LYNDON-DEMUŠKIN METHOD AND CRYSTALLINE LIFTS OF G_2-VALUED GALOIS REPRESENTATIONS

LIN, ZHONGYIPAN

Abstract. 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 $\bar{\rho} : G_K \to G_2(\bar{\mathbb{F}}_p)$ admit a crystalline lift $\rho : G_K \to G_2(\bar{\mathbb{Z}}_p)$, where G_2 is the exceptional Chevalley group of type G_2.

Contents

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 $\bar{\rho} : G_K \to G(\bar{\mathbb{F}}_p)$ 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 multiple papers, for example, (i) irreducible geometric Galois representations [NCS18], (ii) the Serre weight conjecture [GHS18], (iii) ramification theory [CL11].

The pursuit of constructing characteristic 0 lifts of Galois representations (at least in higher dimensions) is, however, resistant to elementary techniques. [B03] is able to lift mod ϖ representations to a mod ϖ^2 one, for $G = \mathrm{GL}_N$. [Mu13] constructed crystalline lifts of mod ϖ represntations valued in $G = \mathrm{GL}_3$, and recently [EG19] worked the GL_N-case for all N. Our earlier work [Lin19] answers this question for semisimple representations valued in general reductive groups G.

The method of [EG19] is purely local, and is based on an analysis of Galois cohomology. In fact, they constructed a moduli stack of mod ϖ Galois representations and investigated how Galois cohomology behaves in families.

If one wants to work with a general reductive group, it seems inevitable to deal with Galois cohomology with non-abelian (in fact, unipotent) coefficients, and in order to construct crystalline lifts, one has to analyze either the integral structure of non-abelian Galois cohomology, or how non-abelian cohomology behaves in families. The main portion of this article is to carry out such an analysis when G is of type B_l, C_l, D_l and G_2.

1.1. Obstruction theory for crystalline lifting

If $\bar{\rho}(G_K)$ is an irreducible subgroup of $G(\bar{\mathbb{F}}_p)$ (that is, it is not contained in any proper parabolic subgroup of $G(\bar{\mathbb{F}}_p)$), then by our previous work [Lin19], $\bar{\rho}$ always admits a crystalline lift. So we assume $\bar{\rho}$ factors through a proper maximal parabolic P. Let $P = L \rtimes U_P$ be the Levi decomposition. Let $\bar{r} : G_K \to L(\bar{\mathbb{F}}_p)$ be the Levi factor of $\bar{\rho}$. Then $\bar{\rho}$ 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 $[c] \in H^1(G_K, U_P(\bar{\mathbb{Z}}_p))$ of $[\bar{c}]$.

In the GL_N-case, all maximal 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 non-abelian unipotent radical.

In this paper, we consider the case where U_P admits a quotient U such that

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

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 subsection 1.3).

Let $\operatorname{Spec} R$ be an irreducible component of a crystalline lifting ring $\operatorname{Spec} R_{\bar{r}}^{\mathrm{crys},\underline{\lambda}}$ (Definition 5.0.1) of $\bar{r}$. Let $r^{\mathrm{univ}} : G_K \to L(R)$ be the universal family. The Levi factor group acts on U via conjugation $\phi : L \to \mathrm{Aut}(U)$. Write $\phi^{\mathrm{ad}} : L \to \mathrm{GL}(U^{\mathrm{ad}})$ and $\phi^z : L \to \mathrm{GL}(Z(U))$ for the graded pieces of ϕ.

The theorem we prove is:

Theorem A (5.2.1). *Let $[\bar{c}] \in H^1(G_K, U(\mathbb{F}))$ be a characteristic p cocycle.*
Assume

[1] $H^2(G_K, \phi^{\mathrm{ad}}(r^{\mathrm{univ}}))$ *is sufficiently generically regular (Definition 5.1.1);*
[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-Demuškin (Definition 2.0.2); and*
[4] *There exists a $\bar{\mathbb{Z}}_p$-point of* $\operatorname{Spec} R$ *which is mildly regular (Definition 3.0.1) when restricted to $G_{K'}$.*

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

Remark [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 $\phi^{\mathrm{ad}}(\underline{\lambda})$ are slightly less then 0 (Definition 3.0.2).

1.1.1. Example: $G = \mathrm{GL}_3$

Let $\bar{\rho} : G_K \to \mathrm{GL}_3(\bar{\mathbb{F}}_p)$ 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 $\bar{r} : G_K \xrightarrow{\bar{\rho}} P(\bar{\mathbb{F}}_p) \to L(\bar{\mathbb{F}}_p)$ 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 $r^\circ : G_K \to \mathrm{GL}_2(\bar{\mathbb{Z}}_p)$ 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 $\bar{r} : G_K \to T(\bar{\mathbb{F}}_p)$ 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 non-abelian Galois cohomology.

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

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

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

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

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

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

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

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 Demuškin groups, there is an explicitly defined cochain complex (the so-called Lyndon-Demuškin 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-Demuškin complexes endowed with $G_K/G_{K'}$-action.

We have the following nice obstruction theory:

Theorem B (4.3.4)**.** *Assume $p \neq 2$. Let L be a reductive group over $\mathcal{O}_E$ and fix an algebraic group homomorphism $L \to \mathrm{Aut}(U)$. Let $r : G_K \to L(\mathcal{O}_E)$ 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-Demuškin and mildly regular, then there is a short exact sequence of pointed sets

$$H^1(G_K, U(\bar{\mathbb{Z}}_p)) \to H^1(G_K, U(\bar{\mathbb{F}}_p)) \xrightarrow{\delta} H^2(G_K, U^{\mathrm{ad}}(\bar{\mathbb{Z}}_p))$$

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

1.2. The existence of crystalline lifts for G_2

The exceptional group G_2 has (up to conjugacy) two maximal parabolics: the short root parabolic, and the long root parabolic. When $\bar{\rho} : G_K \to G_2(\bar{\mathbb{F}}_p)$ factors through the short root parabolic, we can directly apply Theorem A to construct a crystalline lift of $\bar{\rho}$. When $\bar{\rho} : G_K \to G_2(\bar{\mathbb{F}}_p)$ factors through the long root parabolic, we can apply Theorem A to construct a lift modulo the center of the unipotent radical U. If we assume furthermore that $\bar{\rho}$ does not factor through the short root parabolic, then by Tate local duality, $H^2(G_K, Z(U)(\mathbb{F})) = 0$, and it is unobstructed to extend the lift to the whole unipotent radical. Putting everything together, we have the following theorem:

Theorem C (7.2)**.** *Assume $p > 3$. Every mod ϖ Galois representation valued in the exceptional group G_2*

$$\bar{\rho} : G_K \to G_2(\bar{\mathbb{F}}_p)$$

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

Moreover, if $\bar{\rho}$ factors through a maximal parabolic $P = L \ltimes U$ and the Levi factor $\bar{r}_{\bar{\rho}} : G_K \to L(\bar{\mathbb{F}}_p)$ of $\bar{\rho}$ admits a Hodge-Tate regular and crystalline lift $r_1 : G_K \to L(\bar{\mathbb{Z}}_p)$ such that the adjoint representation $G_K \xrightarrow{r_1} L(\bar{\mathbb{Z}}_p) \to \mathrm{GL}(\mathrm{Lie}(U(\bar{\mathbb{Z}}_p)))$ has Hodge-Tate weights slightly less than $\underline{0}$, 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.

1.3. Crystalline lifting for classical groups

A maximal parabolic P of a (split) classical group $G = G(V, \langle, \rangle)$ of type B_l, C_l or D_l is the stablizer of an isotropic subspace $F \subset V$.

Let U_P be the unipotent radical of P. The Levi factor L of P acts on U_P by conjugation. Let λ be the similitude character of G. Fix an isomorphism $\iota : F \cong V/F^\perp$ such that $\langle x, \iota(x)\rangle = 1$ for all x. Then $\iota \otimes \lambda^{-1}$ is L-equivariant.

It is easy to see $U_P^{\mathrm{ad}} := U_P/Z(U_P) \cong \mathrm{Hom}_{\text{Vector space scheme}}(F^\perp/F, F)$ is an abelian group. Moreover, there exists an L-equivariant isomorphism

$$Z(U_P) = \mathrm{Hom}_{\text{Vector space scheme}}(V/F^\perp, F) \otimes \lambda^{-1}.$$

Note that ι induces an abelian group scheme morphism $\mathrm{tr}_\iota : Z(U_P) \to \mathbb{G}_a \otimes \lambda^{-1}$ which is L-equivariant. The quotient group $U := U_P/\ker \mathrm{tr}_\iota$ is a Heisenberg quotient, and thus our obstruction theory applies to it.

Let $\bar{\rho} : G_K \to P(\mathbb{F})$ be a mod ϖ Galois representation with Levi factor $\bar{r} : G_K \to L(\mathbb{F})$. We only need to consider the case where $\bar{\rho}$ is irreducible when restricted to the isotropic subspace F (otherwise replace F by a smaller isotropic subspace). In this case, tr_ι induces an isomorphism

$$H^2(G_K, Z(U_P)(\mathbb{F})) \cong H^2(G_K, \lambda^{-1} \otimes \mathbb{F})$$

by Schur's lemma and local Tate duality. By the long exact sequence of Galois cohomology, we have a bijection of obstructions $H^2(G_K, U_P(\bar{\mathbb{F}}_p)) \cong H^2(G_K, U(\bar{\mathbb{F}}_p))$ and thus the existence of crystalline lifts of $\bar{\rho}$ is equivalent to the existence of crystalline lifts of $\bar{\rho}$ modulo $\ker \mathrm{tr}_\iota$ by the main theorem of [Lin21].

So Theorem (A) and Theorem (B) suffice for classical groups. To establish the existence of crystalline lifts of mod ϖ representations valued in classical groups, we only need to establish a codimension estimate on the moduli stack of (ϕ, Γ)-modules valued in classical groups in the manner of section 6. Our method requires p to be coprime to the cardinality of the Weyl groups of proper Levi subgroups of G (due to Lemma 3.3.1.1, although the assumption on p can possibly be relaxed by Jannsen-Wingberg theory).

The moduli stack of étale ϕ-modules for general reductive groups is constructed in [Lin21B]. The moduli stack of (ϕ, Γ)-modules has not been constructed yet. The author has verified codimension estimates for many small rank groups (for example GSp_4 and GSp_6).

1.4. Organization In section 2, we review the results of Lyndon and Demuškin and establish some notations.

Section 3 and Section 4 form the technical heart of this paper.

Section 5 and Section 6 are mild generalizations of results from [EG19]. The proof is almost unchanged and we often just sketch the ideas of the proof and invite the readers to look at the proofs of [EG19].

We prove the main theorem in Section 7.

1.5. 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 advisoring. I would like to thank Matthew Emerton for teaching me his work [EG19]. I also want to thank Joel Specter and Xiyuan Wang for helpful discussions.

2. Lyndon-Demuškin 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 [Se02, Section II.5.6].

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

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

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.

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

2.1. Comparing cohomology of Demuškin groups and Galois cohomology

Let Γ^{disc} be the discrete group with one relator

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

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

Note that there is a functorial map

$$(\dagger) \;\; H^\bullet(G_K, A) \to H^\bullet(\Gamma^{\mathrm{disc}}, A)$$

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

2.1.1. Lemma Let $\mathbb{F}_p$ be the G_K-module with trivial G_K-action. Then (†) induces isomorphisms:
(1) $H^1(G_K, \mathbb{F}_p) = H^1(\Gamma^{\mathrm{disc}}, \mathbb{F}_p)$;
(2) $H^2(G_K, \mathbb{F}_p) = H^2(\Gamma^{\mathrm{disc}}, \mathbb{F}_p)$;

Proof. (1) We have

$$H^1(G_K, \mathbb{F}_p) = \mathrm{Hom}_{\mathrm{cont}}(G_K, \mathbb{F}_p);$$

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

Since $H^1(G_K, \mathbb{F}_p)$ classifies continuous extension classes of two trivial G_K-modules, (†) is injective. By local Euler characteristic, $\dim H^1(G_K, \mathbb{F}) = [K : \mathbb{Q}_p] + \dim H^0(G_K, \mathbb{F}) + \dim H^2(G_K, \mathbb{F}) = n + 2 = \dim H^1(\Gamma^{\mathrm{disc}}, \mathbb{F})$. So (†) is an isomorphism.

(2) We have a commutative diagram

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

Note that the first row is a non-degenerate pairing, and $H^2(G_K, \mathbb{F}) \cong \mathbb{F}$ by local Tate duality. By Lyndon's theorem or Corollary 2.2.0.3, we have $H^2(\Gamma^{\mathrm{disc}}, \mathbb{F}) \cong \mathbb{F}$. So it remains to show the cup product of the second row is non-trivial. Let $[c_1], [c_2] \in H^1(\Gamma^{\mathrm{disc}}, \mathbb{F}_p)$. $[c_1] \cup [c_2] = 0$ if and only if there exists a group homomorphism

$$\Gamma^{\mathrm{disc}} \to \begin{bmatrix} 1 & c_1 & * \\ & 1 & c_2 \\ & & 1 \end{bmatrix}$$

for some $*$. Define $c_i : \Gamma^{\mathrm{disc}} \to \mathbb{F}_p$ by sending x_i to 1 and other generators to 0, $i = 0, 1$. Then it is clear $[c_1] \cup [c_2] \neq 0$. □

2.1.2. Corollary Let A be a finite $\mathbb{F}_p$-vector space endowed with Lyndon-Demuškin 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

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

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 $H^2(G_K, A) = H^2(\Gamma^{\text{disc}}, A)$. □

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

2.1.3. Corollary Let A be a finite $\mathbb{Z}_p$-module endowed with Lyndon-Demuškin 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 $k > 0$,

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

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-Demuškin complex (see the last subsection of Section 2) computing $H^\bullet(\Gamma^{\text{disc}}, A)$ is the inverse limit of the Lyndon-Demïskin complex mod p^i. So $H^k(\Gamma^{\text{disc}}, A) = \varprojlim_i H^k(\Gamma^{\text{disc}}, A/p^i)$. □

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 Demuškin groups

The main reference of this subsection is [Ly50].

2.2.0.1 Derivations A derivation of a group G is a left G-module M, together with a map $D : G \to M$ 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 $\{dx_i | i = 1, \dots, m\}$.

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 $\frac{\partial u}{\partial x_i} \in \mathbb{Z}[F]$.

2.2.0.2 Theorem (Lyndon) 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

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

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

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

Proof. We have the following computation:

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

Since $H^2(\Gamma^{\text{disc}}, \mathbb{F}_p) = \frac{\mathbb{F}_p}{(\partial R/\partial x_0, \cdots, \partial R/x_{n+1})}$, it suffices to show

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

Since $\mathbb{F}_p$ is a trivial G_K-module, it is clear $\frac{\partial R}{\partial x_1} \mathbb{F}_p = \dots \frac{\partial R}{\partial x_{n+1}} \mathbb{F}_p = 0$. We also have $\frac{\partial R}{\partial x_0} = 1 + 1 + \cdots + 1 = q = 0 \bmod p$. ∎

2.2.1. Proposition 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

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

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

Proof. Combine Lemma 2.1.3 and Lyndon's theorem. □

2.3. Lyndon-Demuškin 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 the image of G_K in $\mathrm{Aut}(A)$ is a pro-p group.

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

Define $C^\bullet_{\mathrm{LD}}(A) = [C^0_{\mathrm{LD}}(A) \xrightarrow{d^1} C^1_{\mathrm{LD}}(A) \xrightarrow{d^2} C^2_{\mathrm{LD}}(A)]$ as the following cochain complex supported on degrees [0,2]

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

Then by [Ly50]

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

The idea of Lyndon Demuškin complex is simple. A 1-cochain $c \in C^1_{\mathrm{LD}}(A)$ is simply a set-theoretical function

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

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

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

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

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

be the single relation defining the Demuškin group. The differential operator $d^2 : C^1_{\mathrm{LD}}(A) \to C^2_{\mathrm{LD}}(A)$ 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 nilpotent (smooth connected) linear algebraic group over $\mathrm{Spec}\,\mathcal{O}_E$. Write

$$1 = U_0 \subset U_1 \dots \subset U_k = U$$

for the upper central series of U.

Assume $p > k$. There is a canonical isomorphism of schemes $U \cong \mathrm{Lie}\,U$ sending $g \mapsto \log g$. To define the logarithm function, it is convenient to choose an embedding $U \hookrightarrow \mathrm{GL}_N$, and define log using the commutative diagram

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

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

Fix a Galois action $G_K \to \mathrm{Aut}(U)(\mathcal{O}_E)$ 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 *non-abelian crossed homomorphism* valued in $U(A)$ is a map $c : G_K \to U(A)$ such that

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

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

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

Our definition of the Lyndon-Demuškin cochain complex is motivated by (†).

2.3.2.1 Definition Let A be an $\mathcal{O}_E$-algebra. The Lyndon-Demuškin complex with nilpotent coefficients is defined to be the following cochain complex $C^\bullet_{\mathrm{LD}}(U(A))$ supported on degrees [0,2]:

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

where d^1 is defined by

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

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

$$c : \langle x_0, \cdots, x_{n+1} \rangle \to \operatorname{Lie} U(A)$$

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

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

2.3.2.2 Remark (1) When U is an abelian group, then we recover the definition in the previous section;

(2) The main reason we define $C^\bullet_{\mathrm{LD}}(U(A))$ this way is because we want to compare it with $C^\bullet_{\mathrm{LD}}(\operatorname{Lie} U(A))$.

Note that $C^\bullet_{\mathrm{LD}}(\operatorname{Lie} U(A))$ and $C^\bullet_{\mathrm{LD}}(U(A))$ 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 $\mathfrak{c} : G_K \to \operatorname{Lie} U(A)$ in the sense of (†).

(4) The differential maps are generally non-linear.

2.3.2.3 Definition We define $Z^i_{\mathrm{LD}} := (d^i)^{-1}(0)$, and $B^i_{\mathrm{LD}} := d^i(C^{i-1}_{\mathrm{LD}})$ for $i = 0, 1, 2$.

2.3.2.4 Proposition We have

$$H^0(G_K, U) \cong Z^0_{\mathrm{LD}}(U(A))$$

and a surjection of pointed sets

$$Z^1_{\mathrm{LD}}(U(A)) \to H^1(G_K, U(A)).$$

Proof. Immediate from definitions. □

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

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

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

It is not hard to see $Q(-)$ is a quadratic form (we fully expand $\tilde{c}(R)$ using the Baker-Campbell-Hausdorff formula, and only keep the terms which are Lie brackets).

We define

$$\begin{aligned} C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(A)) \times C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(A)) &\xrightarrow{\cup} C^2_{\mathrm{LD}}(Z(U)(A)) \\ x \cup y &:= \frac{1}{2}(Q(x+y) - Q(x) - Q(y)) \end{aligned}$$

which is a symmetric bilinear form.

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

2.3.3.1 Lemma Under the identification $C^1_{\mathrm{LD}}(U(A)) = C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(A)) \oplus C^1_{\mathrm{LD}}(Z(U)(A))$, we have

$$Z^1_{\mathrm{LD}}(U(A)) = \{(x, y) \in C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(A)) \oplus C^1_{\mathrm{LD}}(Z(U)(A)) | d^2 x = 0,\ x \cup x + d^2 y = 0\}.$$

Proof. It is obvious from the definition of d^2 and Q. The projection of $d^2(x, y)$ to $C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(A))$ is $d^2 x$; and the projection of $d^2(x, y)$ to $C^1_{\mathrm{LD}}(Z(U)(A))$ is $x \cup x + d^2 y$. □

Write $H^1_{\mathrm{LD}}(U^{\mathrm{ad}})(A)$ for $Z^1_{\mathrm{LD}}(U^{\mathrm{ad}})(A)/B^1_{\mathrm{LD}}(U^{\mathrm{ad}})(A)$.

2.3.3.2 Lemma The pairing $\cup$ on the cochain level induces a symmetric pairing on the cohomology level

$$H^1_{\mathrm{LD}}(U^{\mathrm{ad}}(A)) \times H^1_{\mathrm{LD}}(U^{\mathrm{ad}}(A)) \xrightarrow{\cup} H^2_{\mathrm{LD}}(Z(U)(A)).$$

Proof. It suffices to show for all $x \in Z^1_{\mathrm{LD}}(U^{\mathrm{ad}})(A)$ and $y \in B^1_{\mathrm{LD}}(U^{\mathrm{ad}})(A)$, $Q(x + y) - Q(x) \in B^2_{\mathrm{LD}}(Z(U)(A))$.

Let $\tilde{x} \in C^1_{\mathrm{LD}}(U(A))$ be the unique extension of x such that $\mathrm{pr}\,\tilde{x} = 0$. The cocycle $\tilde{x}$ represents a group homomorphism $\rho_{\tilde{x}} : \langle x_0, \cdots, x_{n+1}\rangle \to U(A) \rtimes \langle x_0, \cdots, x_{n+1} | R\rangle$ such that $\rho_{\tilde{x}}(R) = 1 \bmod Z(U)(A)$. 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 have $n\rho_{\tilde{x}}(R) n^{-1} \rho_{\tilde{x}}(R)^{-1} = 1 \in U(A) \rtimes \langle x_0, \cdots, x_{n+1} | R\rangle$ 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 $Q(x+y) - Q(x) = d^2 f \in B^2_{\mathrm{LD}}(Z(U)(A))$. □

Recall $Z^1_{\mathrm{LD}}(U(A))$ and $Z^1_{\mathrm{LD}}(\operatorname{Lie} U(A))$ are both subsets of $C^1_{\mathrm{LD}}(U(A))$.

2.3.3.3 Lemma If $Z(U)(\mathbb{F}) \cong \mathbb{F}$, then

$$Z^1_{\mathrm{LD}}(U(\mathbb{F})) \subset Z^1_{\mathrm{LD}}(\operatorname{Lie} U(\mathbb{F}))$$

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

Proof. We have remarked in 2.3.2.2(2) that $C^1_{\mathrm{LD}}(U(\mathbb{F}))$ and $C^1_{\mathrm{LD}}(\mathrm{Lie}\,U(\mathbb{F}))$ have the same underlying space. By Lemma 2.3.3.1, an element of $Z^1_{\mathrm{LD}}(U(\mathbb{F}))$ is a pair (x, y) such that $d^2x = 0$ and $x \cup x + d^2y = 0$. By our assumption, $C^2_{\mathrm{LD}}(Z(U)(\mathbb{F})) = H^2(G_K, Z(U)(\mathbb{F}))$ and thus $B^2_{\mathrm{LD}}(Z(U)(\mathbb{F})) = 0$. So $d^2y = 0$ automatically, and (x, y) defines an element of $Z^1_{\mathrm{LD}}(\mathrm{Lie}\,U(\mathbb{F}))$. □

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 nilpotent group of class 2 over $\mathrm{Spec}\,\mathcal{O}_E$, with center $Z(U) \cong \mathbb{G}_a$. Write U^{ad} for $U/Z(U)$.

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

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

(MR2) The bilinear pairing

$$\cup_{\mathbb{F}} : C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F})) \times C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F})) \to C^2_{\mathrm{LD}}(Z(U)(\mathbb{F}))$$

is non-degenerate.

3.0.1.1 Remark 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 notations 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 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 $p \geqslant 5$.

3.0.2. Definition Given a tuple of labeled Hodge-Tate weights $\underline{\lambda}$, we say $\underline{\lambda}$ is slightly less than 0 if for each $\sigma : K \hookrightarrow \bar{\mathbb{Q}}_p$, λ_σ consists of non-positive integers, and for at least one σ, λ_σ consists of negative integers. (The cyclotomic character has Hodge-Tate weight -1.)

3.0.3. Proposition Assume $p \geqslant 5$. 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 $G_{K'} \to \mathrm{Aut}(U)(\mathcal{O}_E)$ is mildly regular if $U^{\mathrm{ad}}(E)$ is Hodge-Tate of labeled Hodge-Tate weights slightly less then 0.

Proof. If $H^0(G_{K'}, U^{\mathrm{ad}}(E)) \neq 0$, then for all label $\sigma : K \hookrightarrow \bar{\mathbb{Q}}_p$, $0 \in \lambda_\sigma$.

The proposition now follows from Proposition 3.0.1.1. □

3.1. Cup products mod ϖ

3.1.1. Lemma The image of $Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E)) \to C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F}))$ has codimension at most $\dim_E U^{\mathrm{ad}}(E)$.

Proof. Say $\dim_{\mathbb{F}} C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F})) = \mathrm{rank}_{\mathcal{O}_E} C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E)) = N$.

Since $Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E))$ is the kernel of $C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E)) \to C^2_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E))$, and $\mathrm{rank}_{\mathcal{O}_E} C^2_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E)) = \dim_E U^{\mathrm{ad}}(E)$, we have

$$\mathrm{rank}_{\mathcal{O}_E} Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E)) \geqslant N - \dim_E U^{\mathrm{ad}}(E).$$

Since $C^2_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E))$ is torsion-free, $Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E))$ is saturated in $C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E))$, and is thus a direct summand. In particular, the image of $Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E))$ in $C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F}))$ has dimension $\geqslant N - \dim_E U^{\mathrm{ad}}(E)$. □

3.1.2. Lemma If

$$\cup_{\mathbb{F}} : C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F})) \times C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F})) \to C^2_{\mathrm{LD}}(Z(U)(\mathbb{F}))$$

is non-degenerate, then the kernel of

$$\cup_{\mathbb{F}} : Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E))/\varpi \times Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E))/\varpi \to C^2_{\mathrm{LD}}(Z(U)(\mathbb{F}))$$

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

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

Proof. For ease of notation, write C for $C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F}))$, and write Z for the image of $Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E))$ in C. Note that $Z \cong Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E))/\varpi$ 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 non-degenerate, 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 non-degenerate. Since $F \cap Z = 0$, $\dim C \geqslant \dim(F + Z) = \dim Z + \dim F = \dim Z + \dim K$. The lemma now follows from the previous lemma. □

We also record the following lemma whose proof is similar.

3.1.3. Lemma (1) The image of $Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F})) \to C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F}))$ has codimension at most $\dim_E U^{\mathrm{ad}}(E)$.

(2) If

$$\cup_{\mathbb{F}} : C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F})) \times C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F})) \to C^2_{\mathrm{LD}}(Z(U)(\mathbb{F}))$$

is non-degenerate, then the kernel of

$$\cup_{\mathbb{F}} : Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F})) \times Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F})) \to C^2_{\mathrm{LD}}(Z(U)(\mathbb{F}))$$

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

3.2. General cup products in group cohomology

In this subsection, we give a reinterpretation of Definition 2.3.3, 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 $\theta : \Gamma \to \mathrm{Aut}(V)(\mathcal{O}_E)$. By the Lie correspondence, $\mathrm{Aut}(\mathrm{Lie}\, V) \cong \mathrm{Aut}(V)$, and thus θ induces a $\mathcal{O}_E$-linear Γ-action on $\mathrm{Lie}\, V$ which respects Lie brackets.

We fix a grading $\mathrm{Lie}\, V = V_1 \oplus V_2$ 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 $f : \Gamma \to V$ 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

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

3.2.1. Lemma 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

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

□

For crossed homomorphisms $a \in H^1(\Gamma, V_1)$, define $Q(a) := B(a, a)$. By comparing $(*)$ and paragraph 2.3.3, it is not hard to see the $Q(-)$ defined in this subsection coincides with that of 2.3.3 for 1-cocycles when Γ is the discrete Demuškin 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 the 2.3.3 when the settings overlap.

3.2.2. Lemma Let $\Gamma' \subset \Gamma$ be a normal subgroup of finite index. Write Δ for Γ/Γ'.

The cup product $\cup : H^1(\Gamma', V_1) \times H^1(\Gamma', V_1) \to H^2(\Gamma', V_2)$ is Δ-equivariant.

Proof. Let $a, b \in H^1(\Gamma^1, V_1)$, 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 [Se02, Section I.5.8]). We immediately have $\sigma \cdot B(a, b) = B(\sigma \cdot a, \sigma \cdot b)$. □

3.2.3. Example: the completely split case In this paragraph we analyze the special case where the $G_{K'}$ action on $U^{\mathrm{ad}}(\mathbb{F})$ 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 $\mathrm{Lie}\, U$ is one-dimensional, the Lie bracket

$$U^{\mathrm{ad}}(\mathbb{F}) \times U^{\mathrm{ad}}(\mathbb{F}) \xrightarrow{[-,-]} Z(U)(\mathbb{F})$$

is a non-degenerate, alternating pairing. Choose a basis $\{e_1, \cdots, e_k, e'_1, \cdots, e'_k\}$ of $U^{\mathrm{ad}}(\mathbb{F})$ 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 $U^{\mathrm{ad}}(\mathbb{F})$ is trivial, the cup product

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

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

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

Write $\wedge$ for the usual cup product $H^1(G_{K'}, \mathbb{F}) \times H^1(G_{K'}, \mathbb{F}) \to H^2(G_{K'}, \mathbb{F})$ 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 $a_1, b_1, a_2, b_2 \in H^1(G_{K'}, \mathbb{F})$

$$B(a_1e_i + b_1e_i', a_2e_i + b_2e_i') = 2(a_1 \wedge b_2 + a_2 \wedge b_2)$$

Since $\wedge$ is a non-degenerate pairing, B is also a non-degenerate pairing.

3.3. Nontriviality of cup products

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

If $r|_{G_{K'}}$ is Lyndon-Demuškin and mildly regular, then one of the following are true:

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

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

is non-trivial.

Remark Note that $H^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E) \cong H^1(G_{K'}, U^{\mathrm{ad}}(\mathcal{O}_E))$, and $H^1(G_{K'}, U^{\mathrm{ad}}(\mathcal{O}_E))^{G_K} = H^1(G_K, U^{\mathrm{ad}}(\mathcal{O}_E))$. The symmetric pairing in the theorem is the restriction to $H^1(G_{K'}, U^{\mathrm{ad}}(\mathcal{O}_E))$ of the symmetric pairing defined in Lemma 2.3.3.2.

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

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

By Lemma 3.1.2, the kernel of

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

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

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

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

is contained in the kernel of

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

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

By the local Euler characteristic,

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

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

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

If $K\neq\mathbb{Q}_p$, then

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

and (iii) must be true.

Case $H^2(G_K,U^{\mathrm{ad}}(\mathbb{F}))=0$. By Nakayama's Lemma, $H^2(G_K,U^{\mathrm{ad}}(\mathcal{O}_E))=0$. By [EG19], there exists a perfect $\mathcal{O}_E$-complex $[C^0\to C^1\to C^2]$ concentrated in degrees $[0,2]$ which computes $H^\bullet(G_K,U^{\mathrm{ad}}(\mathcal{O}_E))$. By the universal coefficient theorem, there exists a short exact sequence

$$0\to H^1(C^\bullet)\otimes\mathbb{F}\to H^1(C^\bullet\otimes\mathbb{F})\to Tor_1^{\mathcal{O}_E}(H^2(C^\bullet),\mathbb{F})\to 0$$

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

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

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

$$(*)\qquad h^1=\dim_E U^{\mathrm{ad}}(E)[K:\mathbb{Q}_p]+\dim_{\mathbb{F}} H^0(G_K,U^{\mathrm{ad}}(\mathbb{F})).$$

By Lemma 3.1.3, the kernel k_Z of

$$Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F}))\times Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F}))\to H^2(G_{K'},Z(U)(\mathbb{F}))$$

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

$$(**)\qquad \dim k_Z\geqslant \dim H^1(G_K,U^{\mathrm{ad}}(\mathbb{F}))+\dim B^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F}))=h^1+\dim B^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F})).$$

Combining $(*)$ and $(**)$, we have

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

So we conclude that

$$\begin{aligned} 1 &= [K : \mathbb{Q}_p] \\ 0 &= H^0(G_K, U^{\mathrm{ad}}(\mathbb{F})) \\ 0 &= B^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F})) \end{aligned}$$

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

Theorem 3.3.1 is used in the following scenerio.

3.3.1.1 Lemma Let L be a split reductive group over $\mathbb{F}$. Let $r : G_K \to L(\mathbb{F})$ be a Galois representation valued in L. Let r^{ss} be the semi-simplification 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 [Lin19], r^{ss} is tamely ramified and factors through the normalizer of a maximal torus of L (after possibly extending the base field). □

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-Demuškin since it has trivial semi-simplification.

4. Non-abelian obstruction theory via Lyndon-Demuškin 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

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

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 $\phi : L \to \mathrm{Aut}(U)$ throughout this section. In particular, there is a Galois action $\phi(r^\circ) : G_K \xrightarrow{r^\circ} L(\mathcal{O}_E) \xrightarrow{\phi(\mathcal{O}_E)} \mathrm{Aut}(U)(\mathcal{O}_E)$. We will talk about non-abelian 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 $\mathrm{Gal}(K'/K)$. Set $\Gamma := G_K$, and $H := G_{K'}$.

4.1. Non-abelian inflation-restriction

Let R be either $\mathcal{O}_E$ or $\mathbb{F}$. For ease of notation, write U for $U(R)$.

4.1.0.1 Non-abelian Galois cohomology We recall a few facts about the non-abelian version of Galois cohomology. Let Γ be a (profinite) group Let

$$0 \to A \to B \to C \to 0$$

be a short exact sequence of groups with continuous Γ-action. If $A \to B$ is *central*, that is, A is contained in the center of B, then we have a long exact sequence ([Se02, Proposition 43, 5.7])

$$\begin{aligned} 1 &\to A^\Gamma \to B^\Gamma \to C^\Gamma \\ &\to H^1(\Gamma, A) \to H^1(\Gamma, B) \to H^1(\Gamma, C) \\ &\xrightarrow{\delta} H^2(\Gamma, A) \end{aligned}$$

Let $H \subset G$ be a closed normal subgroup. Then there is an exact sequence ([Se02, 5.8])

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

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

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

4.1.0.2 Theorem [Ko02, 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 $n \geqslant 1$, and the restriction

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

is an isomorphism.

The fact above implies the following diagram with exact columns

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

4.1.0.3 Proposition The restriction map of non-abelian 1-cocycles

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

is a bijection.

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

4.1.0.4 Representation-theoretic interpretation of non-abelian 1-cocycles Let P be a group which is a semi-direct product $L \ltimes U$. Let $q_L : P \to L$ be the quotient map. Fix a section $L \to P$ of q_L, which allows us to identify (set-theoretically) P with $U \times L$. For $g \in \Gamma$, write $g = g_U g_L$ such that $g_U \in U \times \{1\}$ and $g_L \in \{1\} \times L$. Let Γ be a profinite group. Let $\bar{\tau} : \Gamma \to L$ be a group homomorphism. Let $\tau : \Gamma \to P$ be a lifting of $\bar{\tau}$. Set $c := q_U \circ \tau : \Gamma \to U$. Then

$$\begin{aligned} c(gh) &= q_U(\tau(g)\tau(h)) = q_U(\tau(g)_U\tau(g)_L\tau(h)_U\tau(h)_L) \\ &= q_U(\tau(g)_U\tau(g)_L\tau(h)_U\tau(g)_L^{-1}\tau(gh)_L) \\ &= c(g)(\tau(g)_L c(h)\tau(g)_L^{-1}) \\ &=: c(g)(\tau(g)_L \cdot c(h)) \end{aligned}$$

is a (non-abelian) crossed homomorphism. So $H^1(\Gamma, U)$ classifies liftings τ of $\bar{\tau}$ up to equivalence.

4.1.1. 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 4.1.0.3.

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

4.1.1.1 Lemma If there exists $[c_h] \in H^1(H, U(\mathcal{O}_E))$ and $[d] \in H^1(\Gamma, U^{\mathrm{ad}}(\mathcal{O}_E))$ such that

- $\alpha_2([c_h]) = \mathrm{res}([d])$ and
- $[c_h|_H] \bmod \varpi = [\bar{c}|_H]$

then there exists $[c] \in H^1(\Gamma, U(\mathcal{O}_E))$ which is a lifting of $[\bar{c}]$.

$$\begin{array}{ccccc}
 & H^1(\Gamma, Z(U)) & \overset{}{\underset{\text{res}}{\hookrightarrow}} & H^1(H, Z(U)) & \\
 & \downarrow & & \downarrow & \\
 & H^1(\Gamma, U) & \underset{\text{res}}{\hookrightarrow} & H^1(H, U) & \ni [c_h] \\
 & \downarrow{\scriptstyle \alpha_1} & & \downarrow{\scriptstyle \alpha_2} & \\
[d] \in & H^1(\Gamma, U^{\mathrm{ad}}) & \underset{\text{res}}{\longrightarrow} & H^1(H, U^{\mathrm{ad}}) & \\
 & \downarrow{\scriptstyle \delta_1} & & \downarrow{\scriptstyle \delta_2} & \\
 & H^2(\Gamma, Z(U)) & \hookrightarrow & H^2(H, Z(U)) &
\end{array}$$

Proof. Since

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

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

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

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

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

Therefore

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

and $[\bar{c}'] - [\bar{c}]$ has a characertistic 0 lift $[x]$, and $[c] := [c'] - [x]$ is a lift of $[\bar{c}]$. ☐

The purpose of the whole Section 4 is to prove an upgrade of the above lemma, (that is, Theorem 4.3.2).

4.2. External Galois action on the Lyndon-Demuškin 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

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

is Lyndon-Demuškin. We have a Lyndon-Demuškin complex $C^{\bullet}_{\mathrm{LD}}(U(\mathcal{O}_E))$ computing $H^{\bullet}(H, U(\mathcal{O}_E))$. Recall that a 1-cocycle $c \in C^1_{\mathrm{LD}}(U(\mathcal{O}_E))$ is the same as a function

$$\mathfrak{c} : \langle x_0, \cdots, x_{n+1} \rangle \to (\mathrm{Lie}\, U)(\mathcal{O}_E)$$

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

such that

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

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

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

such that

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

for all g, h.

A cochain $c : \langle x_0, \cdots, x_{n+1} \rangle \to U(\mathcal{O}_E)$ lies in $Z^1_{\mathrm{LD}}(U(\mathcal{O}_E))$ if and only if it factors through the (discrete) Demuškin group $\langle x_0, \cdots, x_{n+1} | R \rangle$.

Let $c \in Z^1_{\mathrm{LD}}(\mathcal{O}_E)$, regarded as a function $\langle x_0, \ldots, x_{n+1} | R \rangle \to U(\mathcal{O}_E)$. 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

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

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

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

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

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.

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

4.2.0.2 Digression We conjecture that the cup product

$$\cup : Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E)) \times Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E)) \to C^2_{\mathrm{LD}}(Z(U(\mathcal{O}_E)))$$

is compatible with G_K-action.

This conjecture would hold, for example, if for each $g \in G_K$, the conjugation by g

$$\phi_g : G_{K'} \to G_{K'}$$

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

$$\phi_g : \langle x_0, \cdots, x_{n+1} \rangle \to \langle x_0, \cdots, x_{n+1} \rangle.$$

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 is induced by a homeomorphism. The algebraic version of Dehn-Nielsen can be formualted as, under the usual presentation of $F = \langle a_1, b_1, \cdots, a_g, b_g \rangle \to \langle a_1, b_1, \cdots, a_g, b_g | [a_1, b_1] \cdots [a_g, b_g] \rangle \cong \pi_1(M_g)$, all automorphism of $\pi_1(M_g)$ is induced from an automorphism of the free group F.

Conjecture Dehn-Nielsen holds for $\operatorname{Spec} K$.

Assume $Z(U(\mathcal{O}_E)) \cong \mathcal{O}_E$ from now on.

4.3. Constructing non-abelian cocycles

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

$$\begin{aligned}(Z^1_{LD})^\Delta &:= \{x \in Z^1_{\mathrm{LD}} | \text{image of } x \text{ in } H^1 \text{ is contained in } (H^1)^\Delta\} \\ &= \{x \in Z^1_{\mathrm{LD}} | g \cdot x - x \in B^1_{\mathrm{LD}} \text{ for all } g \in G_K\}\end{aligned}$$

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

We keep all notations from the previous subsections.

Assume $Z(U)(\mathcal{O}_E) = \mathcal{O}_E$ from now on.

We fix some notations. The quotient $U \to U/Z(U) = U^{\mathrm{ad}}$ induces maps $\mathrm{ad} : Z^1_{\mathrm{LD}}(U(\mathcal{O}_E)) \to Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E))$.

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

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

is non-trivial.

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

Proof. Pick an arbitrary lift $f \in C^1_{\mathrm{LD}}(Z(U)(\mathcal{O}_E))$ 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, we assume $c' \in Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\bar{\mathbb{Z}}_p))^\Delta$.

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

Since the symmetric bilinear pairing $(\dagger)$ is non-trivial, there exists $y \in Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E))^\Delta$ such that $y \cup y \neq 0 \bmod \varpi$. 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. Set $(c, f) := (c' + \lambda_0 y, f)$.

We have $(c, f) \in Z^1_{\mathrm{LD}}(U(\bar{\mathbb{Z}}_p))$ by Lemma 2.3.3.1 and $c \in Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\bar{\mathbb{Z}}_p))^\Delta$. □

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

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

is non-trivial.

Let $[(\bar{c}, \bar{f})] \in H^1(G_K, U(\mathbb{F}))$ be a characteristic p cocycle. If $[\bar{c}|_{G_{K'}}] \in H^1(G_{K'}, U^{\mathrm{ad}}(\mathbb{F}))$ admits a characteristic 0 lift in $H^1(G_{K'}, U^{\mathrm{ad}}(\bar{\mathbb{Z}}_p))$, 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 $(\bar{c}, \bar{f}) \in Z^1_{\mathrm{LD}}(U(\mathbb{F}))$ which defines the cohomology class $[(\bar{c}, \bar{f})]$. Clearly $\bar{c} \in Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F}))^{\Delta}$. Say $[d] \in H^1(G_{K'}, U^{\mathrm{ad}}(\bar{\mathbb{Z}}_p))$ is a lift of $[\bar{c}]$, which is defined by $d \in Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\bar{\mathbb{Z}}_p))$. Write $\bar{d}$ for the image of d in $Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\bar{\mathbb{F}}_p))$. By changing d by a coboundary, we can assume $\bar{d} = \bar{c}$.

Lemma 4.3.1 produces $(c, f) \in Z^1_{\mathrm{LD}}(U(\bar{\mathbb{Z}}_p))$ such that $c \in Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\bar{\mathbb{Z}}_p))^{\Delta}$. Now the theorem follows from Lemma 4.1.1.1. □

Theorem 4.3.2 is saying when U is a nilpotent group of class 2 with 1-dimensional center, there exists a short exact sequence of pointed sets

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

under technical assumptions.

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

4.3.3. Theorem Assume $p \neq 2$. Let $r : G_K \to L(\mathcal{O}_E)$ be a continuous group homomorphism. Let K'/K be a finite Galois extension of prime-to-p degree such that $r|_{G_{K'}}$ is Lyndon-Demuškin and mildly regular.

There is a short exact sequence of pointed sets

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

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

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

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

Case II: $H^2(G_K, Z(U)(\mathbb{F})) = 0$. By Nakayama's lemma, $H^2(G_K, Z(U)(\bar{\mathbb{Z}}_p)) = 0$.

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

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

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

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

4.3.4. Corollary Assume $p \neq 2$. Let $r : G_K \to L(\mathcal{O}_E)$ 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-Demuškin and mildly regular, then there is a short exact sequence of pointed sets

$$H^1(G_K, U(\bar{\mathbb{Z}}_p)) \to H^1(G_K, U(\bar{\mathbb{F}}_p)) \xrightarrow{\delta} H^2(G_K, U^{\mathrm{ad}}(\bar{\mathbb{Z}}_p))$$

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

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

5. The Machinery for lifting non-abelian 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. Crystalline lifting rings Let L be a connected reductive group over $\mathcal{O}_E$, and $\bar{r} : G_K \to L(\mathbb{F})$ be a mod ϖ representation. Let $\underline{\lambda}$ be a Hodge type. The crystalline lifting ring $R_{\bar{r}}^{\mathrm{crys},\underline{\lambda},\mathcal{O}}$ of $\bar{r}$ of p-adic Hodge type $\underline{\lambda}$ is constructed in [BG19, Theorem 3.3.8]. It is an $\mathcal{O}$-flat quotient of the universal lifting ring, and has generic fiber equidimensional of dimension $\dim_E L + \dim_E \mathrm{Res}_{K\otimes E/K} L/P_{\underline{\lambda}}$ where $P_{\underline{\lambda}}$ is the parabolic subgroup determined by the p-adic Hodge type $\underline{\lambda}$. If $\underline{\lambda}$ is a regular p-adic Hodge type, $P_{\underline{\lambda}}$ is a Borel subgroup.

5.1. A geometric argument of Emerton-Gee

5.1.1. Definition Let $\mathcal{F}$ be a coherent sheaf over a scheme X. We say $\mathcal{F}$ is *sufficiently generically regular* (= SGR) if for each $s \geqslant 0$, the locus

$$X_s := \{x \in \mathrm{Spec}\, R |\dim \kappa(x) \otimes_R \mathcal{F} \geqslant s\}$$

has codimension $\geqslant s+1$ in $\mathrm{Spec}\, R$.

5.1.2. Theorem Let $X = \mathrm{Spec}\, R$ be an irreducible component of a crystalline lifting ring of $\bar{r}$. Let $r^{\mathrm{univ}} : G_K \to L(R)$ be the universal family of Galois representations on X. Assume $X[1/p] \neq \varnothing$. Let $F : L \to \mathrm{GL}(V)$ be an algebraic representation where V is a vector space scheme over $\mathcal{O}_E$.

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

Proof. The proof is almost identical to that of [EG19, Theorem 6.3.2].

Instead of repeating their argument, we would like to explain the main ideas behind the proof, and why we need the sufficiently generically regular condition.

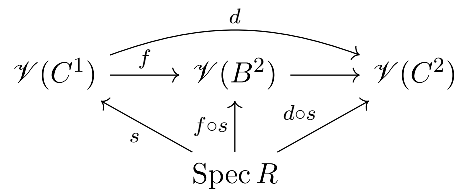
We have a complex of finitely generated projective modules concentrated on degree [0, 2]

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

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

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

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



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

It turns out $\bar{c} \in \ker(C^1/\varpi \to C^2/\varpi)$ admits a lift in Z^1, as long as the section $f \circ s$ intersects with the identity section $e_{\mathscr{V}(B^2)}$ of $\mathscr{V}(B^2)$. The intersection $(d \circ s) \cap e_{\mathscr{V}(C^2)}$ should occur above a codimension 1 locus of $\operatorname{Spec} R$. 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 $x \in \operatorname{Spec} R$ outside of the support of H^2, and we are done. Of course, we oversimplified the situation, see [EG19] for a complete account. □

5.2. A non-abelian lifting theorem

5.2.1. Theorem 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 $\phi : L \to \operatorname{Aut}(U)$ with graded pieces $\phi^{\mathrm{ad}} : L \to \operatorname{GL}(U^{\mathrm{ad}})$ and $\phi^{z} : L \to \operatorname{GL}(Z(U))$.

Fix a mod ϖ representation $\bar{r} : G_K \to L(\mathbb{F})$. Let $[\bar{c}] \in H^1(G_K, U(\mathbb{F}))$ be a characteristic p cocycle. Let $\operatorname{Spec} R$ be an irreducible component of a crystalline lifting ring of $\bar{r}$.

Assume

[1] $H^2(G_K, \phi^{\mathrm{ad}}(r^{\mathrm{univ}}))$ is SGR;

[2] $p \neq 2$;

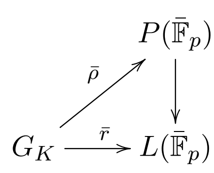
[3] There exists a finite Galois extension K'/K of prime-to-p degree such that $\phi(\bar{r})|_{G_{K'}}$ is Lyndon-Demuškin; and

[4] There exists a $\bar{\mathbb{Z}}_p$-point of $\operatorname{Spec} R$ which is mildly regular when restricted to $G_{K'}$. (In particular, $\operatorname{Spec} R[1/p] \neq 0$.)

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

Proof. Combine Theorem 5.1.2 and 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 $\bar{\rho} : G_K \to G(\mathbb{F})$ be a mod ϖ representation. Assume $\bar{\rho}$ factors through a parabolic $P \subset G$, with Levi decomposition $P = L \ltimes U$. Denote by $\phi : L \to \operatorname{Aut}(U)$ the conjugation action. We assume U is nilpotent of class 2, so U^{ad} is an abelian group. Write $\bar{r}$ for the Levi factor of $\bar{\rho}$.



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.

5.3.1. Proposition 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 $V \to V^{\mathrm{ad}}$ induces a map $\mathrm{ad} : H^1(G_K, V) \to H^1(G_K, V^{\mathrm{ad}})$. Assume $H^2(G_K, Z(V)(\bar{\mathbb{F}}_p)) = 0$.

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

Proof. By [Se02, Proposition 43], since $Z(V)$ is a central normal subgroup of V, there exists a long exact sequence of pointed sets

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

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 $\mathrm{ad}([\bar{c}]) = \mathrm{ad}([c']) \mod \varpi$. Write $[\bar{c}']$ for $[c'] \mod \varpi$. 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 $[\bar{c}]$. ☐

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 [EG19]. For each $d > 0$, [EG19] constructed the moduli stack $\mathcal{X}_d = \mathcal{X}_{K,d}$ of projection étale (ϕ, Γ_K)-modules of rank d.

We prove a mild generalization of [EG19, Proposition 5.4.4(1)].

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

$$\eta : (\mathcal{X}_{a,\mathrm{red}})_{\bar{\mathbb{F}}_p} \times (\mathcal{X}_{d,\mathrm{red}})_{\bar{\mathbb{F}}_p} \to (\mathcal{X}_{ad,\mathrm{red}})_{\bar{\mathbb{F}}_p}$$

sending a pair of (ϕ, Γ)-modules M, N to their hom module $\mathrm{Hom}_{\phi,\Gamma}(M, N)$. 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 $t \in T(\bar{\mathbb{F}}_p)$. By [EG19, Lemma 5.4.4], the coherent sheaf $H^2(G_K, \bar{\rho}_T)$ is locally free of rank r as an $\mathcal{O}_E$-module.

By [EG19, Theorem 5.1.21], we can choose a complex of finite rank locally free $\mathcal{O}_E$-modules

$$C_T^0 \to C_T^1 \to C_T^2$$

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

$$C_T^0 \to Z_T^1$$

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

$$0 \to \bar\rho_{\eta(t)} \to ? \to \bar{\mathbb{F}}_p \to 0, \quad t \in T(\bar{\mathbb{F}}_p)$$

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

$$()_1 : (\mathcal{X}_{a,\mathrm{red}})_{\bar{\mathbb{F}}_p} \times (\mathcal{X}_{d,\mathrm{red}})_{\bar{\mathbb{F}}_p} \to (\mathcal{X}_{a,\mathrm{red}})_{\bar{\mathbb{F}}_p}$$

and

$$()_2 : (\mathcal{X}_{a,\mathrm{red}})_{\bar{\mathbb{F}}_p} \times (\mathcal{X}_{d,\mathrm{red}})_{\bar{\mathbb{F}}_p} \to (\mathcal{X}_{d,\mathrm{red}})_{\bar{\mathbb{F}}_p}$$

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

$$0 \to \bar\rho_{t_1} \to ? \to \bar\rho_{t_2} \to 0, \quad t \in T(\bar{\mathbb{F}}_p)$$

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

$$g : \mathscr{V}(Z^1_T) \to (\mathcal{X}_{a+d,\mathrm{red}})_{\bar{\mathbb{F}}_p}.$$

6.1.0.1 Lemma Let e denote the dimension of the scheme-theoretic image of T in $(\mathcal{X}_{a,\mathrm{red}})_{\bar{\mathbb{F}}_p} \times (\mathcal{X}_{d,\mathrm{red}})_{\bar{\mathbb{F}}_p}$. Then the scheme-theoretic image of $V = \mathscr{V}(Z^1_T)$ in $(\mathcal{X}_{a+d,\mathrm{red}})_{\bar{\mathbb{F}}_p}$ 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 [EG19, Proposition 5.4.4] closely.

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

$$T_{f(t)} := T \underset{f,(\mathcal{X}_{a,\mathrm{red}})_{\bar{\mathbb{F}}_p} \times (\mathcal{X}_{d,\mathrm{red}})_{\bar{\mathbb{F}}_p}, f(t)}{\times} \mathrm{Spec}\, \bar{\mathbb{F}}_p$$

$$V_{g(v)} := V \underset{g,(\mathcal{X}_{a,\mathrm{red}})_{\bar{\mathbb{F}}_p} \times (\mathcal{X}_{d,\mathrm{red}})_{\bar{\mathbb{F}}_p}, g(v)}{\times} \mathrm{Spec}\, \bar{\mathbb{F}}_p$$

$$V_{f(t),g(v)} := V_{g(v)} \underset{(\mathcal{X}_{a,\mathrm{red}})_{\bar{\mathbb{F}}_p} \times (\mathcal{X}_{d,\mathrm{red}})_{\bar{\mathbb{F}}_p}, f(t)}{\times} \mathrm{Spec}\, \bar{\mathbb{F}}_p.$$

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

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

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

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

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

which induces a monomorphism

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

So it suffices to show

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

for v lying in a dense open of V.

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

Let $C^0_S \to Z^1_S$ denote the pullback family of $C^0_T \to Z^1_T$ to S. $C^0_S \to Z^1_S$ is also the pullback family of the fiber $C^0_t \to Z^1_t$ to S. Write W for the affine scheme associated to $H^1(G_K, \bar{\rho}^{\vee}_{f(t)_1} \otimes \bar{\rho}_{f(t)_2})$. By the isomorphism

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

there is a morphism $W \to (\mathcal{X}_{a+d,\mathrm{red}})_{\bar{\mathbb{F}}_p}$. 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 $S \times_T V \to S \times_{\bar{\mathbb{F}}_p} W$, which is a trivial vector bundle over S. We have

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

Note that $\dim V - \dim T = \mathrm{rank}\, Z^1_T$, and by local Euler characteristic $H^0(G_K, \bar{\rho}^{\vee}_{f(t)_1} \otimes \bar{\rho}_{f(t)_2}) - H^1(G_K, \bar{\rho}^{\vee}_{f(t)_1} \otimes \bar{\rho}_{f(t)_2}) + r = -ad[K:\mathbb{Q}_p]$. We can replace T by a dense open of T where $e = \dim T - \dim T_{f(t)} = \dim T - \dim S$. Combine all these equalities, $(\dagger)$ becomes

$$\dim W_{h(w)} \geqslant \dim H^0(G_K, \bar{\rho}^{\vee}_{f(t)_1} \otimes \bar{\rho}_{f(t)_2}) + \dim G_{t_1} + \dim G_{t_2}$$

which follows from the fact that

$$H^0(G_K, \bar{\rho}^{\vee}_{f(t)_1} \otimes \bar{\rho}_{f(t)_2}) \rtimes (G_{t_1} \times G_{t_2}) \subset \mathrm{Aut}(\bar{\rho}_w)$$

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

We recall some terminology from [EG19]. Denote by $\mathrm{ur}_x : \mathbb{G}_m \to \mathcal{X}_1$ the family of unramified characters of G_K. Let T be a reduced finite type $\mathbb{F}$-scheme. Let $T \to \mathcal{X}$ be a morphism, corresponding to a family $\bar{\rho}_T$ of G_K-representations over T. We can construct the family of unramified twisting $\bar{\rho}_T \boxtimes \mathrm{ur}_x$ over $T \times \mathbb{G}_m$. $\bar{\rho}_T$ is said to be *twistable* if whenever $\bar{\rho}_t \cong \bar{\rho}_{t'} \otimes \mathrm{ur}_a$ 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 $\bar{\rho}_t \cong \bar{\rho}_{t'} \otimes \mathrm{ur}_a$ is finite.

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

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

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

6.2. Loci cut out by $H^2(G_K, \mathrm{sym}^3/\det^2)$

Write H^2 for $H^2(G_K, \frac{\mathrm{sym}^3(\bar{r}^{\mathrm{univ}})}{\det(\bar{r}^{\mathrm{univ}})^2})$. Let $x \in \mathcal{X}(\bar{\mathbb{F}}_p)$ with corresponding Galois representation $\bar{r}_x : G_K \to \mathrm{GL}_2(\bar{\mathbb{F}}_p)$.

6.2.0.1 Lemma If $\bar{r}_x$ is irreducible, then

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

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

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

Both $H^2(G_K, \frac{\mathrm{Ind}(\bar{\chi}^3)}{\det(\bar{r}_x)^2})$ and $H^2(G_K, \frac{\mathrm{Ind}(\bar{\chi} \det \bar{r}_x)}{\det(\bar{r}_x)^2})$ has dimension at most 1. This is because the induction of a character can't be a direct sum of two isomorphic characters (when $p \neq 2$). □

6.2.0.2 Corollary H^2 is SGR when restricted on the irreducible locus.

Proof. Up to unramified twist, there are only finitely many irreducible representations. The automorphism group of an irreducible representation is 1-dimensional. By Lemma 6.2.0.1, we have $h_x^2 \leqslant 2$ when $\bar{r}_x$ is irreducible.

We first consider the locus where $h_x^2 = 2$. This locus consists of finitely many irreducible G_K-representations, and has dimension -1. Then we consider the locus where $h_x^2 \leqslant 1$. This locus consists of the unramified twisting of finitely many irreducible G_K-representations, and has dimension 0. In either case, dim of locus $\leqslant [K : \mathbb{Q}_p] - h_x^2$. □

6.2.0.3 Lemma If $\bar{r}_x$ is a non-trivial extension of two characters, then

$$h_x^2 := \dim H^2(G_K, \frac{\mathrm{sym}^3(\bar{r}_x)}{\det(\bar{r}_x)^2}) \leqslant 1$$

and when the equality holds, the quotient character of $\bar{r}_x$ is a character whose cubic 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 have

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

which has a unique G_K-invariant quotient line. We give a proof of the above simple observation. 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 $\mathrm{sym}^3(\bar{r}_x)$. By duality, it is equivalent to saying that $\mathrm{sym}^3(\bar{r}_x)$ has a unique invariant line. Clearly $\{e_1^3\}$ defines an invariant line. Assume there is another invariant line $\mathrm{span}(v)$. We quotient $\mathrm{sym}^3(\bar{r}_x)$ by $\mathrm{span}(e_1)$. The quotient representation has a unique invariant line generated by the image of $e_1^2 e_2$. So $v \in \mathrm{span}(e_1^3, e_1^2 e_2)$. But then we must have $v \in \mathrm{span}(e_1^3)$, since $[\bar{c}]$ is a non-trivial extension class. □

6.2.0.4 Corollary H^2 is SGR when restricted on the locus where $\bar{r}_x$ is a non-trivial extension of two characters.

Proof. Say $\bar{r}_x$ is the extension of $\bar{\beta}$ by $\bar{\alpha}$. By Lemma 6.2.0.3, we have $h^2_x \leqslant 1$ when $\bar{r}_x$ is a nontrivial extension of characters. So the locus where $\bar{r}_x$ is a non-trivial extension of characters consists of four sub-loci:

(i) $h^2_x = 1$ and $\mathrm{Ext}^2(\beta, \alpha) = 0$;
(ii) $h^2_x = 1$ and $\mathrm{Ext}^2(\beta, \alpha) \neq 0$;
(iii) $h^2_x = 0$ and $\mathrm{Ext}^2(\beta, \alpha) = 0$; and
(iv) $h^2_x = 0$ and $\mathrm{Ext}^2(\beta, \alpha) \neq 0$;

Let $T \subset (\mathcal{X}_{1,\mathrm{red}})_{\bar{\mathbb{F}}_p} \times (\mathcal{X}_{1,\mathrm{red}})_{\bar{\mathbb{F}}_p}$ be the locus of the pair (α, β). say $\dim T = e$, and $\dim \mathrm{Ext}^2(\beta, \alpha) = r$. By Lemma 6.1.0.1, each sub-locus has dimension at most

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

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

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

$$H^2(G_K, \frac{\mathrm{sym}^3(\bar{r}_x)}{\det(\bar{r}_x)^2}) \leqslant 2.$$

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

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

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

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

Proof. By Lemma 6.2.0.5, we have $h^2_x \leqslant 2$ when $\bar{x} = \alpha \oplus \beta$ is a direct sum of distinct characters.

In the locus where $h^2_x = 2$, we must have $\pm\alpha = \pm\beta = \mathbb{F}(-1)$. So both α and β lives in a twistable family and this locus has dimension -2.

In the locus where $h^2_x = 1$, 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 $\dim \mathbb{G}_m - \dim \mathrm{Aut}(\bar{r}_x) = 1 - 2 = -1$.

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

6.2.0.7 Lemma If $\bar{r}_x$ is a direct sum of isomorphic characters, then

$$H^2(G_K, \frac{\mathrm{sym}^3(\bar{r}_x)}{\det(\bar{r}_x)^2}) \leqslant 4.$$

Proof. This is trivial because the underlying $\bar{\mathbb{F}}_p$-vector space is 4-dimensional. □

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

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

6.2.0.9 Theorem The locus of $\bar{r}_x$ in $\mathcal{X}$ for which

$$H^2(G_K, \frac{\mathrm{sym}^3(\bar{r}_x)}{\det(\bar{r}_x)^2}) \geqslant r.$$

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

Proof. This theorem follows immediately from Lemma 6.2.0.1, Lemma 6.2.0.3, Lemma 6.2.0.5, Lemma 6.2.0.7, and their corollaries. □

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

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

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

$$\{x \in \mathrm{Spec}\, R | \dim \kappa(x) \otimes_R H^2(G_K, \frac{\mathrm{sym}^3(r^{\mathrm{univ}})}{\det(r^{\mathrm{univ}})^2}) \geqslant s\}$$

has codimension $\geqslant s+1$ in $\mathrm{Spec}\, R$.

Proof. The proof is identical to that of [EG19, Theorem 6.1.1] if we use Theorem 6.2.0.9 instead of [EG19, Theorem 5.5.11]. □

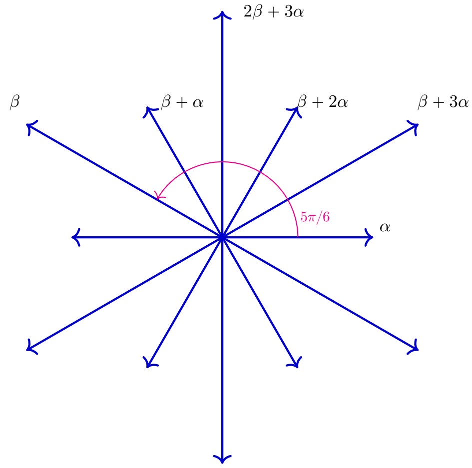
7. The existence of crystalline lifts for the exceptional group G_2

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:



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 nilpotent group of class 2. Write U^{ad} for $U/Z(U)$.

Fix an isomorphism $\mathrm{std} : L \cong \mathrm{GL}_2$. We have

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

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

$$\mathrm{Lie}\, U \cong \frac{1}{\det^2} \mathrm{sym}^3(\mathrm{std}) \oplus \frac{1}{\det}$$

where $\det : L \to \mathbb{G}_m$ is the determinant character, and $\mathrm{std} : L \xrightarrow{\cong} \mathrm{GL}_2$ is the fixed isomorphism. The above short exact sequence can be upgraded to a short exact sequence of groups with L-actions

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

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 $L' \cong \mathrm{GL}_2$ and V is a nilpotent group of class 3. Fix an isomorphism $\mathrm{std} : L' \xrightarrow{\cong} \mathrm{GL}_2$. Write $\det$ for the composition $L' \xrightarrow{\mathrm{std}} \mathrm{GL}_2 \xrightarrow{\det} \mathrm{GL}_1$.

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

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

Moreover, if $\bar{\rho}$ factors through a maximal parabolic and the Levi factor $\bar{r}_{\bar{\rho}}$ of $\bar{\rho}$ admits a Hodge-Tate regular and crystalline lift r_1 such that the adjoint representation $\phi^{\mathrm{Lie}}(r_1)$ 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 [Lin19].

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.

7.2.1. The short root parabolic case

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

By Lemma 3.3.1.1, there exists a finite Galois extension K'/K, of prime-to-p degree such that $\bar{r}|_{K'}$ is Lyndon-Demuškin.

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

7.2.1.1 Lemma Assume $p > 2$. There exists a Hodge-Tate regular crystalline lifting $r^\circ : G_K \to L(\bar{\mathbb{Z}}_p)$ of the Levi factor $\bar{r}$, such that the adoint representation $\phi^{\mathrm{Lie}}(r^\circ) : G_K \xrightarrow{r^\circ} L(\bar{\mathbb{Z}}_p) \to \mathrm{GL}(\mathrm{Lie}\, U(\bar{\mathbb{Z}}_p))$ has labeled Hodge-Tate weights slightly less that $\underline{0}$.

Proof. It is well-known Hodge-Tate regular crystalline lifts of $\bar{r}$ exists. We have $\phi^{\mathrm{Lie}}(r^\circ) = \frac{1}{\det r^{\circ 2}} \mathrm{sym}^3(r^\circ) \oplus \frac{1}{\det r^\circ}$. So by replacing r° by a Tate twist, we can ensure $\phi^{\mathrm{Lie}}(r^\circ)$ labeled Hodge-Tate weights slightly less that $\underline{0}$.

□

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

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

The mod ϖ Galois representation $\bar{r}$ defines a Galois action $\phi(\bar{r}) : G_K \to \mathrm{Aut}(U(\bar{\mathbb{F}}_p))$ on $U(\bar{\mathbb{F}}_p)$. By 4.1.0.4, the datum of $\bar{\rho} : G_K \to G_2(\bar{\mathbb{F}}_p)$ is encoded in a non-abelian cocycle $[\bar{c}] \in H^1(G_K, U(\bar{\mathbb{F}}_p))$.

The strategy for lifting $\bar{\rho}$ is as follows. We choose a suitable $\bar{\mathbb{Z}}_p$-point x of $\mathrm{Spec}\, R$ which defines a lift $r_x : G_K \to L(\bar{\mathbb{Z}}_p)$ of $\bar{r}$, and endow $U(\bar{\mathbb{Z}}_p)$ with the Galois action $\phi(r_x) : G_K \xrightarrow{r_x} L(\bar{\mathbb{Z}}_p) \to \mathrm{Aut}(U(\bar{\mathbb{Z}}_p))$. There is a map of pointed set $H^1(G_K, U(\bar{\mathbb{Z}}_p)) \to H^1(G_K, U(\bar{\mathbb{F}}_p))$. If the cohomology class $[\bar{c}]$ admits a lift $[c] \in H^1(G_K, U(\bar{\mathbb{Z}}_p))$, then $\bar{\rho}$ admits a lift $\rho : G_K \to G_2(\bar{\mathbb{Z}}_p)$ whose datum is encoded in $[c]$. Such a lift ρ is crystalline by the main result of [Lin21], since $\phi^{\mathrm{Lie}}(r^\circ)$ has labeled Hodge-Tate weights slightly less than $\underline{0}$.

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

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

[1] is verified by Theorem 6.2.0.10. Note that since the Hodge type of $\mathrm{Spec}\, R$ is chosen so that $\mathrm{sym}^3(r_x)/\det(r_x)^2$ has labeled Hodge-Tate weights slightly less than $\underline{0}$, $H^2(G_K, \mathrm{sym}^3(r_x)/\det(r_x)^2)$ is torsion for any characteristic 0 point x of $\mathrm{Spec}\, R$. [3] follows from Lemma 3.3.1.1, and [4] follows from Proposition 3.0.3.

7.2.2. 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 $\mathrm{std} : L' \xrightarrow{\cong} \mathrm{GL}_2$. Write det for the composition $L' \xrightarrow{\mathrm{std}} \mathrm{GL}_2 \xrightarrow{\det} \mathrm{GL}_1$.

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

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

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

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

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

$$H^2(G_K, V_3(\bar{\mathbb{F}}_p)/V_2(\bar{\mathbb{F}}_p)) = H^2(G_K, \bar{r} \otimes \det \bar{r}) = 0$$

$$H^2(G_K, V_1(\bar{\mathbb{F}}_p)) = H^2(G_K, \bar{r}) = 0$$

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

The datum of $\bar{\rho}$ is encoded in a non-abelian 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 $\mathrm{ad}([\bar{c}]) \in H^1(G_K, (V/V_1)(\bar{\mathbb{F}}_p))$.

Write U' for V/V_1. Recall that U' is a nilpotent 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 7.2.1.

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 $\mathrm{Spec}\, R$ be the irreducible component of the crystalline lifting ring of $\bar{r}$ containing r°. Write $r^{\mathrm{univ}} : G_K \to \mathrm{GL}_2(R)$ 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 $L' \to \mathrm{Aut}(U'^{\mathrm{ad}})$ and write ϕ^z for the conjugate action $L' \to \mathrm{Aut}(Z(U'))$.

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

We have the following check list:

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

By the assumption $H^2(G_K, \det(r^{\mathrm{univ}})r^{\mathrm{univ}}) = 0$. [3] follows from Lemma 3.3.1.1, and [4] follows from Proposition 3.0.3. □

A. Non-denegeracy 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 $P = L \ltimes U$ be the Levi decomposition. Let a Galois representation $\bar{r} : G_K \to L(\mathbb{F})$ which is Lyndon-Demuškin. Since $L \cong \mathrm{GL}_2$, $\bar{r}$ is the extension of two trivial characters.

Denote by $\phi : L \to \mathrm{Aut}(U)$ the conjugation action.

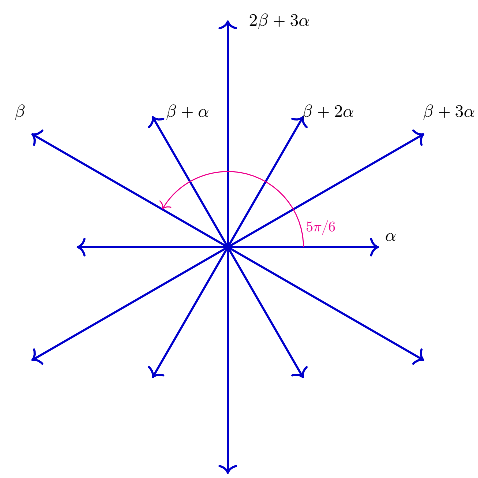
G_K acts on U via the conjugate action $G_K \xrightarrow{r^\circ} L \xrightarrow{\phi} \mathrm{Aut}(U)$.

We set up a computational framework to prove various claims. Let $\{x_0, \cdots, x_n, x_{n+1}\}$ be the Demuškin 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 $i = 0, \cdots, n+1$, $\bar{r}(x_i) = \begin{bmatrix} 1 & l_i \\ & 1 \end{bmatrix}$.

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 $\mathrm{sym}^3(\bar{r})$, which is identified with $U^{\mathrm{ad}}(\mathbb{F})$.

We remind the reader of the root system of G_2



Root system of G_2

In the above diagram, α is the short root, and β is the short root. Each root x has generates a root group $U_x \subset U$. The short root parabolic P has 7 root groups: the 5 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 $\mathrm{std} : L \cong \mathrm{GL}_2$, the matrices $\begin{bmatrix} 0 & * \\ 0 & 0 \end{bmatrix}$ are identified with the root group U_α. Now that we have identifications

$$\begin{aligned} \operatorname{span} e_1^3 &\sim U_\beta \\ \operatorname{span} e_1^2 e_2 &\sim U_{\beta+\alpha} \\ \operatorname{span} e_1 e_2^2 &\sim U_{\beta+2\alpha} \\ \operatorname{span} e_2^3 &\sim U_{\beta+3\alpha} \end{aligned}$$

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

$$C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E)) \cong \{\langle x_0, \cdots, x_{n+1}\rangle \to U_\beta(\mathcal{O}_E) \oplus U_{\beta+\alpha}(\mathcal{O}_E) \oplus U_{\beta+2\alpha}(\mathcal{O}_E) \oplus U_{\beta+3\alpha}(\mathcal{O}_E)\}$$

is given by

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

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

A.0.1. Lemma The cup products on cochains

$$\cup_{\mathbb{F}} : C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F})) \times C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F})) \to C^2_{\mathrm{LD}}(Z(U)(\mathbb{F}))$$

is non-degenerate.

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

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

whose anti-diagonal blocks are constant invertible matrices), and thus non-degenerate.

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

Proof. Recall the relator of the Lyndon-Demuškin group is

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

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

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

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

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

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

The cup product

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

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

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

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

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 anti-diagonal*, and we call M_{41}, M_{32}, M_{23} and M_{14} the anti-diagonal blocks.

$$\begin{array}{c} \\ \beta \\ \beta+\alpha \\ \beta+2\alpha \\ \beta+3\alpha \end{array} \begin{array}{c} \begin{array}{cccc} \beta & \beta+\alpha & \beta+2\alpha & \beta+3\alpha \end{array} \\ \left(\begin{array}{c|c|c|c} & & & \\ \hline & & & M_{24} \\ \hline & & M_{33} & M_{34} \\ \hline & M_{42} & M_{43} & M_{44} \end{array}\right) \end{array}$$

FIGURE 1. Strictly below anti-diagonal

$$\begin{array}{c} \\ \beta \\ \beta+\alpha \\ \beta+2\alpha \\ \beta+3\alpha \end{array} \begin{array}{c} \begin{array}{cccc} \beta & \beta+\alpha & \beta+2\alpha & \beta+3\alpha \end{array} \\ \left(\begin{array}{c|c|c|c} & & & M_{14} \\ \hline & & M_{23} & \\ \hline & M_{32} & & \\ \hline M_{41} & & & \end{array}\right) \end{array}$$

FIGURE 2. Anti-diagonal 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

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

Proof. An immediate consequence of the Baker–Campbell–Hausdorff formula. □

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

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

We have

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

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 $[\cup_{\mathbb{F}}]_{\mathscr{B}}$ which lies strictly below the anti-diagonal, because $(\phi(x_{2k})-1)$ and $(\phi(x_{2k+1})-1)$ moved the appearance of the inderterminant $\lambda_{i,j}$ 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

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

Write

$$\begin{aligned} 2Z'_k &:= [-\widetilde{c}(x_{2k}), -\widetilde{c}(x_{2k+1})] \\ &+ [-\widetilde{c}(x_{2k}), \widetilde{c}(x_{2k})] \\ &+ [-\widetilde{c}(x_{2k}), \widetilde{c}(x_{2k+1})] \\ &+ [-\widetilde{c}(x_{2k+1}), \widetilde{c}(x_{2k})] \\ &+ [-\widetilde{c}(x_{2k+1}), \widetilde{c}(x_{2k+1})] \\ &+ [\widetilde{c}(x_{2k}), \widetilde{c}(x_{2k+1})] \end{aligned}$$

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 $[\cup_{\mathbb{F}}]_{\mathscr{B}}$ with lies strictly below the anti-diagonal for a similar reason (a "shifting" effect). It is easy to see that

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

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

$$\pm M_{41} = \pm M_{14} = \begin{bmatrix} \begin{bmatrix} & -1/2 \\ 1/2 & \end{bmatrix} & & & \\ & \begin{bmatrix} & -1/2 \\ 1/2 & \end{bmatrix} & & \\ & & \cdots & \\ & & & \begin{bmatrix} & -1/2 \\ 1/2 & \end{bmatrix} \end{bmatrix}$$

and

$$\pm M_{32} = \pm M_{23} = \begin{bmatrix} \begin{bmatrix} & -3/2 \\ 3/2 & \end{bmatrix} & & & \\ & \begin{bmatrix} & -3/2 \\ 3/2 & \end{bmatrix} & & \\ & & \cdots & \\ & & & \begin{bmatrix} & -1/2 \\ 1/2 & \end{bmatrix} \end{bmatrix}.$$

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

The long root parabolic case is much simpler.

B. Sagemath code

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

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

$$\begin{aligned} g^q \quad = \quad & (ql; qu_0, -\frac{1}{2}q(q-1)u_0 l + qu_1, \\ & -\frac{1}{6}q(q-1)(2q-1)u_0 l^2 + q(q-1)u_1 l + qu_2, \\ & -\frac{1}{4}q^2(q-1)^2 u_0 l^3 + \frac{1}{2}q(q-1)(2q-1)u_1 l^2 + \frac{3}{2}q(q-1)u_2 l + qu_3, qu_4; \\ & \frac{1}{120}(q-1)q(q+1)(3q^2-2)u_0^2 l^3 - \frac{1}{2}(q-1)q(q+1)(u_1^2 + u_0 u_2) l) \end{aligned}$$

It can be computed by hand, and can be verified by computer algebra system. The Proposition follows from the above computation immediately. □

The following is the SageMath source code for computing cup product.

```

# Generate basis vectors of of C^1_{LD}(U)

def generate_LU(i):
    Ai = var("A%d"%i)
    Bi = var("B%d"%i)
    Ci = var("C%d"%i)
    Di = var("D%d"%i)
    Ei = var("E%d"%i)
    li = var("l%d"%i)
    gi = var("g%d"%i)
    hi = var("h%d"%i)
    Li = matrix(SR, [[gi,li],[0,hi]])
```

```
    ui = vector(SR, [Ai,Bi,Ci,Di,Ei])
    u_i = -phi(Li.inverse())*ui
    return {"L": Li, "L_": Li.inverse(), "U": ui, "U_": u_i}

def generate_LU_pair(i):
    LUi = generate_LU(i)
    LUi1 = generate_LU(i+1)
    return [
        [LUi["L_"], LUi["U_"]],
        [LUi1["L_"], LUi1["U_"]],
        [LUi["L"], LUi["U"]],
        [LUi1["L"], LUi1["U"]],
    ]

# The matrix for r(x_i)

def Levi(i):
    hi = eval("h%d"%i)
    li = eval("l%d"%i)
    gi = eval("g%d"%i)
    return matrix(SR, [[gi, li], [0, hi]])

# Conjugation action of the Levi factor on Lie U

def phi(m):
    a=m[0,0]
    b=m[0,1]
    c=m[1,0]
    d=m[1,1]
    dt = det(m)
    return matrix(SR, [
        [a*a*a,a*a*b,a*b*b,b*b*b,0],
        [3*a*a*c,a*a*d+2*a*c*b,2*a*b*d+b*b*c,3*b*b*d,0],
        [3*a*c*c,2*a*c*d+b*c*c,2*b*c*d+a*d*d,3*b*d*d,0],
        [c*c*c,c*c*d,c*d*d,d*d*d,0],
        [0,0,0,0,dt]])/dt/dt

# Lie bracket on Lie U

def brkt(X,Y):
    return -vector(SR, [0,0,0,0,
        X[0]*Y[3]+3*X[1]*Y[2]-Y[0]*X[3]-3*Y[1]*X[2]])

# The differential
#     d^2: C^1 -> C^2

def general_cup_product(pairs):
    X_list = []
    levi = identity_matrix(SR, 5)
    for pr in pairs:
        X_list.append(levi*pr[1])
        levi = levi*phi(pr[0])
    ret = 0
```

```
    for X in X_list:
        ret += X
    for i in range(0, len(X_list)):
        for j in range(i + 1, len(X_list)):
            ret += (1/2) * brkt(X_list[i], X_list[j])
    return ret

def differential_degree_2(p = 5, g = 5, n = 4):
    pairs = []
    LU01 = generate_LU_pair(0)
    for i in range(0, g - 1):
        pairs.append(LU01[2])
    pairs.append(LU01[1])
    pairs.append(LU01[2])
    pairs.append(LU01[3])
    i = 2
    while i < n + 1:
        for pr in generate_LU_pair(i):
            pairs.append(pr)
        i += 2
    return general_cup_product(pairs)

# Generate the basis of C1

def basis_of_C1(n):
    basis = []
    for letter in "ABCD":
        for i in range(0, n + 2):
            basis.append(eval("%s%d"%(letter, i)))
    return basis

# Organize the boundary map
#                delta: C^1(U^ad) -> C^2(Z(U))
# as a quadratic form
#                cup: C^1 x C^1 -> C^2(Z(U))

def as_quad_form(expr, variables):
    coef = {}
    remain = expr.expand()
    for i1 in range(0, len(variables)):
        for i2 in range(i1, len(variables)):
            var1 = variables[i1]
            var2 = variables[i2]
            coef[(var1*var2).__repr__()] =
                remain.coefficient(var1*var2).expand().factor()
            remain -= coef[(var1*var2).__repr__()]*var1*var2
    BL_arr = []

    for i1 in range(0, len(variables)):
        BL_arr.append([])
        for i2 in range(0, len(variables)):
            var1 = variables[i1]
            var2 = variables[i2]
```

```
            if i1 < i2:
                var_s = (var1 * var2).__repr__()
            else:
                var_s = (var2 * var1).__repr__()
            coef_s = coef[var_s].__repr__()
            if i1 == i2:
                BL_arr[-1].append(coef[var_s].expand())
            else:
                BL_arr[-1].append((1/2)* coef[var_s].expand())

    BL_mat = matrix(SR, BL_arr)
    return coef, BL_mat

# Cup product

def cup_product(p = 5, g = 5, n = 4):
    cR = differential_degree_2(p, g, n)
    return as_quad_form(cR[4], basis_of_C1(n), False)

# Matrix of cup product mod p

def matrix_substitute(mat, subdict, bring=QQ):
    new_arr = []
    for i in range(0, mat.nrows()):
        new_arr.append([])
        for j in range(0, mat.ncols()):
            entry = 0 + mat[i][j]
            entry = entry.subs(subdict)
            new_arr[-1].append(entry)
    return matrix(bring, new_arr)

def cup_product_mod_p(p=5, g=5, n=4):
    coef, BLm = cup_product(p, g, n)
    sub_dict = {}
    for i in range(0, n+2):
        sub_dict[eval("g%d"%i)] = 1
        sub_dict[eval("h%d"%i)] = 1
    BLmod = matrix_substitute(BLm, sub_dict, SR)
    return BLmod
```

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.

References

[B03] G. Böckle. "Lifting mod p representations to characteristics p^2". In: *J. Number Theory* 101.2 (2003), pp. 310–337. ISSN: 0022-314X. DOI: 10.1016/S0022-314X(03)00058-1. URL: https://doi.org/10.1016/S0022-314X(03)00058-1.

[BG19] R. Bellovin and T. Gee. "G-valued local deformation rings and global lifts". In: *Algebra and Number Theory* 13 (2019), pp. 333–378.

[CL11] X. Caruso and T. Liu. "Some bounds for ramification of p^n-torsion semi-stable representations". In: *J. Algebra* 325 (2011), pp. 70–96. ISSN: 0021-8693. DOI: 10.1016/j.jalgebra.2010.10.005. URL: https://doi.org/10.1016/j.jalgebra.2010.10.005.

[EG19] M. Emerton and T. Gee. "Moduli stack of étale (ϕ, Γ)-modules, and the existence of crystalline lifts". In: ().

[NCS18] N. Fakhruddin, C. Khare, and S. Patrikis. *Lifting irreducible Galois representations.* 2018. arXiv: 1810.05803 [math.NT].

[GHLS] T. Gee et al. "Potentially crystalline lifts of certain prescribed types". In: *Documenta* 22 (2017), pp. 391–422.

[GHS18] T. Gee, F. Herzig, and D. Savitt. "General Serre weight conjectures". In: *J. Eur. Math. Soc. (JEMS)* 20.12 (2018), pp. 2859–2949. ISSN: 1435-9855. DOI: 10.4171/JEMS/826. URL: https://doi.org/10.4171/JEMS/826.

[Ko02] H. Koch. *Galois theory of p-extensions.* Springer Monographs in Mathematics. With a foreword by I. R. Shafarevich, Translated from the 1970 German original by Franz Lemmermeyer, With a postscript by the author and Lemmermeyer. Springer-Verlag, Berlin, 2002, pp. xiv+190. ISBN: 3-540-43629-4. DOI: 10.1007/978-3-662-04967-9. URL: https://doi.org/10.1007/978-3-662-04967-9.

[Ko97] H. Koch. *Algebraic Number Theory.* Springer-Verlag Berlin Heidelberg, 1997. ISBN: 978-3-540-63003-6. DOI: 10.1007/978-3-642-58095-6.

[Lin21] Z. Lin. "Extensions of crystalline representations valued in general reductive groups". In: *In preparation* ().

[Lin21B] Z. Lin. "Moduli of étale ϕ-modules valued in general reductive groups". In: ().

[Lin19] Z. Lin. "A variant of Steinberg-Winter theorem and crystalline lifts". In: ().

[Ly50] R. Lyndon. "Cohomology Theory of Groups with a Single Defining Relation". In: *Annals of Math.* 52.3 (1950), pp. 650–665.

[Mu13] A. Muller. "Relèvements cristallins de représentations galoisiennes". In: *Université de Strasbourg* (2013).

[Se02] J.-P. Serre. *Galois cohomology.* English. Springer Monographs in Mathematics. Translated from the French by Patrick Ion and revised by the author. Springer-Verlag, Berlin, 2002, pp. x+210. ISBN: 3-540-42192-0.

[Se98] J.-P. Serre. "Moursund Lectures 1998". In: *arXiv* (1998). URL: https://arxiv.org/abs/math/0305257.

[stacks-project] T. Stacks Project Authors. *Stacks Project.* https://stacks.math.columbia.edu. 2018.