

Algebra & Number Theory

Volume 19
2025
No. 3

**The Lyndon–Demushkin method and crystalline lifts
of G_2 -valued Galois representations**

Zhongyipan Lin



The Lyndon–Demushkin method and crystalline lifts of G_2 -valued Galois representations

Zhongyipan Lin

We develop obstruction theory for lifting characteristic- p local Galois representations valued in reductive groups of type B_l , C_l , D_l or G_2 . An application of the Emerton–Gee stack then reduces the existence of crystalline lifts to a purely combinatorial problem when p is not too small.

As a toy example, we show for all local fields K/\mathbb{Q}_p , with $p > 3$, all representations $\bar{\rho} : G_K \rightarrow G_2(\bar{\mathbb{F}}_p)$ admit a crystalline lift $\rho : G_K \rightarrow G_2(\bar{\mathbb{Z}}_p)$, where G_2 is the exceptional Chevalley group of type G_2 .

1. Introduction

Let K/\mathbb{Q}_p be a p -adic field. Let G be a connected reductive group over $\bar{\mathbb{Z}}_p$. Let $\bar{\rho} : G_K \rightarrow G(\bar{\mathbb{F}}_p)$ be a Galois representation.

We will study whether there exist crystalline lifts of $\bar{\rho}$ to $G(\bar{\mathbb{Z}}_p)$. This question has been raised in various contexts, such as irreducible geometric Galois representations [Fakhruddin et al. 2018], the Serre weight conjecture [Gee et al. 2018] and ramification theory [Caruso and Liu 2011].

The pursuit of constructing characteristic-0 lifts of Galois representations (at least in higher dimensions) is, however, resistant to elementary techniques. Böckle [2003] was able to lift mod ϖ representations to a mod ϖ^2 representation for $G = \mathrm{GL}_N$. Müller [2013] constructed crystalline lifts of mod ϖ representations valued in $G = \mathrm{GL}_3$, and Emerton and Gee [2023] worked the GL_N -case for all N . Our earlier work [Lin 2022] answers this question for semisimple representations valued in general reductive groups G .

The method of [Emerton and Gee 2023] is purely local, and is based on an analysis of Galois cohomology. The image group $\bar{\rho}(G_K)$ is either an irreducible subgroup of $G(\bar{\mathbb{F}}_p)$ or factors through a proper maximal parabolic P of G . In the former case, our previous work [Lin 2022] shows $\bar{\rho}$ always admits a crystalline lift. In this paper, we focus on the latter case. Let $P = L \rtimes U_P$ be the Levi decomposition. Let $\bar{r} : G_K \xrightarrow{\bar{\rho}} P(\bar{\mathbb{F}}_p) \rightarrow L(\bar{\mathbb{F}}_p)$ be the Levi factor of $\bar{\rho}$. Then \bar{r} defines a 1-cocycle $[\bar{c}] \in H^1(G_K, U_P(\bar{\mathbb{F}}_p))$. What we will actually do is to construct a lift $r : G_K \rightarrow L(\bar{\mathbb{Z}}_p)$ of \bar{r} and a lift $[c] \in H^1(G_K, U_P(\bar{\mathbb{Z}}_p))$ of $[\bar{c}]$.

In the GL_N -case, all maximal proper parabolics have abelian unipotent radical, so it suffices to consider abelian cohomology. When G is not GL_N , parabolic subgroups with abelian unipotent radical are rare. For example, when G is the exceptional group G_2 , all parabolics have nonabelian unipotent radical.

MSC2020: 11F80.

Keywords: Galois representations, exceptional group.

Fortunately, for groups of type A , B , C , D or G_2 , the relevant nonabelian Galois cohomology can be replaced by abelian Galois cohomology equipped with a cup product structure and the strategy considered in [Emerton and Gee 2023] can be adapted to work. In this paper, we focus on the G_2 -case, and prove the following theorem:

Theorem A (Theorem 7.1.3). *Assume $p > 3$. Every mod ϖ Galois representation valued in the exceptional group G_2 ,*

$$\bar{\rho} : G_K \rightarrow G_2(\overline{\mathbb{F}}_p),$$

admits a crystalline lift $\rho^\circ : G_K \rightarrow G_2(\overline{\mathbb{Z}}_p)$.

Moreover, if $\bar{\rho}$ factors through a maximal parabolic $P = L \rtimes U$ and the Levi factor $\bar{r}_{\bar{\rho}} : G_K \rightarrow L(\overline{\mathbb{F}}_p)$ of $\bar{\rho}$ admits a Hodge–Tate regular and crystalline lift $r_1 : G_K \rightarrow L(\overline{\mathbb{Z}}_p)$ such that the adjoint representation $G_K \xrightarrow{r_1} L(\overline{\mathbb{Z}}_p) \rightarrow \mathrm{GL}(\mathrm{Lie}(U(\overline{\mathbb{Z}}_p)))$ has Hodge–Tate weights slightly less than $\underline{0}$ (Definition 3.0.4), then ρ° can be chosen such that it factors through the maximal parabolic P and its Levi factor r_{ρ° lies on the same irreducible component of the spectrum of the crystalline lifting ring that r_1 does.

1.1. Overview of the method and comparison with [Lin 2023a]. To establish the existence of crystalline lifts, we proceed in four steps:

Step 1. Construct explicit cochain complexes *equipped with a natural cup product structure* that compute abelian Galois cohomology.

Step 2. Show that the cup product considered in Step 1 is nontrivial in certain special cases.

Step 3. Compute the dimension of certain substacks of the reduced Emerton–Gee stack.

Step 4. Invoke the machinery of [Emerton and Gee 2023] to produce crystalline lifts.

After the first draft of this paper was written, we have a more conceptual understanding of some constructions made in this paper; see the introduction section of [Lin 2023a]. For example, Sections 2 and 4 of this paper are conceptualized under the notion of *Heisenberg equations*. In [loc. cit.], we also establish the existence of de Rham lifts for many classical groups and in particular the existence of crystalline lifts for unramified unitary groups.

However, from the technical perspective, [loc. cit.] parallels this paper, instead of upgrades this paper. In [loc. cit.], we use *Herr complexes* as the explicit cochain complex computing Galois cohomology. Herr complexes are infinite-dimensional cochain complexes and are often not amenable to computation by hand. We can truncate Herr complexes to a finite-dimensional cochain complex but the truncation can't be made explicit in general. The upside of Herr complexes is better functoriality and in the case of classical groups, we can usually reduce the problems to the GL_n -case, which is well-understood.

In this paper, we use Lyndon's cochain complexes instead. Everything in this paper is totally explicit and is computable by hand or by a computer algebra system. The downside of this approach is that the complexity of computation grows exponentially, and quickly becomes out of hand for large-ranked classical groups.

We don't know how to deal with Herr complexes for exceptional groups because of their implicit nature, and the approach in this paper is still the only one we are aware of. In this paper, we establish the existence of crystalline lifts for the exceptional group G_2 , which illustrates the usefulness of Lyndon's cochain complexes. Because of its explicit nature, our approach can potentially be extended to deal with more general exceptional groups, after upgrading the cup product structure to more complicated higher Massey product structures.

1.2. Obstruction theory for crystalline lifting. In this paper, we consider the case where U_P admits a quotient U such that

- the adjoint group $U^{\text{ad}} := U/Z(U)$ is abelian;
- the center $Z(U)$ is isomorphic to \mathbb{G}_a ; and
- there is a bijection of obstructions $H^2(G_K, U_P(\overline{\mathbb{F}}_p)) \cong H^2(G_K, U(\overline{\mathbb{F}}_p))$.

We call U a Heisenberg quotient of U_P . When G is of type B_l, C_l, D_l or G_2 , it is always possible to choose a parabolic P whose unipotent radical admits a Heisenberg quotient (see Section 1.1).

Let $\text{Spec } R$ be an irreducible component of a crystalline lifting ring $\text{Spec } R_{\bar{r}}^{\text{crys}, \lambda}$ (Section 5.0.2) of \bar{r} . Let $r^{\text{univ}} : G_K \rightarrow L(R)$ be the universal family. The Levi factor group acts on U via conjugation $\phi : L \rightarrow \text{Aut}(U)$. Write $\phi^{\text{ad}} : L \rightarrow \text{GL}(U^{\text{ad}})$ and $\phi^z : L \rightarrow \text{GL}(Z(U))$ for the graded pieces of ϕ .

The theorem we prove is:

Theorem B (Theorem 5.2.1). *Let $[\bar{c}] \in H^1(G_K, U(\mathbb{F}))$ be a characteristic- p cocycle, where U is a Heisenberg quotient of U_P .*

Assume

- (1) $H^2(G_K, \phi^{\text{ad}}(r^{\text{univ}}))$ is sufficiently generically regular (Definition 5.1.1) and set-theoretically supported on the special fiber of $\text{Spec } R$;
- (2) $p \neq 2$;
- (3) there exists a finite Galois extension K'/K of prime-to- p degree such that $\phi(\bar{r})|_{G_{K'}}$ is Lyndon–Demushkin (Definition 2.0.2); and
- (4) there exists a $\overline{\mathbb{Z}}_p$ -point of $\text{Spec } R$ which is mildly regular (Definition 3.0.1) when restricted to $G_{K'}$.

Then there exists a $\overline{\mathbb{Z}}_p$ -point of $\text{Spec } R$ which gives rise to a Galois representation $r^\circ : G_K \rightarrow L(\overline{\mathbb{Z}}_p)$ such that if we endow $U(\overline{\mathbb{Z}}_p)$ with the G_K -action $G_K \xrightarrow{r^\circ} L(\overline{\mathbb{Z}}_p) \xrightarrow{\phi} \text{Aut}(U(\overline{\mathbb{Z}}_p))$, the cocycle $[\bar{c}]$ has a characteristic-0 lift $[c] \in H^1(G_K, U(\overline{\mathbb{Z}}_p))$.

Remark. Assumption (3) is automatically satisfied if p is sufficiently large, and (4) is automatically satisfied if p is sufficiently large and the labeled Hodge–Tate weights $\phi^{\text{ad}}(\lambda)$ are slightly less than 0 (Definition 3.0.4).

Example 1.2.1 ($G = \text{GL}_3$). Let $\bar{\rho} : G_K \rightarrow \text{GL}_3(\overline{\mathbb{F}}_p)$ be a completely reducible Galois representation. There are two ways of encoding the data of $\bar{\rho}$ as a 1-cocycle in Galois cohomology.

(I) Use the fact $\bar{\rho}$ factors through a maximal parabolic

$$P = \begin{bmatrix} * & * & * \\ * & * & * \\ 0 & 0 & * \end{bmatrix} = \begin{bmatrix} * & * & 0 \\ * & * & 0 \\ 0 & 0 & * \end{bmatrix} \ltimes \begin{bmatrix} 1 & 0 & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{bmatrix} = L \ltimes A,$$

where $A \cong \mathbb{G}_a^{\oplus 2}$ is a rank-2 abelian group. Let $\bar{r} : G_K \xrightarrow{\bar{\rho}} P(\bar{\mathbb{F}}_p) \rightarrow L(\bar{\mathbb{F}}_p)$ be the Levi factor of $\bar{\rho}$. The information of $\bar{\rho}$ is encoded in a 1-cocycle $[\bar{c}] \in H^1(G_K, \phi(\bar{r})) =: H^1(G_K, A(\bar{\mathbb{F}}_p))$. We first construct a lift $r^\circ : G_K \rightarrow \mathrm{GL}_2(\bar{\mathbb{Z}}_p)$ of \bar{r} . Then we construct a lift $[c] \in H^1(G_K, A(\bar{\mathbb{Z}}_p))$ of $[\bar{c}]$.

(II) Use the fact $\bar{\rho}$ factors through a Borel (minimal parabolic)

$$B = \begin{bmatrix} * & * & * \\ 0 & * & * \\ 0 & 0 & * \end{bmatrix} = \begin{bmatrix} * & 0 & 0 \\ 0 & * & 0 \\ 0 & 0 & * \end{bmatrix} \ltimes \begin{bmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{bmatrix} = T \ltimes H,$$

where the Levi group T is a maximal torus, and the unipotent radical H is the Heisenberg group. Let $\bar{r} : G_K \rightarrow T(\bar{\mathbb{F}}_p)$ be the Levi factor of $\bar{\rho}$. To reconstruct $\bar{\rho}$ from \bar{r} , we only need the information of a 1-cocycle $[\bar{c}] \in H^1(G_K, H(\bar{\mathbb{F}}_p))$. We first construct a lift of \bar{r} , and then construct a lift of \bar{c} . Now $H^1(G_K, H(\bar{\mathbb{F}}_p))$ is nonabelian Galois cohomology.

We make use of the graded structure of Lie H when we construct a lift of $[\bar{c}]$. We have a short exact sequence

$$1 \rightarrow \begin{bmatrix} 1 & 0 & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \rightarrow H \rightarrow \begin{bmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{bmatrix} \rightarrow 1.$$

We will first construct a lift modulo $Z(H)$, and then extend the lift modulo $Z(H)$ to a cocycle on the whole unipotent radical H .

Theorem B applies in this situation, so we have a new proof for the group GL_3 .

1.2.2. We have a short exact sequence of groups $0 \rightarrow Z(U) \rightarrow U \rightarrow U^{\mathrm{ad}} \rightarrow 0$. Since $Z(U)$ is a central, normal subgroup, we have a long exact sequence of pointed sets

$$H^1(G_K, Z(U)) \rightarrow H^1(G_K, U) \rightarrow H^1(G_K, U^{\mathrm{ad}}) \xrightarrow{\delta} H^2(G_K, Z(U)).$$

Note that δ is a quadratic form, and there is an associated bilinear form

$$\cup : H^1(G_K, U^{\mathrm{ad}}) \times H^1(G_K, U^{\mathrm{ad}}) \rightarrow H^2(G_K, Z(U))$$

defined by $x \cup y = (\delta(x + y) - \delta(x) - \delta(y))/2$.

The technical heart of this paper is an analysis of \cup on the cochain/cocycle level. So we need a finite cochain complex computing Galois cohomology which interacts nicely with the bilinear form \cup . Thanks to the theory of Demushkin groups, there is an explicitly defined cochain complex (the so-called Lyndon–Demushkin complex) which computes $H^\bullet(G_{K'}, U^{\mathrm{ad}})$ and $H^\bullet(G_{K'}, Z(U))$ after a finite Galois extension K'/K . When $[K' : K]$ is prime to p , we can fully understand cup products on the cochain/cocycle level via Lyndon–Demushkin complexes endowed with $G_K/G_{K'}$ -action.

We have the following nice obstruction theory:

Theorem C (Corollary 4.3.4). *Let $p \neq 2$ be a prime integer. Let L be a reductive group over \mathcal{O}_E and fix an algebraic group homomorphism $L \rightarrow \text{Aut}(U)$. Let $r : G_K \rightarrow L(\mathcal{O}_E)$ be a Galois representation.*

If there exists a finite Galois extension K'/K of prime-to- p degree such that $r|_{G_{K'}}$ is Lyndon–Demushkin and mildly regular, then there is a short exact sequence of pointed sets

$$H^1(G_K, U(\overline{\mathbb{Z}}_p)) \rightarrow H^1(G_K, U(\overline{\mathbb{F}}_p)) \xrightarrow{\delta} H^2(G_K, U^{\text{ad}}(\overline{\mathbb{Z}}_p)),$$

where δ has a factorization $H^1(G_K, U(\overline{\mathbb{F}}_p)) \xrightarrow{p} H^1(G_K, U^{\text{ad}}(\overline{\mathbb{F}}_p)) \rightarrow H^2(G_K, U^{\text{ad}}(\overline{\mathbb{Z}}_p))$.

1.3. Organization. In Section 2, we review the results of Lyndon and Demushkin and establish some notation. Sections 3 and 4 form the technical heart of this paper. Sections 5 and 6 are mild generalizations of results from [Emerton and Gee 2023]. The proofs are almost unchanged and we often just sketch the ideas of the proof and invite the readers to look at the proofs of [Emerton and Gee 2023].

We prove the main theorem in Section 7.

2. Lyndon–Demushkin theory

Assume $p \neq 2$. Let K/\mathbb{Q}_p be a finite extension containing the p -th root of unity. The maximal pro- p quotient of the absolute Galois group G_K has a very nice description. The following well-known theorem can be found, for example, in [Serre 2002, Section II.5.6].

Theorem 2.0.1. *Let $G_K(p)$ be the maximal pro- p quotient of G_K . Then $G_K(p)$ is the pro- p completion of the one-relator group*

$$\langle x_0, \dots, x_{n+1} \mid x_0^q(x_0, x_1)(x_2, x_3) \cdots (x_n, x_{n+1}) \rangle,$$

where $n = [K : \mathbb{Q}_p]$, and $q = p^s$ is the largest power of p such that K contains the q -th roots of unity. Here $(x, y) = xyx^{-1}y^{-1}$.

Definition 2.0.2. A continuous profinite G_K -module A is said to be *Lyndon–Demushkin* if the image of $G_K \rightarrow \text{Aut}(A)$ is a pro- p group.

2.1. Comparing cohomology of Demushkin groups and Galois cohomology. Let Γ^{disc} be the discrete group with one relator

$$\langle x_0, \dots, x_n, x_{n+1} \mid x_0^q(x_0, x_1)(x_2, x_3) \cdots (x_n, x_{n+1}) \rangle.$$

Let K/\mathbb{Q}_p be a p -adic field containing the group of p -th root of unity. Let A be a Lyndon–Demushkin G_K -module. Write $H^\bullet(\Gamma^{\text{disc}}, A)$ for the usual group cohomology, and write $H^\bullet(G_K, A)$ for the continuous profinite cohomology.

Note that there is a functorial map

$$H^\bullet(G_K, A) \rightarrow H^\bullet(\Gamma^{\text{disc}}, A) \tag{2-1}$$

induced from the forgetful functor $\text{Mod}_{\text{cont}}(G_K(p)) \rightarrow \text{Mod}(\Gamma^{\text{disc}})$.

Lemma 2.1.1. *Let \mathbb{F}_p be the G_K -module with trivial G_K -action. Then (2-1) induces isomorphisms:*

$$(1) H^1(G_K, \mathbb{F}_p) = H^1(\Gamma^{\text{disc}}, \mathbb{F}_p).$$

$$(2) H^2(G_K, \mathbb{F}_p) = H^2(\Gamma^{\text{disc}}, \mathbb{F}_p).$$

Proof. (1) We have

$$\begin{aligned} H^1(G_K, \mathbb{F}_p) &= \text{Hom}_{\text{cont}}(G_K, \mathbb{F}_p) = \text{Hom}_{\text{cont}}(G_K(p), \mathbb{F}_p), \\ H^1(\Gamma^{\text{disc}}, \mathbb{F}_p) &= \text{Hom}(\Gamma^{\text{disc}}, \mathbb{F}_p). \end{aligned}$$

Note that $\text{Hom}_{\text{cont}}(G_K(p), \mathbb{F}_p) = \text{Hom}(\Gamma^{\text{disc}}, \mathbb{F}_p)$ because $G_K(p)$ is the pro- p completion of Γ^{disc} .

(2) We have a commutative diagram

$$\begin{array}{ccc} H^1(G_K, \mathbb{F}_p) \times H^1(G_K, \mathbb{F}_p) & \xrightarrow{\cup} & H^2(G_K, \mathbb{F}_p) \\ \downarrow & & \downarrow \\ H^1(\Gamma^{\text{disc}}, \mathbb{F}_p) \times H^1(\Gamma^{\text{disc}}, \mathbb{F}_p) & \xrightarrow{\cup} & H^2(\Gamma^{\text{disc}}, \mathbb{F}_p) \end{array}$$

Note that the first row is a nondegenerate pairing, and $H^2(G_K, \mathbb{F}_p) \cong \mathbb{F}_p$ by local Tate duality. By Lyndon's theorem or Corollary 2.2.2, we have $H^2(\Gamma^{\text{disc}}, \mathbb{F}_p) \cong \mathbb{F}_p$. So it remains to show the cup product of the second row is nontrivial. Let $[c_1], [c_2] \in H^1(\Gamma^{\text{disc}}, \mathbb{F}_p)$. $[c_1] \cup [c_2] = 0$ if and only if there exists a group homomorphism

$$\Gamma^{\text{disc}} \rightarrow \begin{bmatrix} 1 & c_1 & * \\ & 1 & c_2 \\ & & 1 \end{bmatrix}$$

for some $*$. Indeed, if $c_1 \cup c_2 = dz$ for some $z \in C^1(\Gamma^{\text{disc}}, \mathbb{F}_p)$, then

$$\Gamma^{\text{disc}} \rightarrow \begin{bmatrix} 1 & c_1 & z \\ & 1 & c_2 \\ & & 1 \end{bmatrix}$$

is a group homomorphism by unravelling the definition of cup products; here $C^1(\Gamma^{\text{disc}}, \mathbb{F}_p)$ is the usual cochain group defining group cohomology. Define $c_i : \Gamma^{\text{disc}} \rightarrow \mathbb{F}_p$ by sending x_i to 1 and other generators to 0, $i = 0, 1$. Then it is clear $[c_1] \cup [c_2] \neq 0$. \square

Corollary 2.1.2. *Let A be a finite \mathbb{F}_p -vector space endowed with Lyndon–Demushkin G_K -action. Then there is a canonical isomorphism $H^\bullet(G_K, A) = H^\bullet(\Gamma^{\text{disc}}, A)$.*

Proof. Let $G_K(p)$ be the maximal pro- p quotient of G_K . Then A is a $G_K(p)$ -module. Since $G_K(p)$ is a pro- p group, A must contain the trivial representation \mathbb{F}_p . In particular, there is a short exact sequence

$$0 \rightarrow \mathbb{F}_p \rightarrow A \rightarrow A' \rightarrow 0$$

which induces the long exact sequence

$$\begin{array}{ccccccccc} H^0(G_K, A') & \longrightarrow & H^1(G_K, \mathbb{F}_p) & \longrightarrow & H^1(G_K, A) & \longrightarrow & H^1(G_K, A') & \longrightarrow & H^2(G_K, \mathbb{F}_p) \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ H^0(\Gamma^{\text{disc}}, A') & \longrightarrow & H^1(\Gamma^{\text{disc}}, \mathbb{F}_p) & \longrightarrow & H^1(\Gamma^{\text{disc}}, A) & \longrightarrow & H^1(\Gamma^{\text{disc}}, A') & \longrightarrow & H^2(\Gamma^{\text{disc}}, \mathbb{F}_p) \end{array}$$

We apply induction on the length of A . By the five lemma, we have $H^1(G_K, A) = H^1(\Gamma^{\text{disc}}, A)$.

We also have the long exact sequence

$$\begin{array}{ccccccccc} H^1(G_K, A') & \longrightarrow & H^2(G_K, \mathbb{F}_p) & \longrightarrow & H^2(G_K, A) & \longrightarrow & H^2(G_K, A') & \longrightarrow & H^3(G_K, \mathbb{F}_p) \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ H^1(\Gamma^{\text{disc}}, A') & \longrightarrow & H^2(\Gamma^{\text{disc}}, \mathbb{F}_p) & \longrightarrow & H^2(\Gamma^{\text{disc}}, A) & \longrightarrow & H^2(\Gamma^{\text{disc}}, A') & \longrightarrow & H^3(\Gamma^{\text{disc}}, \mathbb{F}_p) \end{array}$$

By Lyndon’s theorem, $H^3(\Gamma^{\text{disc}}, \mathbb{F}_p) = 0$. By local Tate duality, $H^3(G_K, \mathbb{F}_p) = 0$. Again by the five lemma, we have $H^2(G_K, A) = H^2(\Gamma^{\text{disc}}, A)$. Finally, both cohomology groups are supported on degrees $[0, 2]$. \square

By induction on the order of A , (2-1) is an isomorphism for any finite p -power torsion group A .

Corollary 2.1.3. *Let A be a finite \mathbb{Z}_p -module endowed with the Lyndon–Demushkin G_K -action. Then there is a canonical isomorphism $H^\bullet(G_K, A) = H^\bullet(\Gamma^{\text{disc}}, A)$.*

Proof. We have a short exact sequence for each $k > 0$,

$$0 \rightarrow \varprojlim_i^1 H^{k-1}(G_K, A/p^i A) \rightarrow H^k(G_K, A) \rightarrow \varprojlim_i H^k(G_K, A/p^i A) \rightarrow 0,$$

see, for example [Stacks, Tag 0BKN]; here \varprojlim_i^1 is the derived inverse limit. The first term is 0 due to the finiteness of the cohomology of torsion G_K -modules. So $H^k(G_K, A) = \varprojlim_i H^k(G_K, A/p^i A)$, and the corollary is reduced to the p -power torsion case.

We can do the same thing for the discrete cohomology. Since any finite \mathbb{Z}_p -module is p -adically complete, the Lyndon–Demushkin complex (see Section 2.3.7) computing $H^\bullet(\Gamma^{\text{disc}}, A)$ is the inverse limit of the Lyndon–Demushkin complex mod p^i . So $H^k(\Gamma^{\text{disc}}, A) = \varprojlim_i H^k(\Gamma^{\text{disc}}, A/p^i)$. \square

The lemma above tells us that, for our purposes, the cohomology groups of $G_K(p)$ can be computed via the discrete model. So we can make use of the fine machineries of combinatorial group theory.

2.2. Discrete group cohomology of Demushkin groups. The main reference of this subsection is [Lyndon 1950].

Derivations. A derivation of a group G is a left G -module M , together with a map $D : G \rightarrow M$ such that $D(uv) = Du + uDv$.

Say F is a free group with generators x_1, \dots, x_m . Denote by dFJ the module of universal derivations. Then dFJ is the free $\mathbb{Z}[F]$ -module with basis $\{dx_i \mid i = 1, \dots, m\}$.

Let $u \in F$. We can write $du \in dFJ$ as a linear combination of the basis elements:

$$du = \sum \frac{\partial u}{\partial x_i} dx_i,$$

where $\frac{\partial u}{\partial x_i} \in \mathbb{Z}[F]$. The computation rules for $\frac{\partial u}{\partial x_i}$ can be found in the first line of page 654 of [Lyndon 1950].

Theorem 2.2.1 [Lyndon 1950, Theorem 11.1]. *Let $G = \langle x_1, \dots, x_m | R \rangle$ be a one-relator group where $R = Q^q$ for no $q > 1$. Let K be any left G -module. Then*

$$H^2(G, K) \cong K / \left(\frac{\partial R}{\partial x_1}, \dots, \frac{\partial R}{\partial x_m} \right) K$$

and $H^n(G, K) = 0$ for all $n > 2$.

Corollary 2.2.2. *We have $H^2(\Gamma^{\text{disc}}, \mathbb{F}_p) = \mathbb{F}_p$.*

Proof. We have

$$\begin{aligned} \frac{\partial R}{\partial x_0} &= 1 + x_0 + \dots + x_0^{q-2} + x_0^{q-1} x_1^{-1}, \\ \frac{\partial R}{\partial x_1} &= x_0^{q-1} x_1^{-1} (x_0 - 1), \\ \frac{\partial R}{\partial x_2} &= x_0^q (x_0, x_1) x_2^{-1} (x_3 - 1), \\ \frac{\partial R}{\partial x_3} &= x_0^q (x_0, x_1) x_2^{-1} x_3^{-1} (x_2 - 1), \\ &\vdots \\ \frac{\partial R}{\partial x_{2k}} &= x_0^q (x_0, x_1) \dots (x_{2k-2}, x_{2k-1}) x_{2k}^{-1} (x_{2k+1} - 1), \\ \frac{\partial R}{\partial x_{2k+1}} &= x_0^q (x_0, x_1) \dots (x_{2k-2}, x_{2k-1}) x_{2k}^{-1} x_{2k+1}^{-1} (x_{2k} - 1), \\ &\vdots \end{aligned}$$

Since

$$H^2(\Gamma^{\text{disc}}, \mathbb{F}_p) = \frac{\mathbb{F}_p}{(\partial R / \partial x_0, \dots, \partial R / \partial x_{n+1})},$$

it suffices to show

$$\frac{\partial R}{\partial x_0} \mathbb{F}_p = \dots = \frac{\partial R}{\partial x_{n+1}} \mathbb{F}_p = 0.$$

Since \mathbb{F}_p is a trivial G_K -module, it is clear that

$$\frac{\partial R}{\partial x_1} \mathbb{F}_p = \dots = \frac{\partial R}{\partial x_{n+1}} \mathbb{F}_p = 0.$$

We also have $\frac{\partial R}{\partial x_0} = 1 + 1 + \dots + 1 = q = 0 \pmod{p}$. □

Proposition 2.2.3. *Let A be a G_K -module whose underlying abelian group is a finitely generated \mathbb{Z}_p -module such that the image of G_K in $\text{Aut}(A)$ is a pro- p group. Then*

$$H^2(G_K, A) \cong A / \left(\frac{\partial R}{\partial x_0}, \dots, \frac{\partial R}{\partial x_{n+1}} \right) A,$$

where $R = x_0^q(x_0, x_1)(x_2, x_3) \cdots (x_n, x_{n+1})$.

Proof. Combine Corollary 2.1.3 and Lyndon’s theorem. □

2.3. Lyndon–Demushkin complex.

2.3.1. Abelian coefficient case. Let A be a G_K -module whose underlying abelian group is a finitely generated \mathbb{Z}_p -module such that the image of G_K in $\text{Aut}(A)$ is a pro- p group.

Then there is an explicit co-chain complex computing the Galois cohomology $H^\bullet(G_K, A)$.

Define $C_{LD}^\bullet(A) = [C_{LD}^0(A) \xrightarrow{d^1} C_{LD}^1(A) \xrightarrow{d^2} C_{LD}^2(A)]$ as the following cochain complex supported on degrees $[0, 2]$:

$$A \xrightarrow{\begin{bmatrix} 1-x_0 \\ \vdots \\ 1-x_{n+1} \end{bmatrix}} A^{\oplus(n+2)} \xrightarrow{\begin{bmatrix} \partial R/\partial x_0 \\ \vdots \\ \partial R/\partial x_{n+1} \end{bmatrix}^T} A.$$

Then, by [Lyndon 1950, Theorem 11.1],

$$H^\bullet(C_{LD}^\bullet(A)) = H^\bullet(G_K, A).$$

The idea of a Lyndon–Demushkin complex is simple. A 1-cochain $c \in C_{LD}^1(A)$ is simply a set-theoretical function

$$c : \{x_0, \dots, x_{n+1}\} \rightarrow A.$$

We can extend c to be a function on the free group

$$c : \langle x_0, \dots, x_{n+1} \rangle \rightarrow A$$

by setting $c(gh) := c(g) + g \cdot c(h)$ for any g, h in the free group with $n+2$ generators. Let

$$R = x_0^q(x_0, x_1)(x_2, x_3) \cdots (x_n, x_{n+1})$$

be the single relation defining the Demushkin group. The differential operator $d^2 : C_{LD}^1(A) \rightarrow C_{LD}^2(A)$ is nothing but the evaluation of the extended map c at the relation R , that is, $d^2(c) = c(R)$. So a 1-cochain c is a 1-cocycle if and only if its evaluation at R is 0.

2.3.2. Nilpotent coefficients. Let E/\mathbb{Q}_p be a finite extension with ring of integers \mathcal{O}_E , residue field \mathbb{F} , and uniformizer ϖ .

Let U be a unipotent (smooth connected) linear algebraic group over $\text{Spec } \mathcal{O}_E$, admitting an upper central series

$$1 = U_0 \subset U_1 \cdots \subset U_k = U.$$

Assume there exists an embedding $\iota : U \hookrightarrow \mathrm{GL}_N \subset \mathrm{Mat}_{N \times N}$ such that $(\iota(x) - 1)^{k+1} = 0$ for all $x \in U$. Write $\log = \log_{\leq k}$ for the truncated logarithmic function $1 + x \mapsto x - x^2/2 + \cdots + (-1)^{k+1}x^k/k$.

Assume $p > k$. There is an isomorphism of schemes $U \cong \mathrm{Lie} U$ sending $g \mapsto \log g$, defined through the commutative diagram

$$\begin{array}{ccc} U & \longrightarrow & \mathrm{GL}_N \\ \downarrow \log & & \downarrow \log \\ \mathrm{Lie} U & \longrightarrow & \mathrm{Mat}_{N \times N} \end{array}$$

We assume $k = 2$ from now on because it suffices for our applications.

Fix a Galois action $G_K \rightarrow \mathrm{Aut}(U)(\mathcal{O}_E)$ such that the image group is a pro- p subgroup of $\mathrm{Aut}(U)(\mathcal{O}_E)$.

Let A be an \mathcal{O}_E -algebra. Recall that a *nonabelian crossed homomorphism* valued in $U(A)$ is a map $c : G_K \rightarrow U(A)$ such that

$$c(gh) = c(g)(g \cdot c(h))$$

for all $g, h \in G_K$. Set $\mathfrak{c} := \log(c) : G_K \rightarrow \mathrm{Lie} U(A)$. By the Baker–Campbell–Hausdorff formula,

$$\mathfrak{c}(gh) = \mathfrak{c}(g) + g \cdot \mathfrak{c}(h) + \frac{1}{2}[\mathfrak{c}(g), g \cdot \mathfrak{c}(h)]. \quad (2-2)$$

Our definition of the Lyndon–Demushkin cochain complex is motivated by (2-2).

Definition 2.3.3. Let A be an \mathcal{O}_E -algebra. The Lyndon–Demushkin complex with unipotent coefficients is defined to be the following cochain complex $C_{\mathrm{LD}}^\bullet(U(A))$ supported in degrees $[0, 2]$:

$$\mathrm{Lie} U(A) \xrightarrow{d^1} (\mathrm{Lie} U(A))^{\oplus n+2} \xrightarrow{d^2} \mathrm{Lie} U(A),$$

where d^1 is defined by

$$d^1(v) = \left(-v + x_i \cdot v + \frac{1}{2}[-v, x_i \cdot v]\right)_{i=0, \dots, n+1}.$$

We need some preparations before we define d^2 . An element $c = (\alpha_0, \dots, \alpha_{n+1}) \in C_{\mathrm{LD}}^1(U(A))$ can be regarded as a function on the free group with $(n+2)$ generators

$$c : \langle x_0, \dots, x_{n+1} \rangle \rightarrow \mathrm{Lie} U(A)$$

by setting $c(x_i) = \alpha_i$ for each i and extending it to the whole free group by

$$c(gh) := c(g) + g \cdot c(h) + \frac{1}{2}[c(g), g \cdot c(h)]$$

We define d^2 as

$$d^2(c) := c(R) = c(x_0^q(x_0, x_1)(x_2, x_3) \cdots (x_n, x_{n+1})).$$

Remark 2.3.4. (1) When U is an abelian group, we recover the definition in the previous section for the cohomology of the abelian $U(A)$.

(2) The main reason we define $C_{\mathrm{LD}}^\bullet(U(A))$ this way is because we want to compare it with $C_{\mathrm{LD}}^\bullet(\mathrm{Lie} U(A))$. Note that $C_{\mathrm{LD}}^\bullet(\mathrm{Lie} U(A))$ and $C_{\mathrm{LD}}^\bullet(U(A))$ have the same underlying group, but their differential d^\bullet is different.

- (3) Note that $d^2(c) = 0$ if and only if c defines a crossed homomorphism $c : G_K \rightarrow \text{Lie } U(A)$ in the sense of (2-2). See the proof of Proposition 2.3.6.
- (4) The differential maps are generally nonlinear.

Definition 2.3.5. We define $Z_{\text{LD}}^i := (d^{i+1})^{-1}(0)$, and $B_{\text{LD}}^i := d^i(C_{\text{LD}}^{i-1})$ for $i = 0, 1, 2$.

Proposition 2.3.6. *We have*

$$H^0(G_K, U(A)) \cong Z_{\text{LD}}^0(U(A))$$

and a surjection of pointed sets

$$Z_{\text{LD}}^1(U(A)) \rightarrow H^1(G_K, U(A)).$$

Proof. $H^0(G_K, U(A))$ is by definition the G_K -fixed point subset of $U(A)$, while $Z_{\text{LD}}^0(U(A))$ is the subset of $U(A)$ whose elements are fixed by the x_0, \dots, x_{n+1} : if $u \in U(A)$ is fixed by x_i , then $u^{-1}(x_i \cdot u) = 1$ and taking truncated log of both sides we get $d^1(\log u) = 0$.

$H^1(G_K, U(A))$ is by definition the set of equivalence classes of crossed homomorphisms, and $Z_{\text{LD}}^1(U(A))$ is the set of crossed homomorphisms. □

Lie U has a lower central series filtration. Let $Z(U)$ be the center of U . Write U^{ad} for $U/Z(U)$. Since U is unipotent of class 2, Lie U is isomorphic to its graded Lie algebra $\text{Lie } U \cong \text{gr}^*(\text{Lie } U)$. We will fix a grading $\text{Lie } U \cong Z(U) \oplus U^{\text{ad}}$ of the Lie algebra Lie U once for all. In particular, we fix a projection $\text{pr} : \text{Lie } U \rightarrow Z(U)$.

2.3.7. Cup products. Let $c \in C_{\text{LD}}^1(U^{\text{ad}}(A))$. Let $\tilde{c} \in C_{\text{LD}}^1(U(A))$ be the (unique) lift of c such that $\text{pr}(\tilde{c}(x_0)) = \dots = \text{pr}(\tilde{c}(x_{n+1})) = 0$. Define

$$Q(c) := \text{pr}(d^2(\tilde{c})) = \text{pr}(\tilde{c}(R)) \in C_{\text{LD}}^2(Z(U)(A)).$$

Lemma. $Q(-)$ is a quadratic form, that is, $(x, y) \mapsto Q(x + y) - Q(x) - Q(y)$ is a bilinear form.

Proof. In Definition 2.3.3, we defined it so that $\tilde{c}(gh) := \tilde{c}(g) + g \cdot \tilde{c}(h) + \frac{1}{2}[\tilde{c}(g), g \cdot \tilde{c}(h)]$. So after fully expanding the expression, $\tilde{c}(R) = \sum_i \alpha_i c(x_i) + \sum_{i < j} [\beta_i c(x_i), \gamma_j c(x_j)]$, where $\alpha_i, \beta_i, \gamma_j \in \langle x_0, \dots, x_{n+1} \rangle$. It follows that

$$Q(c) = \text{pr} \left(\sum_i \alpha_i c(x_i) + \sum_{i < j} [\beta_i c(x_i), \gamma_j c(x_j)] \right) = \sum_{i < j} \text{pr}([\beta_i c(x_i), \gamma_j c(x_j)]),$$

which is clearly a quadratic form. □

We define

$$C_{\text{LD}}^1(U^{\text{ad}}(A)) \times C_{\text{LD}}^1(U^{\text{ad}}(A)) \xrightarrow{\cup} C_{\text{LD}}^2(Z(U)(A)), \quad x \cup y := \frac{1}{2}(Q(x + y) - Q(x) - Q(y)),$$

which is a symmetric bilinear form.

Remark. Alternatively, we can choose an arbitrary lift \tilde{c} of c . Now $\text{pr}(d^2(\tilde{c}))$ is an inhomogeneous polynomial of degree two. We recover Q by taking the homogeneous part of degree two.

Lemma 2.3.8. *Under the identification $C_{\text{LD}}^1(U(A)) = C_{\text{LD}}^1(U^{\text{ad}}(A)) \oplus C_{\text{LD}}^1(Z(U)(A))$, we have*

$$Z_{\text{LD}}^1(U(A)) = \{(x, y) \in C_{\text{LD}}^1(U^{\text{ad}}(A)) \oplus C_{\text{LD}}^1(Z(U)(A)) \mid d^2x = 0, x \cup x + d^2y = 0\}.$$

Proof. This is obvious from the definition of d^2 and Q . The projection of $d^2(x, y)$ to $C_{\text{LD}}^2(U^{\text{ad}}(A))$ is d^2x ; and the projection of $d^2(x, y)$ to $C_{\text{LD}}^2(Z(U)(A))$ is $x \cup x + d^2y$. \square

Write $H_{\text{LD}}^i(U^{\text{ad}}(A))$ for

$$Z_{\text{LD}}^i(U^{\text{ad}}(A))/B_{\text{LD}}^i(U^{\text{ad}}(A))$$

and write $H_{\text{LD}}^i(Z(U)(A))$ for

$$Z_{\text{LD}}^i(Z(U)(A))/B_{\text{LD}}^i(Z(U)(A)).$$

Lemma 2.3.9. *The pairing \cup on the cochain level induces a symmetric pairing on the cohomology level*

$$H_{\text{LD}}^1(U^{\text{ad}}(A)) \times H_{\text{LD}}^1(U^{\text{ad}}(A)) \xrightarrow{\cup} H_{\text{LD}}^2(Z(U)(A)).$$

Proof. It suffices to show, for all $x \in Z_{\text{LD}}^1(U^{\text{ad}}(A))$ and $y \in B_{\text{LD}}^1(U^{\text{ad}}(A))$, that

$$Q(x + y) - Q(x) \in B_{\text{LD}}^2(Z(U)(A)).$$

Let $\tilde{x} \in C_{\text{LD}}^1(U(A))$ be the unique extension of x such that $\text{pr } \tilde{x} = 0$. The cochain \tilde{x} represents a group homomorphism $\rho_{\tilde{x}} : \langle x_0, \dots, x_{n+1} \rangle \rightarrow U(A) \rtimes \langle x_0, \dots, x_{n+1} \mid R \rangle$ such that $\rho_{\tilde{x}}(R) = 1 \pmod{Z(U)(A)}$. More explicitly, we define $\rho_{\tilde{x}}(x_i) = (\exp(\tilde{x}(x_i)), x_i)$ where \exp is the truncated exponential map (the inverse to the truncated log map). Since y is a coboundary, there exists $n \in U(A)$ such that $n\rho_{\tilde{x}}n^{-1}$ is represented by a cocycle $(x + y, f)$ extending $x + y$ (we are exploiting the abelian coefficients here). We have $n\rho_{\tilde{x}}(R)n^{-1}\rho_{\tilde{x}}(R)^{-1} = 1 \in U(A) \rtimes \langle x_0, \dots, x_{n+1} \mid R \rangle$ since $\rho_{\tilde{x}}(R)$ lies in the center of $U(A)$. Since $Q(x + y) - d^2(f) = n\rho_{\tilde{x}}(R)n^{-1}$ and $Q(x) = \rho_{\tilde{x}}(R)$, we have $Q(x + y) - Q(x) = d^2f \in B_{\text{LD}}^2(Z(U)(A))$. \square

Recall $Z_{\text{LD}}^1(U(A))$ and $Z_{\text{LD}}^1(\text{Lie } U(A))$ are both subsets of $C_{\text{LD}}^1(U(A))$.

Lemma 2.3.10. *If $Z(U)(\mathbb{F}) \cong \mathbb{F}$, then*

$$Z_{\text{LD}}^1(U(\mathbb{F})) \subset Z_{\text{LD}}^1(\text{Lie } U(\mathbb{F})),$$

that is, the nonabelian cocycles with $U(\mathbb{F})$ -coefficients are automatically abelian cocycles with $(\text{Lie } U(\mathbb{F}))$ -coefficients.

Proof. We have noted in Remark 2.3.4(2) that $C_{\text{LD}}^1(U(\mathbb{F}))$ and $C_{\text{LD}}^1(\text{Lie } U(\mathbb{F}))$ have the same underlying space. By Lemma 2.3.8, an element of $Z_{\text{LD}}^1(U(\mathbb{F}))$ is a pair (x, y) such that $d^2x = 0$ and $x \cup x + d^2y = 0$. By our assumption, $C_{\text{LD}}^2(Z(U)(\mathbb{F})) = H^2(G_K, Z(U)(\mathbb{F}))$ (Corollary 2.2.2) and thus $B_{\text{LD}}^2(Z(U)(\mathbb{F})) = 0$ and $d^2 = 0$. So $d^2y = 0$ automatically, and (x, y) defines an element of $Z_{\text{LD}}^1(\text{Lie } U(\mathbb{F}))$. \square

3. An analysis of cup products

Let E be a p -adic field with ring of integers \mathcal{O}_E , residue field \mathbb{F} and uniformizer ϖ .

Let U be a smooth connected unipotent group of class 2 over $\text{Spec } \mathcal{O}_E$, with center $Z(U) \cong \mathbb{G}_a$. Write U^{ad} for $U/Z(U)$. Assume $U^{\text{ad}} \cong \mathbb{G}_a^{\oplus s}$ is a vector group.

Definition 3.0.1. Let K' be a p -adic field. A Lyndon–Demushkin action $G_{K'} \rightarrow \text{Aut}(U)(\mathcal{O}_E)$ is said to be *mildly regular* if the following are satisfied:

(MR1) $H^0(G_{K'}, U^{\text{ad}}(E)) = 0$.

(MR2) The bilinear pairing

$$\cup_{\mathbb{F}} : C_{\text{LD}}^1(U^{\text{ad}}(\mathbb{F})) \times C_{\text{LD}}^1(U^{\text{ad}}(\mathbb{F})) \rightarrow C_{\text{LD}}^2(Z(U)(\mathbb{F}))$$

is nondegenerate.

Remark 3.0.2. In practice U is the unipotent radical of a parabolic subgroup of a reductive group and (MR2) is equivalent to “ p being not too small”. We worked out the G_2 -case in Appendix A, and showed that if $p > 5$, (MR2) always holds. The same proof but with more complicated notation should work for general reductive groups.

In general, (MR2) can be checked by computer algebra systems because it is a finite field vector space question for a finite number of small p 's. We include an algorithm (written in SageMath) in Appendix B.

The following proposition is a summary of Appendix A:

Proposition 3.0.3. *If U is the unipotent radical of the short root parabolic of G_2 or the quotient of the unipotent radical of the long root parabolic of G_2 by its center, then (MR2) is true when $p \geq 5$.*

Definition 3.0.4. Given a tuple of labeled Hodge–Tate weights (see [Emerton and Gee 2023, Subsection 1.12] for the definition) $\underline{\lambda}$, we say $\underline{\lambda}$ is slightly less than 0 if for each $\sigma : K' \hookrightarrow \overline{\mathbb{Q}}_p$, λ_σ consists of nonpositive integers, and for at least one σ , λ_σ consists of negative integers. (The cyclotomic character has Hodge–Tate weight -1 .)

Proposition 3.0.5. *Assume $p \geq 5$. If U is the unipotent radical of the short root parabolic of G_2 or the quotient of the unipotent radical of the long root parabolic of G_2 by its center, then $G_{K'} \rightarrow \text{Aut}(U)(\mathcal{O}_E)$ is mildly regular if $U^{\text{ad}}(E)$ is Hodge–Tate of labeled Hodge–Tate weights slightly less than 0.*

Proof. If $H^0(G_{K'}, U^{\text{ad}}(E)) \neq 0$, then for all embeddings $\sigma : K \hookrightarrow \overline{\mathbb{Q}}_p$, $0 \in \lambda_\sigma$. The proposition now follows from Proposition 3.0.3 and Appendix A. \square

3.1. Cup products mod ϖ .

Lemma 3.1.1. *The image of $Z_{\text{LD}}^1(U^{\text{ad}}(\mathcal{O}_E)) \rightarrow C_{\text{LD}}^1(U^{\text{ad}}(\mathbb{F}))$ has codimension at most $\dim_E U^{\text{ad}}(E)$.*

Proof. Say $\dim_{\mathbb{F}} C_{\text{LD}}^1(U^{\text{ad}}(\mathbb{F})) = \text{rank}_{\mathcal{O}_E} C_{\text{LD}}^1(U^{\text{ad}}(\mathcal{O}_E)) = N$. Since $Z_{\text{LD}}^1(U^{\text{ad}}(\mathcal{O}_E))$ is the kernel of $C_{\text{LD}}^1(U^{\text{ad}}(\mathcal{O}_E)) \rightarrow C_{\text{LD}}^2(U^{\text{ad}}(\mathcal{O}_E))$, and $\text{rank}_{\mathcal{O}_E} C_{\text{LD}}^2(U^{\text{ad}}(\mathcal{O}_E)) = \dim_E U^{\text{ad}}(E)$, we have

$$\text{rank}_{\mathcal{O}_E} Z_{\text{LD}}^1(U^{\text{ad}}(\mathcal{O}_E)) \geq N - \dim_E U^{\text{ad}}(E).$$

Since $C_{\text{LD}}^2(U^{\text{ad}}(\mathcal{O}_E))$ is torsion-free, $Z_{\text{LD}}^1(U^{\text{ad}}(\mathcal{O}_E))$ is saturated in $C_{\text{LD}}^1(U^{\text{ad}}(\mathcal{O}_E))$, and is thus a direct summand. In particular, the image of $Z_{\text{LD}}^1(U^{\text{ad}}(\mathcal{O}_E))$ in $C_{\text{LD}}^1(U^{\text{ad}}(\mathbb{F}))$ has dimension $\geq N - \dim_E U^{\text{ad}}(E)$. \square

Lemma 3.1.2. *If*

$$\cup_{\mathbb{F}} : C_{\text{LD}}^1(U^{\text{ad}}(\mathbb{F})) \times C_{\text{LD}}^1(U^{\text{ad}}(\mathbb{F})) \rightarrow C_{\text{LD}}^2(Z(U)(\mathbb{F}))$$

is nondegenerate, then the kernel of

$$\cup_{\mathbb{F}} : Z_{\text{LD}}^1(U^{\text{ad}}(\mathcal{O}_E))/\varpi \times Z_{\text{LD}}^1(U^{\text{ad}}(\mathcal{O}_E))/\varpi \rightarrow C_{\text{LD}}^2(Z(U)(\mathbb{F}))$$

has dimension at most $\dim_E U^{\text{ad}}(E)$.

Remark. Note that $Z_{\text{LD}}^1(U^{\text{ad}}(\mathbb{F})) \neq Z_{\text{LD}}^1(U^{\text{ad}}(\mathcal{O}_E))/\varpi$ in general.

The kernel of a bilinear pairing is also called the annihilator.

Proof. For ease of notation, write C for $C_{\text{LD}}^1(U^{\text{ad}}(\mathbb{F}))$, and write Z for the image of $Z_{\text{LD}}^1(U^{\text{ad}}(\mathcal{O}_E))$ in C . Note that $Z \cong Z_{\text{LD}}^1(U^{\text{ad}}(\mathcal{O}_E))/\varpi$ by the proof of the above lemma.

Let $K \subset Z$ be the kernel of $\cup_{\mathbb{F}}$. Since the cup product on C is nondegenerate, there exists a subspace $F \subset C$ of dimension equal to that of K , such that the restriction of the cup product to $(F + K)$ is also nondegenerate. Since $F \cap Z = 0$, $\dim C \geq \dim(F + Z) = \dim Z + \dim F = \dim Z + \dim K$. The lemma now follows from the previous lemma. \square

We also record the following lemma whose proof is similar.

Lemma 3.1.3. (1) *The image of $Z_{\text{LD}}^1(U^{\text{ad}}(\mathbb{F})) \rightarrow C_{\text{LD}}^1(U^{\text{ad}}(\mathbb{F}))$ has codimension at most $\dim_E U^{\text{ad}}(E)$.*

(2) *If*

$$\cup_{\mathbb{F}} : C_{\text{LD}}^1(U^{\text{ad}}(\mathbb{F})) \times C_{\text{LD}}^1(U^{\text{ad}}(\mathbb{F})) \rightarrow C_{\text{LD}}^2(Z(U)(\mathbb{F}))$$

is nondegenerate, then the kernel of

$$\cup_{\mathbb{F}} : Z_{\text{LD}}^1(U^{\text{ad}}(\mathbb{F})) \times Z_{\text{LD}}^1(U^{\text{ad}}(\mathbb{F})) \rightarrow C_{\text{LD}}^2(Z(U)(\mathbb{F}))$$

has dimension at most $\dim_E U^{\text{ad}}(E)$.

3.2. General cup products in group cohomology. In this subsection, we give a reinterpretation of Section 2.3.7, which is convenient for theoretic applications.

Let V be a unipotent algebraic group of class 2 over \mathcal{O}_E . Let Γ be an abstract group, together with a homomorphism $\theta : \Gamma \rightarrow \text{Aut}(V)(\mathcal{O}_E)$. By the Lie correspondence, $\text{Aut}(\text{Lie } V) \cong \text{Aut}(V)$, and thus θ induces a \mathcal{O}_E -linear Γ -action on $\text{Lie } V$ which respects Lie brackets.

We fix a grading $\text{Lie } V = V_1 \oplus V_2$ such that $[V_1, V_1] \subset V_2$, and $[V, V_2] = 0$. We will write V for $V(\mathcal{O}_E)$ for simplicity.

Let $f : \Gamma \rightarrow V$ be a crossed homomorphism. By definition, for any $g_1, g_2 \in \Gamma$, $f(g_1g_2) = f(g_1)g_1f(g_2)$. Write $c = c_1 + c_2$ for $\log(f)$, where c_1 values in V_1 and c_2 values in V_2 . By the Baker–Campbell–Hausdorff formula, we have

$$\begin{aligned} c(gh) &= c(g) + gc(h) + [c(g), gc(h)]/2 \\ &= (c_1(g) + gc_1(h)) + (c_2(g) + gc_2(h)) + [c_1(g), gc_1(h)]/2 \end{aligned} \tag{3-1}$$

Lemma 3.2.1. *Let $a, b \in H^1(\Gamma, V_1)$ be two crossed homomorphisms. The 2-cochain $B(a, b) : (g, h) \mapsto [a(g), gb(h)]$ is a 2-cocycle.*

Proof. By definition, we have

$$\begin{aligned} d^2(B(a, b))(g_1, g_2, g_3) &= g_1[a(g_2), g_2b(g_3)] - [d^1a(g_1, g_2), g_1g_2b(g_3)] + [a(g_1), g_1d^1b(g_2, g_3)] + [a(g_1), g_1b(g_2)] \\ &= g_1[a(g_2), g_2b(g_3)] - [a(g_1) + g_1a(g_2), g_1g_2b(g_3)] + [a(g_1), g_1b(g_2) + g_1g_2b(g_3)] + [a(g_1), g_1b(g_2)] \\ &= 0. \end{aligned} \quad \square$$

For crossed homomorphisms $a \in H^1(\Gamma, V_1)$, define $Q(a) := B(a, a)$. By comparing (3-1) and Section 2.3.7, it is not hard to see the $Q(-)$ defined in this subsection coincides with that of Section 2.3.7 for 1-cocycles when Γ is the discrete Demushkin group.

Since $a \cup b := (Q(a+b, a+b) - Q(a) - Q(b))/2 = (B(a, b) + B(b, a))/2$, we have $a \cup b \in H^2(\Gamma, V_2)$. Again the cup product defined in this subsection coincides with that of Section 2.3.7 when the settings overlap.

Lemma 3.2.2. *Let $\Gamma' \subset \Gamma$ be a normal subgroup of finite index. Write Δ for Γ/Γ' . The cup product $\cup : H^1(\Gamma', V_1) \times H^1(\Gamma', V_1) \rightarrow H^2(\Gamma', V_2)$ is Δ -equivariant.*

Proof. Let $a, b \in H^1(\Gamma', V_1)$, and let $\sigma \in \Gamma$. We have by definition $\sigma \cdot a(g) = \sigma a(\sigma^{-1}g\sigma)$, and $\sigma \cdot B(a, b)(g, h) = \sigma B(a, b)(\sigma^{-1}g\sigma, \sigma^{-1}h\sigma)$ (see [Serre 2002, Section I.5.8]). We immediately have $\sigma \cdot B(a, b) = B(\sigma \cdot a, \sigma \cdot b)$. □

Example 3.2.3 (the completely split case). In this paragraph we analyze the special case where the $G_{K'}$ action on $U^{\text{ad}}(\mathbb{F}) \cong \text{Lie } U^{\text{ad}}(\mathbb{F})$ is trivial and $H^2(G_{K'}, Z(U)(\mathbb{F})) = Z(U)(\mathbb{F}) = \mathbb{F}$. It will be used in the proof of Theorem 3.3.1.

Since the center of $\text{Lie } U$ is one-dimensional, the Lie bracket

$$\text{Lie } U^{\text{ad}}(\mathbb{F}) \times \text{Lie } U^{\text{ad}}(\mathbb{F}) \xrightarrow{[\cdot, \cdot]} Z(U)(\mathbb{F})$$

is a nondegenerate, alternating pairing. Choose a basis $\{e_1, \dots, e_k, e'_1, \dots, e'_k\}$ of $\text{Lie } U^{\text{ad}}(\mathbb{F})$ such that $[e'_i, e'_j] = [e_i, e_j] = 0$ and $[e_i, e'_j] = -[e'_i, e_j] = \delta_{i,j}$. Since by assumption the $G_{K'}$ -action on $U^{\text{ad}}(\mathbb{F})$ is trivial, the cup product

$$\cup : H^1(G_{K'}, U^{\text{ad}}(\mathbb{F})) \times H^1(G_{K'}, U^{\text{ad}}(\mathbb{F})) \rightarrow H^2(G_{K'}, Z(U)(\mathbb{F}))$$

is isomorphic to the (exterior) direct sum of cup products

$$\cup_i : H^1(G_{K'}, \mathbb{F}e_i \oplus \mathbb{F}e'_i) \times H^1(G_{K'}, \mathbb{F}e_i \oplus \mathbb{F}e'_i) \rightarrow H^1(G_{K'}, \mathbb{F}).$$

Write \wedge for the usual cup product $H^1(G_{K'}, \mathbb{F}) \times H^1(G_{K'}, \mathbb{F}) \rightarrow H^2(G_{K'}, \mathbb{F})$ which appears in local Tate duality. By definition, for $a, b \in H^1(G_{K'}, \mathbb{F})$ we have

$$\begin{aligned} Q(ae_i + be'_i) &= B(ae_i + be'_i, ae_i + be'_i) \\ &= ((g, h) \mapsto [a(g)e_i + b(g)e'_i, a(h)e_i + b(h)e'_i]) \\ &= ((g, h) \mapsto (a(g)b(h) - b(g)a(h))) \\ &= a \wedge b - b \wedge a \\ &= 2a \wedge b \end{aligned}$$

and thus, for $a_1, b_1, a_2, b_2 \in H^1(G_{K'}, \mathbb{F})$,

$$B(a_1e_i + b_1e'_i, a_2e_i + b_2e'_i) = 2(a_1 \wedge b_2 + a_2 \wedge b_1).$$

Since \wedge is a nondegenerate pairing, B is also a nondegenerate pairing.

3.3. Nontriviality of cup products.

Theorem 3.3.1. *Let K'/K be a finite Galois extension of p -adic fields of prime-to- p degree. Let $r : G_K \rightarrow \text{Aut}(U)(\mathcal{O}_E)$ be a continuous group homomorphism.*

If $r|_{G_{K'}}$ is Lyndon–Demushkin and mildly regular, then either

- (i) $H^2(G_K, Z(U)(\mathbb{F})) = 0$, or
- (ii) *the symmetric bilinear pairing*

$$H^1(G_K, U^{\text{ad}}(\mathcal{O}_E)) \otimes \mathbb{F} \times H^1(G_K, U^{\text{ad}}(\mathcal{O}_E)) \otimes \mathbb{F} \rightarrow H^2(G_K, Z(U)(\mathcal{O}_E)) \otimes \mathbb{F}$$

is nontrivial.

Remark. Notice that

$$H_{\text{LD}}^1(U^{\text{ad}}(\mathcal{O}_E)) \cong H^1(G_{K'}, U^{\text{ad}}(\mathcal{O}_E)) \quad \text{and} \quad H^1(G_{K'}, U^{\text{ad}}(\mathcal{O}_E))^{G_K} = H^1(G_K, U^{\text{ad}}(\mathcal{O}_E)).$$

The symmetric pairing in the theorem is the restriction to $H^1(G_{K'}, U^{\text{ad}}(\mathcal{O}_E))$ of the symmetric pairing defined in Lemma 2.3.9.

Proof. Assume $H^2(G_K, Z(U)(\mathbb{F})) \neq 0$. Consider the diagram

$$\begin{array}{ccc} H^1(G_K, U^{\text{ad}}(\mathcal{O}_E)) \times H^1(G_K, U^{\text{ad}}(\mathcal{O}_E)) & \longrightarrow & H^2(G_K, Z(U)(\mathcal{O}_E)) \\ \downarrow & & \downarrow \cong \\ H^1(G_{K'}, U^{\text{ad}}(\mathcal{O}_E)) \times H^1(G_{K'}, U^{\text{ad}}(\mathcal{O}_E)) & \longrightarrow & H^2(G_{K'}, Z(U)(\mathcal{O}_E)) \\ \uparrow & & \uparrow \\ Z_{\text{LD}}^1(U^{\text{ad}}(\mathcal{O}_E)) \times Z_{\text{LD}}^1(U^{\text{ad}}(\mathcal{O}_E)) & \longrightarrow & C^2(Z(U)(\mathcal{O}_E)) \end{array}$$

By Lemma 3.1.2, the kernel of

$$H^1(G_{K'}, U^{\text{ad}}(\mathcal{O}_E))/\varpi \times H^1(G_{K'}, U^{\text{ad}}(\mathcal{O}_E))/\varpi \rightarrow H^2(G_{K'}, Z(U)(\mathbb{F}))$$

has \mathbb{F} -dimension at most $\dim_E U^{\text{ad}}(E)$. Write Δ for $G_K/G_{K'}$, which acts on $H^1(G_{K'}, U^{\text{ad}}(\mathcal{O}_E))$ with fixed-point subspace $H^1(G_K, U^{\text{ad}}(\mathcal{O}_E))$.

By an averaging argument (explained below), the kernel of

$$H^1(G_K, U^{\text{ad}}(\mathcal{O}_E))/\varpi \times H^1(G_K, U^{\text{ad}}(\mathcal{O}_E))/\varpi \rightarrow H^2(G_K, Z(U)(\mathbb{F}))$$

is contained in the kernel of

$$H^1(G_{K'}, U^{\text{ad}}(\mathcal{O}_E))/\varpi \times H^1(G_{K'}, U^{\text{ad}}(\mathcal{O}_E))/\varpi \rightarrow H^2(G_{K'}, Z(U)(\mathbb{F}))$$

and thus has \mathbb{F} -dimension at most $\dim_E U^{\text{ad}}(E)$. (Let $[c] \in H^1(G_K, U^{\text{ad}}(\mathcal{O}_E))/\varpi$ and suppose $[c] \cup [d] = 0$ for all $[d] \in H^1(G_K, U^{\text{ad}}(\mathcal{O}_E))/\varpi$. Let $[c'] \in H^1(G_{K'}, U^{\text{ad}}(\mathcal{O}_E))/\varpi$. Then $\sum_{\sigma \in \Delta} \sigma([c] \cup [c']) = [c] \cup \sum_{\sigma \in \Delta} \sigma([c']) = 0$. Since $H^2(G_K, Z(U)(\mathbb{F})) \neq 0$, we have $H^2(G_K, Z(U)(\mathbb{F})) = H^2(G_{K'}, Z(U)(\mathbb{F}))$ and thus $\sum_{\sigma \in \Delta} \sigma([c] \cup [c']) = \#\Delta \sigma([c] \cup [c'])$.)

We remark that as a finitely generated module over a DVR, $H^1(G_K, U^{\text{ad}}(\mathcal{O}_E))$ is the direct sum of its torsion-free part and its torsion part; and $H^1(G_K, U^{\text{ad}}(E)) = H^1(G_K, U^{\text{ad}}(\mathcal{O}_E))_{\text{torsion-free}} \otimes_{\mathcal{O}_E} E$.

By the local Euler characteristic,

$$\begin{aligned} \dim_E H^1(G_K, U^{\text{ad}}(E)) &= \dim_E H^2(G_K, U^{\text{ad}}(E)) + \dim_E H^0(G_K, U^{\text{ad}}(E)) + \dim_E U^{\text{ad}}(E)[K : \mathbb{Q}_p] \\ &\geq \dim_E H^2(G_K, U^{\text{ad}}(E)) + \dim_E U^{\text{ad}}(E). \end{aligned}$$

We will now consider two possibilities: $H^2(G_K, U^{\text{ad}}(\mathbb{F})) \neq 0$ and $H^2(G_K, U^{\text{ad}}(\mathbb{F})) = 0$.

Case $H^2(G_K, U^{\text{ad}}(\mathbb{F})) \neq 0$. Since $H^2(G_K, U^{\text{ad}}(\mathbb{F})) \neq 0$, $H^2(G_K, U^{\text{ad}}(\mathcal{O}_E))$ is nontrivial. So either we have $\dim_E H^2(G_K, U^{\text{ad}}(E)) > 0$, or $H^2(G_K, U^{\text{ad}}(\mathcal{O}_E))$ has nontrivial torsion. If $H^2(G_K, U^{\text{ad}}(\mathcal{O}_E))$ has nontrivial torsion, then again by the local Euler characteristic (mod ϖ version), $H^1(G_K, U^{\text{ad}}(\mathcal{O}_E))$ also has nontrivial torsion. In either case, $\dim_{\mathbb{F}} H^1(G_K, U^{\text{ad}}(\mathcal{O}_E))/\varpi \geq \dim_E U^{\text{ad}}(E) + 1$. So the kernel of the cup product is a proper subspace of $H^1(G_K, U^{\text{ad}}(\mathcal{O}_E))/\varpi$.

Case $H^2(G_K, U^{\text{ad}}(\mathbb{F})) = 0$. By Nakayama’s lemma, $H^2(G_K, U^{\text{ad}}(\mathcal{O}_E)) = 0$. By [Emerton and Gee 2023], there exists a perfect \mathcal{O}_E -complex $[C^0 \rightarrow C^1 \rightarrow C^2]$ concentrated in degrees $[0, 2]$ which computes $H^*(G_K, U^{\text{ad}}(\mathcal{O}_E))$. By the universal coefficient theorem, there exists a short exact sequence

$$0 \rightarrow H^1(C^\bullet) \otimes \mathbb{F} \rightarrow H^1(C^\bullet \otimes \mathbb{F}) \rightarrow \text{Tor}_1^{\mathcal{O}_E}(H^2(C^\bullet), \mathbb{F}) \rightarrow 0.$$

So $H^1(G_K, U^{\text{ad}}(\mathcal{O}_E)) \otimes_{\mathcal{O}_E} \mathbb{F} = H^1(G_K, U^{\text{ad}}(\mathbb{F}))$. We assume (i) and (ii) are false, and try to get a contradiction. The kernel of

$$H^1(G_K, U^{\text{ad}}(\mathcal{O}_E)) \otimes \mathbb{F} \times H^1(G_K, U^{\text{ad}}(\mathcal{O}_E)) \otimes \mathbb{F} \rightarrow H^2(G_K, Z(U)(\mathcal{O}_E)) \otimes \mathbb{F}$$

has dimension $h^1 := \dim_{\mathbb{F}} H^1(G_K, U^{\text{ad}}(\mathbb{F}))$. By the local Euler characteristic,

$$h^1 = \dim_E U^{\text{ad}}(E)[K : \mathbb{Q}_p] + \dim_{\mathbb{F}} H^0(G_K, U^{\text{ad}}(\mathbb{F})). \tag{3-2}$$

By Lemma 3.1.3, the kernel k_Z of

$$Z_{\text{LD}}^1(U^{\text{ad}}(\mathbb{F})) \times Z_{\text{LD}}^1(U^{\text{ad}}(\mathbb{F})) \rightarrow H^2(G_{K'}, Z(U)(\mathbb{F}))$$

has dimension at most $\dim_E U^{\text{ad}}(E)$. Since the cup product is trivial on $H^1(G_K, U^{\text{ad}}(\mathbb{F}))$, we have

$$\dim k_Z \geq \dim H^1(G_K, U^{\text{ad}}(\mathbb{F})) + \dim B_{\text{LD}}^1(U^{\text{ad}}(\mathbb{F})) = h^1 + \dim B_{\text{LD}}^1(U^{\text{ad}}(\mathbb{F})). \quad (3-3)$$

Combining (3-2) and (3-3), we have

$$\dim_E U^{\text{ad}}(E) \geq \dim_{\mathbb{F}} k_Z \geq \dim_E U^{\text{ad}}(E)[K : \mathbb{Q}_p] + \dim_{\mathbb{F}} H^0(G_K, U^{\text{ad}}(\mathbb{F})) + \dim B_{\text{LD}}^1(U^{\text{ad}}(\mathbb{F}))$$

So we conclude that

$$1 = [K : \mathbb{Q}_p], \quad 0 = H^0(G_K, U^{\text{ad}}(\mathbb{F})), \quad 0 = B_{\text{LD}}^1(U^{\text{ad}}(\mathbb{F})).$$

In particular, we have $H^0(G_{K'}, U^{\text{ad}}(\mathbb{F})) = U^{\text{ad}}(\mathbb{F})$, and the kernel of the cup product on $H^1(G_{K'}, U^{\text{ad}}(\mathbb{F}))$ has dimension exactly $\dim_E U^{\text{ad}}(E)$. However, by Example 3.2.3, the cup product on $H^1(G_{K'}, U^{\text{ad}}(\mathbb{F}))$ is nondegenerate by local Tate duality. \square

Theorem 3.3.1 is used in the following scenario.

Lemma 3.3.2. *Let L be a split reductive group over \mathbb{F} . Let $r : G_K \rightarrow L(\mathbb{F})$ be a Galois representation valued in L . Let r^{ss} be the semisimplification of r . Write $G_{K'}$ for the kernel of r^{ss} . Then the degree $[K' : K]$ divides $(q - 1)^r \#W_L$, where*

- r is the rank of L ,
- q is a power of p , and
- $\#W_L$ is the cardinality of the Weyl group of L .

Proof. By [Lin 2022], r^{ss} is tamely ramified and factors through the normalizer of a maximal torus of L (after possibly extending the base field). \square

In particular, if $L = G_2$ and $p > 3$, the kernel of r^{ss} defines a Galois extension K'/K of prime-to- p degree, and $r|_{G_{K'}}$ is Lyndon–Demushkin since it has trivial semisimplification.

4. Nonabelian obstruction theory via the Lyndon–Demushkin cocycle group with external Galois action

Let K/\mathbb{Q}_p be a p -adic field. Let E/\mathbb{Q}_p be a finite extension with ring of integers \mathcal{O}_E , residue field \mathbb{F} , and uniformizer ϖ .

Let L be a split reductive group over \mathcal{O}_E . Fix a Galois representation

$$r^\circ : G_K \rightarrow L(\mathcal{O}_E)$$

throughout this section.

Let U be a unipotent group over \mathcal{O}_E whose adjoint group is abelian. Let $Z(U)$ be the center of U . The adjoint group U^{ad} is defined to be $U/Z(U)$.

Fix a group scheme homomorphism $\phi : L \rightarrow \text{Aut}(U)$ throughout this section. In particular, there is a Galois action $\phi(r^\circ) : G_K \xrightarrow{r^\circ} L(\mathcal{O}_E) \xrightarrow{\phi(\mathcal{O}_E)} \text{Aut}(U)(\mathcal{O}_E)$. We will talk about nonabelian Galois cohomology $H^\bullet(G_K, U(\mathcal{O}_E))$ and $H^\bullet(G_K, U(\mathbb{F}))$ using this Galois action throughout this section.

Let K'/K be a prime-to- p , finite Galois extension of K containing the group of p -th root of unity, such that $r^\circ(G_{K'}) \subset L(\mathcal{O}_E)$ is a pro- p group. Write Δ for $\text{Gal}(K'/K)$. Set $\Gamma := G_K$, and $H := G_{K'}$.

4.1. Nonabelian inflation-restriction.

Nonabelian Galois cohomology. We recall a few facts about the nonabelian version of Galois cohomology. Let

$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$$

be a short exact sequence of groups with continuous Γ -action. If $A \rightarrow B$ is *central*, that is, A is contained in the center of B , then we have a long exact sequence of pointed sets (see [Serre 2002, Proposition 43, 5.7])

$$1 \rightarrow A^\Gamma \rightarrow B^\Gamma \rightarrow C^\Gamma \rightarrow H^1(\Gamma, A) \rightarrow H^1(\Gamma, B) \rightarrow H^1(\Gamma, C) \xrightarrow{\delta} H^2(\Gamma, A).$$

Let $H \subset \Gamma$ be a closed normal subgroup. Then there is an exact sequence (see [Serre 2002, 5.8])

$$1 \rightarrow H^1(\Gamma/H, A^H) \rightarrow H^1(\Gamma, A) \rightarrow H^1(H, A)^{\Gamma/H}. \tag{4-1}$$

If A is an abelian group, then the sequence above can be upgraded to the inflation-restriction exact sequence:

$$1 \rightarrow H^1(\Gamma/H, A^H) \rightarrow H^1(\Gamma, A) \rightarrow H^1(H, A)^{\Gamma/H} \rightarrow H^2(\Gamma, A^H).$$

Theorem 4.1.1 [Koch 2002, Theorem 3.15]. *Let Γ be a profinite group, H a normal subgroup of finite index, and A an (abelian) G -module whose elements have finite order coprime to $(\Gamma : H)$. Then*

$$H^n(\Gamma/H, A^H) = 0$$

for all $n \geq 1$, and the restriction

$$H^n(\Gamma, A) \rightarrow H^n(H, A)^{\Gamma/H}$$

is an isomorphism.

Let R be either \mathcal{O}_E or \mathbb{F} . For ease of notation, write U for $U(R)$ in this paragraph. The fact above implies the following diagram commutes, with exact columns:

$$\begin{array}{ccc} H^1(\Gamma, Z(U)) & \xrightarrow[\text{res}]{\cong} & H^1(H, Z(U))^\Delta \\ \downarrow & & \downarrow \\ H^1(\Gamma, U) & \xrightarrow[\text{res}]{} & H^1(H, U)^\Delta \\ \downarrow \alpha_1 & & \downarrow \alpha_2 \\ H^1(\Gamma, U^{\text{ad}}) & \xrightarrow[\text{res}]{\cong} & H^1(H, U^{\text{ad}})^\Delta \\ \downarrow \delta_1 & & \downarrow \delta_2 \\ H^2(\Gamma, Z(U)) & \xrightarrow{} & H^2(H, Z(U)) \end{array}$$

The injectivity of the second line follows from (4-1).

Proposition 4.1.2. *The restriction map of nonabelian 1-cocycles*

$$H^1(\Gamma, U) \rightarrow H^1(H, U)^\Delta$$

is a bijection.

Proof. This follows from diagram chasing: Let $[c] \in H^1(H, U)^\Delta$. Since $\delta_1(\text{res}^{-1}(\alpha_2([c])) = \delta_2(\alpha_2([c])) = 0$, there exists $[b] \in H^1(\Gamma, U)$ such that $\alpha_1(\text{res}([b])) = \alpha_2([c])$. Since $\alpha_2^{-1}(\alpha_2([c]))$ is a $H^1(H, Z(U))^\Delta$ -torsor, we can twist $[b]$ to make $\text{res}([b]) = [c]$. \square

4.1.3. Representation-theoretic interpretation of nonabelian 1-cocycles. Let \mathfrak{P} be a group which is a semidirect product $\mathfrak{L} \rtimes \mathfrak{U}$. Let $q_{\mathfrak{L}} : \mathfrak{P} \rightarrow \mathfrak{L}$ be the quotient map. Fix a section $\mathfrak{L} \rightarrow \mathfrak{P}$ of $q_{\mathfrak{L}}$, which allows us to identify (set-theoretically) \mathfrak{P} with $\mathfrak{U} \times \mathfrak{L}$, and write $q_{\mathfrak{U}} : \mathfrak{P} \rightarrow \mathfrak{U}$ be the projection map. For $g \in \mathfrak{P}$, write $g = g_{\mathfrak{U}}g_{\mathfrak{L}}$ such that $g_{\mathfrak{U}} \in \mathfrak{U} \times \{1\}$ and $g_{\mathfrak{L}} \in \{1\} \times \mathfrak{L}$. Let $\bar{\tau} : \Gamma \rightarrow \mathfrak{L}$ be a group homomorphism. Let $\tau : \Gamma \rightarrow \mathfrak{P}$ be a lifting of $\bar{\tau}$. Set $c := q_{\mathfrak{U}} \circ \tau : \Gamma \rightarrow \mathfrak{U}$. Then

$$\begin{aligned} c(gh) &= q_{\mathfrak{U}}(\tau(g)\tau(h)) = q_{\mathfrak{U}}(\tau(g)_{\mathfrak{U}}\tau(g)_{\mathfrak{L}}\tau(h)_{\mathfrak{U}}\tau(h)_{\mathfrak{L}}) \\ &= q_{\mathfrak{U}}(\tau(g)_{\mathfrak{U}}\tau(g)_{\mathfrak{L}}\tau(h)_{\mathfrak{U}}\tau(g)_{\mathfrak{L}}^{-1}\tau(gh)_{\mathfrak{L}}) = c(g)(\tau(g)_{\mathfrak{L}}c(h)\tau(g)_{\mathfrak{L}}^{-1}) \\ &=: c(g)(\tau(g)_{\mathfrak{L}} \cdot c(h)) \end{aligned}$$

is a (nonabelian) crossed homomorphism. Two liftings τ_1 and τ_2 are equivalent if there exists an element $n \in \mathfrak{U}$ such that $\tau_1 = n\tau_2n^{-1}$. So $H^1(\Gamma, \mathfrak{U})$ classifies liftings τ of $\bar{\tau}$ up to equivalence.

4.1.4. Lifting characteristic- p cocycles via inflation-restriction. Let $[\bar{c}] \in H^1(\Gamma, U(\mathbb{F}))$ be a characteristic- p cocycle. Assume the restriction $[\bar{c}|_H] \in H^1(H, U(\mathbb{F}))$ has a characteristic-0 lift $[c_h] \in H^1(H, U(\mathcal{O}_E))$. We want to build a lift $[c] \in H^1(\Gamma, U(\mathcal{O}_E))$ of $[\bar{c}]$ using $[c_h]$.

Note that when U is an abelian group, this can be easily achieved by taking the average

$$[c] := \frac{1}{\#\Delta} \sum_{g \in \Delta} g \cdot [c_h].$$

Here we identify $H^1(\Gamma, U(\mathcal{O}_E))$ with a subset of $H^1(H, U(\mathcal{O}_E))$ via Proposition 4.1.2.

Such a trick does not work anymore when U is nonabelian. Nonetheless, we have the following:

Lemma 4.1.5. *If there exists $[c_h] \in H^1(H, U(\mathcal{O}_E))$ and $[d] \in H^1(\Gamma, U^{\text{ad}}(\mathcal{O}_E))$ such that $\alpha_2([c_h]) = \text{res}([d])$ and $[c_h] \bmod \varpi = [\bar{c}|_H]$, then there exists $[c] \in H^1(\Gamma, U(\mathcal{O}_E))$ which is a lifting of $[\bar{c}]$.*

$$\begin{array}{ccc} H^1(\Gamma, Z(U)(\mathcal{O}_E)) & \xrightarrow{\text{res}} & H^1(H, Z(U)(\mathcal{O}_E)) \\ \downarrow & & \downarrow \\ H^1(\Gamma, U(\mathcal{O}_E)) & \xrightarrow{\text{res}} & H^1(H, U(\mathcal{O}_E)) \ni [c_h] \\ \downarrow \alpha_1 & & \downarrow \alpha_2 \\ [d] \in H^1(\Gamma, U^{\text{ad}}(\mathcal{O}_E)) & \xrightarrow{\text{res}} & H^1(H, U^{\text{ad}}(\mathcal{O}_E)) \\ \downarrow \delta_1 & & \downarrow \delta_2 \\ H^2(\Gamma, Z(U)(\mathcal{O}_E)) & \xrightarrow{\text{res}} & H^2(H, Z(U)(\mathcal{O}_E)) \end{array}$$

Proof. Since

$$\delta_1([d]) = \delta_2(\alpha_2([c_h])) = 0,$$

we have $[d] = \alpha_1([c'])$ for some $[c'] \in H^1(\Gamma, U(\mathcal{O}_E))$. Since $\text{res}([c'])$ and $[c_h] \in H^1(H, U(\mathcal{O}_E))$ have the same image in $H^1(H, U^{\text{ad}}(\mathcal{O}_E))$ (via α_2), it makes sense to talk about the difference $\text{res}([c']) - [c_h] \in H^1(H, Z(U)(\mathcal{O}_E))$.¹ Consider the diagram

$$\begin{array}{ccccc} H^1(\Gamma, Z(U)(\mathcal{O}_E)) & \longrightarrow & H^1(\Gamma, Z(U)(\mathbb{F})) & \xrightarrow{\delta} & H^2(\Gamma, Z(U)(\mathcal{O}_E)) \\ \downarrow \text{res} & & \downarrow \text{res} & & \downarrow \\ H^1(H, Z(U)(\mathcal{O}_E)) & \longrightarrow & H^1(H, Z(U)(\mathbb{F})) & \xrightarrow{\delta} & H^2(H, Z(U)(\mathcal{O}_E)) \end{array}$$

Let $[\bar{c}'] \in H^1(\Gamma, Z(U)(\mathbb{F}))$ be the reduction mod ϖ of $[c']$. Since $\text{res}([\bar{c}'] - [\bar{c}_h])$ has a lift,

$$\delta(\text{res}([\bar{c}'] - [\bar{c}_h])) = 0 \in H^2(H, Z(U)(\mathbb{F}))$$

by the exactness of the second row of the diagram above. Therefore

$$\delta([\bar{c}'] - [\bar{c}]) = \delta(\text{res}([\bar{c}'] - [\bar{c}])) = \delta(\text{res}([\bar{c}'] - [\bar{c}_h])) = 0$$

and $[\bar{c}'] - [\bar{c}] \in H^1(\Gamma, Z(U)(\mathbb{F}))$ has a characteristic-0 lift $[x]$, and $[c] := [c'] - [x]$ is a lift of $[\bar{c}]$. \square

The purpose of the whole Section 4 is to prove Theorem 4.3.2, which extends the above lemma.

4.2. External Galois action on the Lyndon–Demushkin cocycle group. The earlier subsection shows there is an identification

$$H^1(\Gamma, U(\mathcal{O}_E)) \cong H^1(H, U(\mathcal{O}_E))^\Delta.$$

The goal of this subsection is to upgrade this identification to the cochain level.

Since the Galois action

$$\phi(r^\circ)|_{G_{K'}} : G_{K'} \rightarrow U(\mathcal{O}_E)$$

is Lyndon–Demushkin, we have a Lyndon–Demushkin complex $C_{\text{LD}}^\bullet(U(\mathcal{O}_E))$ computing $H^\bullet(H, U(\mathcal{O}_E))$. Recall from Section 2.3.2 that a 1-cochain $c \in C_{\text{LD}}^1(U(\mathcal{O}_E))$ is the same as a function

$$c : \langle x_0, \dots, x_{n+1} \rangle \rightarrow (\text{Lie } U)(\mathcal{O}_E)$$

such that

$$c(gh) = c(g) + g \cdot c(h) + \frac{1}{2}[c(g), g \cdot c(h)]$$

for all g, h ; or, equivalently, a function

$$c : \langle x_0, \dots, x_{n+1} \rangle \rightarrow U(\mathcal{O}_E)$$

such that

$$c(gh) = c(g)(g \cdot c(h))$$

for all g, h .

¹ $H^1(H, U(\mathcal{O}_E))$ is a $H^1(H, Z(U)(\mathcal{O}_E))$ -principle homogeneous space.

A cochain $c : \langle x_0, \dots, x_{n+1} \rangle \rightarrow U(\mathcal{O}_E)$ lies in $Z_{\text{LD}}^1(U(\mathcal{O}_E))$ if and only if it factors through the (discrete) Demushkin group $\langle x_0, \dots, x_{n+1} | R \rangle$ (see the proof of Proposition 2.3.6).

Let $c \in Z_{\text{LD}}^1(\mathcal{O}_E)$, regarded as a function $\langle x_0, \dots, x_{n+1} | R \rangle \rightarrow U(\mathcal{O}_E)$. Since $U(\mathcal{O}_E)$ is a pro- p group, the crossed homomorphism necessarily factors through the pro- p completion, that is, we have a commutative diagram

$$\begin{array}{ccc}
 \langle x_0, \dots, x_{n+1} | R \rangle & \xrightarrow{c} & U(\mathcal{O}_E) \\
 \downarrow \pi & \nearrow \hat{c} & \\
 G_{K'}(p) \cong \langle x_0, \dots, x_{n+1} | R \rangle^p & &
 \end{array}$$

Since we have identified the pro- p quotient of $G_{K'}$ with the pro- p completion of $\langle x_0, \dots, x_{n+1} | R \rangle$, we can define, for each $g \in G_K$, an automorphism α_g of $Z_{\text{LD}}^1(U(\mathcal{O}_E))$ via

$$\alpha_g(c) := (h \mapsto g \cdot \hat{c}(g^{-1}\pi(h)g)).$$

So we defined an action of G_K on $Z_{\text{LD}}^1(U(\mathcal{O}_E))$.

For ease of notation, write $g \cdot c$ for $\alpha_g(c)$. Note that $(g \cdot c)(h) = (\alpha_g(c))(h)$ is different from $g \cdot c(h)$. We apologize for the confusing notation.

Remark 4.2.1. We don't know whether or not we can define a G_K -action on the whole cochain group $C_{\text{LD}}^1(U(\mathcal{O}_E))$. It seems to involve some subtle combinatorial group theory.

Digression. It is curious to know if the cup product

$$\cup : Z_{\text{LD}}^1(U^{\text{ad}}(\mathcal{O}_E)) \times Z_{\text{LD}}^1(U^{\text{ad}}(\mathcal{O}_E)) \rightarrow C_{\text{LD}}^2(Z(U(\mathcal{O}_E)))$$

is compatible with the G_K -action.

This answer would be affirmative if, for example, for each $g \in G_K$, the conjugation by g ,

$$\phi_g : G_{K'} \rightarrow G_{K'},$$

can be lifted to an automorphism of free pro- p groups on $(n+2)$ -generators,

$$\phi_g : \langle x_0, \dots, x_{n+1} \rangle \rightarrow \langle x_0, \dots, x_{n+1} \rangle.$$

This is closely related to the so-called *Dehn–Nielsen* theorem. Classically, Dehn–Nielsen is saying all automorphism of the fundamental group of the genus g closed surface M_g are induced by a homeomorphism. The algebraic version of Dehn–Nielsen can be formulated as, under the usual presentation of $F = \langle a_1, b_1, \dots, a_g, b_g \rangle \rightarrow \langle a_1, b_1, \dots, a_g, b_g | [a_1, b_1] \cdots [a_g, b_g] \rangle \cong \pi_1(M_g)$, all automorphism of $\pi_1(M_g)$ are induced from an automorphism of the free group F .

Conjecture (pro- p Dehn–Nielsen). *All automorphisms of the pro- p completion of $\langle x_0, \dots, x_{n+1} | R \rangle$ are induced by an automorphism of the pro- p completion of $\langle x_0, \dots, x_{n+1} \rangle$.*

4.3. Constructing nonabelian cocycles. Recall that $H^1(H, U^{\text{ad}})^{\Delta} = H^1(G_K, U^{\text{ad}})$, where $H = G_{K'}$ and K'/K is a normal extension of prime-to- p degree. Define

$$\begin{aligned} (Z_{\text{LD}}^1)^{\Delta} &:= \{x \in Z_{\text{LD}}^1 \mid \text{image of } x \text{ in } H^1 \text{ is contained in } (H^1)^{\Delta}\} \\ &= \{x \in Z_{\text{LD}}^1 \mid g \cdot x - x \in B_{\text{LD}}^1 \text{ for all } g \in G_K\}. \end{aligned}$$

Since $Z_{\text{LD}}^1(U^{\text{ad}}(\mathcal{O}_E))^{\Delta}$ is a submodule of a finite flat \mathcal{O}_E -module, it is finite \mathcal{O}_E -flat.

We keep all notation from the previous subsections.

Assume $Z(U)(\mathcal{O}_E) = \mathcal{O}_E$ from now on. We fix some notation. The quotient $U \rightarrow U/Z(U) = U^{\text{ad}}$ induces maps $\text{ad} : Z_{\text{LD}}^1(U(\mathcal{O}_E)) \rightarrow Z_{\text{LD}}^1(U^{\text{ad}}(\mathcal{O}_E))$.

Lemma 4.3.1. *Assume that $p \neq 2$ and that the cup product*

$$\cup : H^1(G_K, U^{\text{ad}}(\mathcal{O}_E)) \otimes \mathbb{F} \times H^1(G_K, U^{\text{ad}}(\mathcal{O}_E)) \otimes \mathbb{F} \rightarrow H^2(G_K, Z(U)(\mathbb{F})) \quad (4-2)$$

is nontrivial.

Let $(\bar{c}, \bar{f}) \in Z_{\text{LD}}^1(U(\mathbb{F}))$ (using Lemma 2.3.8). Assume $\bar{c} \in Z_{\text{LD}}^1(U^{\text{ad}}(\mathbb{F}))^{\Delta}$. If \bar{c} admits a characteristic-0 lift $c' \in Z_{\text{LD}}^1(U^{\text{ad}}(\mathcal{O}_E))$, then (\bar{c}, \bar{f}) admits a lift $(c, f) \in Z_{\text{LD}}^1(U(\bar{\mathbb{Z}}_p))$ such that $c \in Z_{\text{LD}}^1(U^{\text{ad}}(\bar{\mathbb{Z}}_p))^{\Delta}$.

Proof. Pick an arbitrary lift $f \in C_{\text{LD}}^1(Z(U)(\mathcal{O}_E))$ of \bar{f} . Choose a system of representatives $\{g_i\} \subset G_K$ of Δ . By replacing c' by the Δ -average $\frac{1}{\#\Delta} \sum g_i \cdot c' +$ some coboundary (which is also a lift of $[\bar{c}]$), we assume $c' \in Z_{\text{LD}}^1(U^{\text{ad}}(\bar{\mathbb{Z}}_p))^{\Delta}$.

Let $\lambda \in \bar{\mathbb{Z}}_p^{\times}$ be a scalar.

Since the symmetric bilinear pairing (4-2) is nontrivial, there exists $y \in Z_{\text{LD}}^1(U^{\text{ad}}(\mathcal{O}_E))^{\Delta}$ such that $y \cup y \neq 0 \pmod{\varpi}$. Consider

$$(c' + \lambda y) \cup (c' + \lambda y) + d^2(f) = c' \cup c' + d^2(f) + 2\lambda c' \cup y + \lambda^2 y \cup y \in C^2(Z(U)(\mathcal{O}_E)) \cong \mathcal{O}_E,$$

which is a degree two polynomial in λ whose Newton polygon has vertices $(0, +)$, $(1, + \text{ or } 0)$, $(2, 0)$ and thus has at least one solution λ_0 with positive p -adic valuation; here “+” means a positive number. Set $(c, f) := (c' + \lambda_0 y, f)$.

We have $(c, f) \in Z_{\text{LD}}^1(U(\bar{\mathbb{Z}}_p))$ by Lemma 2.3.8 and $c \in Z_{\text{LD}}^1(U^{\text{ad}}(\bar{\mathbb{Z}}_p))^{\Delta}$. □

Theorem 4.3.2. *Assume that $p \neq 2$ and that the cup product*

$$\cup : H^1(G_K, U^{\text{ad}}(\mathcal{O}_E)) \otimes \mathbb{F} \times H^1(G_K, U^{\text{ad}}(\mathcal{O}_E)) \otimes \mathbb{F} \rightarrow H^2(G_K, Z(U)(\mathbb{F}))$$

is nontrivial.

Let $[(\bar{c}, \bar{f})] \in H^1(G_K, U(\mathbb{F}))$ be a characteristic- p cocycle. If $[\bar{c}]_{G_{K'}} \in H^1(G_{K'}, U^{\text{ad}}(\mathbb{F}))$ admits a characteristic-0 lift in $H^1(G_{K'}, U^{\text{ad}}(\bar{\mathbb{Z}}_p))$, then $[(\bar{c}, \bar{f})]$ admits a characteristic-0 lift $[(c, f)] \in H^1(G_K, U(\bar{\mathbb{Z}}_p))$.

Proof. We choose a cocycle $(\bar{c}, \bar{f}) \in Z_{\text{LD}}^1(U(\mathbb{F}))$ which defines the cohomology class $[(\bar{c}, \bar{f})]$. Clearly $\bar{c} \in Z_{\text{LD}}^1(U^{\text{ad}}(\mathbb{F}))^{\Delta}$. Say $[d] \in H^1(G_{K'}, U^{\text{ad}}(\bar{\mathbb{Z}}_p))$ is a lift of $[\bar{c}]$, which is defined by $d \in Z_{\text{LD}}^1(U^{\text{ad}}(\bar{\mathbb{Z}}_p))$. Write \bar{d} for the image of d in $Z_{\text{LD}}^1(U^{\text{ad}}(\bar{\mathbb{F}}_p))$. By changing d by a coboundary, we can assume $\bar{d} = \bar{c}$.

Lemma 4.3.1 produces $(c, f) \in Z_{\text{LD}}^1(U(\bar{\mathbb{Z}}_p))$ such that $c \in Z_{\text{LD}}^1(U^{\text{ad}}(\bar{\mathbb{Z}}_p))^\Delta$. Now the theorem follows from Lemma 4.1.5. \square

Theorem 4.3.2 is saying that when U is a unipotent group of class 2 with one-dimensional center, there exists a short exact sequence of pointed sets

$$H^1(G_K, U(\bar{\mathbb{Z}}_p)) \rightarrow H^1(G_K, U(\bar{\mathbb{F}}_p)) \xrightarrow{\delta} H^2(G_{K'}, U^{\text{ad}}(\bar{\mathbb{Z}}_p))$$

under technical assumptions.

Combining Theorems 4.3.2 and 3.3.1, we have very nice obstruction theory for lifting mod ϖ cohomology classes in the mildly regular case.

Theorem 4.3.3. *Assume $p \neq 2$ and $Z(U)(\mathcal{O}_E) = \mathcal{O}_E$. Let $r : G_K \rightarrow L(\mathcal{O}_E)$ be a fixed continuous group homomorphism and equip $U(\bar{\mathbb{Z}}_p)$ with the G_K -action $G_K \xrightarrow{r} L(\bar{\mathbb{Z}}_p) \rightarrow \text{Aut}(U(\bar{\mathbb{Z}}_p))$. Let K'/K be a finite Galois extension of prime-to- p degree such that $r|_{G_{K'}}$ is Lyndon–Demushkin and mildly regular.*

There is a short exact sequence of pointed sets

$$H^1(G_K, U(\bar{\mathbb{Z}}_p)) \rightarrow H^1(G_K, U(\bar{\mathbb{F}}_p)) \xrightarrow{\delta} H^2(G_{K'}, U^{\text{ad}}(\bar{\mathbb{Z}}_p)),$$

where δ has a factorization $H^1(G_K, U(\bar{\mathbb{F}}_p)) \xrightarrow{z} H^1(G_K, U^{\text{ad}}(\bar{\mathbb{F}}_p)) \rightarrow H^2(G_{K'}, U^{\text{ad}}(\bar{\mathbb{Z}}_p))$.

Proof. Write Δ for $G_K/G_{K'}$. By the moreover part of Theorem 3.3.1, there are two cases to consider.

Case I: the cup product (4-2), $H^1(G_K, U^{\text{ad}}(\bar{\mathbb{Z}}_p)) \otimes \mathbb{F} \times H^1(G_K, U^{\text{ad}}(\bar{\mathbb{Z}}_p)) \otimes \mathbb{F} \rightarrow H^2(G_K, Z(U)(\bar{\mathbb{Z}}_p)) \otimes \mathbb{F}$, is nontrivial. This is a corollary of Theorem 4.3.2.

Case II: $H^2(G_K, Z(U)(\mathbb{F})) = 0$. The short exact sequence $0 \rightarrow Z(U)(\mathcal{O}_E) \rightarrow Z(U)(\mathcal{O}_E) \rightarrow Z(U)(\mathbb{F}) \rightarrow 0$ induces a long exact sequence $H^2(G_K, Z(U)(\mathcal{O}_E)) \rightarrow H^2(G_K, Z(U)(\mathbb{F})) \rightarrow 0$. By Nakayama's lemma, $H^2(G_K, Z(U)(\mathcal{O}_E)) = 0$, and thus $H^2(G_K, Z(U)(\bar{\mathbb{Z}}_p)) = 0$ by flat base change.

Let $[(\bar{c}, \bar{f})] \in H^1(G_K, U(\bar{\mathbb{F}}_p))$ be a cohomology class defined by $(\bar{c}, \bar{f}) \in Z_{\text{LD}}^1(U(\bar{\mathbb{F}}_p))$.

Set $\delta : H^1(G_K, U(\bar{\mathbb{F}}_p)) \rightarrow H^2(G_{K'}, U^{\text{ad}}(\bar{\mathbb{Z}}_p))$ to be the composite

$$H^1(G_K, U(\bar{\mathbb{F}}_p)) \xrightarrow{[(\bar{c}, \bar{f})] \mapsto [\bar{c}]} H^1(G_K, U^{\text{ad}}(\bar{\mathbb{F}}_p)) \rightarrow H^2(G_{K'}, U^{\text{ad}}(\bar{\mathbb{Z}}_p)).$$

If $\delta([(c, f)]) = 0$, then there exists a lift $c \in Z_{\text{LD}}^1(U^{\text{ad}}(\bar{\mathbb{Z}}_p))$ of \bar{c} . By replacing c by the Δ -average of c , we assume $c \in Z_{\text{LD}}^1(U^{\text{ad}}(\bar{\mathbb{Z}}_p))^\Delta$. Since $H^2(G_K, Z(U)(\bar{\mathbb{Z}}_p)) = 0$, $[c \cup c] = 0$ and thus there exists $g \in C_{\text{LD}}^1(Z(U)(\bar{\mathbb{Z}}_p))^\Delta$ such that $c \cup c = -d^2(g)$. Write \bar{g} for the image of g in $C_{\text{LD}}^1(Z(U)(\bar{\mathbb{F}}_p))$. We have $\bar{g} - \bar{f} \in Z_{\text{LD}}^1(Z(U)(\bar{\mathbb{F}}_p))^\Delta$. Since $H^2(G_K, Z(U)(\bar{\mathbb{Z}}_p)) = 0$, there exists a lift $h \in Z_{\text{LD}}^1(Z(U)(\bar{\mathbb{Z}}_p))^\Delta$ of $\bar{f} - \bar{g}$. It is clear that $[(c, g + h)] \in H^1(G_K, U(\bar{\mathbb{Z}}_p))$ is a lift of $[(\bar{c}, \bar{f})]$. \square

Corollary 4.3.4. *Assume $p \neq 2$ and $Z(U)(\mathcal{O}_E) = \mathcal{O}_E$. Let $r : G_K \rightarrow L(\mathcal{O}_E)$ be a continuous group homomorphism.*

If there exists a finite Galois extension K'/K of prime-to- p degree such that $r|_{G_{K'}}$ is Lyndon–Demushkin and mildly regular, then there is a short exact sequence of pointed sets

$$H^1(G_K, U(\overline{\mathbb{Z}}_p)) \rightarrow H^1(G_K, U(\overline{\mathbb{F}}_p)) \xrightarrow{\delta} H^2(G_K, U^{\text{ad}}(\overline{\mathbb{Z}}_p))$$

where δ has a factorization $H^1(G_K, U(\overline{\mathbb{F}}_p)) \xrightarrow{z} H^1(G_K, U^{\text{ad}}(\overline{\mathbb{F}}_p)) \rightarrow H^2(G_K, U^{\text{ad}}(\overline{\mathbb{Z}}_p))$.

Proof. This is an immediate consequence of Theorem 4.3.3. □

5. The machinery for lifting nonabelian cocycles

Let K/\mathbb{Q}_p be a p -adic field. Let E/\mathbb{Q}_p be the coefficient field with ring of integers \mathcal{O}_E , residue field \mathbb{F} and uniformizer ϖ .

5.0.1. Emerton–Gee stacks. Let H be a connected reductive group over K which splits over a tame extension K_H/K . Denote by ${}^L H$ the Langlands dual group $\widehat{H} \rtimes \text{Gal}(K_H/K)$ where \widehat{H} is the split connected reductive group over \mathbb{Z} whose root datum is dual to that of H . The reduced Emerton–Gee stack $\mathcal{X}_{L_H, \text{red}}$ is a reduced algebraic stack defined over \mathbb{F}_p (see [Lin 2023b, Theorem 1]).

Moreover, it is proved in many cases that $\mathcal{X}_{K, {}^L H, \text{red}}$ is equidimensional of dimension $[K:\mathbb{Q}_p] \dim \widehat{H}/B_{\widehat{H}}$, where $B_{\widehat{H}}$ is a Borel of \widehat{H} (see [Lin 2023b]).

5.0.2. Potentially semistable lifting rings. Write $L := {}^L H$ for simplicity. Let $\bar{r} : G_K \rightarrow L(\mathbb{F})$ be a mod ϖ Langlands parameter, that is, a continuous group homomorphism such that the composite $G_K \rightarrow {}^L H(\overline{\mathbb{F}}_p) \rightarrow \text{Gal}(K_H/K)$ is the canonical quotient map. Let $\underline{\lambda}$ be a Hodge type and let τ be an inertial Galois type (see [Lin 2023c] for the definitions). The potentially semistable deformation ring $R_{\bar{r}}^{\underline{\lambda}, \tau, \mathcal{O}}$ of p -adic Hodge type $\underline{\lambda}$ is constructed in [Bellovin and Gee 2019, Theorem 3.3.8]. It is an \mathcal{O} -flat quotient of the universal lifting ring, and is equidimensional of dimension $(1 + \dim \widehat{H} + [K:\mathbb{Q}_p] \dim \widehat{H}/B_{\widehat{H}})$ when $\underline{\lambda}$ is a regular Hodge type.

5.1. A geometric argument of Emerton–Gee.

Definition 5.1.1. Let \mathcal{F} be a coherent sheaf over a scheme $X = \text{Spec } R$. We say \mathcal{F} is *sufficiently generically regular* (SGR) if for each $s \geq 1$, the locus

$$X_s := \{x \in \text{Spec } R \mid \dim \kappa(x) \otimes_R \mathcal{F} \geq s\}$$

has codimension $\geq s + 1$ in $\text{Spec } R$.

Theorem 5.1.2. Let $X = \text{Spec } R$ with R a complete reduced, \mathbb{Z}_p -flat local ring that is equidimensional of dimension $(1 + \dim L + \dim \mathcal{X}_{L, \text{red}})$. Let $r^{\text{univ}} : G_K \rightarrow L(R)$ be a family of L -parameters on X . Assume $X[1/p] \neq \emptyset$. Let $F : L \rightarrow \text{GL}(V)$ be an algebraic representation where V is a vector space scheme over \mathcal{O}_E .

Assume $H^2(G_K, F(r^{\text{univ}}))$ is SGR over X and is supported on $X \otimes_{\mathbb{Z}_p} \mathbb{F}_p$. Given any $[\bar{c}] \in H^1(G_K, F(\bar{r}))$, there exists a $\overline{\mathbb{Z}}_p$ -point of X giving rise to a Galois representation $r^\circ : G_K \rightarrow L(\overline{\mathbb{Z}}_p)$, such that the 1-cocycle $[\bar{c}]$ admits a lift $[c] \in H^1(G_K, F(r^\circ))$.

Remark 5.1.3. Since $H^2(G_K, -)$ (abelian coefficients) is the highest degree cohomology ($H^i(G_K, -) = 0$ for $i > 2$), $H^2(G_K, -)$ commutes with base change. Thus we may view $H^2(G_K, F(r^{\text{univ}}))$ as a coherent sheaf over X .

The proof is almost identical to that of [Emerton and Gee 2023, Theorem 6.3.2].

We would like to explain the main ideas behind the proof, and why we need the sufficiently generically regular condition.

We have a complex of finitely generated projective modules over R concentrated on degree $[0, 2]$

$$C^0 \rightarrow C^1 \xrightarrow{d} C^2$$

which computes the Galois cohomology $H^*(G_K, F(r^{\text{univ}}))$. Let $Z^1 := \ker(d)$ and $B^2 := \text{Im}(d)$. A mod ϖ cocycle $[\bar{c}]$ is represented by an element \bar{c} in the kernel of $C^1/\varpi \rightarrow C^2/\varpi$. We fix an arbitrary lift $\tilde{c} \in C^1$ of \bar{c} . We can do a formal blowup $\text{Spec } \tilde{R} \rightarrow \text{Spec } R$, so that the pullback of B^2 on $\text{Spec } \tilde{R}$ is a locally free sheaf. To make the exposition short, we simply assume B^2 is locally free over $\text{Spec } R$, but we should not think of $\text{Spec } R$ as a local ring anymore, because after formal blow-up, there are more closed points in the special fiber. Now we have a sequence of locally free sheaves of modules

$$C^1 \rightarrow B^2 \rightarrow C^2.$$

The key here is we want to regard this as a sequence of vector bundles instead of sheaves of modules. Write $\mathcal{V}(\mathcal{F})$ for $\underline{\text{Spec}}(\text{Sym } \mathcal{F}^\vee)$, the vector bundle associated to the coherent sheaf \mathcal{F} . So we have a sequence of scheme morphisms

$$\begin{array}{ccccc}
 & & d & & \\
 & \nearrow & & \searrow & \\
 \mathcal{V}(C^1) & \xrightarrow{f} & \mathcal{V}(B^2) & \longrightarrow & \mathcal{V}(C^2) \\
 & \nwarrow & \uparrow f \circ s & \nearrow d \circ s & \\
 & & \text{Spec } R & &
 \end{array}$$

The element \tilde{c} of C^1 defines a section $s : \text{Spec } R \rightarrow \mathcal{V}(C^1)$ such that the section $d \circ s : \text{Spec } R \rightarrow \mathcal{V}(C^2)$ intersects with the identity section $e_{\mathcal{V}(C^2)} : \text{Spec } R \rightarrow \mathcal{V}(C^2)$.

It turns out $\tilde{c} \in \ker(C^1/\varpi \rightarrow C^2/\varpi)$ admits a lift in Z^1 , as long as the section $f \circ s$ intersects with the identity section $e_{\mathcal{V}(B^2)}$ of $\mathcal{V}(B^2)$. The intersection $(d \circ s) \cap e_{\mathcal{V}(C^2)}$ should occur above a codimension 1 locus of $\text{Spec } R$. If the support of $H^2 = C^2/B^2$ is small (that is, has big codimension), then the intersection should happen at some point $x \in \text{Spec } R$ outside of the support of H^2 , and we are done.

We include a formal proof here, as suggested by a referee.

Proof. We follow the notation of [Emerton and Gee 2023, Theorem 6.3.2] closely. The Herr complex C^\bullet (supported in degrees $[0, 2]$) computes $H^*(G_K, F(r^{\text{univ}}))$. Since B^2 equals to C^2 over the generic fiber $U = X[1/p]$, by [Stacks, Tag 0815], there exists a U -admissible blowup $\pi : \tilde{X} \rightarrow X$ such that π^*B^2 is locally free. Let \tilde{C}^\bullet be the pullback complex $\pi^*(C^\bullet)$. The corresponding 2-coboundaries $\tilde{B}^2 = \pi^*B^2$ (since it is the highest degree coboundary). Thus the 1-cocycles \tilde{Z}^1 is locally free and $[\tilde{C}^0 \rightarrow \tilde{Z}^1]$ is a good complex.

Lifting the class $[\bar{c}]$ to an element of $\kappa \otimes C^1$ (where κ is the residue field of R) and then to an element c of C^1 . c can be thought of as a homomorphism $R \rightarrow C^1$ whose image under the coboundary lies in $m_R C^2$. The composite $b : R \xrightarrow{c} C^1 \rightarrow B^2$ pulls back to a section $\tilde{b} : \mathcal{O}_{\tilde{X}} \rightarrow \tilde{B}^2$. By [Emerton and Gee 2023, Lemma 6.2.7] and the SGR property, \tilde{b} has nonempty zero locus, which contain a point \tilde{x} lying over the closed point $x \in X$. The section c pulls back to a section $\tilde{c} : \mathcal{O}_{\tilde{X}} \rightarrow \tilde{C}^1$, whose valued at the point \tilde{x} lies in the fiber of \tilde{Z}^1 . In other words, the fiber of \tilde{c} at \tilde{x} defines a 1-cocycle in the complex $\kappa(\tilde{x}) \otimes [\tilde{C}^0 \rightarrow \tilde{Z}^1]$, giving rise to a class $\bar{e} \in H^1(\kappa(\tilde{x}) \otimes [\tilde{C}^0 \rightarrow \tilde{Z}^1])$ lifting the original class $[\bar{c}]$.

Since \tilde{X} is \mathbb{Z}_p -flat, there exists a morphism $\tilde{f} : \text{Spec } \bar{\mathbb{Z}}_p \rightarrow \tilde{X}$ lifting \tilde{x} . The composite $f : \text{Spec } \bar{\mathbb{Z}}_p \xrightarrow{\tilde{f}} \tilde{X} \rightarrow X$ lifts the closed point $x \in X$, and determines an L -parameter $r^\circ : G_K \rightarrow L(\bar{\mathbb{Z}}_p)$. Since $H^2(\tilde{C}^\bullet)$ is the kernel of the homomorphism of locally free sheaves $\tilde{B}^2 \hookrightarrow \tilde{C}^2$ and is torsion, by [Emerton and Gee 2023, Lemma 6.2.1] there is an effective Cartier divisor D contained in the special fiber of \tilde{X} with the property that for any morphism to \tilde{X} that meets D properly, the higher derived pullbacks of $H^2(\tilde{C}^\bullet)$ under this morphism vanish. Since \tilde{f} meets the special fiber of \tilde{X} properly and thus meets D properly, $L_i \tilde{f}^* H^2(\tilde{C}^\bullet) = 0$ for $i > 0$. Thus

$$H^1(G_K, F(r^\circ)) = H^1(\tilde{f}^* \tilde{C}^\bullet) = \tilde{f}^* H^1(\tilde{C}^\bullet) = H^1(\tilde{f}^* [\tilde{C}^0 \rightarrow \tilde{Z}^1]).$$

(See the last two paragraphs of the proof [Emerton and Gee 2023, Theorem 6.3.2] for explanations). Choose a class $e \in H^1(\tilde{f}^* [\tilde{C}^0 \rightarrow \tilde{Z}^1])$ lifting \bar{e} , which corresponds to a 1-cocycle c lifting \bar{e} by the identifications above. □

5.2. A nonabelian lifting theorem.

Theorem 5.2.1. *Let U be a unipotent linear algebraic group of class 2 whose center is isomorphic to \mathbb{G}_a . Write $Z(U)$ for the center of U and U^{ad} for $U/Z(U)$. Fix an algebraic group homomorphism $\phi : L \rightarrow \text{Aut}(U)$ with graded pieces $\phi^{\text{ad}} : L \rightarrow \text{GL}(U^{\text{ad}})$ and $\phi^z : L \rightarrow \text{GL}(Z(U))$.*

Fix a mod ϖ representation $\bar{r} : G_K \rightarrow L(\mathbb{F})$. Let $[\bar{c}] \in H^1(G_K, U(\mathbb{F}))$ be a characteristic- p cocycle.

Let $\text{Spec } R$ be an irreducible component of a crystalline lifting ring of \bar{r} . Assume

- (1) $H^2(G_K, \phi^{\text{ad}}(r^{\text{univ}}))$ is SGR and is supported on the special fiber of $\text{Spec } R$;
- (2) $p \neq 2$;
- (3) *there exists a finite Galois extension K'/K of prime-to- p degree such that $\phi(\bar{r})|_{G_{K'}}$ is Lyndon–Demushkin; and*
- (4) *there exists a $\bar{\mathbb{Z}}_p$ -point of $\text{Spec } R$ which is mildly regular when restricted to $G_{K'}$. (In particular, $\text{Spec } R[1/p] \neq \emptyset$.)*

Then there exists a $\bar{\mathbb{Z}}_p$ -point of $\text{Spec } R$ which gives rise to a Galois representation $r^\circ : G_K \rightarrow L(\bar{\mathbb{Z}}_p)$ such that if we endow $U(\bar{\mathbb{Z}}_p)$ with the G_K -action $G_K \xrightarrow{r^\circ} L(\bar{\mathbb{Z}}_p) \xrightarrow{\phi} \text{Aut}(U)(\bar{\mathbb{Z}}_p)$, the cocycle $[\bar{c}]$ has a characteristic-0 lift $[c] \in H^1(G_K, U(\bar{\mathbb{Z}}_p))$.

Proof. Take $F = \phi^{\text{ad}}$ in Theorem 5.1.2. The theorem follows from Corollary 4.3.4. □

We explain how the above theorem will be used. Let G be a connected reductive group over \mathcal{O}_E . Let $\bar{\rho} : G_K \rightarrow G(\mathbb{F})$ be a mod ϖ representation. Assume $\bar{\rho}$ factors through a parabolic $P \subset G$, with Levi decomposition $P = L \ltimes U$. Denote by $\phi : L \rightarrow \text{Aut}(U)$ the conjugation action. We assume U is unipotent of class 2, so U^{ad} is an abelian group. Write \bar{r} for the Levi factor of $\bar{\rho}$.

$$\begin{array}{ccc} & & P(\bar{\mathbb{F}}_p) \\ & \nearrow \bar{\rho} & \downarrow \\ G_K & \xrightarrow{\bar{r}} & L(\bar{\mathbb{F}}_p) \end{array}$$

Then $\bar{\rho}$ defines a cohomology class $[\bar{c}] \in H^1(G_K, \phi(\bar{r}))$, and the theorem above can be used to lift $[\bar{c}]$.

5.3. An unobstructed lifting theorem. The following result will be used in the proof of the main theorem.

Proposition 5.3.1. *Let V be a unipotent linear algebraic group such that $V(\bar{\mathbb{Z}}_p)$ is equipped with a continuous G_K -action. Let $[\bar{c}] \in H^1(G_K, V(\bar{\mathbb{F}}_p))$ be a characteristic- p cocycle. Let $Z(V)$ be the center of V , and write V^{ad} for $V/Z(V)$. The quotient $V \rightarrow V^{\text{ad}}$ induces a map $\text{ad} : H^1(G_K, V) \rightarrow H^1(G_K, V^{\text{ad}})$. Assume $H^2(G_K, Z(V)(\bar{\mathbb{F}}_p)) = 0$.*

If $\text{ad}([\bar{c}])$ admits a lift in $H^1(G_K, V^{\text{ad}}(\bar{\mathbb{Z}}_p))$, then $[\bar{c}]$ admits a lift in $H^1(G_K, V(\bar{\mathbb{Z}}_p))$.

Proof. By [Serre 2002, Proposition 43], since $Z(V)$ is a central normal subgroup of V , there exists a long exact sequence of pointed sets

$$\begin{array}{ccccc} H^1(G_K, V(\bar{\mathbb{Z}}_p)) & \xrightarrow{\text{ad}} & H^1(G_K, V^{\text{ad}}(\bar{\mathbb{Z}}_p)) & \xrightarrow{\delta} & H^2(G_K, Z(V)(\bar{\mathbb{Z}}_p)) \\ \downarrow & & \downarrow & & \downarrow \\ H^1(G_K, V(\bar{\mathbb{F}}_p)) & \xrightarrow{\text{ad}} & H^1(G_K, V^{\text{ad}}(\bar{\mathbb{F}}_p)) & \longrightarrow & H^2(G_K, Z(V)(\bar{\mathbb{F}}_p)) \end{array}$$

By Nakayama’s lemma, we have $H^2(G_K, Z(V)(\bar{\mathbb{Z}}_p)) = 0$. In particular, there exists $[c'] \in H^1(G_K, V(\bar{\mathbb{Z}}_p))$ such that $\text{ad}([\bar{c}]) = \text{ad}([c']) \bmod \varpi$. Write $[\bar{c}']$ for $[c'] \bmod \varpi$. Say $[\bar{c}] = [\bar{c}'] + [\bar{f}]$ for some $[\bar{f}] \in H^1(G_K, Z(V)(\bar{\mathbb{F}}_p))$ (recall that $H^1(G_K, V)$ is a $H^1(G_K, Z(V))$ -torsor). Since $H^1(G_K, Z(V)(\bar{\mathbb{Z}}_p)) = 0$, there exists a lift $[f]$ of \bar{f} . The cocycle $[c] := [c'] + [f]$ is a lift of $[\bar{c}]$. \square

6. Codimension estimates of loci cut out by H^2

Assume $p > 3$. Let K/\mathbb{Q}_p be a finite extension. Let E/\mathbb{Q}_p be a finite extension with ring of integers \mathcal{O}_E , uniformizer ϖ , and residue field \mathbb{F} .

6.1. The Emerton–Gee stack. We follow the notation of [Emerton and Gee 2023]. For each $d > 0$, Emerton and Gee [2023] constructed the moduli stack $\mathcal{X}_d = \mathcal{X}_{K,d}$ of projective étale (ϕ, Γ_K) -modules of rank d , which is a finite-type algebraic stack over \mathbb{F} .

We prove a mild generalization of [Emerton and Gee 2023, Proposition 5.4.4(1)].

Let T be a reduced finite-type $\overline{\mathbb{F}}_p$ -scheme. Let $f : T \rightarrow (\mathcal{X}_{a,\text{red}})_{\overline{\mathbb{F}}_p} \times (\mathcal{X}_{d,\text{red}})_{\overline{\mathbb{F}}_p}$ be a morphism. There is a morphism

$$\eta : (\mathcal{X}_{a,\text{red}})_{\overline{\mathbb{F}}_p} \times (\mathcal{X}_{d,\text{red}})_{\overline{\mathbb{F}}_p} \rightarrow (\mathcal{X}_{ad,\text{red}})_{\overline{\mathbb{F}}_p}$$

sending a pair of (ϕ, Γ) -modules M, N to their hom module $\text{Hom}_{\phi, \Gamma}(M, N)$, by the moduli interpretation. The morphism $\eta(f)$ corresponds to a family $\bar{\rho}_T$ of rank ad Galois representations over T . We assume $H^2(G_K, \bar{\rho}_{\eta(t)})$ is of constant rank for all $t \in T(\overline{\mathbb{F}}_p)$. By [Emerton and Gee 2023, Lemma 5.4.1], the coherent sheaf $H^2(G_K, \bar{\rho}_T)$ is locally free of rank r as an \mathcal{O}_E -module.

By [Emerton and Gee 2023, Theorem 5.1.22], we can choose a complex of finite rank locally free \mathcal{O}_E -modules

$$C_T^0 \rightarrow C_T^1 \rightarrow C_T^2$$

computing $H^\bullet(G_K, \bar{\rho}_T)$. Since $H^2(G_K, \bar{\rho}_T)$ is a locally free sheaf, the truncated complex

$$C_T^0 \rightarrow Z_T^1$$

is again a complex of locally free \mathcal{O}_T -modules. The vector bundle $\mathcal{V}(Z_T^1) := \underline{\text{Spec}}(\text{Sym}(Z_T^1)^\vee)$ associated to the locally free sheaf Z_T^1 parametrizes all extensions

$$0 \rightarrow \bar{\rho}_{\eta(t)} \rightarrow ? \rightarrow \overline{\mathbb{F}}_p \rightarrow 0, \quad t \in T(\overline{\mathbb{F}}_p)$$

of the trivial G_K -representation $\overline{\mathbb{F}}_p$ by $\bar{\rho}_{\eta(t)}$. There are two projection morphisms

$$()_1 : (\mathcal{X}_{a,\text{red}})_{\overline{\mathbb{F}}_p} \times (\mathcal{X}_{d,\text{red}})_{\overline{\mathbb{F}}_p} \rightarrow (\mathcal{X}_{a,\text{red}})_{\overline{\mathbb{F}}_p} \quad \text{and} \quad ()_2 : (\mathcal{X}_{a,\text{red}})_{\overline{\mathbb{F}}_p} \times (\mathcal{X}_{d,\text{red}})_{\overline{\mathbb{F}}_p} \rightarrow (\mathcal{X}_{d,\text{red}})_{\overline{\mathbb{F}}_p}.$$

For each $t \in T(\overline{\mathbb{F}}_p)$, $f(t)_1 \in (\mathcal{X}_{a,\text{red}})_{\overline{\mathbb{F}}_p}$ corresponds to a rank- a Galois representation $\bar{\rho}_{t_1}$, and $f(t)_2 \in (\mathcal{X}_{d,\text{red}})_{\overline{\mathbb{F}}_p}$ corresponds to a rank- d Galois representation $\bar{\rho}_{t_2}$. We have $\bar{\rho}_{\eta(t)} = \text{Hom}_{G_K}(\bar{\rho}_{t_1}, \bar{\rho}_{t_2})$. So we can also regard $\mathcal{V}(Z_T^1)$ is a scheme parametrizing all extensions

$$0 \rightarrow \bar{\rho}_{t_1} \rightarrow ? \rightarrow \bar{\rho}_{t_2} \rightarrow 0, \quad t \in T(\overline{\mathbb{F}}_p)$$

and we have a morphism sending extension classes to equivalence classes of G_K -representations,

$$g : \mathcal{V}(Z_T^1) \rightarrow (\mathcal{X}_{a+d,\text{red}})_{\overline{\mathbb{F}}_p}.$$

Lemma 6.1.1. *Let e denote the dimension of the scheme-theoretic image of T in $(\mathcal{X}_{a,\text{red}})_{\overline{\mathbb{F}}_p} \times (\mathcal{X}_{d,\text{red}})_{\overline{\mathbb{F}}_p}$. Then the scheme-theoretic image of $V = \mathcal{V}(Z_T^1)$ in $(\mathcal{X}_{a+d,\text{red}})_{\overline{\mathbb{F}}_p}$ has dimension at most*

$$e + r + ad[K : \mathbb{Q}_p].$$

Proof. Without loss of generality, we assume T (and hence V) is irreducible. The proof is a routine calculation using stacks. We follow the proof of [Emerton and Gee 2023, Proposition 5.4.4] closely.

Let $v \in V(\bar{\mathbb{F}}_p)$. Write t for the composite $\text{Spec } \bar{\mathbb{F}}_p \xrightarrow{v} V \rightarrow T$. Write $f(t)$ for the composite $f \circ t$. Write $g(v)$ for the composite $g \circ v$. Define

$$\begin{aligned} T_{f(t)} &:= T \times_{f, (\mathcal{X}_{a,\text{red}})_{\bar{\mathbb{F}}_p} \times (\mathcal{X}_{d,\text{red}})_{\bar{\mathbb{F}}_p}, f(t)} \text{Spec } \bar{\mathbb{F}}_p, \\ V_{g(v)} &:= V \times_{g, (\mathcal{X}_{a,\text{red}})_{\bar{\mathbb{F}}_p} \times (\mathcal{X}_{d,\text{red}})_{\bar{\mathbb{F}}_p}, g(v)} \text{Spec } \bar{\mathbb{F}}_p, \\ V_{f(t), g(v)} &:= V_{g(v)} \times_{(\mathcal{X}_{a,\text{red}})_{\bar{\mathbb{F}}_p} \times (\mathcal{X}_{d,\text{red}})_{\bar{\mathbb{F}}_p}, f(t)} \text{Spec } \bar{\mathbb{F}}_p. \end{aligned}$$

Note that $V_{f(t), g(v)} \cong T_{f(t)} \times_T V_{g(v)}$.

By [Stacks, Tag 0DS4], it suffices to show, for v lying in some dense open subset of V ,

$$\dim V_{f(t), g(v)} \geq \dim V - (e + r + ad[K : \mathbb{Q}_p]).$$

Let $\bar{\rho}_{f(t)_1}$ denote the Galois representation corresponding to $f(t)_1 : \text{Spec } \bar{\mathbb{F}}_p \rightarrow (\mathcal{X}_{a,\text{red}})_{\bar{\mathbb{F}}_p}$. Let $\bar{\rho}_{f(t)_2}$ denote the Galois representation corresponding to $f(t)_2 : \text{Spec } \bar{\mathbb{F}}_p \rightarrow (\mathcal{X}_{d,\text{red}})_{\bar{\mathbb{F}}_p}$. Say $G_{t_1} := \text{Aut}(\bar{\rho}_{f(t)_1})$, and $G_{t_2} := \text{Aut}(\bar{\rho}_{f(t)_2})$. The morphism $f(t)$ factors through a monomorphism

$$[\text{Spec } \bar{\mathbb{F}}_p / G_{t_1}] \times [\text{Spec } \bar{\mathbb{F}}_p / G_{t_2}] \hookrightarrow (\mathcal{X}_{a,\text{red}})_{\bar{\mathbb{F}}_p} \times (\mathcal{X}_{d,\text{red}})_{\bar{\mathbb{F}}_p}$$

which induces a monomorphism

$$([\text{Spec } \bar{\mathbb{F}}_p / G_{t_1}] \times [\text{Spec } \bar{\mathbb{F}}_p / G_{t_2}]) \times_{(\mathcal{X}_{a,\text{red}})_{\bar{\mathbb{F}}_p} \times (\mathcal{X}_{d,\text{red}})_{\bar{\mathbb{F}}_p}} V_{g(v)} \hookrightarrow V_{g(v)}.$$

So it suffices to show

$$\dim V_{f(t), g(v)} \geq \dim V - (e + r + ad[K : \mathbb{Q}_p]) + \dim G_{t_1} + \dim G_{t_2} \quad (6-1)$$

for v lying in a dense open of V .

There exists an étale cover S of $(T_{f(t)})_{\text{red}}$ such that the pullback family $\bar{\rho}_S$ is a trivial family with fiber $\bar{\rho}_t$.

Let $C_S^0 \rightarrow Z_S^1$ denote the pullback family of $C_T^0 \rightarrow Z_T^1$ to S . $C_S^0 \rightarrow Z_S^1$ is also the pullback family of the fiber $C_t^0 \rightarrow Z_t^1$ to S . Write W for the affine scheme associated to $H^1(G_K, \bar{\rho}_{f(t)_1}^\vee \otimes \bar{\rho}_{f(t)_2})$. By the isomorphism

$$H^1(G_K, \bar{\rho}_{f(t)_1}^\vee \otimes \bar{\rho}_{f(t)_2}) \cong \text{Ext}_{G_K}(\bar{\rho}_{f(t)_1}, \bar{\rho}_{f(t)_2})$$

there is a morphism $W \rightarrow (\mathcal{X}_{a+d,\text{red}})_{\bar{\mathbb{F}}_p}$. Denote by w the image of v in w . We have

$$S \times_T V_{g(v)} = S \times_T V \times_W W_{h(w)}.$$

Let V' be the kernel of $S \times_T V \rightarrow S \times_{\bar{\mathbb{F}}_p} W$, which is a trivial vector bundle over S . We have

$$\begin{aligned} \dim V_{f(t), g(v)} &= \dim S \times_T V_{g(v)} \\ &= \text{rank } V' + \dim S + \dim W_{h(w)} \\ &= \text{rank } Z_T^1 - \dim H^1(G_K, \bar{\rho}_{f(t)_1}^\vee \otimes \bar{\rho}_{f(t)_2}) + \dim S + \dim W_{h(w)}. \end{aligned}$$

Note that $\dim V - \dim T = \text{rank } Z_T^1$, and, by the local Euler characteristic,

$$H^0(G_K, \bar{\rho}_{f(t_1)}^\vee \otimes \bar{\rho}_{f(t_2)}) - H^1(G_K, \bar{\rho}_{f(t_1)}^\vee \otimes \bar{\rho}_{f(t_2)}) + r = -ad[K : \mathbb{Q}_p].$$

We can replace T by a dense open of T where $e = \dim T - \dim T_{f(t)} = \dim T - \dim S$. Combining all these equalities, (6-1) becomes

$$\dim W_{h(w)} \geq \dim H^0(G_K, \bar{\rho}_{f(t_1)}^\vee \otimes \bar{\rho}_{f(t_2)}) + \dim G_{t_1} + \dim G_{t_2}$$

which follows from the fact that

$$H^0(G_K, \bar{\rho}_{f(t_1)}^\vee \otimes \bar{\rho}_{f(t_2)}) \times (G_{t_1} \times G_{t_2}) \subset \text{Aut}(\bar{\rho}_w)$$

and $\dim W_{h(w)} \geq \dim \text{Aut}(\bar{\rho}_w)$. □

We recall some terminology from [Emerton and Gee 2023]. Denote by $\text{ur}_x : \mathbb{G}_m \rightarrow \mathcal{X}_1$ the family of unramified characters of G_K . Let T be a reduced finite-type \mathbb{F} -scheme. Let $T \rightarrow \mathcal{X}$ be a morphism, corresponding to a family $\bar{\rho}_T$ of G_K -representations over T . We can construct the family of unramified twisting $\bar{\rho}_T \boxtimes \text{ur}_x$ over $T \times \mathbb{G}_m$. $\bar{\rho}_T$ is said to be *twistable* if whenever $\bar{\rho}_t \cong \bar{\rho}_{t'} \otimes \text{ur}_a$ for $t, t' \in T(\bar{\mathbb{F}}_p)$ and $a \in \bar{\mathbb{F}}_p^\times$, we have $a = 1$. $\bar{\rho}_T$ is said to be *essentially twistable* if for each $t \in T(\bar{\mathbb{F}}_p)$, the set of $a \neq 1$ for which $\bar{\rho}_t \cong \bar{\rho}_{t'} \otimes \text{ur}_a$ is finite.

We say $\bar{\rho}_T$ is *untwistable* if $\bar{\rho}$ is not essentially twistable.

From now on, write $\mathcal{X} = (\mathcal{X}_{2,\text{red}})_{\bar{\mathbb{F}}_p}$ for the moduli stack parametrizing (ϕ, Γ) -modules of rank 2.

Let \bar{r}^{univ} be the universal family of (ϕ, Γ) -modules over \mathcal{X} .

6.1.2. Remarks on the word use “locus”. Let (P) be a property that can be written as

$$(P) = (P1) - (P2)$$

where both (P1) and (P2) are closed conditions.

If \mathcal{X} be a moduli stack of finite type over $\bar{\mathbb{F}}_p$, the *locus of objects satisfying property (Pi)* is by definition the scheme-theoretic of a finite-type morphism $Y \rightarrow \mathcal{X}$ such that all objects of $\mathcal{X}(\bar{\mathbb{F}}_p)$ satisfying property (Pi) are in the image of $Y(\bar{\mathbb{F}}_p)$, $i = 1, 2$.

The *locus of objects satisfying property (P)* is by definition the locus of objects satisfying (P1) – locus of objects satisfying (P2).

6.2. Loci cut out by $H^2(G_K, \text{sym}^3 / \det^2)$. Write H^2 for $H^2(G_K, \text{sym}^3(\bar{r}^{\text{univ}}) / \det(\bar{r}^{\text{univ}})^2)$. Let $x \in \mathcal{X}(\bar{\mathbb{F}}_p)$ with corresponding Galois representation $\bar{r}_x : G_K \rightarrow \text{GL}_2(\bar{\mathbb{F}}_p)$.

We are interested in $H^2(G_K, \text{sym}^3 / \det^2)$ because it is a composition factor of the unipotent radical of the short root parabolic of the exceptional group G_2 , regarded as a representation of the corresponding Levi factor.

Lemma 6.2.1. *If \bar{r}_x is irreducible, then*

$$h_x^2 := \dim_{\bar{\mathbb{F}}_p} H^2\left(G_K, \frac{\text{sym}^3(\bar{r}_x)}{\det(\bar{r}_x)^2}\right) \leq 2.$$

Proof. An irreducible mod ϖ representation is of the shape $\text{Ind}_{G_{K_2}}^{G_K} \bar{\chi}$ for some character $\bar{\chi}$ of the degree 2 unramified extension K_2 of K . A direct computation shows

$$\text{sym}^3(\bar{r}_x) = \text{Ind}(\bar{\chi}^3) \oplus \text{Ind}(\bar{\chi} \det \bar{r}_x).$$

Both

$$H^2\left(G_K, \frac{\text{Ind}(\bar{\chi}^3)}{\det(\bar{r}_x)^2}\right) \quad \text{and} \quad H^2\left(G_K, \frac{\text{Ind}(\bar{\chi} \det \bar{r}_x)}{\det(\bar{r}_x)^2}\right)$$

have dimension at most 1. This is because the induction of a character can't be a direct sum of two isomorphic characters (when $p \neq 2$), by Shapiro's lemma and local Tate duality. \square

Corollary 6.2.2. *H^2 is SGR when restricted to the irreducible locus.*

Proof. Up to unramified twist, there are only finitely many irreducible representations. By Lemma 6.2.1, we have $h_x^2 \leq 2$ when \bar{r}_x is irreducible.

We first consider the sublocus where $h_x^2 = 2$. This sublocus consists of finitely many irreducible G_K -representations. Thus the sublocus in question is the scheme-theoretic union of the scheme-theoretic images of finitely many morphisms $\text{Spec } \bar{\mathbb{F}}_p \rightarrow \mathcal{X}$ corresponding to the finitely many irreducibles. The automorphism group of such an irreducible representation is \mathbb{G}_m and the morphisms $\text{Spec } \bar{\mathbb{F}}_p \rightarrow \mathcal{X}$ factor through $[\text{Spec } \bar{\mathbb{F}}_p / \mathbb{G}_m] \rightarrow \mathcal{X}$. The sublocus has dimension at most -1 .

Then we consider the locus where $h_x^2 \leq 1$. This sublocus consists of the unramified twists of finitely many irreducible G_K -representations. Thus the sublocus in question is the scheme-theoretic union of the scheme-theoretic images of finitely many morphisms $\mathbb{G}_m \rightarrow [\mathbb{G}_m / \mathbb{G}_m] \rightarrow \mathcal{X}$ corresponding to the finitely many irreducibles, and has dimension at most $\dim[\mathbb{G}_m / \mathbb{G}_m] = 0$.

In either case, the dimension of the locus is at most $[K : \mathbb{Q}_p] - h_x^2$. \square

Lemma 6.2.3. *If \bar{r}_x is a nontrivial extension of two characters, then*

$$h_x^2 := \dim H^2\left(G_K, \frac{\text{sym}^3(\bar{r}_x)}{\det(\bar{r}_x)^2}\right) \leq 1$$

and when the equality holds, the quotient character of \bar{r}_x is a character whose third power is $\bar{\mathbb{F}}_p(1)$.

Proof. This is where we make use of the assumption $p > 3$. Say $\bar{r}_x \sim \begin{bmatrix} \bar{\chi}_1 & \bar{c} \\ & \bar{\chi}_2 \end{bmatrix}$. We claim

$$\text{sym}^3(\bar{r}_x) \sim \begin{bmatrix} \bar{\chi}_1^3 & \bar{\chi}_1^2 \bar{c} & * & * \\ & \bar{\chi}_1^2 \bar{\chi}_2 & 2\bar{\chi}_1 \bar{\chi}_2 \bar{c} & * \\ & & \bar{\chi}_1 \bar{\chi}_2^2 & 3\bar{\chi}_2^2 \bar{c} \\ & & & \bar{\chi}_2^3 \end{bmatrix},$$

which has a unique G_K -invariant quotient line. Let $\{e_1, e_2\}$ be a basis of the representation space of \bar{r}_x such that e_1 is an invariant line. Then $\{e_1^3, e_1^2 e_2, e_1 e_2^2, e_2^3\}$ is a basis of the representation space of $\text{sym}^3(\bar{r}_x)$. By duality, we only need to show $\text{sym}^3(\bar{r}_x)$ has a unique invariant line. Clearly $\{e_1^3\}$ defines an invariant line. Assume there is another invariant line $\text{span}(v)$. We quotient $\text{sym}^3(\bar{r}_x)$ by $\text{span}(e_1^3)$. The quotient

representation has a unique invariant line generated by the image of $e_1^2 e_2$ (we postpone the explanation to the next paragraph). So $v \in \text{span}(e_1^3, e_1^2 e_2)$. But then we must have $v \in \text{span}(e_1^3)$, since $[\bar{c}]$ is a nontrivial extension class.

The quotient representation $\text{sym}^3(\bar{r}_x)/\text{span}(e_1^3)$ has a G_K -invariant line spanned by the image of $e_1^2 e_2$. Say $\text{span}(u)$ is another invariant line of $\text{sym}^3(\bar{r}_x)/\text{span}(e_1^3)$. We have $u \in \text{span}(e_1^2 e_2, e_1 e_2^2) \cong \bar{\chi}_1 \bar{\chi}_2 \otimes \bar{r}_x$. Thus $u \in \text{span}(e_1^2 e_2)$ since \bar{c} is a nontrivial extension. \square

Corollary 6.2.4. H^2 is SGR when restricted to the locus where \bar{r}_x is a nontrivial extension of two characters.

Proof. Say \bar{r}_x is the extension of $\bar{\beta}$ by $\bar{\alpha}$. By Lemma 6.2.3, we have $h_x^2 \leq 1$ when \bar{r}_x is a nontrivial extension of characters. So the locus where \bar{r}_x is a nontrivial extension of characters consists of four subloci:

- (i) $h_x^2 = 1$ and $\text{Ext}^2(\beta, \alpha) = 0$;
- (ii) $h_x^2 = 1$ and $\text{Ext}^2(\beta, \alpha) \neq 0$;
- (iii) $h_x^2 = 0$ and $\text{Ext}^2(\beta, \alpha) = 0$; and
- (iv) $h_x^2 = 0$ and $\text{Ext}^2(\beta, \alpha) \neq 0$.

Let $T \subset (\mathcal{X}_{1,\text{red}})_{\bar{\mathbb{F}}_p} \times (\mathcal{X}_{1,\text{red}})_{\bar{\mathbb{F}}_p}$ be the locus of the pair (α, β) , $\alpha, \beta \in \mathcal{X}_{1,\text{red}}(\bar{\mathbb{F}}_p)$; say $\dim T = e$, and $\dim \text{Ext}^2(\beta, \alpha) = r$. By Lemma 6.1.1, each sublocus has dimension at most

$$e + r + [K : \mathbb{Q}_p].$$

In sublocus (i), β has only finitely many choices once α is chosen, so $e = -1$, $r = 0$; in sublocus (ii), both β and α have only finitely many choices, so $e = -2$, $r = 1$; in sublocus (iii), both β and α can vary in a dense open of $(\mathcal{X}_{1,\text{red}})_{\bar{\mathbb{F}}_p}$, so $e = 2 \dim(\mathcal{X}_{1,\text{red}})_{\bar{\mathbb{F}}_p} = 0$, $r = 0$; in sublocus (iv), when α is chosen, β has only finitely many choices, so $e = -1$, $r = 1$. We can verify that in each case $e + r + [K : \mathbb{Q}_p] \leq \dim \mathcal{X} - h_x^2 = [K : \mathbb{Q}_p] - h_x^2$. \square

Lemma 6.2.5. If \bar{r}_x is a direct sum of distinct characters, then

$$H^2\left(G_K, \frac{\text{sym}^3(\bar{r}_x)}{\det(\bar{r}_x)^2}\right) \leq 2.$$

Proof. Say $\bar{r}_x \sim \begin{bmatrix} \bar{\chi}_1 \\ \bar{\chi}_2 \end{bmatrix}$. We have

$$\frac{\text{sym}^3(\bar{r}_x)}{\det(\bar{r}_x)^2} \cong \bar{\chi}_1 \bar{\chi}_2^{-2} \oplus \bar{\chi}_2^{-1} \oplus \bar{\chi}_1^{-1} \oplus \bar{\chi}_2 \bar{\chi}_1^{-2}.$$

If $\bar{\chi}_1 \neq \bar{\chi}_2$, then the multiset $\{\bar{\chi}_1 \bar{\chi}_2^{-2}, \bar{\chi}_2^{-1}, \bar{\chi}_1^{-1}, \bar{\chi}_2 \bar{\chi}_1^{-2}\}$ contains at most 2 isomorphic characters. \square

Corollary 6.2.6. H^2 is SGR when restricted to the locus where \bar{r}_x is a direct sum of distinct characters.

Proof. By Lemma 6.2.5, we have $h_x^2 \leq 2$ when $\bar{x} = \alpha \oplus \beta$ is a direct sum of distinct characters.

In the sublocus where $h_x^2 = 2$, we must have $\pm\alpha = \pm\beta = \mathbb{F}(-1)$. The sublocus is the scheme-theoretic union of the scheme-theoretic image of finitely many $\text{Spec } \bar{\mathbb{F}}_p \times \text{Spec } \bar{\mathbb{F}}_p \rightarrow \mathcal{X}$ and has dimension $0 - 2 = -2$.

In the locus where $h_x^2 = 1$, we have one of the following:

- (i) $\alpha = \mathbb{F}(-1)$, (ii) $\beta = \mathbb{F}(-1)$,
- (iii) $\alpha = \beta^2(-1)$, (iv) $\beta = \alpha^2(-1)$.

In each of these cases, the locus has dimension $\dim \mathbb{G}_m - \dim \text{Aut}(\bar{r}_x) = 1 - 2 = -1$.

In the locus where $h_x^2 = 0$, both α and β lives in an untwistable family, and the locus has dimension $2 \dim \mathbb{G}_m - \dim \text{Aut}(\bar{r}_x) = 2 - 2 = 0$. □

Lemma 6.2.7. *If \bar{r}_x is a direct sum of isomorphic characters, then*

$$H^2\left(G_K, \frac{\text{sym}^3(\bar{r}_x)}{\det(\bar{r}_x)^2}\right) \leq 4.$$

Proof. This is trivial because the underlying $\bar{\mathbb{F}}_p$ -vector space is four-dimensional. □

Corollary 6.2.8. *H^2 is SGR when restricted to the locus where \bar{r}_x is a direct sum of isomorphic characters.*

Proof. The automorphism group is four-dimensional. So the locus in the moduli stack has dimension $\dim \mathbb{G}_m - \dim \text{Aut}(\bar{r}_x) = 1 - 4 = -3$. □

Theorem 6.2.9. *The locus of \bar{r}_x in \mathcal{X} for which*

$$H^2\left(G_K, \frac{\text{sym}^3(\bar{r}_x)}{\det(\bar{r}_x)^2}\right) \geq r$$

is of dimension at most $[K : \mathbb{Q}_p] - r$.

Proof. This theorem follows immediately from Lemmas 6.2.1, 6.2.3, 6.2.5, 6.2.7, and their corollaries. □

Fix a mod ϖ representation $\bar{r} : G_K \rightarrow GL_2(\mathbb{F})$. Let $\underline{\lambda}$ be a Hodge type. Let R be an irreducible component of the crystalline lifting ring $R_{\bar{r}}^{\text{crys}, \underline{\lambda}, \mathcal{O}_E}$. Assume $\text{Spec } R[1/p] \neq \emptyset$. Let r^{univ} be the universal family of Galois representations on R .

Since $H^2(G_K, \text{sym}^3(r^{\text{univ}})/\det(r^{\text{univ}})^2)$ is a coherent sheaf, by the semicontinuity theorem, the locus $X_s := \{x \in \text{Spec } R \mid \dim \kappa(x) \otimes_R H^2 \geq s\}$ is locally closed, and has a reduced induced scheme structure.

Theorem 6.2.10. *Let R be an irreducible component of the crystalline lifting ring of regular labeled Hodge–Tate weights. If $H^2(G_K, \text{sym}^3(r^{\text{univ}})/\det(r^{\text{univ}})^2)$ is ϖ -torsion, the locus*

$$\left\{ x \in \text{Spec } R \mid \dim \kappa(x) \otimes_R H^2\left(G_K, \frac{\text{sym}^3(r^{\text{univ}})}{\det(r^{\text{univ}})^2}\right) \geq s \right\}$$

has codimension $\geq s + 1$ in $\text{Spec } R$ for $s \geq 1$.

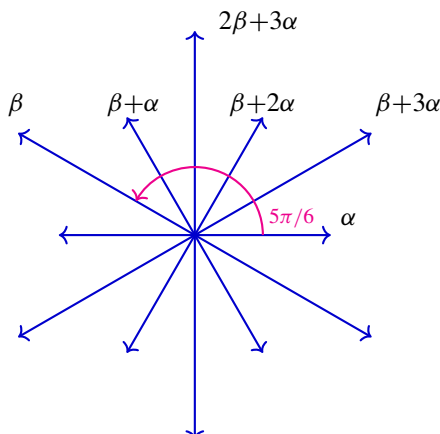
Proof. The proof is identical to that of [Emerton and Gee 2023, Theorem 6.1.1] if we use Theorem 6.2.9 instead of [Emerton and Gee 2023, Theorem 5.5.12]. □

7. The existence of crystalline lifts for the exceptional group G_2

7.1. Parabolics of G_2 . Let G_2 be the Chevalley group over \mathcal{O}_E of type G_2 .

Let E/\mathbb{Q}_p be a finite extension with ring of integers \mathcal{O}_E , residue field \mathbb{F} and uniformizer ϖ .

We remind the reader of the root system of G_2 :



7.1.1. The short root parabolic. Let $P \subset G_2$ be the short root parabolic, which admits a Levi decomposition $P = L \ltimes U$. The Levi factor L is a copy of GL_2 and the unipotent radical U is a unipotent group of class 2. Write U^{ad} for $U/Z(U)$.

Fix an isomorphism $\text{std} : L \cong GL_2$. We have

- $Z(U) \cong \mathbb{G}_a$; and
- $U^{\text{ad}} \cong \mathbb{G}_a^{\oplus 4}$.

Write $\text{Lie } U = Z(U) \oplus U^{\text{ad}}$. The Levi factor acts on U by conjugation. We have an isomorphism of L -modules

$$\text{Lie } U \cong \frac{1}{\det^2} \text{sym}^3(\text{std}) \oplus \frac{1}{\det} \tag{7-1}$$

where $\det : L \rightarrow \mathbb{G}_m$ is the determinant character, and $\text{std} : L \xrightarrow{\cong} GL_2$ is the fixed isomorphism. The above short exact sequence can be upgraded to a short exact sequence of groups with L -actions

$$0 \rightarrow \frac{1}{\det} \rightarrow U \rightarrow \frac{1}{\det^2} \text{sym}^3(\text{std}) \rightarrow 0.$$

For lack of reference, we explain how to get (7-1). By inspecting the root system for G_2 , we find that the roots whose root group is contained in U^{ad} lie in a single line. Therefore U^{ad} is an irreducible L -module, and is thus isomorphic to $\text{sym}^3(\text{std})$ up to an algebraic character; then computation shows the character is $1/\det^2$ (also see the SageMath code on my homepage).

7.1.2. The long root parabolic. Let $Q \subset G_2$ be the long root parabolic, which admits a Levi decomposition $Q = L' \ltimes V$ where $L' \cong GL_2$ and V is a unipotent group of class 3. Fix an isomorphism $\text{std} : L' \xrightarrow{\cong} GL_2$. Write \det for the composition $L' \xrightarrow{\text{std}} GL_2 \xrightarrow{\det} GL_1$.

Write U' for $V/Z(V)$. Then U' is a unipotent group of class 2 whose center is isomorphic to \mathbb{G}_a . The conjugation action of L' on U' is given by $U'/Z(U') \cong \text{std}$, and $Z(U') \cong \text{det}$, as L' -modules.

Theorem 7.1.3. *Assume $p > 3$. Let K/\mathbb{Q}_p be a p -adic field. Let $\bar{\rho} : G_K \rightarrow G_2(\overline{\mathbb{F}}_p)$ be a mod ϖ Galois representation. Then $\bar{\rho}$ admits a crystalline lift $\rho^\circ : G_K \rightarrow G_2(\overline{\mathbb{Z}}_p)$ of $\bar{\rho}$.*

Moreover, if $\bar{\rho}$ factors through a maximal parabolic and the Levi factor $\bar{r} := \bar{r}_\rho$ of $\bar{\rho}$ admits a Hodge–Tate regular and crystalline lift r_1 such that the adjoint representation $\phi^{\text{Lie}}(r_1)$ has Hodge–Tate weights slightly less than $\underline{0}$, then ρ° can be chosen such that it factors through the same maximal parabolic and its Levi factor r_{ρ° lies on the same irreducible component of the spectrum of the crystalline lifting ring that r_1 does.

Proof. If $\bar{\rho}$ is irreducible, then $\bar{\rho}$ admits a crystalline lift by [Lin 2022].

The exceptional group G_2 has two maximal parabolic subgroups: the short root parabolic, and the long root parabolic.

If $\bar{\rho}$ is reducible, then it factors through either parabolic subgroups.

7.1.4. The short root parabolic case. Let $P \subset G_2$ be the short root parabolic. Recall that P has a Levi decomposition $P = L \rtimes U$. Fix an isomorphism $L \cong \text{GL}_2$.

By Lemma 3.3.2, there exists a finite Galois extension K'/K , of prime-to- p degree such that $\bar{r}|_{K'}$ is Lyndon–Demushkin.

Write $Z(U)$ for center of U , and write U^{ad} for $U/Z(U)$. Write $\phi : L \rightarrow \text{Aut}(U)$ for the conjugation action, with graded pieces $\phi^{\text{ad}} : L \rightarrow \text{GL}(U^{\text{ad}})$ and $\phi^z : L \rightarrow \text{GL}(Z(U))$. Write ϕ^{Lie} for $\phi^{\text{ad}} \oplus \phi^z$.

Lemma 7.1.5. *Assume $p > 2$. There exists a Hodge–Tate regular crystalline lifting $r^\circ : G_K \rightarrow L(\overline{\mathbb{Z}}_p)$ of the Levi factor \bar{r} , such that the adjoint representation $\phi^{\text{Lie}}(r^\circ) : G_K \xrightarrow{r^\circ} L(\overline{\mathbb{Z}}_p) \rightarrow \text{GL}(\text{Lie } U(\overline{\mathbb{Z}}_p))$ has labeled Hodge–Tate weights slightly less than $\underline{0}$.*

Proof. It is well known Hodge–Tate regular crystalline lifts of \bar{r} exists since $L \cong \text{GL}_2$. We have

$$\phi^{\text{Lie}}(r^\circ) = \frac{1}{\det r^{\circ 2}} \text{sym}^3(r^\circ) \oplus \frac{1}{\det r^\circ}.$$

So by replacing r° by a Tate twist, we can ensure $\phi^{\text{Lie}}(r^\circ)$ has labeled Hodge–Tate weights slightly less than $\underline{0}$. □

Let $\text{Spec } R$ be an irreducible component (with nonempty generic fiber) of a crystalline lifting ring $R_{\bar{r}}^{\text{crys}, \underline{\lambda}}$ of regular labeled Hodge–Tate weights $\underline{\lambda}$ such that the labeled Hodge–Tate weights $\phi^{\text{Lie}}(\underline{\lambda})$ are slightly less than 0. By the lemma above, such a $\text{Spec } R$ exists.

Let $r^{\text{univ}} : G_K \rightarrow L(R)$ be the universal Galois representation.

The mod ϖ Galois representation \bar{r} defines a Galois action $\phi(\bar{r}) : G_K \rightarrow \text{Aut}(U(\overline{\mathbb{F}}_p))$ on $U(\overline{\mathbb{F}}_p)$. By Section 4.1.3, the datum of $\bar{\rho} : G_K \rightarrow G_2(\overline{\mathbb{F}}_p)$ is encoded in a nonabelian cocycle $[\bar{c}] \in H^1(G_K, U(\overline{\mathbb{F}}_p))$.

The strategy for lifting $\bar{\rho}$ is as follows. We choose a suitable $\overline{\mathbb{Z}}_p$ -point x of $\text{Spec } R$ which defines a lift $r_x : G_K \rightarrow L(\overline{\mathbb{Z}}_p)$ of \bar{r} , and endow $U(\overline{\mathbb{Z}}_p)$ with the Galois action $\phi(r_x) : G_K \xrightarrow{r_x} L(\overline{\mathbb{Z}}_p) \rightarrow \text{Aut}(U(\overline{\mathbb{Z}}_p))$. There is a map of pointed set $H^1(G_K, U(\overline{\mathbb{Z}}_p)) \rightarrow H^1(G_K, U(\overline{\mathbb{F}}_p))$. If the cohomology class $[\bar{c}]$ admits a lift $[c] \in H^1(G_K, U(\overline{\mathbb{Z}}_p))$, then $\bar{\rho}$ admits a lift $\rho : G_K \rightarrow G_2(\overline{\mathbb{Z}}_p)$ whose datum is encoded in $[c]$. Such

a lift ρ is crystalline by the main result of [Lin 2019], since $\phi^{\text{Lie}}(r^\circ)$ has labeled Hodge–Tate weights slightly less than $\underline{0}$.

By Theorem 5.2.1, to lift the nonabelian 1-cocycle $[\bar{c}]$, it suffices to verify the following:

- (1) $H^2(G_K, \text{sym}^3(r^{\text{univ}})/\det^2(r^{\text{univ}}))$ is SGR and supported on the special fiber of $\text{Spec } R$.
- (2) $p \neq 2$.
- (3) There exists a finite Galois extension K'/K of prime-to- p degree such that $\phi(\bar{r})|_{G_{K'}}$ is Lyndon–Demushkin.
- (4) There exists a $\bar{\mathbb{Z}}_p$ -point of $\text{Spec } R$ which is mildly regular when restricted to $G_{K'}$.

Item (1) is verified by Theorem 6.2.10. Note that since the Hodge type of $\text{Spec } R$ is chosen so that $\text{sym}^3(r_x)/\det(r_x)^2$ has labeled Hodge–Tate weights slightly less than $\underline{0}$, $H^2(G_K, \text{sym}^3(r_x)/\det(r_x)^2)$ is torsion for any characteristic-0 point x of $\text{Spec } R$. Item (3) follows from Lemma 3.3.2, and (4) follows from Proposition 3.0.5.

7.1.6. The long root parabolic case. Let $Q \subset G_2$ be the long root parabolic. Q has a Levi decomposition $Q = L' \ltimes V$. Fix an isomorphism $\text{std} : L' \xrightarrow{\cong} \text{GL}_2$. Write \det for the composition $L' \xrightarrow{\text{std}} \text{GL}_2 \xrightarrow{\det} \text{GL}_1$.

Let $\{1\} = V_0 \subset V_1 \subset V_2 \subset V_3 = V$ be the upper central series of V . Then the conjugation action of L' on each graded piece is given by

- $V_3/V_2 \cong \det \otimes \text{std}$;
- $V_2/V_1 \cong \det$;
- $V_1 \cong \text{std}$.

Suppose $\bar{\rho}$ factors through the long root parabolic Q , but not the short root parabolic P . Then the Levi factor

$$\bar{r} : G_K \xrightarrow{\bar{\rho}} Q(\bar{\mathbb{F}}_p) \rightarrow L'(\bar{\mathbb{F}}_p)$$

is necessarily an irreducible representation. If we endow each graded piece of $V(\bar{\mathbb{F}}_p)$ with the Galois action $G_K \xrightarrow{\bar{r}} L(\bar{\mathbb{Z}}_p) \rightarrow \text{GL}(V_{i+1}(\bar{\mathbb{F}}_p)/V_i(\bar{\mathbb{F}}_p))$, then we have, by local Tate duality,

$$\begin{aligned} H^2(G_K, V_3(\bar{\mathbb{F}}_p)/V_2(\bar{\mathbb{F}}_p)) &= H^2(G_K, \bar{r} \otimes \det \bar{r}) = 0, \\ H^2(G_K, V_1(\bar{\mathbb{F}}_p)) &= H^2(G_K, \bar{r}) = 0. \end{aligned}$$

So the only cohomological obstruction occurs in the second graded piece.

The datum of $\bar{\rho}$ is encoded in a nonabelian cocycle $[\bar{c}] \in H^1(G_K, V(\bar{\mathbb{F}}_p))$. Just as is done in the short root parabolic case, it suffices to lift the cocycle $[\bar{c}]$. By Proposition 5.3.1, since the only cohomological obstruction lies in the second graded piece, it suffices to lift $\text{ad}([\bar{c}]) \in H^1(G_K, (V/V_1)(\bar{\mathbb{F}}_p))$.

Write U' for V/V_1 . Recall that U' is a unipotent group of class 2 with rank-1 center, and we can directly appeal to Theorem 5.2.1. We repeat the procedure worked out in the short root case 7.1.4.

Let r° be a lift of \bar{r} such that r° is Hodge–Tate regular and crystalline and the Hodge–Tate weights of r° are strictly less than $\underline{0}$.

Let $\text{Spec } R$ be the irreducible component of the crystalline lifting ring of \bar{r} containing r° . Write $r^{\text{univ}} : G_K \rightarrow \text{GL}_2(R)$ for the universal family.

Write $Z(U')$ for the center of U' , and write U'^{ad} for $U'/Z(U')$. Write ϕ^{ad} for the conjugate action $L' \rightarrow \text{Aut}(U'^{\text{ad}})$ and write ϕ^z for the conjugate action $L' \rightarrow \text{Aut}(Z(U'))$.

Note that $\phi^{\text{ad}}(r^{\text{univ}}) = r^{\text{univ}}$ and $\phi^z(r^{\text{univ}}) = \det r^{\text{univ}}$.

We have the following checklist:

- (1) $H^2(G_K, \det(r^{\text{univ}})r^{\text{univ}})$ is SGR.
- (2) $p \neq 2$.
- (3) There exists a finite Galois extension K'/K of prime-to- p degree such that $\phi(\bar{r})|_{G_{K'}}$ is Lyndon–Demushkin.
- (4) There exists a $\bar{\mathbb{Z}}_p$ -point of $\text{Spec } R$ which is mildly regular when restricted to $G_{K'}$.

By the assumption $H^2(G_K, \det(r^{\text{univ}})r^{\text{univ}}) = 0$, (3) follows from Lemma 3.3.2, and (4) follows from Proposition 3.0.5. □

Appendix A: Nondegeneracy of mod ϖ cup product for G_2

Let \mathbb{F} be a finite field of characteristic $p > 3$. Write G_2 for the Chevalley group over \mathbb{F} of type G_2 .

Let P be the short root parabolic of G_2 . Let $P = L \times U$ be the Levi decomposition. Let $\bar{r} : G_K \rightarrow L(\mathbb{F})$ be a Galois representation which is Lyndon–Demushkin. Since $L \cong \text{GL}_2$, \bar{r} is the extension of two trivial characters. Denote by $\phi : L \rightarrow \text{Aut}(U)$ the conjugation action. G_K acts on U via the conjugate action $G_K \xrightarrow{r^\circ} L \xrightarrow{\phi} \text{Aut}(U)$.

We set up a computational framework to prove various claims. Let $\{x_0, \dots, x_n, x_{n+1}\}$ be the Demushkin generators.

Let $\{e_1, e_2\}$ be a basis of the representation space of \bar{r} such that r° is upper-triangular with respect to this basis. Without loss of generality, assume $e_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, $e_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$. Say for $i = 0, \dots, n + 1$, $\bar{r}(x_i) = \begin{bmatrix} 1 & l_i \\ & 1 \end{bmatrix}$.

The set $\{e_1^3, e_1^2 e_2, e_1 e_2^2, e_2^3\}$ is a basis of the representation space $\text{sym}^3(\bar{r})$, which is identified with $U^{\text{ad}}(\mathbb{F})$.

The root system of G_2 can be found in Section 7.1. In the diagram, α is the short root, and β is the long root. Each root x generates a root group $U_x \subset U$. The short root parabolic P has seven root groups: the five root groups

$$\{U_\beta, U_{\beta+\alpha}, U_{\beta+2\alpha}, U_{\beta+3\alpha}, U_{2\beta+3\alpha}\}$$

lying above the x -axis generates the unipotent radical U , the two root groups $\{U_\alpha, U_{-\alpha}\}$ lying on the x -axis are the root groups of the Levi factor group L . Say under the identification $\text{std} : L \cong \text{GL}_2$, the matrices $\begin{bmatrix} 0 & * \\ 0 & 0 \end{bmatrix}$ are identified with the root group U_α . Now we have identifications

$$\text{span } e_1^3 \sim U_\beta, \quad \text{span } e_1^2 e_2 \sim U_{\beta+\alpha}, \quad \text{span } e_1 e_2^2 \sim U_{\beta+2\alpha}, \quad \text{span } e_2^3 \sim U_{\beta+3\alpha}.$$

For ease of notation, write $E_0 := e_1^3$, $E_1 := e_1^2 e_2$, $E_2 := e_1 e_2^2$, $E_3 := e_2^3$. A basis of

$$C_{\text{LD}}^1(U^{\text{ad}}(\mathcal{O}_E)) \cong \{\langle x_0, \dots, x_{n+1} \rangle \rightarrow U_\beta(\mathcal{O}_E) \oplus U_{\beta+\alpha}(\mathcal{O}_E) \oplus U_{\beta+2\alpha}(\mathcal{O}_E) \oplus U_{\beta+3\alpha}(\mathcal{O}_E)\}$$

is given by

$$\mathcal{B} = \begin{Bmatrix} x_0^* E_0, x_1^* E_0, \dots, x_{n+1}^* E_0, \\ x_0^* E_1, x_1^* E_1, \dots, x_{n+1}^* E_1, \\ x_0^* E_2, x_1^* E_2, \dots, x_{n+1}^* E_2, \\ x_0^* E_3, x_1^* E_3, \dots, x_{n+1}^* E_3 \end{Bmatrix},$$

where $x_i^* E_j$ is the cochain $c : \langle x_0, \dots, x_{n+1} \rangle$ such that $c(x_k) = \delta_{ik} E_j$, where δ_{ik} is the Kronecker delta. For any $c \in C_{LD}^1(U^{\text{ad}})$, we can write down the \mathcal{B} -coordinates $[c]_{\mathcal{B}} := (c_v)_{v \in \mathcal{B}}$ of c .

Lemma A.0.1. *The cup products on cochains*

$$\cup_{\mathbb{F}} : C_{LD}^1(U^{\text{ad}}(\mathbb{F})) \times C_{LD}^1(U^{\text{ad}}(\mathbb{F})) \rightarrow C_{LD}^2(Z(U)(\mathbb{F}))$$

is nondegenerate.

Ideas. We compute the cup products $v \cup w$ for $v, w \in \mathcal{B}$. The matrix $[\cup_{\mathbb{F}}]_{\mathcal{B}}$ is anti-lower-triangular, (that is, of the shape

$$\begin{bmatrix} 0 & 0 & 0 & * \\ 0 & 0 & * & * \\ 0 & * & * & * \\ * & * & * & * \end{bmatrix}$$

whose antidiagonal blocks are constant invertible matrices), and thus nondegenerate.

To help the reader better understand what’s going on, we attached SageMath code in Appendix B.

Proof. Recall the relator of the Lyndon–Demushkin group is

$$R = x_0^g(x_0, x_1)(x_2, x_3) \cdots (x_n, x_{n+1}).$$

Since we are working mod ϖ , we have for any $p > 5$, any $g \in G_{K'}$, $\phi(\bar{r}(g))^p \equiv \text{id} \pmod{\varpi}$ (See Appendix B for the verification). In particular, the relator R reduces to

$$(x_0, x_1) \cdots (x_n, x_{n+1})$$

when we compute mod ϖ . (When $p = 5$, things are still good, and can be confirmed by running the SageMath code in Appendix B.)

We regard cochains in $C_{LD}^1(U^{\text{ad}}(\mathbb{F}))$ as a $(U^{\text{ad}}(\mathbb{F}))$ -valued function on the free group with generators $\{x_0, \dots, x_{n+1}\}$,

Now we let c be the “universal” mod ϖ 1-cochain. That is, we let

$$\begin{Bmatrix} \lambda_{0,0}, \lambda_{1,0}, \dots, \lambda_{n+1,0}, \\ \lambda_{0,1}, \lambda_{1,1}, \dots, \lambda_{n+1,1}, \\ \lambda_{0,2}, \lambda_{1,2}, \dots, \lambda_{n+1,2}, \\ \lambda_{0,3}, \lambda_{1,3}, \dots, \lambda_{n+1,3} \end{Bmatrix}$$

be indeterminants, and set

$$c := \sum \lambda_{i,j} x_i^* E_j \in C_{LD}^1(U^{\text{ad}}(\mathbb{F})) \otimes \mathbb{Z}[\lambda_{i,j}].$$

The cup product

$$c \cup c = Q(c) \in C_{LD}^2(Z(U)(\mathbb{F})) \otimes \mathbb{Z}[\lambda_{i,j}] = Z(U)(\mathbb{F}) \otimes \mathbb{Z}[\lambda_{i,j}] \cong \mathbb{F}[\lambda_{i,j}]$$

will be a quadratic form in variables $\{\lambda_{i,j}\}$, and the matrix of this quadratic form is nothing but the matrix $[\cup_{\mathbb{F}}]_{\mathcal{B}}$. Recall that $c \cup c = Q(c)$ is defined to be the projection of $\tilde{c}(R)$ onto the center of the Lie algebra $\text{Lie } U$, where $\tilde{c} \in C^1_{\text{LD}}(U(\mathbb{F}))$ is the unique extension of c to a $U(\mathbb{F})$ -valued cochain as is explained in Section 2.

Write $[\cup_{\mathbb{F}}]_{\mathcal{B}}$ as a block matrix

$$[\cup_{\mathbb{F}}]_{\mathcal{B}} = \begin{matrix} & \beta & \beta+\alpha & \beta+2\alpha & \beta+3\alpha \\ \beta & \left(\begin{array}{c|c|c|c} M_{11} & M_{12} & M_{13} & M_{14} \\ \hline M_{21} & M_{22} & M_{23} & M_{24} \\ \hline M_{31} & M_{32} & M_{33} & M_{34} \\ \hline M_{41} & M_{42} & M_{43} & M_{44} \end{array} \right) \\ \beta+\alpha & & & & \\ \beta+2\alpha & & & & \\ \beta+3\alpha & & & & \end{matrix},$$

where each M_{ij} is an $(n + 2) \times (n + 2)$ matrix. We say the blocks $M_{24}, M_{33}, M_{34}, M_{42}, M_{43}, M_{44}$ are strictly below the antidiagonal, and we call M_{41}, M_{32}, M_{23} and M_{14} the antidiagonal blocks:

$$\begin{matrix} \beta & \beta+\alpha & \beta+2\alpha & \beta+3\alpha \\ \beta & \left(\begin{array}{c|c|c|c} & & & \\ \hline & & & M_{24} \\ \hline & & M_{33} & M_{34} \\ \hline & M_{42} & M_{43} & M_{44} \end{array} \right) \\ \beta+\alpha & & & \\ \beta+2\alpha & & & \\ \beta+3\alpha & & & \end{matrix} \quad \begin{matrix} \beta & \beta+\alpha & \beta+2\alpha & \beta+3\alpha \\ \beta & \left(\begin{array}{c|c|c|c} & & & M_{14} \\ \hline & & M_{23} & \\ \hline & M_{32} & & \\ \hline M_{41} & & & \end{array} \right) \\ \beta+\alpha & & & \\ \beta+2\alpha & & & \\ \beta+3\alpha & & & \end{matrix}$$

strictly below antidiagonal antidiagonal blocks

Sublemma. Let $g = g_1 g_2 \dots g_s$. Write ϕ_i for $\phi(\bar{r}(g_1, \dots, g_{i-1}))$. We have

$$\tilde{c}(g) = \sum \phi_i \tilde{c}(g_i) + \frac{1}{2} \sum_{i < j} [\phi_i \tilde{c}(g_i), \phi_j \tilde{c}(g_j)].$$

Proof. This is an immediate consequence of the Baker–Campbell–Hausdorff formula. □

Note that $\phi(\bar{r}((x_i, x_j))) = \text{id}$, so

$$\begin{aligned} \tilde{c}(R) &= \tilde{c}(x_0^q(x_0, x_1)(x_2, x_3) \cdots (x_n, x_{n+1})) \\ &= \sum \tilde{c}((x_{2k}, x_{2k+1})) + \frac{1}{2} \sum_{j < k} [\tilde{c}((x_{2j}, x_{2j+1})), \tilde{c}((x_{2k}, x_{2k+1}))]. \end{aligned}$$

We have

$$\tilde{c}((x_{2k}, x_{2k+1})) = -\phi(x_{2k}^{-1})(\phi(x_{2k+1}) - 1)\tilde{c}(x_{2k}) + \phi(x_{2k}^{-1}x_{2k+1}^{-1})(\phi(x_{2k}) - 1)\tilde{c}(x_{2k+1}) + Z_k = Y_k + Z_k,$$

where Z_k is a sum of Lie brackets (see below), and lies in the center of the Lie U . Note that $[Y_j, Y_k]$ only contributes to the part of $[\cup_{\mathbb{F}}]_{\mathcal{B}}$ which lies strictly below the antidiagonal, because $(\phi(x_{2k}) - 1)$ and $(\phi(x_{2k+1}) - 1)$ moved the appearance of the indeterminant $\lambda_{i,j}$ from the root group $U_{\beta+j\alpha}$ to the root group $U_{\beta+(j+1)\alpha}$.

So it remains to analyze $\sum Z_k$. We have

$$\begin{aligned} 2Z_k &= [-\phi(x_{2k}^{-1})\tilde{c}(x_{2k}), -\phi(x_{2k}^{-1}x_{2k+1}^{-1})\tilde{c}(x_{2k+1})] + [-\phi(x_{2k}^{-1})\tilde{c}(x_{2k}), +\phi(x_{2k}^{-1}x_{2k+1}^{-1})\tilde{c}(x_{2k})] \\ &\quad + [-\phi(x_{2k}^{-1})\tilde{c}(x_{2k}), +\phi(x_{2k}^{-1}x_{2k+1}^{-1}x_{2k})\tilde{c}(x_{2k+1})] + [-\phi(x_{2k}^{-1}x_{2k+1}^{-1})\tilde{c}(x_{2k+1}), +\phi(x_{2k}^{-1}x_{2k+1}^{-1})\tilde{c}(x_{2k})] \\ &\quad + [-\phi(x_{2k}^{-1}x_{2k+1}^{-1})\tilde{c}(x_{2k+1}), +\phi(x_{2k}^{-1}x_{2k+1}^{-1}x_{2k})\tilde{c}(x_{2k+1})] \\ &\quad + [\phi(x_{2k}^{-1}x_{2k+1}^{-1})\tilde{c}(x_{2k}), +\phi(x_{2k}^{-1}x_{2k+1}^{-1}x_{2k})\tilde{c}(x_{2k+1})] \end{aligned}$$

Write

$$2Z'_k := [-\tilde{c}(x_{2k}), -\tilde{c}(x_{2k+1})] + [-\tilde{c}(x_{2k}), \tilde{c}(x_{2k})] + [-\tilde{c}(x_{2k}), \tilde{c}(x_{2k+1})] + [-\tilde{c}(x_{2k+1}), \tilde{c}(x_{2k})] \\ + [-\tilde{c}(x_{2k+1}), \tilde{c}(x_{2k+1})] + [\tilde{c}(x_{2k}), \tilde{c}(x_{2k+1})].$$

Z'_k is obtained by replacing all Galois action in Z_k by the trivial action. $Z_k - Z'_k$ only contributes to the part of $[\cup_{\mathbb{F}}]_{\mathcal{B}}$ with lies strictly below the antidiagonal for a similar reason (a “shifting” effect). It is easy to see that

$$Z'_k = [\tilde{c}(x_{2k}), \tilde{c}(x_{2k+1})] = \pm\lambda_{2k,0}\lambda_{2k+1,3} \pm \lambda_{2k+1,0}\lambda_{2k,3} \pm 3\lambda_{2k,1}\lambda_{2k+1,2} \pm 3\lambda_{2k+1,2}\lambda_{2k,1}.$$

As a consequence of these computations, we see that each of the antidiagonal blocks of $[\cup]_{\mathcal{B}}$ are constant matrices:

$$\pm M_{41} = \pm M_{14} = \begin{bmatrix} [1/2 \quad -1/2] & & & & \\ & [1/2 \quad -1/2] & & & \\ & & \ddots & & \\ & & & \ddots & \\ & & & & [1/2 \quad -1/2] \end{bmatrix},$$

$$\pm M_{32} = \pm M_{23} = \begin{bmatrix} [3/2 \quad -3/2] & & & & \\ & [3/2 \quad -3/2] & & & \\ & & \ddots & & \\ & & & \ddots & \\ & & & & [1/2 \quad -1/2] \end{bmatrix}.$$

So $[\cup_{\mathbb{F}}]_{\mathcal{B}}$ is an invertible matrix. □

The long root parabolic case is much simpler.

Appendix B: Sagemath code

Proposition B.0.1. *Let $V \subset B$ be the unipotent radical of the Borel of G_2 . Let $g \in V(\overline{\mathbb{Z}}_p)$. If $p > 5$, then $g^p = \text{id mod } \varpi$.*

Proof. Let $P \supset B$ be the short root parabolic. Let $P = L \ltimes U$ be the Levi decomposition. Let $\pi : P \rightarrow L$ be the quotient. Say $\pi(g) = \begin{bmatrix} 1 & l \\ 0 & 1 \end{bmatrix}$. Fix a projection $P \rightarrow U$. Also fix a projection $U \rightarrow Z(U)$. Say the projection of g onto $U/Z(U) \cong \mathbb{A}^4$ via $P \rightarrow U \rightarrow U/Z(U)$ is (u_0, u_1, u_2, u_3) . Say the projection of g onto $Z(U) \cong \mathbb{A}^1$ via $P \rightarrow U \rightarrow Z(U)$ is u_4 .

For simplicity, we write $g = (l; u_0, u_1, u_2, u_3; u_4)$. We have, for any integer q ,

$$g^q = \left(ql; qu_0, -\frac{1}{2}q(q-1)u_0l + qu_1, -\frac{1}{6}q(q-1)(2q-1)u_0l^2 + q(q-1)u_1l + qu_2, \right. \\ \left. -\frac{1}{4}q^2(q-1)^2u_0l^3 + \frac{1}{2}q(q-1)(2q-1)u_1l^2 + \frac{3}{2}q(q-1)u_2l + qu_3, qu_4; \right. \\ \left. \frac{1}{120}(q-1)q(q+1)(3q^2-2)u_0^2l^3 - \frac{1}{2}(q-1)q(q+1)(u_1^2 + u_0u_2)l \right).$$

This can be computed by hand, and can be verified by a computer algebra system. The proposition follows from the above computation immediately. \square

The SageMath source code for computing is on the website sharkoko.space.

If we compute `cup_product_mod_p(5, 4, 4)` in SageMath notebook, we'll get an anti-lower-triangular matrix in the sense of Lemma A.0.1.

Acknowledgement

I would like to thank David Savitt, for suggesting to me the project of constructing crystalline lifts of Galois representations valued in general reductive groups, and for his excellent advising. I would like to thank Matthew Emerton for teaching me his work [Emerton and Gee 2023]. I also want to thank the referees for very careful reading and thank Joel Specter and Xiyuan Wang for helpful discussions.

References

- [Bellovin and Gee 2019] R. Bellovin and T. Gee, “ G -valued local deformation rings and global lifts”, *Algebra Number Theory* **13**:2 (2019), 333–378. MR Zbl
- [Böckle 2003] G. Böckle, “Lifting mod p representations to characteristics p^2 ”, *J. Number Theory* **101**:2 (2003), 310–337. MR Zbl
- [Caruso and Liu 2011] X. Caruso and T. Liu, “Some bounds for ramification of p^n -torsion semi-stable representations”, *J. Algebra* **325** (2011), 70–96. MR Zbl
- [Emerton and Gee 2023] M. Emerton and T. Gee, *Moduli stacks of étale (φ, Γ) -modules and the existence of crystalline lifts*, Ann. of Math. Stud. **215**, Princeton Univ. Press, 2023. MR Zbl
- [Fakhruddin et al. 2018] N. Fakhruddin, C. Khare, and S. Patrikis, “Lifting irreducible Galois representations”, preprint, 2018. arXiv 1810.05803
- [Gee et al. 2018] T. Gee, F. Herzig, and D. Savitt, “General Serre weight conjectures”, *J. Eur. Math. Soc.* **20**:12 (2018), 2859–2949. MR Zbl
- [Koch 2002] H. Koch, *Galois theory of p -extensions*, Springer, 2002. MR Zbl
- [Lin 2019] Z. Lin, “Extensions of crystalline representations valued in general reductive groups”, preprint, 2019, available at <https://sharkoko.space/pdf/unobs.pdf>.
- [Lin 2022] Z. Lin, “Crystalline lifts and a variant of the Steinberg–Winter theorem”, *Doc. Math.* **27** (2022), 2441–2468. MR Zbl
- [Lin 2023a] Z. Lin, “A Deligne–Lusztig type correspondence for tame p -adic groups”, preprint, 2023. arXiv 2306.02093
- [Lin 2023b] Z. Lin, “The Emerton–Gee stacks for tame groups, I”, preprint, 2023. arXiv 2304.05317
- [Lin 2023c] Z. Lin, “The Emerton–Gee stacks for tame groups, II”, preprint, 2023. arXiv 2309.05773
- [Lyndon 1950] R. C. Lyndon, “Cohomology theory of groups with a single defining relation”, *Ann. of Math. (2)* **52**:3 (1950), 650–665. MR Zbl
- [Muller 2013] A. Muller, *Relèvements cristallins de représentations galoisiennes*, Ph.D. thesis, Université de Strasbourg, 2013, available at <https://theses.hal.science/tel-00873407>.
- [Serre 2002] J.-P. Serre, *Galois cohomology*, Springer, 2002. MR Zbl
- [Stacks] “The Stacks project”, electronic reference, available at <http://stacks.math.columbia.edu>.

Communicated by Frank Calegari

Received 2021-08-25 Revised 2023-12-25 Accepted 2024-03-05

ygwcpoi@gmail.com

Northwestern University, Evanston, IL, United States

Algebra & Number Theory

msp.org/ant

EDITORS

MANAGING EDITOR
Antoine Chambert-Loir
Université Paris-Diderot
France

EDITORIAL BOARD CHAIR
David Eisenbud
University of California
Berkeley, USA

BOARD OF EDITORS

Jason P. Bell	University of Waterloo, Canada	Philippe Michel	École Polytechnique Fédérale de Lausanne
Bhargav Bhatt	University of Michigan, USA	Martin Olsson	University of California, Berkeley, USA
Frank Calegari	University of Chicago, USA	Irena Peeva	Cornell University, USA
J.-L. Colliot-Thélène	CNRS, Université Paris-Saclay, France	Jonathan Pila	University of Oxford, UK
Brian D. Conrad	Stanford University, USA	Anand Pillay	University of Notre Dame, USA
Samit Dasgupta	Duke University, USA	Bjorn Poonen	Massachusetts Institute of Technology, USA
Hélène Esnault	Freie Universität Berlin, Germany	Victor Reiner	University of Minnesota, USA
Gavril Farkas	Humboldt Universität zu Berlin, Germany	Peter Sarnak	Princeton University, USA
Sergey Fomin	University of Michigan, USA	Michael Singer	North Carolina State University, USA
Edward Frenkel	University of California, Berkeley, USA	Vasudevan Srinivas	SUNY Buffalo, USA
Wee Teck Gan	National University of Singapore	Shunsuke Takagi	University of Tokyo, Japan
Andrew Granville	Université de Montréal, Canada	Pham Huu Tiep	Rutgers University, USA
Ben J. Green	University of Oxford, UK	Ravi Vakil	Stanford University, USA
Christopher Hacon	University of Utah, USA	Akshay Venkatesh	Institute for Advanced Study, USA
Roger Heath-Brown	Oxford University, UK	Melanie Matchett Wood	Harvard University, USA
János Kollár	Princeton University, USA	Shou-Wu Zhang	Princeton University, USA
Michael J. Larsen	Indiana University Bloomington, USA		

PRODUCTION

production@msp.org
Silvio Levy, Scientific Editor

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2025 is US \$565/year for the electronic version, and \$820/year (+\$70, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online.

ANT peer review and production are managed by EditFLOW[®] from MSP.

PUBLISHED BY

 **mathematical sciences publishers**
nonprofit scientific publishing

<http://msp.org/>

© 2025 Mathematical Sciences Publishers

Algebra & Number Theory

Volume 19 No. 3 2025

The Lyndon–Demushkin method and crystalline lifts of G_2 -valued Galois representations ZHONGYIPAN LIN	415
Fermat’s last theorem over $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ MALEEHA KHAWAJA and FRAZER JARVIS	457
Moments in the Chebotarev density theorem: general class functions RÉGIS DE LA BRETÈCHE, DANIEL FIORILLI and FLORENT JOUVE	481
Abelian varieties over finite fields and their groups of rational points STEFANO MARSEGLIA and CALEB SPRINGER	521
Algebraic cycles and functorial lifts from G_2 to PGSp_6 ANTONIO CAUCHI, FRANCESCO LEMMA and JOAQUÍN RODRIGUES JACINTO	551