LIFTING GALOIS REPRESENTATIONS VIA GALOIS COHOMOLOGY

MATHIEU FLORENCE

Abstract. This is a survey on some recent developments about lifting Galois representations.

Contents

2020 *Mathematics Subject Classification.* Primary: 12G05.

1. Introduction.

This paper surveys recent progress on lifting Galois representations. We focus on approaches that solely rely on Galois cohomology: [2], [3], [10], [12] and [13]. For an overview of this widely investigated topic, also beyond the scope of this survey, see for instance [2] or [12]. Observe that sections 3 and 7 actually contain new material. In section 6, emphasis is laid on results of [2], on which I gave a talk at the conference held in Ottawa in June 2024, to celebrate Ján Mináč's 71th birthday.
Dear Ján, it is a pleasure to know you. I wish you lots of enjoyable mathematics in your life!

2. General facts on lifting problems.

Let p be a prime. In this text, G always denotes a profinite group.

Definition 2.1. *A homomorphism from G to an abstract group is said to be continuous, if its kernel is open.*

Definition 2.2. *Let R be a commutative ring. An (R, G)-module is a finite locally free R-module, equipped with an R-linear G-action, whose kernel is open in G.*

Consider the following general question.

Question 2.3. Let G be a profinite group. Let Γ be an affine and smooth $\mathbb{Z}$-group scheme. Consider a continuous representation

$$\rho : G \longrightarrow \Gamma(\mathbb{F}_p).$$

Does ρ admit a continuous lift

$$\rho_2 : G \longrightarrow \Gamma(\mathbb{Z}/p^2)?$$

When G is an absolute Galois group and $\Gamma := \mathbf{GL}_d$, Question 2.3 yields the main problem of interest in this paper- ubiquitous in arithmetic.

Question 2.4. Let F be a field, with a separable closure F_s.
For some integer $d \geq 1$, consider a (continuous) Galois representation

$$\rho : \mathrm{Gal}(F_s/F) \longrightarrow \mathbf{GL}_d(\mathbb{F}_p).$$

Does ρ admit a lift, to some

$$\rho_2 : \mathrm{Gal}(F_s/F) \longrightarrow \mathbf{GL}_d(\mathbb{Z}/p^2)?$$

2.1. Variants and generalisations.

Denote by $\mathbf{B}_d \subset \mathbf{GL}_d$ the Borel subgroup of upper triangular matrices, and by $\mathbf{U}_d \subset \mathbf{B}_d$ its unipotent radical, consisting of strictly upper triangular matrices. There is a 'triangular' (resp. 'strictly triangular') variant of Question 2.4, replacing $\mathbf{GL}_d$ by $\mathbf{B}_d$ (resp. by $\mathbf{U}_d$). In some cases, these triangular variants are easier to handle, by recursive lifting algorithms. This is the main guideline of [2].

In the formulation of Question 2.3, the field of coefficients of ρ is $\mathbb{F}_p$. One may replace it by an arbitrary field k of characteristic p, and accordingly, replace $\mathbb{Z}/p^2$ by $\mathbf{W}_2(k)$ (truncated Witt vectors of length two). Depending on the results aimed at, this may, or may not, make a difference. For instance, the proof of Proposition 4.3 (liftability of two-dimensional Galois representations) is insensitive to k. On the other hand, for $p = 2$, both statement and proof of Theorem 5.1 (that includes the non-liftability of the generic Galois representation of dimension 5 over $k = \mathbb{F}_2$) highly depend on k.

One may also search for liftings modulo p^r, for $r \geq 3$. This topic is addressed in Section 6, for absolute Galois groups of local fields (and more generally, for the so-called p-manageable profinite groups).

2.2. Cohomological obstructions to lifting.

Let us place ourselves in the context of Question 2.3. Endow the Lie algebra $\mathrm{Lie}(\Gamma)$ with its natural (adjoint) linear Γ-action. Denote by

$$\mathbf{End}_{\mathbb{F}_p}(\rho) := \rho^*(\mathrm{Lie}_{\mathbb{F}_p}(\Gamma))$$

the Lie algebra of Γ over $\mathbb{F}_p$, considered as a representation of G, by group-change via ρ. By the general formalism of (group) cohomology, the obstruction to the existence of ρ_2, is a natural class

$$\mathrm{Obs}(\rho_2) \in H^2(G, \mathbf{End}_{\mathbb{F}_p}(\rho)).$$

This class can be described explicity via group extensions; see e.g. section 2.2 of [12] for the cases $\Gamma = \mathbf{GL}_d, \mathbf{B}_d$.

Remark 2.5. (Arbitrary field of coefficients.)
Let k be a field of characteristic p. Denote by

$$\mathrm{frob} : k \xrightarrow{x \mapsto x^p} k$$

the frobenius endomorphism of k. For a k-vector space V, denote by

$$V^{(1)} := V \otimes_{\mathrm{frob}} k$$

its frobenius twist. Consider a continuous representation

$$\rho : G \longrightarrow \Gamma(k).$$

Then, the obstruction to lifing ρ to

$$\rho_2 : G \longrightarrow \Gamma(\mathbf{W}_2(k)),$$

is a natural class

$$\mathrm{Obs}(\rho_2) \in H^2(G, \mathbf{End}_k(\rho)^{(1)}).$$

The frobenius twist, invisible when $k = \mathbb{F}_p$, is actually essential.

2.3. Subgroups of prime-to-p index, reduction to the triangular case. Let G be a profinite group, and consider a representation

$$\rho : G \longrightarrow \mathbf{GL}_d(\mathbb{F}_p).$$

There is an open subgroup $G_0 \subset G$, of prime-to-p index, such that the restriction $\rho_{|G_0}$ is upper triangular, up to conjugation. One may thus assume that $\rho_{|G_0}$ reads as

$$\rho_{|G_0} : G_0 \longrightarrow \mathbf{B}_d(\mathbb{F}_p) \subset \mathbf{GL}_d(\mathbb{F}_p).$$

Assume that $\rho_{|G_0}$ lifts to a representation

$$G_0 \longrightarrow \mathbf{B}_d(\mathbb{Z}/p^2).$$

Then ρ lifts to a representation

$$\rho_2 : G \longrightarrow \mathbf{GL}_d(\mathbb{Z}/p^2).$$

The same result holds, replacing $\mathbf{B}_d \subset \mathbf{GL}_d$, by $\mathbf{U}_d \subset \mathbf{B}_d$.
The proof is a classical restriction-corestriction argument, to a pro-p-Sylow $G_p \subset G$. See for instance [13], Lemma 2.6.

Remark 2.6. This restriction-corestriction argument typically does not apply to lifting modulo higher powers of p. Precisely, if one replaces $\mathbb{Z}/p^2$ by $\mathbb{Z}/p^3$, it is likely that the analoguous result is false- though I do not have a counter-example in mind. In general, there is the following fact, that one should relate to Hensel's Lemma. For some $n \geq 1$, consider a representation $\rho_n : G \longrightarrow \Gamma(\mathbb{Z}/p^n)$. Then, liftability of ρ_n, to a representation $\rho_{2n} : G \longrightarrow \Gamma(\mathbb{Z}/p^{2n})$, is an abelian problem: it is obstructed by a natural class

$$\mathrm{Obs}(\rho_{2n}) \in H^2(G, \mathbf{End}_{\mathbb{Z}/p^n}(\rho)).$$

However, lifting ρ_n, to $\rho_{2n+1} : G \longrightarrow \Gamma(\mathbb{Z}/p^{2n+1})$ is not an abelian question: there is no natural cohomology class (with values in a G-module) that obstructs it.

2.4. A simple descent Lemma.

Lemma 2.7. *Let G be a (profinite) group, and let V, V' be (k, G)-modules. Let l/k be an extension of fields of characteristic p. The following holds.*

1. *If $(V \oplus V')$ lifts to a $(\mathbf{W}_2(k), G)$-module, then so does V.*
2. *If the (l, G)-module $V \otimes_k l$ lifts to a $(\mathbf{W}_2(l), G)$-module, then V lifts to a $(\mathbf{W}_2(k), G)$-module V_2.*

Proof. Item (1) is [3], Lemma 3.4. Item (2) is classical. It follows from the facts, that the obstruction to the existence of V_2, reading as

$$\mathrm{Obs}(V_2) \in H^2(G, \mathbf{End}_k(V)^{(1)})$$

(see section 2.2) is compatible to base-change, and that the injection

$$\mathbf{End}_k(V)^{(1)} \hookrightarrow \mathbf{End}_l(V \otimes_k l)^{(1)} = \mathbf{End}_k(V^{(1)}) \otimes_k l$$

has a G-equivariant retraction- provided by the choice of a k-linear retraction of the inclusion $k \hookrightarrow l$. □

3. A non-liftable Heisenberg-Galois representation.

In this survey, we mostly (but not exclusively) focus on lifting mod p Galois representations. By definition, they are representations of $G := \mathrm{Gal}(F_s/F)$, where F is a field, with values in $\mathbf{GL}_d(k)$, where k is a field of characteristic p. Such a representation that takes values in $\mathbf{B}_d(k)$ resp. $\mathbf{U}_d(k)$, is called triangular, resp. strictly triangular.
We begin with a simple significant example, taken from an unpublished earlier version of [6]. It was removed from recent versions.

For $p \geq 3$, we give an elementary example of a field F, containing $\mathbb{C}$, such that the following natural arrow is not surjective:

$$H^1(\mathrm{Gal}(F_s/F), \mathbf{U}_3(\mathbb{Z}/p^2)) \longrightarrow H^1(\mathrm{Gal}(F_s/F), \mathbf{U}_3(\mathbb{F}_p)).$$

Thus, there exist mod p "Heisenberg-Galois" representations which not lift mod p^2.

Start with a field F, containing $\mathbb{C}$. Set G to be its absolute Galois group. For each $n \geq 1$, use $e^{\frac{2\pi i}{n}} \in F$ to identify μ_n to $\mathbb{Z}/n$, as finite G-modules. Pick $x, y \in F^\times$.

By Kummer theory, there are two classes

$$(x)_p, (y)_p \in H^1(F, \mu_p),$$

respectively associated to extensions of $(\mathbb{F}_p, G)$-modules

$$\mathcal{E}_x : 0 \longrightarrow \mathbb{F}_p = \mu_p \longrightarrow E_x \longrightarrow \mathbb{F}_p \longrightarrow 0$$

and

$$\mathcal{E}_y : 0 \longrightarrow \mathbb{F}_p = \mu_p \longrightarrow E_y \longrightarrow \mathbb{F}_p \longrightarrow 0.$$

These give rise to group homomorphisms

$$\rho_x : G \longrightarrow \mathbf{U}_2(\mathbb{F}_p) = \mathbb{F}_p$$

and

$$\rho_y : G \longrightarrow \mathbf{U}_2(\mathbb{F}_p) = \mathbb{F}_p.$$

Definition 3.1. *Assume there exists a complete flag of $(\mathbb{F}_p, G)$-modules*

$$\nabla_3 : 0 \subset V_1 \subset V_2 \subset V_3,$$

such that the truncated extension of $(\mathbb{F}_p, G)$-modules

$$0 \longrightarrow V_1 \longrightarrow V_2 \longrightarrow V_2/V_1 \longrightarrow 0$$

is isomorphic to $\mathcal{E}_x$, and such that the quotient extension

$$0 \longrightarrow V_2/V_1 \longrightarrow V_3/V_1 \longrightarrow V_3/V_2 \longrightarrow 0$$

is isomorphic to $\mathcal{E}_y$. We then say that $\mathcal{E}_x$ and $\mathcal{E}_y$ glue, to the complete flag ∇_3.

A fundamental fact is that the extensions $\mathcal{E}_x$ and $\mathcal{E}_y$ glue to a ∇_3 as above, if and only if the cup-product

$$a = (x)_p \cup (y)_p \in H^2(F, \mu_p^{\otimes 2}) = H^2(F, \mu_p) = \mathrm{Br}(F)[p]$$

vanishes.
Assume that this is the case, and let ∇_3 be such a gluing. Using the same construction as above, for coefficients in $\mathbb{Z}/p^2$, we get the following.
The complete flag ∇_3 lifts to a complete flag of $(\mathbb{Z}/p^2, G)$-modules

$$\nabla_{3,2} : 0 \subset V_{1,2} \subset V_{2,2} \subset V_{3,2},$$

with trivial graded pieces

$$L_{i,2} = \mathbb{Z}/p^2,$$

if and only if $(x)_p$ and $(y)_p$, respectively, lift to classes

$$(X)_{p^2}, (Y)_{p^2} \in H^1(F, \mu_{p^2}),$$

such that

$$(X)_{p^2} \cup (Y)_{p^2} = 0 \in H^2(F, \mu_{p^2}^{\otimes 2}) = H^2(F, \mu_{p^2}) = \mathrm{Br}(K)[p^2].$$

We now show that

F, x and y can be chosen, so that the liftability property above fails.

Equivalently:

- The extensions $\mathcal{E}_x$ and $\mathcal{E}_y$ glue, to a ∇_3 as above.
- The flag ∇_3 does not admit a lift to a flag of $(G, \mathbb{Z}/p^2)$-modules $\nabla_{3,2}$, with trivial graded pieces.

It follows that $[\nabla_3] \in H^1(\mathrm{Gal}(F_s/F), \mathbf{U}_3(\mathbb{F}_p))$ cannot be lifted via

$$H^1(\mathrm{Gal}(F_s/F), \mathbf{U}_3(\mathbb{Z}/p^2)) \longrightarrow H^1(\mathrm{Gal}(F_s/F), \mathbf{U}_3(\mathbb{F}_p)),$$

completing the goal of this section. The following elementary result is the key. Alternatively, one may use a deeper, yet more involved result: [9], Theorem 2.1.

Proposition 3.2 ([14, Théorème 1] or [15, Exercise 10.5]).
Let p be an odd prime. Put

$$F := \mathbb{C}(x_1, x_2, y),$$

$$x := (x_1^p - y)(x_2^p - y) \in F$$

and

$$M := F(x^{\frac{1}{p}}, y^{\frac{1}{p}}).$$

Consider the cyclic algebra

$$A := (x)_{p^2} \cup (y)_{p^2} \in \mathrm{Br}(F).$$

It is of exponent p, split by M/F. There do not exist elements $u, v \in F$ such that

$$[A] = (u)_p \cup (y)_p + (v)_p \cup (x)_p \in \mathrm{Br}_p(F).$$

This proposition being granted, assume that $(x)_p$ and $(y)_p$ lift to classes

$$(X)_{p^2}, (Y)_{p^2} \in H^1(F, \mu_{p^2}),$$

such that $(X)_{p^2} \cup (Y)_{p^2} = 0$. Write

$$(X)_{p^2} = (x)_{p^2} - p(u)_{p^2}$$

and

$$(Y)_{p^2} = (y)_{p^2} - p(v)_{p^2},$$

for $u, v \in F^\times$. Expanding the equality $(X)_{p^2} \cup (Y)_{p^2} = 0$, we get

$$[A] = (u)_p \cup (y)_p + (x)_p \cup (v)_p \in \mathrm{Br}(F),$$

contradicting the above.

We did not exclude the possibility that ρ_1 lifts to a representation

$$G \longrightarrow \mathbf{B}_3(\mathbb{Z}/p^2),$$

but I believe it does not. This would imply the non-liftability of the versal $\mathbf{B}_3(\mathbb{F}_p)$-Galois representation (over $K = \mathbb{C}$). From there, one could derive an alternate proof of Theorem 5.1, for p odd (see section 5 for the definition of 'versal', and more).

Actually, in the literature, the first simple triangular counter-example (i.e. for $\mathbf{B}_3$) was given in the note [7]. Observe that its construction heavily relies on the assumption $\mu_{p^2} \nsubseteq F$, and would not work over number fields containing μ_{p^2}.
In the sequel, write $\mathrm{Gal}(F)$ for $\mathrm{Gal}(F_s/F)$. For the sake of concreteness, the statement given in Proposition 3.4 below slightly differs from [7], that only deals with fields of Laurent series (i.e. with representations of the absolute Galois groups $\mathrm{Gal}(F((T)))$). It is clear however, that the construction thereof is 'non-formal': it indeed provides a ρ_1 as in Proposition 3.4. Let us begin with a preparatory Lemma, whose proof is a nice exercise.

Lemma 3.3. *Let p be a prime.*
Let F be a number field, such that $\mu_p \subset F$ but $\mu_{p^2} \nsubseteq F$.
There exists a 1-cocycle

$$c : \mathrm{Gal}(F) \longrightarrow \mathbb{F}_p \simeq \mu_p^{\otimes 2},$$

that does not lift to a 1-cocycle

$$\mathrm{Gal}(F) \longrightarrow \mu_{p^2}^{\otimes 2}.$$

Proof. Consider the (Kummer) exact sequences of $\mathrm{Gal}(F)$-modules

$$(\mathcal{K}) := 0 \longrightarrow \mu_p \longrightarrow \mu_{p^2} \xrightarrow{x\mapsto x^p} \mu_p \longrightarrow 0$$

and

$$(\mathcal{K}^{\otimes 2}) := 0 \longrightarrow \mu_p^{\otimes 2} \longrightarrow \mu_{p^2}^{\otimes 2} \longrightarrow \mu_p^{\otimes 2} \longrightarrow 0.$$

The choice of a primitive p-th root of 1 in F, yields an isomorphism of $\mathrm{Gal}(F)$-modules $\mathbb{F}_p \simeq \mu_p$. Use it to rewrite these sequences, as

$$(\mathcal{K}) : 0 \longrightarrow \mu_p \longrightarrow \mu_{p^2} \longrightarrow \mathbb{F}_p \longrightarrow 0$$

and

$$(\mathcal{K}^{\otimes 2}) : 0 \longrightarrow \mu_p \longrightarrow \mu_{p^2}^{\otimes 2} \longrightarrow \mathbb{F}_p \longrightarrow 0.$$

Form the Baer difference

$$\Delta := (\mathcal{K}^{\otimes 2}) - (\mathcal{K}) : 0 \longrightarrow \mu_p \longrightarrow * \longrightarrow \mathbb{F}_p \longrightarrow 0.$$

One checks that Δ is an extension of $(\mathbb{F}_p, \mathrm{Gal}(F))$-modules. To do so, one may use the connecting arrow κ, introduced in [4], section 3.5. This connecting arrow is compatible to Baer sum. Since $(\mathcal{K})$ and $(\mathcal{K}^{\otimes 2})$ share the same connecting arrow (viz. the chosen isomorphism $\mathbb{F}_p \xrightarrow{\sim} \mu_p$), it follows that Δ has $\kappa = 0$, meaning that its middle term $*$ is an $\mathbb{F}_p$-vector space, as desired. Consequently, the isomorphism class $[\Delta]$ of the extension Δ belongs to

$$\mathrm{Ext}^1_{(\mathbb{F}_p,\mathrm{Gal}(F))-\mathrm{mod}}(\mathbb{F}_p, \mu_p) = H^1(F, \mu_p) = F^\times / F^{\times p},$$

where equality on the right is provided by Kummer theory. Write $[\Delta] = (b)$, for some $b \in F^\times$. By assumption, the $\mathrm{Gal}(F)$-modules μ_{p^2} and $\mu_{p^2}^{\otimes 2}$ are not isomorphic, so that Δ is non-split. Equivalently, $(b) \neq 0$. Denote by

$$\beta_1, \beta_2, \delta : H^1(., \mathbb{F}_p) \longrightarrow H^2(., \mu_p)$$

the Bockstein maps of $(\mathcal{K}), (\mathcal{K}^{\otimes 2})$ and Δ, respectively. By Kummer theory, $\beta_1 = 0$. By compatibility of Bockstein maps to Baer sum, one computes, for every $x \in H^1(F, \mathbb{F}_p)$:

$$\beta_2(x) = \delta(x) + \beta_1(x) = \delta(x) = x \cup (b) \in \mathrm{Br}(F)[p].$$

Pick a place v of F, such that the image of (b), under the restriction $H^1(F, \mu_p) \xrightarrow{(t)\mapsto(t)_v} H^1(F_v, \mu_p)$, is non-zero. [As usual, F_v stands here for the completion of F at v]. Then, by local class field theory and weak approximation, there exists $x \in H^1(F, \mathbb{F}_p)$ such that the cup-product $x_v \cup (b)_v \in \mathrm{Br}(F_v)[p]$ is non-zero. A fortiori, one has $x \cup (b) \neq 0 \in \mathrm{Br}(F)[p]$. Let c be a 1-cocycle representing x. The fact that $\beta_2(x) \neq 0$, exactly means that c does not lift to a 1-cocycle of the requested shape. □

PROPOSITION 3.4. *(See* [7]*.)*
Let p be an odd prime.
Let F and c be as in Lemma 3.3. Denote by

$$t : \mathrm{Gal}(F(T)) \longrightarrow \mu_p$$

the 1*-cocycle (which is here a homomorphism) corresponding, via Kummer theory, to*

$$(T) \in H^1(F(T), \mu_p) = F(T)^\times / F(T)^{\times p}.$$

Consider the representation

$$\rho_1 : \mathrm{Gal}(F(T)) \longrightarrow \mathbf{B}_3(\mathbb{F}_p),$$

given by the formula

$$\begin{pmatrix} 1 & t & t^2 + c \\ 0 & 1 & 2t \\ 0 & 0 & 1 \end{pmatrix}.$$

It does not lift to a representation

$$\rho_2 : \mathrm{Gal}(F(T)) \longrightarrow \mathbf{B}_3(\mathbb{Z}/p^2).$$

In fact, it does not even lift formally at T: the composite representation

$$\widehat{\rho}_1 : \mathrm{Gal}(F((T))) \xrightarrow{\mathrm{nat}} \mathrm{Gal}(F(T)) \xrightarrow{\rho_1} \mathbf{B}_3(\mathbb{F}_p)$$

does not lift to a representation

$$\mathrm{Gal}(F((T))) \longrightarrow \mathbf{B}_3(\mathbb{Z}/p^2).$$

The raw idea of proof goes like this. By contradiction, suppose that $\widehat{\rho}_1$ lifts to

$$\tilde{\rho}_2 : \mathrm{Gal}(F((T))) \longrightarrow \mathbf{B}_3(\mathbb{Z}/p^2).$$

Via a computation of residues in Galois cohomology, one shows that $\tilde{\rho}_2$ can be picked of the shape

$$\begin{pmatrix} \chi^2 & * & * \\ 0 & \chi & * \\ 0 & 0 & 1 \end{pmatrix},$$

where $\chi : \mathrm{Gal}(F) \longrightarrow (\mathbb{Z}/p^2)^\times$ is the cyclotomic character modulo p^2 (that is trivial modulo p, by the assumption $\mu_p \subset F$). Observe that the Galois module corresponding to χ^2 is $\mu_{p^2}^{\otimes 2}$.
Using that the center of $\mathbf{U}_3(\mathbb{F}_p)$ is

$$\mathbb{Z}/p \simeq \begin{pmatrix} 1 & 0 & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

another computation shows that c would lift, to a 1-cocycle with values in $\mu_{p^2}^{\otimes 2}$, contradicting the initial assumption.

4. Positive results, over all fields.

For a detailed exposition of the results stated here (in a slightly different language), the reader may consult section 3 of [13].

4.1. When p is odd...

... two-dimensional Galois representations always lift, as the following general statement shows. It is Theorem 6.1 of [3], whose main contribution is to provide a formalism that is insensitive to k.

Theorem 4.1. *Let F be a field. Let k be a field of characteristic p. Then, the arrow*

$$H^1(\mathrm{Gal}(F_s/F), \mathbf{GL}_2(\mathbf{W}_2(k))) \longrightarrow H^1(\mathrm{Gal}(F_s/F), \mathbf{GL}_2(k))$$

is surjective.

It is natural to ask, if this generalises to Witt vectors of higher length.

Question 4.2. Let F be a field. Let k be a field of characteristic p. Is the arrow

$$H^1(\mathrm{Gal}(F_s/F), \mathbf{GL}_2(\mathbf{W}_3(k))) \longrightarrow H^1(\mathrm{Gal}(F_s/F), \mathbf{GL}_2(k))$$

surjective?

To my knowledge, the answer is not known. A partial result is *stable* liftability of two-dimensional Galois representations, again furnished by [3], Theorem 6.1. Precisely, given a two-dimensional (Galois) representation V over k, there exists another (explicit) representation V', such that $V \bigoplus V'$ lifts to a representation over $\mathbf{W}(k)$ (the ring of full p-typical Witt vectors. Proving/disproving actual liftability to $\mathbf{W}_3(k)$, would definitely require some new insight.

4.2. When $p = 2$...

...Galois representations over $\mathbb{F}_2$ lift up to dimension four, as follows.

Proposition 4.3. *[dimension three, over $\mathbb{F}_2$.]*
Let F be a field of characteristic not 2, containing μ_4. Then, the arrow

$$H^1(\mathrm{Gal}(F_s/F), \mathbf{U}_3(\mathbb{Z}/4)) \longrightarrow H^1(\mathrm{Gal}(F_s/F), \mathbf{U}_3(\mathbb{Z}/2))$$

is surjective.

Proof. It is a straighforward adaptation of the construction of section 3, to the case $p = 2$. This is done using the following fact, well-known to specialists (see Proposition 5.2 of [11]). Let $M := F(x^{\frac{1}{2}}, y^{\frac{1}{2}})/F$ be a biquadratic extension. Then, every central simple algebra

$$[A] \in \mathrm{Br}_2(M/F)$$

is of the shape

$$[A] = (u)_2 \cup (y)_2 + (x)_2 \cup (v)_2,$$

for some $u, v \in F^\times$. Details are left to the interested reader. □
To my knowledge, it is unknown whether the surjectivity statement of Proposition 4.3 holds for $\mathbf{U}_4$ (I believe it does not). However, there is the following result.

PROPOSITION 4.4. *[dimension four over $\mathbb{F}_2$, See [3], Theorem 6.1.] Let F be a field. Then, the arrows*

$$H^1(\mathrm{Gal}(F_s/F), \mathbf{B}_4(\mathbb{Z}/4)) \longrightarrow H^1(\mathrm{Gal}(F_s/F), \mathbf{B}_4(\mathbb{Z}/2))$$

and

$$H^1(\mathrm{Gal}(F_s/F), \mathbf{GL}_4(\mathbb{Z}/4)) \longrightarrow H^1(\mathrm{Gal}(F_s/F), \mathbf{GL}_4(\mathbb{Z}/2))$$

are surjective.

Remark 4.5. Let k be a field of characteristic 2. If $k \neq \mathbb{F}_2$, Proposition 4.3 actually fails over k; see Theorem 5.1.

Remark 4.6. In [3], Theorem 6.1 is stated for $\mathbf{GL}_4$ only, but the proof clearly gives the same result for $\mathbf{B}_4$.

5. Negative generic results.

In their recent work [12] and [13], Merkurjev and Scavia gave the list of all pairs (p, d), such that Question 2.4 has an affirmative answer, whatever the field F. They also solve the same problem, replacing $\mathbf{GL}_d$ by $\mathbf{B}_d$, and $\mathbb{F}_p$ (resp. $\mathbb{Z}/p^2$) by an arbitrary field k of characteristic p (resp. $\mathbf{W}_2(k)$). Their result can be formulated in a simple way: for $\mathbf{GL}_d$ or $\mathbf{B}_d$, there are no other cases in which *all* Galois representations lift mod p^2, than those listed in Section 4. Precisely:

THEOREM 5.1. *Let k be a field of characteristic p, and let $d \geq 1$ be an integer. The following are equivalent.*

(1) The arrow

$$H^1(\mathrm{Gal}(F_s/F), \mathbf{GL}_d(\mathbf{W}_2(k))) \longrightarrow H^1(\mathrm{Gal}(F_s/F), \mathbf{GL}_d(k))$$

is surjective for all fields F.

(2) If $|k| \geq 3$, then $d \leq 2$.
If $|k| = 2$ (equivalently, if $p = 2$ and $k = \mathbb{F}_2$), then $d \leq 4$.

In fact, Theorem 1.1 of [13] is slightly more precise. Here are some details. The crucial case is that of a finite field of coefficients (and, when $p = 2$, of the field $k = \mathbb{F}_2(t)$, that we do not discuss here). Henceforth, assume that $k = \mathbb{F}_q$, for $q = p^r$. Starting with any field K, one can then consider the generic d-dimensional Galois representation over K, with coefficients in k. It consists of a field extension F/K, together with a representation

$$\rho_{d,\mathrm{vers}} : \mathrm{Gal}(F_s/F) \longrightarrow \mathbf{GL}_d(k)$$

that is *versal*. Roughly speaking, this means that, for every field exension L/K, and for every Galois representation

$$\rho : \mathrm{Gal}(L_s/L) \longrightarrow \mathbf{GL}_d(k),$$

$\rho_{d,\mathrm{vers}}$ has a specialisation that is conjugate to ρ. Equivalently, it is a *versal torsor* over K, for the finite group $\mathbf{GL}_d(k)$, in the sense of [8]. Liftability of all d-dimensional representations, over all field extensions of K, is thus equivalent to that of $\rho_{d,\mathrm{vers}}$. Therefore, one focuses on disproving liftability of $\rho_{d,\mathrm{vers}}$. A meaningful observation, is that

Non-liftability of $\rho_{d,\mathrm{vers}}$ implies that of $\rho_{d',\mathrm{vers}}$, for all $d' > d$.

This is a consequence of item (1) of Lemma 2.7, applied to $V := \rho_{d,\mathrm{vers}}$ and to the trivial representation $V' = k^{d'-d}$. In light of this Lemma, the work is thus to disprove liftability of $\rho_{d,\mathrm{vers}}$, in the following cases:

(1) $p \geq 3$, $k = \mathbb{F}_p$, and $d = 3$,
(2) $p = 2$, $k = \mathbb{F}_{2^r}$ for $r \geq 2$, and $d = 3$,
(3) $p = 2$, $k = \mathbb{F}_2$ and $d = 5$.

Item (1) is treated in [12], as an application of a result of independent interest: the computation of *negligible* cohomology classes in $H^2(G, M)$, for all finite groups G and all finite G-modules M, over fields containing enough roots of unity. This result is explicit, and its proof is nicely constructive.
In item (2), the crucial case is $k = \mathbb{F}_4$. As far as I can see, this definitely requires more subtlety, than in the arguments of section 3.
In the current version of [13], item (3) is the hardest one- dealt with by intricate (though elementary) computations. These can hopefully be simplified.

6. Positive results, over specific fields.

In [10], Khare and Larsen prove lifting statements for Heisenberg-Galois representations (=representations of absolute Galois groups, with values in $\mathbf{U}_3$), when the field F is a global field, or a non-archimedean local field, containing μ_{p^2}.
In particular, they prove the following Proposition. At the time this survey is written, it is one of the few general results available in the literature, about Question 2.4 for global fields, in dimension $d \geq 3$. See also Theorem 1.5 of [1], that applies in any dimension for number fields, at the cost of a strong assumption on the representation.

Proposition 6.1. *[See* [10]*, Theorem 5.4.] Suppose that p is odd. Let F be a local field, or a number field, containing μ_{p^2}. Then, the following arrows are surjective:*

$$H^1(\mathrm{Gal}(F_s/F), \mathbf{U}_3(\mathbb{Z}/p^2)) \longrightarrow H^1(\mathrm{Gal}(F_s/F), \mathbf{U}_3(\mathbb{F}_p))$$

and

$$H^1(\mathrm{Gal}(F_s/F), \mathbf{GL}_3(\mathbb{Z}/p^2)) \longrightarrow H^1(\mathrm{Gal}(F_s/F), \mathbf{GL}_3(\mathbb{F}_p)).$$

Remark 6.2. Here again, the case of $\mathbf{GL}_3$ follows from that of $\mathbf{U}_3$, for purely group-theoretic reasons- see section 2.3.

Remark 6.3. Proposition 6.1 still holds upon replacing $\mathbb{F}_p$ by a field k of characteristic p (and accordingly, replacing $\mathbb{Z}/p^2$ by $\mathbf{W}_2(k)$). This upgrade is at the cost of minor modifications in proofs, as the interested reader may check.

For local fields, the proof of Proposition 6.1 just uses the following properties of F.

(1) It contains p^2-th roots of unity.
(2) The $\mathbb{F}_p$-vector space $H^2(F, \mathbb{F}_p)$ is one-dimensional.
(3) The cup-product

$$H^1(F, \mathbb{F}_p) \times H^1(F, \mathbb{F}_p) \longrightarrow H^2(F, \mathbb{F}_p)$$

is a perfect pairing of finite-dimensional $\mathbb{F}_p$-vector spaces.

In the recent work [2], very general lifting theorems are proved for the so-called *p-manageable* profinite groups. We refer to [2] for details on the material presented next.

Definition 6.4. *Let G_p be a pro-p-group. Say that G_p is p-manageable if the following conditions are satisfied.*

(1) The $\mathbb{F}_p$-vector space $H^2(G_p, \mathbb{F}_p)$ is one-dimensional.
(2) The cup-product pairing of (possibly infinite-dimensional) $\mathbb{F}_p$-vector spaces

$$H^1(G_p, \mathbb{F}_p) \times H^1(G_p, \mathbb{F}_p) \longrightarrow H^2(G_p, \mathbb{F}_p) \simeq \mathbb{F}_p,$$

has trivial (left) kernel.
(3) There exists a continuous character

$$\theta_p : G_p \longrightarrow \mathbb{Z}_p^\times,$$

with the following property. Set $\mathbb{Z}_p(1) := \mathbb{Z}_p$, on which G_p acts via θ_p. Then, for every $r \geq 2$, the natural arrow

$$H^1(G_p, (\mathbb{Z}/p^r)(1)) \longrightarrow H^1(G_p, \mathbb{F}_p(1))$$

is onto.
Let G be any profinite group. Let $G_p \subset G$ be a pro-p-Sylow. Say that G is p-manageable, if G_p is p-manageable, and the character θ_p of item (3) extends to a character

$$\theta : G \longrightarrow \mathbb{Z}_p^\times.$$

Remark 6.5. Let G_p be a p-manageable pro-p-group. Using item (2), one can prove that the character $\theta_p : G_p \longrightarrow \mathbb{Z}_p^\times$ in item (3) is unique.

Let us give three famous examples of p-manageable profinite groups.

Example 6.6. (Absolute Galois groups of local fields.)
Let F be a finite extension of $\mathbb{Q}_l$, or of $\mathbb{F}_l((T))$, with $l = p$ allowed. Then $G := \mathrm{Gal}(F_s/F)$ is p-manageable. Moreover, in (3), $\mathbb{Z}_p(1)$ is the Tate module (of roots of unity of p-primary order) if $\mathrm{char}(F) \neq p$, or $\mathbb{Z}_p(1) = \mathbb{Z}_p$ if $\mathrm{char}(F) = p$.

Example 6.7. (Fundamental groups of curves.)
Let G be the algebraic fundamental group of a smooth proper complex curve of genus $g > 0$. Then G is p-manageable. Moreover, in (3), θ is trivial, i.e. $\mathbb{Z}_p(1) = \mathbb{Z}_p$.

Example 6.8. (Demushkin groups.)
Let G be a pro-p-group. If G satisfies items (1) and (2) of Definition 6.4, say that G is a Demushkin group. [In the classical terminology, one also requires that G be finitely generated, or equivalently that $H^1(G_p, \mathbb{F}_p)$ is finite.] If G is finitely generated, then a character θ as in item (3) exists, so that G is p-manageable. For a proof that does not use dualizing modules, see [2], Proposition 5.1.

Until the end of this section, G is a p-manageable profinite group, and $\theta, \mathbb{Z}_p(1)$ are as in item (3) of Definition 6.4.

A variant of Question 2.3 for G, then has a very strong positive answer. To state it, we introduce the following notation.

Definition 6.9. *For $r \geq 2$, consider a triangular representation*

$$\rho_r \colon G \longrightarrow \mathbf{B}_d(\mathbb{Z}/p^r).$$

Denote its mod p reduction by

$$\rho_1 \colon G \longrightarrow \mathbf{B}_d(\mathbb{F}_p).$$

Denote by V_r the representation of G on the free $\mathbb{Z}/p^r$-module $(\mathbb{Z}/p^r)^d$, furnished by ρ_r. Observe that V_r is naturally equipped with a complete flag of representations of G over $\mathbb{Z}/p^r$.

Definition 6.10. *(Wound Kummer flag, for $r = 1$.)*
Consider a triangular representation

$$\rho_1 \colon G \longrightarrow \mathbf{B}_d(\mathbb{F}_p).$$

Observe that ρ_1 gives rise to homomorphisms, for $i = 1, 2, \ldots d-1$,

$$\lambda_i : G \longrightarrow \mathbf{B}_2(\mathbb{F}_p),$$

corresponding matrixwise, to the (2×2) blocks centered at the diagonal. If one of the following three equivalent conditions is satisfied, we say that the (triangular) representation ρ_1 is wound Kummer.

1. *For all i, p divides $|\mathrm{Im}(\lambda_i)|$.*
2. *For all i, the extension (of one-dimensional representations of G over $\mathbb{F}_p$) corresponding to λ_i is non-split.*
3. *There is a unique G-invariant complete flag on V_1, given by ρ_1.*

DEFINITION 6.11. *(Wound Kummer flag, general case.)*
For $r \geq 1$, consider a triangular representation

$$\rho_r \colon G \longrightarrow \mathbf{B}_d(\mathbb{Z}/p^r).$$

The diagonal of ρ_r gives d multiplicative characters (for $i = 1, 2, \dots d$)

$$\chi_i : G \longrightarrow (\mathbb{Z}/p^r)^\times.$$

Say that ρ_r is wound Kummer if the following conditions hold.

(1) ρ_1 is wound Kummer, in the sense of Definition 6.10.
(2) For $i = 1, \dots, d$, the order of the character

$$\chi_i.\theta^i : G \longrightarrow (\mathbb{Z}/p^r)^\times$$

divides $(p-1)$.

Remark 6.12. Item (2) of Definition 6.11 can be reformulated as: the p-primary parts of χ_i and (the reduction modulo p^r of) θ^{-i} coincide.

The precise definition of a Kummer representation (=Kummer flag) is given in [2], Definition 7.13. The rough idea goes like this. A flag

$$\rho_r \colon G \longrightarrow \mathbf{U}_d(\mathbb{Z}/p^r)$$

is Kummer, if the combinatorics of partial splittings of ρ_r, is the same as that of its mod p reduction ρ_1. One may then think of a wound Kummer flag ρ_r (defined precisely above) as a Kummer flag such that ρ_1 has no partial splittings at all.

A very strong step-by-step lifting result is available for wound Kummer, resp. for Kummer representations: Theorems 7.10, resp. 7.21 of [2]. In this survey, we content ourselves with two corollaries of these: Theorems 6.13 and 6.15 below. Separately, they illustrate the two meanings of "step-by-step":

- On the one hand, w.r.t. the depth r of the flag- see Theorem 6.13.
- On the other hand, w.r.t. the dimension d- see item (2) of Theorem 6.15.

The construction of the liftings is explicit, using an iterative deformation process, along which extensions are manipulated via elementary operations: Baer sum, push-forward and pull-back. A key technique is a mixture of gluing and lifting, called "gluifting" ([2], section 5).

THEOREM 6.13. *Let $d, r \geq 1$ be integers. Let ρ_r be a d-dimensional wound Kummer, resp. a Kummer representation. In the Kummer case, assume that $\mathbb{Z}/p^{r+1}(1) = \mathbb{Z}/p^{r+1}$. Then ρ_r lifts to a wound Kummer, resp. to a Kummer representation ρ_{r+1}.*

Remark 6.14. Kummer representations provide a natural framework, where one can lift certain Galois representations via the arrow

$$H^1(\mathrm{Gal}(F_s/F), \mathbf{GL}_d(\mathbb{Z}/p^{r+1})) \longrightarrow H^1(\mathrm{Gal}(F_s/F), \mathbf{GL}_d(\mathbb{Z}/p^r)),$$

for $d \geq 1$ and $r \geq 2$. Results of this kind are very rare. Observe that, for general F, this arrow is never surjective. Here is an example. Take $r = 2$ if p is odd, or $r = 3$ if $p = 2$. Then, surjectivity fails already for $d = 1$. Indeed, it is not hard to check, that it is equivalent to surjectivity of

$$H^1(\mathrm{Gal}(F_s/F), \mathbb{Z}/p^2) \longrightarrow H^1(\mathrm{Gal}(F_s/F), \mathbb{F}_p),$$

which does not hold in general, e.g. for $F = \mathbf{Q}$. For fields containing $\mathbb{C}$, there should be counter-examples also for $d = 2$, but I do not have any in mind.

THEOREM 6.15. *[[2], Corollary 7.22.]*
Consider a representation

$$\rho_1 \colon G \longrightarrow \mathbf{U}_d(\mathbb{F}_p).$$

Let $r \geq 2$, and assume that $\mathbb{Z}/p^r(1) = \mathbb{Z}/p^r$. Then, the following hold.

(1) There exists a lift of ρ_1, to a representation

$$\rho_r \colon G \longrightarrow \mathbf{U}_d(\mathbb{Z}/p^r).$$

(2) Futhermore, ρ_r can be picked such that the natural map

$$H^1(G, V_r) \longrightarrow H^1(G, V_1)$$

is surjective.

Remark 6.16. For item (1) to hold, the condition $\mathbb{Z}/p^r(1) = \mathbb{Z}/p^r$ is necessary.

Remark 6.17. For absolute Galois groups of local fields, it follows from results of [5], that item (1) holds with $\mathbf{B}_d$ in place of $\mathbf{U}_d$, without the assumption $\mathbb{Z}/p^r(1) = \mathbb{Z}/p^r$. However, by [2], Example 7.23, this cannot be achieved using powers of the cyclotomic character for the diagonal of ρ_r. In other terms, the d one-dimensional graded pieces of V_r cannot in general be of the form $L_{i,r} := \mathbb{Z}/p^r(n_i)$, for $i = 1, \dots d$.

Remark 6.18. It is not clear to me how to prove item (2) of Theorem 6.15, using the material of [5].

Remark 6.19. Item (2) can be thought of as "higher-dimensional Kummer theory", where the d-dimensional representation V_r replaces the one-dimensional cyclotomic module $\mathbb{Z}/p^r(1)$. Meanwhile, this analogy is seriously limited: in general, there is no choice of ρ_r, such that

$$H^1(H, V_r) \longrightarrow H^1(H, V_1)$$

is surjective *for all open subgroups $H \subset G$.*
Details are provided in the last section of this paper.

7. There is no "naive" two-dimensional Kummer theory.

In the literature, the next result is new.

Proposition 7.1. *Let $p \geq 5$ be a prime, and let F be a field of characteristic not p, containing all p^2-th roots of unity. Set $G := \mathrm{Gal}(F_s/F)$. Assume that, for every open subgroup $H \subset G$, the cup-product pairing*

$$H^1(H, \mathbb{F}_p) \times H^1(H, \mathbb{F}_p) \longrightarrow H^2(H, \mathbb{F}_p)$$

is non-degenerate, meaning that its left kernel is trivial. [This is the case if F is a local field. By Lemma 3.6 of [2]*, it is also the case if F is infinite and finitely generated over its prime subfield.]*
Consider a two-dimensional representation

$$\rho_1 \colon G \longrightarrow \mathbf{GL}_2(\mathbb{F}_p),$$

such that $|\mathrm{Im}(\rho_1)|$ is divisible by p.
Then, there does not exist a lift of ρ_1 to a representation

$$\rho_2 \colon G \longrightarrow \mathbf{GL}_2(\mathbb{Z}/p^2),$$

such that, with notation of Definition 6.9, the natural map

$$H^1(H, V_2) \longrightarrow H^1(H, V_1)$$

is surjective for every open subgroup $H \subset G$.

Proof. For the sake of contradiction, assume that such a ρ_2 exists. By assumption, there exists an open subgroup $G' \subset G$, such that $\rho_1(G')$ is cyclic of order p. Replacing G by G', and replacing ρ by a conjugate representation, one thus reduces to the case where $\rho_1 \neq 1$ takes values onto $\mathbf{U}_2(\mathbb{F}_p) = \mathbb{Z}/p$. Set $H := \mathrm{Ker}(\rho_1)$. If $\rho_2(H) = 1$, then the matrix

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathbf{GL}_2(\mathbb{F}_p)$$

would lift (via ρ_2) to an element of $\mathbf{GL}_2(\mathbb{Z}/p^2)$ of order p. This is impossible because $p \geq 5$ (classical check, left to the reader). Consequently, it suffices to prove that $\rho_2(H) = 1$. Since V_2 is a free $\mathbb{Z}/p^2$-module, the natural exact sequence of H-modules

$$0 \longrightarrow pV_2 \longrightarrow V_2 \longrightarrow V_2/pV_2 \longrightarrow 0$$

reads as

$$0 \longrightarrow V_1 \longrightarrow V_2 \longrightarrow V_1 \longrightarrow 0,$$

i.e.

$$(E) : 0 \longrightarrow \mathbb{F}_p^2 \longrightarrow V_2 \xrightarrow{q} \mathbb{F}_p^2 \longrightarrow 0.$$

By assumption, the arrow

$$q_* : H^1(H, V_2) \longrightarrow H^1(H, \mathbb{F}_p^2)$$

is onto. Since $\mu_{p^2} \subset F$, Kummer theory implies that the arrow

$$H^1(H, \mathbb{Z}/p^2) \longrightarrow H^1(H, \mathbb{F}_p)$$

is onto. Define

$$V_2' := (\mathbb{Z}/p^2)^2.$$

It is another (obvious) lift of the trivial representation H over $\mathbb{F}_p$, to a representation of H over $\mathbb{Z}/p^2$. There is a natural extension of (trivial) H-modules

$$(E') : 0 \longrightarrow \mathbb{F}_p^2 \longrightarrow V_2' \xrightarrow{q'} \mathbb{F}_p^2 \longrightarrow 0,$$

and by Kummer theory recalled above,

$$q'_* : H^1(H, V_2') \longrightarrow H^1(H, \mathbb{F}_p^2)$$

is onto as well. Consider (E) and (E') as extensions of $\mathbb{Z}/p^2$-modules (with an action of H). As such, form their Baer difference

$$(E) - (E') : 0 \longrightarrow \mathbb{F}_p^2 \longrightarrow D \xrightarrow{\pi} \mathbb{F}_p^2 \longrightarrow 0,$$

and denote it by Δ. Since q_* and q'_* are onto, so is the arrow

$$\pi_* : H^1(H, D) \longrightarrow H^1(H, \mathbb{F}_p^2).$$

To check this, observe first that surjectivity of q_* amounts to vanishing of the connecting map associated to the extension (E), reading as

$$\beta_E : H^1(H, \mathbb{F}_p^2) \longrightarrow H^2(H, \mathbb{F}_p^2).$$

The same fact holds for q'_*. Using that the formation of Baer sum is compatible to connecting maps, it follows that

$$\beta_\Delta : H^1(H, \mathbb{F}_p^2) \longrightarrow H^2(H, \mathbb{F}_p^2)$$

vanishes, whence the sought-for surjectivity. Next, since V_2 and V_2' are both lifts of the $\mathbb{F}_p$-vector space $V_1 (= \mathbb{F}_p^2)$ to free $\mathbb{Z}/p^2$-modules, it follows that D is in fact an $\mathbb{F}_p$-vector space. The proof is elementary, and left to the reader. [One may use the connecting arrow κ, introduced in [4], section 3.5.] Consequently, the extension of $(\mathbb{F}_p, H)$-modules Δ is provided by a matrix

$$\begin{pmatrix} D_{1,1} & D_{1,2} \\ D_{2,1} & D_{2,2} \end{pmatrix},$$

where each $D_{i,j}$ is an extension of $(\mathbb{F}_p, H)$-modules, of the shape

$$D_{i,j} : 0 \longrightarrow \mathbb{F}_p \longrightarrow P_{i,j} \longrightarrow \mathbb{F}_p \longrightarrow 0.$$

Denote by

$$d_{i,j} = [D_{i,j}] \in H^1(H, \mathbb{F}_p)$$

the cohomology class of $D_{i,j}$. The connecting map

$$\beta_\Delta : H^1(H, \mathbb{F}_p)^2 \longrightarrow H^2(H, \mathbb{F}_p)^2$$

is thus given (up to sign) by the formula

$$(x_1, x_2) \mapsto (x_1 \cup d_{1,1} + x_2 \cup d_{2,1} \ , \ x_1 \cup d_{1,2} + x_2 \cup d_{2,2}).$$

By the above, this connecting map identically vanishes, which implies that the four $d_{i,j}$'s lie in the kernel of the cup-product pairing

$$H^1(H,\mathbb{F}_p)\times H^1(H,\mathbb{F}_p)\longrightarrow H^2(H,\mathbb{F}_p).$$

By the non-degeneracy assumption, the $d_{i,j}$'s vanish. Consequently, the extension Δ is trivial, which implies that $V_2\simeq V_2'$, as $(\mathbb{Z}/p^2,H)$-modules. Equivalently, H acts trivially on V_2, as was to be shown. □

Remark 7.2. Assume that $p=2$, and that F is a field of characteristic not 2, containing μ_4. Let $\rho_1 : G\longrightarrow \mathbf{GL}_2(\mathbb{F}_2)$ be a representation, whose image is of order 2. Set $K:=\mathrm{Ker}(\rho_1)$. Then $V_1\simeq \mathbb{F}_2^{G/K}$ is a permutation G-module. Define $V_2:=(\mathbb{Z}/4)^{G/K}$. Then V_2 lifts V_1, and by Kummer theory combined to Shapiro's Lemma, the natural map

$$H^1(H,V_2)\longrightarrow H^1(H,V_1)$$

is surjective, for every open subgroup $H\subset G$. In that particular case, we have just shown that a two-dimensional Kummer theory exists.

I think it is fairly doable to provide a full answer to the existence problem, for two-dimensional Kummer theory as addressed above. One would need to examine the cases $p=2$ and $p=3$ thoroughly, and also the case $p\geq 5$, with no assumption on roots of unity.

8. Acknowledgements.

Thanks to Charles De Clercq, Federico Scavia, the anonymous referee for their reading and remarks. I am grateful to Jean-Pierre Tignol, for suggesting an improved presentation of section 3.

Bibliography

[1] Böckle, G. *Lifting mod p representations to characteristics p^2*. J. of Number Theory, 101(2):310–337, 2003.

[2] Conti, A., Florence, M. and Demarche, C. *Lifting Galois representations via Kummer flags*. arxiv:2403.08888.

[3] De Clercq, C. and Florence, M. *Lifting low-dimensional local systems*. Mathematische Zeitschrift, 300(1):125–138, 2022.

[4] De Clercq, C., Florence, M. and Lucchini-Arteche, G. *Lifting vector bundles to Witt vector bundles*. Israel J. of Math.

[5] Emerton, M. and Gee, T. *Moduli stacks of étale (Φ,Γ)-modules and the existence of crystalline lifts*. Ann. Math. Stud. 215. Princeton, NJ: Princeton University Press, 2023.

[6] Florence, M. *Smooth profinite groups, II : the Uplifting Pattern*. arxiv:2009.11140.

[7] Florence, M. *Triangular Galois representations that do not lift*. Available on the author's webpage.

[8] Garibaldi, S., Merkurjev, A., Serre, J.-P. *Cohomological invariants in Galois cohomology.*, volume 28 of *Univ. Lecture Series*. AMS, 2003.

[9] Karpenko, N. A. *Torsion in CH^2 of Severi-Brauer varieties and indecomposability of generic algebras*. Manuscr. Math., 88(1):109–117, 1995.
[10] Khare, C. B., Larsen, M. *Liftable groups, negligible cohomology and Heisenberg representations*. (arxiv:2009.01301).
[11] Lam, T. Y., Leep, D. B. and Tignol, J.-P. *Biquaternion algebras and quartic extensions*. Publ. Math., Inst. Hautes Étud. Sci., 77:63–102, 1993.
[12] Merkurjev, A. S. and Scavia, F. *Galois representations modulo p that do not lift modulo p^2. J. Am. Math. Soc.*, published online.
[13] Merkurjev, A. S. and Scavia, F. *The lifting problem for Galois representations*. arxiv:2501.18906.
[14] Tignol, J.-P. *Indecomposable algebras of prime exponent.* Adv. Math., 65:205–228, 1987.
[15] Tignol, J.-P. and Wadsworth, A. R. *Value functions on simple algebras, and associated graded rings*. Springer Monogr. Math. Springer, 2015.

Sorbonne Université, Université Paris Cité, CNRS, IMJ-PRG, F-75005 Paris, France
Email address: mathieu.florence@imj-prg.fr