subgroup $1 + \varpi_D \mathcal{O}_D$ of $D^\times$, in GL_2 we will compute the $\mathcal{H}_{I_1}$-module structure of $\mathrm{H}^1(I_1, \overline{\mathbf{F}}_p) = \mathrm{Hom}(I_1, \overline{\mathbf{F}}_p)$, where I_1 is a certain pro-p Iwahori subgroup.

We will first define the Bruhat-Tits tree of $\mathrm{GL}_2(D)$.

Definition. The Bruhat-Tits tree $\mathfrak{X}$ of $\mathrm{GL}_2(D)$ is a 1-dimensional simplicial complex. The vertices are given by homethety classes of $\mathcal{O}_D$-lattices in D^2. Two lattices Λ, Λ' are neighboring if

$$\varpi_D \Lambda \subsetneq \Lambda' \subsetneq \Lambda.$$

The edges of the Bruhat-Tits tree are given by connecting neighboring lattices.

The Bruhat-Tits tree of $\mathrm{GL}_2(D)$ gives us a great deal of geometric information about the group. The stabilizer of an edge is the stabilizer of a lattice chain of neighboring lattices - these give Iwahori subgroups.

Proposition. The Bruhat-Tits tree $\mathfrak{X}$ of $\mathrm{GL}_2(D)$ is a $|\mathbf{P}^1(k_D)|$-regular tree.

Within $\mathrm{GL}_2(D)$, we will make a choice of an Iwahori subgroup I which corresponds to the lattice chain $\mathcal{O}_D \oplus \varpi_D \mathcal{O}_D \subset \mathcal{O}_D \oplus \mathcal{O}_D$. For our results in this section, the choice of such a subgroup does not matter as the corresponding pro-p Iwahori subgroups will be conjugate and hence isomorphic. Just as we had the filtration $\mathcal{O}_D^\times \triangleright 1 + \varpi_D \mathcal{O}_D \triangleright 1 + \varpi_D^2 \mathcal{O}_D \triangleright \cdots$ in the GL_1 case, we have a Moy-Prasad filtration $I \triangleright I_1 \triangleright I_2 \triangleright I_3 \triangleright \cdots$ of normal subgroups that will aid in our computations. Explicitly, I and these subgroups are given by

$$I = \begin{pmatrix} \mathcal{O}_D^\times & \mathcal{O}_D \\ \varpi_D \mathcal{O}_D & \mathcal{O}_D^\times \end{pmatrix}, \; I_n = \begin{pmatrix} 1 + \varpi_D^{\lfloor (n+1)/2 \rfloor} \mathcal{O}_D & \varpi_D^{\lfloor n/2 \rfloor} \mathcal{O}_D \\ \varpi_D^{1+\lfloor n/2 \rfloor} \mathcal{O}_D & 1 + \varpi_D^{\lfloor (n+1)/2 \rfloor} \mathcal{O}_D \end{pmatrix}$$

where at each step $n \geq 1$ we alternate between raising the powers of ϖ_D on the diagonal and off-diagonal entries. Similarly to the filtration of K, these subgroups have easy to understand quotients.

Lemma 39. We have $I_n / I_{n+1} \simeq k_D^2$. The quotient is identified with $\begin{pmatrix} k_D & \\ & k_D \end{pmatrix}$ if n is even, and $\begin{pmatrix} & k_D \\ k_D & \end{pmatrix}$ if n is odd.

It is the subgroup

$$I_1 = \begin{pmatrix} 1 + \varpi_D \mathcal{O}_D & \mathcal{O}_D \\ \varpi_D \mathcal{O}_D & 1 + \varpi_D \mathcal{O}_D \end{pmatrix}$$

whose degree-1 cohomology we are interested in computing. This is the pro-p Sylow subgroup of I. Note that, unlike K which is normal in $D^\times$, we do not have that I_1 is normal in $\mathrm{GL}_2(D)$.

As in §3, we first compute an upper bound on the dimension of $\mathrm{Hom}(I_1, \overline{\mathbf{F}}_p)$ by looking at commutators. Then we will explicitly construct enough linearly independent homomorphisms to meet this upper bound, hence concluding that they must form a basis.

With T, U^+, and U^- we denote the subgroups of diagonal, upper unipotent, and lower unipotent matrices in I_1. Then we have the following decomposition of I_1, known as the Iwahori decomposition.

Lemma 40. The subgroup I_1 can be written as $U^+ \cdot T \cdot U^-$.

Proof. Given any $\begin{pmatrix} w & x \\ y & z \end{pmatrix} \in I_1$, we can write

$$\begin{pmatrix} w & x \\ y & z \end{pmatrix} = \begin{pmatrix} 1 & xz^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} w - xz^{-1}y & 0 \\ 0 & z \end{pmatrix} \begin{pmatrix} 1 & 0 \\ z^{-1}y & 1 \end{pmatrix},$$

where all three of these matrices lie in I_1 because $\begin{pmatrix} w & x \\ y & z \end{pmatrix}$ does. □

This decomposition also descends to the filtration I_n, so that each I_n has a decomposition $(U^+ \cap I_n) \cdot (T \cap I_n) \cdot (U^- \cap I_n)$. The formula to prove this is the same.

One important homomorphism that we will need to compute $\mathrm{Hom}(I_1, \overline{\mathbf{F}}_p)$ is the Dieudonné determinant. For a central simple division algebra D over F, it is shown in [Die43] that there is a group homomorphism of the form

$$\alpha : \mathrm{GL}_n(D)_{\mathrm{ab}} \to D^\times / [D^\times, D^\times] \simeq F^\times.$$

Composing with the quotient q onto the abelianization, we obtain a map

$$\det := \alpha \circ q : \mathrm{GL}_n(D) \to F^\times.$$

Explicitly, for $\mathrm{GL}_2(D)$ we have the expression

$$\det \begin{pmatrix} w & x \\ y & z \end{pmatrix} = \begin{cases} \overline{-yx} \text{ if } w = 0 \\ \overline{wz - wyw^{-1}x} \text{ if } w \neq 0 \end{cases},$$

where $\overline{a}$ denotes the image of $a \in D^\times$ in $D^\times/[D^\times, D^\times] \simeq F^\times$.

By using facts about the Moy-Prasad filtration, the Iwahori decomposition, the Dieudonné determinant, and our computations for $[K,K]K^p$ in $D^\times$ in §3, we now compute a large subset of the Frattini subgroup $[I_1, I_1]I_1^p$. Later we will show that this subset is actually equal to the entire Frattini subgroup.

Proposition 41. We have

$$[I_1, I_1]I_1^p \supset (U^+ \cap I_2) \cdot T_{\det=1} \cdot T^p \cdot (U^- \cap I_2).$$

Proof. We observe that $[I_1, I_1] \subset I_2$. The Iwahori decomposition restricts to I_2, simply by replacing each component with the intersection with I_2. We first show how to produce $U^+ \cap I_2$ and $U^- \cap I_2$ as commutators. Let $x \in 1 + \varpi_D \mathcal{O}_D$. We can compute that

$$\left[\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & x^{-1} \end{pmatrix}\right] = \begin{pmatrix} 1 & x-1 \\ 0 & 1 \end{pmatrix},$$

and

$$\left[\begin{pmatrix} 1 & 0 \\ -\varpi_D & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix}\right] = \begin{pmatrix} 1 & 0 \\ (x-1)\varpi_D & 1 \end{pmatrix}.$$

As $x \in 1 + \varpi_D \mathcal{O}_D$, we get $U^+ \cap I_2$ and $U^- \cap I_2$ in $[I_1, I_1]$.

What remains is to determine the elements of $T \cap I_2 = T$ that lie in $[I_1, I_1]I_1^p$. We will show that these include every element of $T_{\det=1} \cdot T^p$ by constructing a sufficiently large subset of $T_{\det=1}$ as commutators to generate every element.

By Lemma 18, we can write $T_{\det=1}$ as

$$T_{\det=1} = \left\{ \begin{pmatrix} 1 + x\pi_F & 0 \\ 0 & (1 + x\pi_F)^{-1} \end{pmatrix} : x \in \mathcal{O}_F \right\} \begin{pmatrix} K_{\mathrm{Nrd}=1} & 0 \\ 0 & K_{\mathrm{Nrd}=1} \end{pmatrix}. \tag{2}$$

Thus, we have a component with entries in $1 + \pi_F \mathcal{O}_F$ to produce, and a component with reduced norm one entries. Note that $K_{\mathrm{Nrd}=1} \subset [D^\times, D^\times]$, which is why the second component always has determinant one. On $1 + \pi_F \mathcal{O}_F$, the reduction modulo $[D^\times, D^\times]$ map is injective, which is why the diagonal entries on the first component must be inverses.

To produce this first component, we compute a commutator of the form

$$\left[\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ \pi_F & 1 \end{pmatrix}\right] = \begin{pmatrix} 1 + x\pi_F + x^2\pi_F^2 & -x^2\pi_F \\ x\pi_F^2 & 1 - x\pi_F \end{pmatrix}$$

where $x \in \mathcal{O}_F$, so this is now a commutator calculation in a pro-p Iwahori subgroup of $\mathrm{GL}_2(F)$. Extracting the element of T from the Iwahori decomposition of this commutator by multiplying on the left and right by the inverses of the $U^+ \cap I_2$ and $U^- \cap I_2$ components (which we have already shown to be commutators), we obtain

$$\begin{pmatrix} (1 - x\pi_F)^{-1} & 0 \\ 0 & 1 - x\pi_F \end{pmatrix} \in [I_1, I_1],$$

where the bottom right entry follows from by the explicit form of the Iwahori decomposition in Lemma 40. The top left entry follows from the fact that the determinant of this matrix must be one because it is a product of unipotent matrices. Thus, we can obtain $\mathrm{diag}(x, x^{-1}) \in [I_1, I_1]$, where $x \in 1 + \pi_F \mathcal{O}_F$ is arbitrary.

We now turn to producing the elements of T in the second component of the decomposition given by equation 2. We have, for $x, y \in \mathcal{O}_D$,

$$\left[\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ y\varpi_D & 1 \end{pmatrix}\right] = \begin{pmatrix} (1 + xy\varpi_D)^2 - xy\varpi_D & -xy\varpi_D x \\ (y\varpi_D)x(y\varpi_D) & 1 - y\varpi_D x \end{pmatrix}.$$

We can again compute the T component of this commutator in the Iwahori decomposition. Taking entries on the diagonal modulo $1 + \varpi_D^2 \mathcal{O}_D$, the formula in Lemma 40 yields $\begin{pmatrix} 1 + xy\varpi_D & 0 \\ 0 & 1 - y\varpi_D x \end{pmatrix}$. This becomes $\begin{pmatrix} \overline{xy} & 0 \\ 0 & -\overline{y}\sigma(\overline{x}) \end{pmatrix}$ when we apply the isomorphism $I_2/I_3 \simeq k_D^2$, where $\overline{x}$ is the image of $x \in \mathcal{O}_D$ in the reside field. By choosing $x = 1$ and $y = [a]$, we can thus produce the elements of $T \pmod{I_3}$ isomorphic to $\mathrm{diag}(a, -a)$ for all $a \in k_D$. By choosing $x = [a]$ and $y = [b]$, the sum of the diagonal entries of the isomorphic matrix is $(a - \sigma(a))b$. Because σ is non-trivial, there exists some $a \in k_D$ such that $a - \sigma(a) \neq 0$. Hence, we can obtain any diagonal sum since b can be arbitrary. The set of all $\mathrm{diag}(a, -a)$ for $a \in k_D$, together with a set of diagonal matrices with entries summing to any element of k_D, generates all of k_D^2, so we are producing representatives of every element of $T \pmod{I_3}$ from products of commutators.

We have now produced determinant one elements in $[I_1, I_1]$ which when reduced yield all representatives for $T \pmod{I_3}$. Using equation 2, we may factor out the central component of these. This does not affect the residue modulo $1+\varpi_D^2\mathcal{O}_D$ of the remaining factor because $d \geq 2$. As we have shown that the central component lies in $[I_1, I_1]$, we have as the remaining factor representatives of $T \pmod{I_3}$ in $[I_1, I_1]$ which also lie in $\begin{pmatrix} K_{\mathrm{Nrd}=1} & 0 \\ 0 & K_{\mathrm{Nrd}=1} \end{pmatrix}$.

By looking at commutators in $[T, T]T^p \subset [I_1, I_1]I_1^p$, Corollary 19 implies that we also have elements in $[I_1, I_1]I_1^p \cap T$ where the diagonal entries are arbitrary in $K_{\mathrm{Nrd}=1}K^p \cap (1 + \varpi_D^2 \mathcal{O}_D)$. Thus, we may generate all of $\begin{pmatrix} K_{\mathrm{Nrd}=1} & 0 \\ 0 & K_{\mathrm{Nrd}=1} \end{pmatrix}$ using elements of $[I_1, I_1]I_1^p$, where we use the representatives of $T \pmod{I_3}$ from the previous paragraph to fix the coefficients on ϖ_D in each entry and the elements of $[T, T]T^p$ to give all remaining coefficients. Thus, we can use equation 2 to conclude that we have all of $T_{\det=1}$ in $[I_1, I_1]I_1^p$, and since $T^p \subset [I_1, I_1]I_1^p$ the claim follows. □

Corollary 42. If F is a p-adic field, then $\mathrm{Hom}(I_1, \overline{\mathbf{F}}_p)$ is an $\overline{\mathbf{F}}_p$ vector space of dimension at most $2df + ef$.

If F is a local function field, then

$$\dim_{\overline{\mathbf{F}}_p} \mathrm{Hom}(I_1/I_{2di+1}, \overline{\mathbf{F}}_p) \leq 2df + \left(i - \left\lfloor \frac{i}{p} \right\rfloor\right) f.$$

Proof. We start with the p-adic case. We have

$$\mathrm{Hom}(I_1, \overline{\mathbf{F}}_p) = \mathrm{Hom}(I_1/[I_1, I_1]I_1^p, \overline{\mathbf{F}}_p),$$

where $I_1/[I_1, I_1]I_1^p$ is an abelian group in which every element is p-torsion. Thus, $I_1/[I_1, I_1]I_1^p \simeq (\mathbf{Z}/p\mathbf{Z})^n$ for some n which is exactly the dimension of $\mathrm{Hom}(I_1, \overline{\mathbf{F}}_p)$.

Because the Iwahori decomposition of every element of I_1 is unique, the previous proposition implies that

$$[I_1 : [I_1, I_1]I_1^p] \leq [U^+ : U^+ \cap I_2] \cdot [T : T_{\det=1} \cdot T^p] \cdot [U^- : U^- \cap I_2].$$

From the natural isomorphisms $U^+ \simeq \mathcal{O}_D \simeq U^-$, we have $[U^+ : U^+ \cap I_2] = [U^- : U^- \cap I_2] = [\mathcal{O}_D : \varpi_D \mathcal{O}_D] = p^{df}$. From equation 2 in the proof of Proposition 41, we have $[T : T_{\det=1} \cdot T^p] = p^{ef}$, as we can identify the representatives with elements of $(1 + \pi_F \mathcal{O}_F)/(1 + \pi_F \mathcal{O}_F)^p$ via the determinant.

For the local function field case, the argument is nearly identical, but we cut off after a certain power of ϖ_D in each entry. More explicitly, the subgroup we quotient by is

$$I_{2di+1} = \begin{pmatrix} 1 + \varpi_D^{di+1}\mathcal{O}_D & \varpi_D^{di}\mathcal{O}_D \\ \varpi_D^{di+1} & 1 + \varpi_D^{di+1}\mathcal{O}_D \end{pmatrix}.$$

When computing the order of the quotient of I_1/I_{2di+1} by its Frattini subgroup, the upper bound of p^{2df} coming from the U^+ and U^- components of the commutators still holds, however we must now also compute $[T \pmod{I_{2di+1}} : (T_{\det=1} \cdot T^p) \pmod{I_{2di+1}}]$. Here we identify representatives with elements of

$$\frac{1 + \pi_F \mathcal{O}_F \pmod{1 + \pi_F^{i+1}\mathcal{O}_F}}{(1 + \pi_F \mathcal{O}_F) \cap (1 + (\varpi_D \mathcal{O}_D)^p) \pmod{1 + \pi_F^{i+1}\mathcal{O}_F}}$$

because we are in characteristic p, so $(1 + \varpi_D \mathcal{O}_D)^p = 1 + (\varpi_D \mathcal{O}_D)^p$. This gives the desired bound by the same reasoning as in the proof of Corollary 16. □

We now show that these upper bounds actually give equality by breaking $\mathrm{H}^1(I_1, \overline{\mathbf{F}}_p)$ into components which we can easily compute.

Theorem 43. Let W_ϕ denote the space of homomorphisms $I_1 \to \overline{\mathbf{F}}_p$ factoring through the quotient by I_2, and let W_ψ denote the space of homomorphisms factoring through the Dieudonné determinant $\det : I_1 \to 1 + \pi_F \mathcal{O}_F$. We have a decomposition

$$\mathrm{H}^1(I_1, \overline{\mathbf{F}}_p) = W_\phi \oplus W_\psi.$$

Additionally, we have isomorphisms

$$W_\phi \simeq \mathrm{Hom}(I_1/I_2, \overline{\mathbf{F}}_p) \simeq \mathrm{Hom}(k_D^2, \overline{\mathbf{F}}_p) \simeq \overline{\mathbf{F}}_p^{2df}$$

as a vector space and $W_\psi \simeq \mathrm{Hom}(1 + \pi_F \mathcal{O}_F, \overline{\mathbf{F}}_p)$. As an immediate corollary, the inclusion in Proposition 41 is an equality.

Proof. As $I_1/I_2 \simeq k_D^2$, it has dimension $2df$ as an $\mathbf{F}_p$-vector space, so $W_\phi \simeq \overline{\mathbf{F}}_p^{2df}$. Because det surjects onto $1 + \pi_F \mathcal{O}_F$, we have $W_\psi \simeq \mathrm{Hom}(1 + \pi_F \mathcal{O}_F, \overline{\mathbf{F}}_p)$, a space whose dimension we computed in the proof of Theorem 17. As $\det|_{I_2}$ surjects onto $1 + \pi_F \mathcal{O}_F$ as well, if any element $\psi^\eta = \eta \circ \det \in W_\psi$ is 0 on I_2 it must be 0 everywhere. Hence, $W_\phi \cap W_\psi$ is trivial, and we conclude that $W_\phi \oplus W_\psi \subset \mathrm{H}^1(I_1, \overline{\mathbf{F}}_p)$. All that remains is to show that this containment is equality.

By Corollary 42, we may conclude in the p-adic case that we have produced enough homomorphisms to meet the upper bound. In the local function field case, taking a quotient by I_{2di+1} we similarly have the right number of homomorphisms to meet the upper bound for all i. Because any homomorphism not included in $W_\phi \oplus W_\psi$ would have to be equal to zero on the quotient by every I_{2di+1}, it would have to be the zero map. We conclude that $\mathrm{H}^1(I_1, \overline{\mathbf{F}}_p) = W_\phi \oplus W_\psi$, and can also immediately conclude that in Proposition 41 the inclusion is an equality. □

Corollary 44. We can compute bases of W_ϕ and W_ψ:

- We have a decomposition $W_\phi = W_{\phi,U^+} \oplus W_{\phi,U^-}$. These spaces each have dimension df.
  - The space W_{ϕ,U^+} consists of maps corresponding to topological generators of U^+. The basis elements are $\phi^{\eta_j}_{U^+}$, where for $A = \begin{pmatrix} 1+w\varpi_D & x \\ y\varpi_D & 1+z\varpi_D \end{pmatrix}$ with $w,x,y,z \in \mathcal{O}_D$ we let
  $$\phi^{\eta_j}_{U^+} : A \mapsto \eta_j(\overline{x}).$$
  Here, $\eta_j \in \mathrm{Hom}(k_D, \overline{\mathbf{F}}_p)$ sends $a \mapsto a^{p^j}$. The bar denotes reduction modulo $\varpi_D\mathcal{O}_D$.
  - The space W_{ϕ,U^-} has basis of maps
  $$\phi^{\eta_j}_{U^-} : A \mapsto \eta_j(\overline{y})$$
  where the notation is the same.
- A basis of W_ψ consists of the maps $\psi^{\eta_i} = \eta_i \circ \det$ where the η_i form a basis of $\mathrm{Hom}(1+\pi_F\mathcal{O}_F, \overline{\mathbf{F}}_p)$. As $p > de+1$, there is no p-torsion, so this is isomorphic to $\overline{\mathbf{F}}_p^{ef}$ in the p-adic case or $\bigoplus_{i\in\mathbf{N}} \overline{\mathbf{F}}_p$ in the local function field case.

Proof. The maps ψ^{η_i} are homomorphisms because they are compositions of homomorphisms. To see why the $\phi^{\eta_j}_{U^+}$ and $\phi^{\eta_j}_{U^+}$ are homomorphisms, note that for $A_i = \begin{pmatrix} 1+w_i\varpi_D & x_i \\ y_i\varpi_D & 1+z_i\varpi_D \end{pmatrix}$ we have
$$A_1A_2 = \begin{pmatrix} 1+O(\varpi_D) & (x_1+x_2)+O(\varpi_D) \\ (y_1+y_2)\varpi_D + O(\varpi_D^2) & 1+O(\varpi_D) \end{pmatrix},$$
so we get homomorphisms when we apply the reduction modulo $\varpi_D\mathcal{O}_D$ in the definitions of these maps.

All that remains is to show that these maps form bases. This follows from the previous theorem, and dimension counting to make sure we actually have a basis. In the case of W_ψ elements are linearly independent by definition, and in the case of W_ϕ the proof of linear independence is very similar to that of the ϕ^{η_j} in Theorem 17. ☐

Using this explicit basis, we will compute the structure of $\mathrm{H}^1(I_1, \overline{\mathbf{F}}_p)$ in terms of the Hecke algebra $\mathcal{H}_{I_1} := \mathrm{End}_{\mathrm{GL}_2(D)}(c-\mathrm{Ind}_{I_1}^{\mathrm{GL}_2(D)} \overline{\mathbf{F}}_p)$. This can also be viewed as the algebra of locally constant compactly supported functions on $\mathrm{GL}_2(D)$ which are bi-I_1-invariant.

Proposition 45 ([Ly13])**.** We have a double coset decomposition
$$\mathrm{GL}_2(D) = \bigsqcup_{\substack{\alpha,\beta\in k_D^\times \\ m,n\in\mathbf{Z}}} I_1 \begin{pmatrix} [\alpha] & 0 \\ 0 & [\beta] \end{pmatrix} \begin{pmatrix} \varpi_D^n & 0 \\ 0 & \varpi_D^m \end{pmatrix} I_1 \sqcup \bigsqcup_{\substack{\alpha,\beta\in k_D^\times \\ m,n\in\mathbf{Z}}} I_1 \begin{pmatrix} [\alpha] & 0 \\ 0 & [\beta] \end{pmatrix} \begin{pmatrix} 0 & \varpi_D^n \\ \varpi_D^m & 0 \end{pmatrix} I_1.$$

A basis for the algebra $\mathcal{H}_{I_1}$ as a vector space will consist of the characteristic functions on these cosets.

Definition 46. For $g \in \mathrm{GL}_2(D)$, we use $[I_1gI_1]$ to denote the characteristic function on the coset I_1gI_1 in $\mathcal{H}_{I_1}$.

The element $[I_1gI_1]$ acts on the right on $\mathrm{H}^1(I_1, \overline{\mathbf{F}}_p)$. In particular,
$$\mathrm{H}^1(I_1, \overline{\mathbf{F}}_p) \cdot [I_1gI_1] := \mathrm{Cor}^{I_1}_{I_1\cap g^{-1}I_1g} \circ g_*^{-1} \circ \mathrm{Res}^{I_1}_{I_1\cap gI_1g^{-1}} \mathrm{H}^1(I_1, \overline{\mathbf{F}}_p),$$
where g_*^{-1} is the conjugation map $x \mapsto g^{-1}xg$. When g normalizes I_1, this reduces to the conjugation action on homomorphisms. The following corollary allows us to reduce

the problem of computing the action of $[I_1 g I_1]$ in general to computing the action of a few finite families of generators.

Corollary 47 ([Ly13], Lemma 1.4.4)**.** The Hecke algebra $\mathcal{H}_{I_1}$ is generated as an algebra by the elements

$$\left[I_1 \begin{pmatrix} [\alpha] & 0 \\ 0 & [\beta] \end{pmatrix} I_1\right], \left[I_1 \begin{pmatrix} 0 & 1 \\ \varpi_D & 0 \end{pmatrix} I_1\right], \left[I_1 \begin{pmatrix} 0 & \varpi_D^{-1} \\ 1 & 0 \end{pmatrix} I_1\right], \text{ and } \left[I_1 \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} I_1\right],$$

where $\alpha, \beta \in k_D^\times$.

All but the last element normalize I_1, so the action is by conjugation. However, $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ does not normalize I_1, so the action is more difficult to compute.

Lemma 48. Let $g_0 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Then the double coset $I_1 g_0 I_1$ decomposes into left cosets as

$$I_1 g_0 I_1 = \bigsqcup_{a \in k_D} I_1 g_a := \bigsqcup_{a \in k_D} I_1 \begin{pmatrix} 0 & 1 \\ -1 & [a] \end{pmatrix}.$$

Proof. We first compute which matrices $A \in I_1$ remain in I_1 after being conjugated by g_0. Writing $A = \begin{pmatrix} w & x \\ y & z \end{pmatrix}$, we have

$$g_0 A g_0^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} w & x \\ y & z \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} z & -y \\ -x & w \end{pmatrix}.$$

Because $w, z \in 1 + \varpi_D \mathcal{O}_D$, $x \in \mathcal{O}_D$, and $y \in \varpi_D \mathcal{O}_D$, $g_0 A g_0^{-1}$ is in I_1 if and only if ϖ_D divides x in $\mathcal{O}_D$.

Now we can determine the conditions on $A_1, A_2 \in I_1$ for which $I_1 g_0 A_1 = I_1 g_0 A_2$. This is true if and only if $g_0 A_1 A_2^{-1} g_0^{-1} \in I_1$, which holds if and only if ϖ_D divides the top right entry of $A_1 A_2^{-1}$ by the previous paragraph. Writing $A_i = \begin{pmatrix} w_i & x_i \\ y_i & z_i \end{pmatrix}$, we reduce modulo $\varpi_D \mathcal{O}_D$ to obtain $\overline{A}_i = \begin{pmatrix} 1 & \overline{x}_i \\ 0 & 1 \end{pmatrix}$, so $\overline{A}_1 \overline{A}_2^{-1} = \begin{pmatrix} 1 & \overline{x}_1 - \overline{x}_2 \\ 0 & 1 \end{pmatrix}$. Hence, $I_1 g_0 A_1 = I_1 g_0 A_2$ if and only if $\overline{x}_1 = \overline{x}_2$.

Therefore, $I_1 g_0 I_1$ consists of a disjoint union of $|k_D| = p^{df}$ left cosets $I_1 g A$ where each coset corresponds to a different choice of the reduction of the top right entry of A in the residue field. Choosing representatives of the form $A_a = \begin{pmatrix} 1 & [-a] \\ 0 & 1 \end{pmatrix}$ for each $a \in k_D$ gives the cosets $I_1 g_0 A_a = I_1 \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & [-a] \\ 0 & 1 \end{pmatrix} = I_1 \begin{pmatrix} 0 & 1 \\ -1 & [a] \end{pmatrix} = I_1 g_a$ as desired. $\square$

Proposition 49. For $A = \begin{pmatrix} w & x \\ y & z \end{pmatrix} \in I_1$ and $a \in k_D$, define

$$\xi_a(A) := g_a A g_{a-\overline{x}}^{-1} = \begin{pmatrix} y[a - \overline{x}] + z & -y \\ (-w + [a]y)[a - \overline{x}] - x + [a]z & w - [a]y \end{pmatrix}.$$

Then $\xi_a(A) \in I_1$ and for all $\varphi \in \mathrm{Hom}(I_1, \overline{\mathbf{F}}_p)$ we have

$$(\varphi \cdot [I_1 g_0 I_1])(A) = \sum_{a \in k_D} \varphi(\xi_a(A)).$$

Proof. Because $A \in I_1$, the previous lemma implies that

$$\bigsqcup_{a \in k_D} I_1 g_a A = I_1 g_0 I_1 A = I_1 g_0 I_1 = \bigsqcup_{a' \in k_D} I_1 g_{a'},$$

so for each $a \in k_D$ there exists some unique $a' \in k_D$ such that $g_a A g_{a'}^{-1} \in I_1$. Direct computation gives

$$g_a A g_{a'}^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & [a] \end{pmatrix} \begin{pmatrix} w & x \\ y & z \end{pmatrix} \begin{pmatrix} [a'] & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} y[a'] + z & -y \\ (-w + [a]y)[a'] - x + [a]z & w - [a]y \end{pmatrix},$$

and reducing modulo $\varpi_D \mathcal{O}_D$ yields $\begin{pmatrix} 1 & 0 \\ -a' - \overline{x} + a & 1 \end{pmatrix}$. Therefore, $g_a A g_{a'}^{-1} \in I_1$ if and only if $a' = a - \overline{x}$. Hence, $\xi_a(A) \in I_1$.

By definition, we have

$$(\varphi \cdot [I_1 g_0 I_1])(A) = (\mathrm{Cor}^{I_1}_{I_1 \cap g_0^{-1} I_1 g_0} \circ g_{0*}^{-1} \circ \mathrm{Res}^{I_1}_{I_1 \cap g_0 I_1 g_0^{-1}} \varphi)(A).$$

Applying the explicit form of the corestriction map gives the formula. □

With this explicit formula, we can compute how $[I_1 g_0 I_1]$ acts on any $\varphi \in \mathrm{Hom}(I_1, \overline{\mathbf{F}}_p)$. Fortunately, the action simplifies considerably in every case. We first recall a basic fact of finite fields.

Lemma 50. If k is a finite field, then $\sum_{a \in k} a^n = 0$ for all $n > 0$ with $|k^\times| \nmid n$.

Proof. Let α generate $k^\times$. Then $\alpha^n \neq 1$, and $\alpha^n \sum_{a \in k} a^n = \sum_{a \in k} (\alpha a)^n = \sum_{a \in k} a^n$ because multiplication by α is an automorphism of $k^\times$ fixing 0. Hence, $\sum_{a \in k} a^n = 0$. □

Corollary 51. For all $\varphi \in \mathrm{Hom}(I_1, \overline{\mathbf{F}}_p)$, we have $\varphi \cdot [I_1 g_0 I_1] = 0$.

Proof. We will use the formula in Proposition 49 to show that $[I_1 g_0 I_1]$ sends every element of our basis from Corollary 44 to zero. Throughout, let $A = \begin{pmatrix} w & x \\ y & z \end{pmatrix} \in I_1$.

For any basis vector ψ^{η_i} in W_ψ, we have that $(\psi^{\eta_i} \cdot [I g_0 I])(A)$ is equal to

$$\sum_{a \in k_D} \psi^{\eta_i}(\xi_a(A)) = \sum_{a \in k_D} \eta_i(\det(g_a A g_{a-\overline{x}}^{-1})) = \sum_{a \in k_D} \psi^{\eta_i}(A) + \eta_i(\det(g_a g_{a-\overline{x}}^{-1}))$$

because det maps into an abelian group. The matrix $g_a g_{a-\overline{x}}^{-1} = \begin{pmatrix} 1 & 0 \\ [a] - [a - \overline{x}] & 1 \end{pmatrix}$ has determinant 1, so we have

$$(\psi^{\eta_i} \cdot [I g_0 I])(A) = \sum_{a \in k_D} \psi^{\eta_i}(A) = |k_D| \psi^{\eta_i}(A) = 0$$

because $|k_D| = p^{df}$ and we are in characteristic p.

For $\phi^{\eta_j}_{U^+} \in W_{\phi, U^+}$, we have

$$(\phi^{\eta_j}_{U^+} \cdot [I g_0 I])(A) = \sum_{a \in k_D} \phi^{\eta_j}_{U^+}(\xi_a(A)) = \sum_{a \in k_D} \eta_j(\overline{-y}) = 0$$

because $y \in \varpi_D \mathcal{O}_D$.

Finally, consider a map $\phi^{\eta_j}_{U^-} \in W_{\phi, U^-}$. If we write

$$A = \begin{pmatrix} 1 + [w_1]\varpi_D + O(\varpi_D^2) & [x_0] + [x_1]\varpi_D + O(\varpi_D^2) \\ [y_1]\varpi_D + O(\varpi_D^2) & 1 + [z_1]\varpi_D + O(\varpi_D^2) \end{pmatrix},$$

then we have

$$(\phi_{U^-}^{\eta_j}\cdot[Ig_0I])(A)=\sum_{a\in k_D}\phi_{U^-}^{\eta_j}(\xi_a(A))=\sum_{a\in k_D}\eta_j(\overline{((-w+[a]y)[a-x_0]-x+[a]z)\varpi_D^{-1}})$$

$$=\eta_j\left(\sum_{a\in k_D}(-w_1+ay_1)(a-x_0)-x_1+az_1\right)$$

$$=\eta_j\left(y_1\sum_{a\in k_D}a^2+(-w_1-y_1x_0+z_1)\sum_{a\in k_D}a+(w_1x_0-x_1)|k_D|\right)=0$$

by Lemma 50. Note that in the second line we use the fact that $d\geq 2$ to ensure that any error term coming from $-[a-x_0]-[x_0]+[a]=0+O(p)$ does not affect the value once we multiply by ϖ_D^{-1} and pass to the residue field. We also use $d\geq 2$ to ensure that $|k_D^\times|\nmid 2$ so we can apply Lemma 50 to sum over the squares of elements of k_D.

Hence, $[I_1gI_1]$ sends all three types of basis vectors to 0. ☐

Computing how the remaining generators from Corollary 47 act is relatively straightforward.

Corollary 52. The action of the remaining generators of $\mathcal{H}_{I_1}$ is given as follows:

· On W_ψ, the remaining generators act as the identity.

· For $\phi_{U+}^{\eta_j},\phi_{U-}^{\eta_{j'}}\in W_\phi$, we have for $g=\begin{pmatrix}[\alpha]&0\\0&[\beta]\end{pmatrix}$ that

$$\phi_{U+}^{\eta_j}\cdot[I_1gI_1]=\frac{\alpha}{\beta}\phi_{U+}^{\eta_j},\ \text{and}\ \phi_{U-}^{\eta_{j'}}\cdot[I_1gI_1]=\frac{\beta}{\sigma(\alpha)}\phi_{U-}^{\eta_{j'}}.$$

· For $\phi_{U+}^{\eta_j},\phi_{U-}^{\eta_{j'}}\in W_\phi$, we have for $g=\begin{pmatrix}0&1\\\varpi_D&0\end{pmatrix}$ that

$$\phi_{U+}^{\eta_j}\cdot[I_1gI_1]=\phi_{U-}^{\eta_j},\ \text{and}\ \phi_{U-}^{\eta_{j'}}\cdot[I_1gI_1]=\sigma(\phi_{U+}^{\eta_{j'}})=\phi_{U+}^{\eta_{j'+rf}},$$

where r is an integer such that $\sigma(x)=x^{p^{rf}}$. The inverse $g^{-1}=\begin{pmatrix}0&\varpi_D^{-1}\\1&0\end{pmatrix}$ must then act by

$$\phi_{U+}^{\eta_j}\cdot[I_1g^{-1}I_1]=\sigma^{-1}(\phi_{U-}^{\eta_j})=\phi_{U-}^{\eta_{j-rf}},\ \text{and}\ \phi_{U-}^{\eta_{j'}}\cdot[I_1g^{-1}I_1]=\phi_{U+}^{\eta_{j'}}.$$

Proof. Because the remaining generators g normalize I_1, the action of $[I_1gI_1]$ sends a homomorphism $\varphi(x)\mapsto\varphi(gxg^{-1})$.

On W_ψ, the determinant is invariant under conjugation, so the action is trivial.

Now we turn to $\phi\in W_\phi$. Since ϕ factors through I_2, we need only compute the action on $I_1/I_2\simeq k_D^2$. For $x_1,x_2\in k_D$, we have

$$\begin{pmatrix}[\alpha]&0\\0&[\beta]\end{pmatrix}\begin{pmatrix}1&[x_1]\\ [x_2]\varpi_D&1\end{pmatrix}\begin{pmatrix}[\alpha^{-1}]&0\\0&[\beta^{-1}]\end{pmatrix}=\begin{pmatrix}1&[\alpha x_1\beta^{-1}]\\ [\beta x_2]\varpi_D[\alpha^{-1}]&1\end{pmatrix}.$$

Applying the commutation relation for ϖ_D, the claim follows by looking at the upper right and bottom left entries. Similarly, we have

$$\begin{pmatrix}0&1\\\varpi_D&0\end{pmatrix}\begin{pmatrix}1&[x_1]\\ [x_2]\varpi_D&1\end{pmatrix}\begin{pmatrix}0&\varpi_D^{-1}\\1&0\end{pmatrix}=\begin{pmatrix}1&[x_2]\\ [\sigma(x_1)]\varpi_D&1\end{pmatrix}.$$

Thus, we can read off the action of $g=\begin{pmatrix}0&1\\\varpi_D&0\end{pmatrix}$. ☐

Together with the previous corollary, this determines the $\mathcal{H}_{I_1}$-module structure of $\mathrm{H}^1(I_1, \overline{\mathbf{F}}_p)$. We use $\mathbf{1}$ to denote the trivial character of $\mathcal{H}_{I_1}$, which is the $\mathcal{H}_{I_1}$-module $\overline{\mathbf{F}}_p$ with all of the generators from Corollary 47 acting trivially except for $[I_1 g_0 I_1]$, which sends everything to 0.

Theorem 53. As an $\mathcal{H}_{I_1}$ module, we have

$$\mathrm{H}^1(I_1, \overline{\mathbf{F}}_p) = W_\psi \oplus \bigoplus_{j \in \mathbf{Z}/f\mathbf{Z}} W_j,$$

where the W_j are the submodules of W_ϕ spanned by all $\phi_{U+}^{\eta_i}$ and $\phi_{U-}^{\eta_i}$ with $i \equiv j \pmod f$. Moreover, W_ψ is a direct sum of copies of $\mathbf{1}$ and all of the W_j are simple.

Proof. Corollaries 51 and 52 immediately imply that the decomposition $\mathrm{H}^1(I_1, \overline{\mathbf{F}}_p) = W_\phi \oplus W_\psi$ is a decomposition of $\mathcal{H}_{I_1}$ modules, and that W_ψ is a direct sum of copies of $\mathbf{1}$. Moreover, the decomposition $W_\phi = \bigoplus_{j \in \mathbf{Z}/f\mathbf{Z}} W_j$ follows directly from the Corollary 52 because the $\phi_{U+}^{\eta_i}$ and $\phi_{U-}^{\eta_i}$ are eigenvectors of the $\begin{pmatrix} [\alpha] & 0 \\ 0 & [\beta] \end{pmatrix}$ actions, while $\begin{pmatrix} 0 & 1 \\ \varpi_D & 0 \end{pmatrix}$ acts by cycling through all $\phi_{U+}^{\eta_i}$ and $\phi_{U-}^{\eta_i}$ in each W_j. These two actions are analogous to how $k_D^\times$ and $\varpi_D^{\mathbf{Z}}$ respectively act on the V_j in the proof of Proposition 23, and the proof that the W_j are simple modules is the same as the proof that the V_j are irreducible representations. □

Acknowledgments

The authors would like to thank Tasho Kaletha and Karol Koziol for providing valuable mentorship throughout this project. They would also like to thank the University of Michigan Math REU for making this project possible. This research was supported by NSF grant DMS-1801687.

References

[Bre10] Christophe Breuil, *The emerging p-adic Langlands programme*, Proceedings of the international congress of mathematicians, vol. 2, Hindustan Book Agency, 2010, pp. 203–230.

[DDSMS03] John D Dixon, Marcus PF Du Sautoy, Avinoam Mann, and Dan Segal, *Analytic pro-p groups*, no. 61, Cambridge University Press, 2003.

[Die43] Jean Dieudonné, *Les déterminants sur un corps non commutatif*, Bulletin de la Société Mathématique de France **71** (1943), 27–45.

[Eme10] Matthew Emerton, *Ordinary parts of admissible representations of p-adic reductive groups ii. derived functors*, Astérisque **331** (2010), 403–459.

[Has32] Helmut Hasse, *Theory of cyclic algebras over an algebraic number field*, Transactions of the American Mathematical Society **34** (1932), no. 1, 171–214.

[Koz17] Karol Koziol, *Hecke module structure on first and top pro-p-iwahori cohomology*, arXiv preprint arXiv:1708.03013 (2017).

[Koz20] Karol Kozioł, *Functorial properties of pro-p-iwahori cohomology*, Journal of the London Mathematical Society (2020).

[Laz65] Michel Lazard, *Groupes analytiques p-adiques*, Publications Mathématiques de l'IHÉS **26** (1965), 5–219.

[Ly13] Tony Ly, *Représentations modulo p de GL(m, D), D algèbre à division sur un corps local*, Ph.D. thesis, Ph. D. thesis, Université Paris Diderot 7, 2013.

[PY96] V. P. Platonov and V. I. Yanchevskii, *Algebra IX*, Encyclopaedia of Mathematical Sciences, vol. 77, Springer Berlin Heidelberg, Berlin, Heidelberg, 1996 (en).

[Sch15] Peter Scholze, *On the p-adic cohomology of the Lubin-Tate tower*, arXiv preprint arXiv:1506.04022 (2015).

[Ser13a] Jean-Pierre Serre, *Galois cohomology*, Springer Science & Business Media, 2013.

[Ser13b] ———, *Local fields*, vol. 67, Springer Science & Business Media, 2013.

[SK79] Tetsuji Shioda and Toshiyuki Katsura, *On Fermat varieties*, Tohoku Mathematical Journal, Second Series **31** (1979), no. 1, 97–115.

[SW00] Peter Symonds and Thomas Weigel, *Cohomology of p-adic analytic groups*, New horizons in pro-p groups, Springer, 2000, pp. 349–410.

[Tot99] Burt Totaro, *Euler characteristics forp-adic lie groups*, Publications Mathématiques de l'Institut des Hautes Études Scientifiques **90** (1999), no. 1, 169–225.

[W+49] André Weil et al., *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc **55** (1949), no. 5, 497–508.

[Wan50] Shianghaw Wang, *On the commutator group of a simple algebra*, American Journal of Mathematics **72** (1950), no. 2, 323–334.