Lifting Galois representations via Kummer flags

Andrea Conti, Cyril Demarche, Mathieu Florence

LIFTING GALOIS REPRESENTATIONS VIA KUMMER FLAGS

ANDREA CONTI, CYRIL DEMARCHE AND MATHIEU FLORENCE

Abstract. Let Γ be either i) the absolute Galois group of a local field F, or ii) the topological fundamental group of a closed connected orientable surface of genus g. In case i), assume that $\mu_{p^2} \subset F$. We give an elementary and unified proof that every representation $\rho_1 : \Gamma \longrightarrow \mathbf{GL}_d(\mathbb{F}_p)$ lifts to a representation $\rho_2 : \Gamma \longrightarrow \mathbf{GL}_d(\mathbb{Z}/p^2)$. [In case i), it is understood these are continuous.] The actual statement is much stronger: for all $r \geq 1$, under "suitable" assumptions, strictly upper triangular representations $\rho_r : \Gamma \longrightarrow \mathbf{U}_d(\mathbb{Z}/p^r)$ lift to $\rho_{r+1} : \Gamma \longrightarrow \mathbf{U}_d(\mathbb{Z}/p^{r+1})$, in the strongest possible step-by-step sense. Here "suitable" is made precise by the concept of *Kummer flag*. An essential aspect of this work, is to identify the common properties of groups i) and ii), that suffice to ensure the existence of such lifts.

Contents

1. Introduction

Let p be a prime. This paper presents a common framework to tackle lifting problems (from $\mathbb{Z}/p^r$ to $\mathbb{Z}/p^{r+1}$) for representations of two kinds of groups Γ: absolute Galois groups of local fields (which we refer to as the arithmetic case), and topological fundamental groups of closed connected orientable surfaces (the topological case). The challenge here is to achieve a reasonable degree of generality (say, in the arithmetic case, compared to the results of [2] and [7]), with a light toolkit and little effort.

Using local class field theory in the arithmetic case, and Poincaré duality in the topological case – both being very standard results – we derive common properties of groups of the above type. Namely, in both cases, the group Γ is *p-manageable* (a cohomological condition, similar to the notion of Demuškin group, see Definition 3.2) and Γ satisfies W90 (a weak formal version of Hilbert's Theorem 90, see Definition 3.9). Our lifting theorems are valid for all groups satisfying these two properties (including two-dimensional Poincaré groups, see Section 5). Via basic operations for extensions of representations of (pro-)finite groups, we are able to lift a reducible $\mathbb{Z}/p^r$-representation ρ_r of Γ to a $\mathbb{Z}/p^{r+1}$-representation, whenever we can equip ρ_r with a *Kummer flag*: loosely speaking, this means that ρ_r is unipotent, and every sub-extension of ρ_r which is trivial mod p is also trivial mod p^r. This is a combinatorial property, for which we refer to Definition 7.13.

We give a more precise statement of our results. To fix ideas, let Γ be one of the following groups:

- the absolute Galois group of a local field F ($\mathbb{R}$, or a finite extension of $\mathbb{Q}_\ell$ or $\mathbb{F}_\ell((t))$, with $\ell = p$ allowed);
- the topological fundamental group of a closed connected orientable surface.

Then our Theorem 7.21 implies the following.

Theorem. *Let $d, r \geq 1$ be two integers, and let $\rho_r \colon \Gamma \longrightarrow \mathbf{GL}_d(\mathbb{Z}/p^r)$ be a continuous representation equipped with a Kummer flag. In the arithmetic case, assume that F contains a primitive p^{r+1}-th root of unity.*

Then ρ_r admits a lift $\rho_{r+1}\colon \Gamma \longrightarrow \mathbf{GL}_d(\mathbb{Z}/p^{r+1})$, equipped with a Kummer flag lifting the given one on ρ_r.

For mod p unipotent representations, there is the following immediate corollary.

COROLLARY. *Let $\rho_1\colon \Gamma \longrightarrow \mathbf{U}_d(\mathbb{Z}/p) \subset \mathbf{GL}_d(\mathbb{Z}/p)$ be a strictly upper triangular representation. In the arithmetic case, assume that F contains a primitive p^{r+1}-th root of unity. Then ρ_1 lifts, to a strictly upper triangular representation $\rho_{r+1}\colon \Gamma \longrightarrow \mathbf{U}_d(\mathbb{Z}/p^{r+1}) \subset \mathbf{GL}_d(\mathbb{Z}/p^{r+1})$.*

The proof of Theorem 7.21 goes by induction on the dimension of the representation, and actually gives a much finer result: given a $(d-1)$-dimensional Kummer flag $\nabla_{d-1,r}$ mod p^r, an extension of $\nabla_{d-1,r}$ to a d-dimensional mod p^r Kummer flag $\nabla_{d,r}$, and a lift $\nabla_{d-1,r+1}$ of $\nabla_{d-1,r}$ to a $(d-1)$-dimensional Kummer flag mod p^{r+1}, we can "glue" $\nabla_{d,r}$ and $\nabla_{d-1,r+1}$ along $\nabla_{d-1,r}$ to obtain a d-dimensional Kummer flag mod p^{r+1} that lifts $\nabla_{d,r}$ and extends $\nabla_{d-1,r+1}$ (a process that we refer to as "gluifting"). This stronger statement has the following cohomological consequence.

COROLLARY. *(See Corollary 7.22)*
Let $r \geq 2$ be an integer. Assume, in the arithmetic case, that F contains a primitive p^r-th root of unity. Let V_1 be a unipotent representation of Γ over $\mathbb{F}_p$. There exists a lift of V_1, to a unipotent representation V_r over $\mathbb{Z}/p^r$, such that the natural map

$$H^1(\Gamma, V_r) \longrightarrow H^1(\Gamma, V_1 = V_r/p)$$

is surjective.

Via classical cohomological arguments, our main theorem implies the liftability of arbitrary (=not necessarily triangularizable) representations, from $\mathbb{Z}/p$ to $\mathbb{Z}/p^2$.

COROLLARY. *(See Corollary 7.25)*
Let $d \geq 1$ be an integer, and let $\rho_1 : \Gamma \longrightarrow \mathbf{GL}_d(\mathbb{F}_p)$ be a mod p representation. In the arithmetic case, assume that F contains a primitive p^2-th root of unity. Then ρ_1 lifts to a representation $\rho_2 : \Gamma \longrightarrow \mathbf{GL}_d(\mathbb{Z}/p^2)$.

Remark. If F is a field, and $k \geq 1$, let $F(\mu_k)$ denote the extension of F generated by k-th roots of unity. In the previous theorem and its corollaries, one can replace the condition about roots of unity (in the arithmetic case) by the slightly more general assumption that $F(\mu_p) = F(\mu_{p^{r+1}})$, where $r = 1$ in the last corollary (see Remark 7.14).

In addition, we prove stronger results for ρ_r admitting a unique complete Γ-invariant flag, with no assumption on roots of unity in the arithmetic case. See Proposition 7.10, where we call such a unique flag a *wound Kummer flag*.
In all of our results, $\mathbb{Z}/p^r$ can be replaced with the ring of Witt vectors $\mathbf{W}_r(k)$ of a finite field k (see Section 7.2). For simplicity, we stick to $k = \mathbb{Z}/p$.
We remark in particular that we are able to control the coefficients of the lifts, which is not the case in previous arithmetic results that we recall below.
On the topological side, as far as we know, our results are new. In the course of an email exchange, Hélène Esnault observed that the case of an absolutely irreducible ρ_1, in Item (2), is simple to handle. Indeed, the corresponding $\mathbb{F}_p$-point of the character variety of Γ is then smooth. As such, it lifts to a $\mathbb{Z}_p$-point, producing a lift of ρ_1 to $\rho_\infty : \Gamma \longrightarrow \mathbf{GL}_d(\mathbb{Z}_p)$. This fact illustrates that, with regards to liftability, the (opposite) case of unipotent representations is the most delicate.

Relating our results to other works, on the arithmetic side.
In this number-theoretic context, liftability of a mod p representation, to coefficients in $\mathbb{Z}_p$ or a DVR containing it, has been widely investigated. One typically requires such a lift to possess certain p-adic Hodge theoretic properties (i.e. crystalline, semistable, de Rham) so that one can (conjecturally) attach to it an automorphic representation of a suitable reductive group. We refer to the introduction of [9] for a brief summary of this line of work, prior to the very recent works of Emerton-Gee [7] and Böckle-Iyengar-Paškūnas [2]. To conclude, we briefly relate our work to theirs, as well as to earlier works of Böckle, Clozel-Harris-Taylor, and Khare-Larsen.

Emerton and Gee [7] rely on advanced techniques in arithmetic geometry to prove that every continuous representation $\overline{\rho}\colon \Gamma_F \longrightarrow \mathbf{GL}_d(\mathbb{F}_p)$, F a p-adic field, admits a crystalline lift $\rho\colon \Gamma_F \longrightarrow \mathbf{GL}_d(\mathcal{O})$, $\mathcal{O}$ the valuation ring of a p-adic field. Their proof goes via a study of the geometry of the stack of (φ,Γ)-modules that they construct. Specializing ρ modulo p^r, $r \geq 1$, gives a mod p^r lift of ρ_1. When ρ_1 is triangular (i.e. admits a complete flag of sub-representations), the Emerton-Gee lift ρ is also triangular, since it is constructed via recursive liftings of the Jordan-Hölder factors of ρ_1 and of their extensions [7, Theorem 6.4.4]. In particular, they produce triangular mod p^r lifts of ρ_1, as we do in the case when F contains the p^r-th roots of unity. However, their lifting result does not imply ours: in Theorem 7.21, for $r \geq 2$, one starts with a mod p^r representation ρ_r, equipped with a Kummer flag, and one constructs a mod p^{r+1} lift, also equipped with a Kummer flag. Emerton and Gee's method, on the other hand, does not directly produce a lift of ρ_r: one first needs to reduce ρ_r mod p, and then lift (mod p^{r+1}) the resulting ρ_1 to a $\tilde{\rho}_{r+1}$ with $\mathcal{O}$-coefficients. Its mod p^r reduction is in general not isomorphic to ρ_r. Also, it is not guaranteed that a given sub-extension of $\tilde{\rho}_{r+1}$ is trivial, as soon as the corresponding sub-extension of ρ_1 is.

Böckle, Iyengar and Paškūnas [2] also prove the existence of lifts of an arbitrary ρ_1 to $\mathcal{O}$-coefficients as above (hence to $\mathcal{O}/p^r$), via deformation theory. However, they do not mention that if ρ_1 is triangular then one can always find a triangular $\mathbb{Z}/p^r$-lift in its deformation space.

For an arbitrary local field F, and for global F in some cases when the corresponding deformation problem is unobstructed, Böckle [1] is able to lift continuous $\mathbb{Z}/p$-linear representations of Γ_F to $\mathbb{Z}/p^2$, using a description of the absolute Galois group via generators and relations. Therefore, Corollary 7.25(2) follows from his work. As far as explicitly shown, Böckle's method produces lifts to $\mathbb{Z}_p$ (hence to $\mathbb{Z}/p^r$, $r > 2$) only in special cases – see [1, Theorem 1.3, Proposition 1.4].

Suppose that F is a local field of characteristic 0 and residual characteristic $\ell \neq p$. Then Clozel, Harris and Taylor [3, Section 2.4.4] prove that every ρ_1 admitting a complete flag lifts to a $\mathbb{Z}_p$-representation also admitting a complete flag, with no assumption on roots of unity.

Finally, Khare and Larsen [9, Theorem 5.4] prove the following special case of our Corollary 7.25: $d = 3$, $r = 2$, and the diagonal is trivial mod p. Then, by an approximation process, they obtain the same lifting result for global fields. We did not try to adapt our results to the global arithmetic case. Hopefully this will be done in future works.

2. Notation and conventions

Let Γ be a profinite group and p be a prime number. For an integer $d \geq 1$, denote by $\mathbf{B}_d \subset \mathbf{GL}_d$ the subgroup formed by upper triangular matrices, and by $\mathbf{U}_d \subset \mathbf{B}_d$ the subgroup of $\mathbf{B}_d$ consisting of unipotent matrices.
Let $r \geq 1$ be an integer. A (Γ, r)-module is a finite $(\mathbb{Z}/p^r)$-module M, equipped with a continuous Γ-action. Here "continuous" just means that Γ acts on M through a finite quotient Γ/Γ_0, where $\Gamma_0 \subset \Gamma$ is an open normal subgroup. Set

$$M^\vee := \mathrm{Hom}_{\mathbb{Z}/p^r}(M, \mathbb{Z}/p^r),$$

viewed as (Γ, r)-module in the natural way. If M is moreover free of rank d as a $(\mathbb{Z}/p^r)$-module, we say that M is a (Γ, r)-bundle of rank d. Then, $M^\vee$ is a (Γ, r)-bundle of rank d, as well.
Let M_r be a (Γ, r)-bundle. For $1 \leq s < r$, there is the natural *reduction* exact sequence of (Γ, r)-bundles

$$0 \longrightarrow M_{r-s} \xrightarrow{i} M_r \xrightarrow{q} M_s \longrightarrow 0.$$

Here i denotes the injection arising from $M_r \xrightarrow{p^s \mathrm{Id}} M_r$ upon modding out $p^{r-s}M_r$, and q stands for the natural quotient (reduction).

2.1. Flags. A complete (Γ, r)-flag $\nabla_d = (V_i)_{1 \leq i \leq d}$ of rank d is the data of a (Γ, r)-bundle V_d, of rank d, together with a complete filtration by sub-(Γ, r)-bundles

$$0 = V_0 \subset V_1 \subset \cdots \subset V_{d-1} \subset V_d,$$

with $\mathrm{rank}(V_i) = i$ for all i. Thus, for all i, $L_i := V_i/V_{i-1}$ is a (Γ, r)-bundle of rank one. Up to isomorphism, it is given by a character $\chi_i : \Gamma \longrightarrow (\mathbb{Z}/p^r)^\times$. For $i \leq j$, set

$$V_{j/i} := V_j/V_i.$$

In particular, a complete (Γ, r) flag defines, for all $1 \leq i \leq d$, a character

$$\chi_i : \Gamma \longrightarrow \mathbf{GL}(L_i) = (\mathbb{Z}/p^r)^\times.$$

We denote by $\mathbf{End}(\nabla_d)$ the (Γ, r)-module of endomorphisms of ∇_d. It is the subring of $\mathbf{End}(V_d)$, that preserves the given complete filtration. Write $\mathbf{Aut}(\nabla_d)$ for $\mathbf{End}(\nabla_d)^\times$, the group of invertible elements in the ring $\mathbf{End}(\nabla_d)$.
For $0 \leq i < j < k \leq d$, there are extensions of (Γ, r)-modules

$$\mathcal{E}_{k/j,j/i} : 0 \longrightarrow V_{j/i} \xrightarrow{\iota} V_{k/i} \xrightarrow{\pi} V_{k/j} \longrightarrow 0\,,$$

naturally attached to ∇_d.
Denote by

$$\nabla_{d-1} : 0 = V_0 \subset V_1 \subset \cdots \subset V_{d-1},$$

resp. by

$$\nabla_{d/1} : 0 = V_0 \subset V_{2/1} \subset V_{3/1} \subset \cdots \subset V_{d/1},$$

the truncation, resp. the quotient, of ∇_d. These are complete $(d-1)$-dimensional (Γ, r)-flags.
A complete (Γ, r)-flag ∇_d can be seen as a triangular representation of Γ over $(\mathbb{Z}/p^r)$: given a basis of V_d compatible with ∇_d, one gets a representation

$$\rho : \Gamma \longrightarrow \mathbf{B}_d(\mathbb{Z}/p^r) \subset \mathbf{GL}_d(\mathbb{Z}/p^r).$$

Note that ρ factors through $\mathbf{U}_d(\mathbb{Z}/p^r) \subset \mathbf{B}_d(\mathbb{Z}/p^r)$, if and only if the Γ-action on every L_i is trivial, or equivalently if every $\chi_i = 1$.

From now on, the notation $V_{i,r}$ stands for a (Γ, r)-bundle of rank i, and accordingly, $\nabla_{d,r}$ denotes a complete d-dimensional flag of (Γ, r)-bundles. If $V_{i,r}$ is given, then for all $1 \leq s \leq r$, we denote its reduction $V_{i,r} \otimes_{\mathbb{Z}} \mathbb{Z}/p^s$ by $V_{i,s}$. It is a (Γ, s)-bundle. The similar convention for complete flags $\nabla_{d,r}$ is adopted.

2.2. Teichmüller lift. Let L be an invertible $(\Gamma, 1)$-bundle, given by a character

$$\chi_L : \Gamma \longrightarrow \mathbb{F}_p^\times.$$

Consider the multiplicative (Teichmüller) section

$$\tau : \mathbb{F}_p^\times \longrightarrow (\mathbb{Z}/p^r)^\times,$$

identifying $\mathbb{F}_p^\times$ with the group of $(p-1)$-th roots of unity in the ring $\mathbb{Z}/p^r$. Postcomposing by τ yields a character

$$\tau(\chi_L) : \Gamma \longrightarrow (\mathbb{Z}/p^r)^\times,$$

providing a natural (Γ, r)-bundle of rank one, denoted by $\mathbf{W}_r(L)$. It is the r-th Teichmüller lift of L.

3. Galois cohomology: p-manageable groups, and the W90 property

Let p be a prime. In this section, we introduce the notions of p-manageable profinite group, and the W90 property. We state in particular Lemma 3.8, the key tool for proving our lifting theorems in the next sections. These apply to all p-manageable profinite groups, satisfying W90. In Proposition 4.3, we provide two important examples of such groups: the absolute Galois group of a local field, and the profinite completion of the fundamental group of a closed connected orientable surface.

Definition 3.1. *Let*

$$(.,.) : V \times W \longrightarrow \mathbb{F}_p$$

be a bilinear pairing of $\mathbb{F}_p$-vector spaces. Consider it as a linear map

$$L : V \longrightarrow W^\vee,$$

$$v \mapsto (w \mapsto (v, w)).$$

The left kernel of $(.,.)$ is the subspace $\mathrm{Ker}(L) \subset V$.

Definition 3.2. *Let Γ_p be a pro-p-group. Let us say that Γ_p is p-manageable if the following conditions are satisfied.*

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

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

has trivial (left) kernel.

More generally, if Γ is a profinite group, one says that Γ is p-manageable if it admits a p-manageable pro-p-Sylow subgroup $\Gamma_p \subset \Gamma$.

Remark 3.3. This definition is slightly weaker than that of Demuškin groups (=Poincaré pro-p-groups of dimension 2), see [10], I.4.5, since one does not assume that the group $H^1(\Gamma_p, \mathbb{F}_p)$ is finite. In particular, the group Γ_p is not necessarily topologically finitely generated. Nevertheless, Demuškin groups are crucial examples of p-manageable groups.

Remark 3.4. If Γ is the absolute Galois group of a "reasonable" field F, condition (2) is very mild- see Lemma 3.6. By contrast, condition (1) is extremely strong. It does typically not hold for an F which is finitely generated over its prime subfield.

Remark 3.5. For $p = 2$, the group $\Gamma := \mathbb{Z}/2\mathbb{Z}$ is easily checked to be 2-manageable. This fails for $p \geq 3$: the group $\Gamma := \mathbb{Z}/p\mathbb{Z}$ satisfies condition (1), but not (2). Indeed, the cup-product pairing then identically vanishes. These assertions are straightforward, from the usual computation of the cohomology of cyclic groups.

LEMMA 3.6. *Let F be an infinite field of characteristic $\neq p$, finitely generated over its prime subfield. Condition (2) of Definition 3.2 then holds for $\Gamma = \mathrm{Gal}(F^{sep}/F)$.*

PROOF.
By a limit argument, using restriction/corestriction for finite extensions of degree prime-to-p, one can assume that $\mathbb{F}_p \simeq \mu_p \subset F^\times$, and reduce the question to proving that the cup-product

$$H^1(F, \mu_p) \times H^1(F, \mu_p) \longrightarrow \mathrm{Br}(F)$$

has trivial kernel. [This reduction applies to any field F.] Pick a non-zero element in $H^1(F, \mu_p)$, corresponding via Kummer theory to $(x) \in F^\times/(F^\times)^p$, where x is not a p-th power. We need to find some $(y) \in H^1(F, \mu_p)$, such that

$$(x) \cup (y) \neq 0 \in H^2(F, \mu_p).$$

Assume that F is a global field, and denote by V the set of all its places. One knows that the group

$$Ш^1(F, \mu_p) := \mathrm{Ker}(H^1(F, \mu_p) \longrightarrow \prod_{v \in V} H^1(F_v, \mu_p))$$

vanishes. Let $v \in V$ be such that x is unramified at v, and $(x)_v \neq 0 \in H^1(F_v, \mu_p)$. By local class field theory, there exists $y_v \in H^1(F_v, \mu_p)$, such that

$$(x)_v \cup (y_v) \neq 0 \in \mathrm{Br}(F_v).$$

Since the restriction map $H^1(F, \mu_p) \longrightarrow H^1(F_v, \mu_p)$ is surjective, one may assume that $y_v = y \in F^\times$. Then indeed, one has $(x) \cup (y) \neq 0 \in \mathrm{Br}(F)$. It remains to deal with an F which is not a global field. In that case, denote by $\mathbb{F} \subset F$ the prime subfield. Denote by d the transcendence degree of F over $\mathbb{F}$. If $\mathbb{F} = \mathbb{F}_l$, then $d \geq 2$. If $\mathbb{F} = \mathbb{Q}$, then $d \geq 1$. Replacing x by xt^p for some $t \in F^\times$, one may assume that x is transcendental over $\mathbb{F}$. Pick a transcendence basis $x = x_1, x_2, \ldots, x_d$ of F over $\mathbb{F}$. Set $E := \mathbb{F}(x_2, \ldots, x_d)$. Denote by $F' \subset F$ the separable closure of $E(x)$ in F. The extension F/F' is finite and purely inseparable, hence of degree prime-to-p. Moreover, $x \in F'$. For our purpose, using restriction/corestriction, we may replace F by F', thus reducing to the case $F/E(x)$ separable. Replacing E by its algebraic closure in F, one may further assume that E is algebraically closed in F. Thus, F is the function field $E(C)$ of a geometrically connected proper smooth E-curve C. The extension $F/E(x)$ corresponds to a finite separable E-morphism $C \longrightarrow \mathbb{P}^1$. Define $K := E(x)[T]/(T^p - x)$. The assumption $x \notin (F^\times)^p$ translates as: $L := K \otimes_{E(x)} F$ is a field. It is a finite separable extension of $E(x)$. Since E is an infinite field, finitely generated over its prime subfield, it is Hilbertian. Hence, there exist infinitely many $e \in E$, such that the specialisation of $L/E(x)$ at $x \mapsto e$ is a field extension L_e/E. In particular, there is a unique closed point of C lying above such an e. This way, one produces infinitely many closed points $c \in C$, such that $v_c(x) = 0$, and $x(c) \in E(c)^\times$ is not a p-th power, where $E(c)/E$ denotes the residue field of c. Let $\pi_c \in F^\times$ be a uniformizer at c (in other terms, $v_c(\pi_c) = 1$). Then,

$$(x) \cup (\pi_c) \neq 0 \in H^2(F, \mu_p),$$

e.g. because its residue at c is non-vanishing, namely

$$\mathrm{Res}_c((x) \cup (\pi_c)) = x(c) \neq 0 \in H^1(E(c), \mu_p).$$

This finishes the proof. □

the following lemma is an analogue of [10], I.4.5, Proposition 30:

LEMMA 3.7. *Let Γ be a p-manageable pro-p-group. Let V be a $(\Gamma, 1)$-bundle. Then, the cup-product pairing*

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

has trivial (left) kernel.

PROOF.
Since $\Gamma = \Gamma_p$ is pro-p, there exists an extension of $(\Gamma, 1)$-bundles

$$(E) : 0 \longrightarrow W \xrightarrow{i} V \xrightarrow{\pi} \mathbb{F}_p \longrightarrow 0.$$

We may then prove the result by induction on the dimension. The case $\dim(V) = 1$ follows from the definition of p-manageable. Suppose the Lemma holds for W. Denote the cohomology class of (E) by

$$e \in H^1(\Gamma, W).$$

If $e = 0$, then $V = W \bigoplus \mathbb{F}_p$, and the statement readily follows from the induction hypothesis. Henceforth, assume $e \neq 0$. Dualising (E), one gets the extension of $(\Gamma, 1)$-bundles

$$(E^\vee) : 0 \longrightarrow \mathbb{F}_p \longrightarrow V^\vee \xrightarrow{q} W^\vee \longrightarrow 0.$$

By induction, one knows that the pairing

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

has trivial left kernel. We shall thus tacitly identify $H^1(\Gamma, W)$ to an $\mathbb{F}_p$-subspace of $H^1(\Gamma, W^\vee)^\vee$. W.r.t. this pairing, the orthogonal of the one-dimensional space

$$\mathbb{F}_p \cdot e \subset H^1(\Gamma, W)$$

is the hyperplane

$$\mathrm{Ker}(H^1(\Gamma, W^\vee) \xrightarrow{\delta} H^2(\Gamma, \mathbb{F}_p) \simeq \mathbb{F}_p),$$

where δ is the connecting map in cohomology arising from the extension $(E^\vee)$. Indeed, the kernel of the linear form δ is the image of the map $i_*^\vee : H^1(\Gamma, V^\vee) \longrightarrow H^1(\Gamma, W^\vee)$, and for all $f \in H^1(\Gamma, V^\vee)$, we have (up to sign) $e \cup i_*^\vee(f) = i(e) \cup f = 0$ since $i(e) = 0$. Hence $\ker(\delta) = e^\perp$.
Consider a class $v \in H^1(\Gamma, V)$. Assume that $v \cup x = 0$, for all $x \in H^1(\Gamma, V^\vee)$. By naturality of the cup-product, and a little diagram chase left to the reader, this implies that $\pi_*(v) \in H^1(\Gamma, \mathbb{F}_p)$ is orthogonal to the whole of $H^1(\Gamma, \mathbb{F}_p)$. By condition (2) of Definition 3.2, one gets $\pi_*(v) = 0$, so that there exists $w \in H^1(\Gamma, W)$, with $i_*(w) = v$. Then, one checks as above that the class w is orthogonal to the image of

$$q_* : H^1(\Gamma, V^\vee) \longrightarrow H^1(\Gamma, W^\vee),$$

which is the hyperplane $\mathrm{Ker}(\delta)$. Thus the kernel of the $\mathbb{F}_p$-linear form $(w, .)$ is contained in that of $(e, .)$. It follows that $(w, .)$ is a multiple of $(e, .)$, implying (by induction assumption) that w is zero or collinear to e, hence $v = i_*(w) = 0$. □

LEMMA 3.8. *Let Γ be a p-manageable profinite group. Consider a non-split extension of $(\Gamma,1)$-bundles*

$$(E): 0 \longrightarrow L \xrightarrow{i} W \xrightarrow{\pi} V \longrightarrow 0,$$

where L is invertible. Denote its cohomology class by

$$e \neq 0 \in \mathrm{Ext}^1_{(\Gamma,1)}(V,L) = H^1(\Gamma, V^\vee \otimes L).$$

Then, the map

$$H^2(\Gamma,L) \xrightarrow{i_*} H^2(\Gamma,W)$$

is zero. Equivalently, the connecting arrow arising from (E),

$$H^1(\Gamma,V) \longrightarrow H^2(\Gamma,L),$$
$$v^1 \mapsto e \cup v^1$$

is onto.

PROOF.
Let us prove the first assertion, which is easily seen to be equivalent to the second one. By restriction/corestriction, and a limit argument (w.r.t. a pro-p-Sylow subgroup $\Gamma_p \subset \Gamma$), one sees that $\mathrm{Res}(E)$ is a non-split extension of $(\Gamma_p,1)$-bundles. Likewise, the question is then reduced to the case where Γ is a pro-p-group. Then $L \simeq \mathbb{F}_p$, and $H^2(\Gamma,\mathbb{F}_p)$ is one-dimensional. It thus suffices to prove that the connecting arrow $H^1(\Gamma,V) \longrightarrow H^2(\Gamma,L)$ is non-vanishing. This follows from Lemma 3.7 (applied to $V^\vee$). □

DEFINITION 3.9. *(The W90 property).*
Let Γ be a profinite group. Let $\Gamma_p \subset \Gamma$ be a pro-p-Sylow. Let $\mathbb{Z}_p(1)$ be a $\mathbb{Z}_p$-module of rank one, equipped with a Γ-action, occurring via a continuous character $\Gamma \xrightarrow{\chi} \mathbb{Z}_p^\times$. Say that the pair $(\Gamma,\mathbb{Z}_p(1))$ satisfies W90 (for Weak formal Hilbert 90), if the reduction map

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

is onto, for every $r \geq 2$.

Remark 3.10. For $p=2$, take the cyclic group of order 2, $\Gamma := C_2$. It acts on $\mathbb{Z}_2$ non-trivially, by the sign character. Define this Γ-module to be $\mathbb{Z}_2(1)$. It is then standard, that $(\Gamma,\mathbb{Z}_2(1))$ satisfies W90.

Remark 3.11. In [4], the pair $(\Gamma,\mathbb{Z}_p(1))$ is said to be $(1,\infty)$-cyclotomic, if surjectivity above holds not only for Γ_p, but also for every closed subgroup $\Gamma' \subset \Gamma$ (whose index might be divisible by p). Here, we just require surjectivity for Γ_p, because we shall be dealing exclusively with p-manageable profinite groups. Altogether, it might be the case that the main results of this paper, up to suitable modifications, are valid for these groups (dismissing the $W90$ assumption).

We end this section with a lemma:

LEMMA 3.12. *Let $(\Gamma,\mathbb{Z}_p(1))$ be a pair satisfying (W90) and L be a Γ-module of order p. Then the natural morphism $H^1(\Gamma,\mathbf{W}_{r+1}(L)(1)) \longrightarrow H^1(\Gamma,\mathbf{W}_r(L)(1))$ is surjective.*

Proof. There exists an isomorphism $L \simeq \mathbb{Z}/p\mathbb{Z}$ as Γ_p-modules. The morphism $H^1(\Gamma_p,\mathbf{W}_{r+1}(L)(1)) \longrightarrow H^1(\Gamma_p,\mathbf{W}_r(L)(1))$ identifies to $H^1(\Gamma_p,\mathbb{Z}/p^{r+1}(1)) \longrightarrow H^1(\Gamma_p,\mathbb{Z}/p^r(1))$. This last map is surjective by induction on r and reduction to the (W90) property. Therefore, by restriction-corestriction, the cokernel of the morphism $H^1(\Gamma,\mathbf{W}_{r+1}(L)(1)) \longrightarrow H^1(\Gamma,\mathbf{W}_r(L)(1))$ is both p-torsion and prime-to-p-torsion, hence it is trivial. □

4. Common properties shared by (seemingly) unrelated groups

We begin with gathering classical material about topological fundamental groups of surfaces. For convenience, short proofs are included.

Proposition 4.1. *Let Γ be the topological fundamental group of a closed connected orientable surface S_g, of genus $g \geq 1$. Let M be a finite abelian group, equipped with an action of Γ. The following holds.*

(1) The abelianisation Γ_{ab} is isomorphic to $\mathbb{Z}^{2g}$.

(2) If the Γ-action on M is trivial, there are natural isomorphisms

$$H^i(\Gamma, M) \xrightarrow{\sim} H^i_{singular}(S, M)$$

and

$$H^2(\Gamma, M) \xrightarrow{\sim} M.$$

(3) The cup-product

$$H^1(\Gamma, M) \times H^1(\Gamma, \mathrm{Hom}(M, \mathbb{Q}/\mathbb{Z})) \longrightarrow H^2(\Gamma, \mathbb{Q}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$$

is a perfect pairing of finite abelian groups.

(4) Denote by $\widehat{\Gamma}$ the profinite completion of Γ. For $i \leq 2$, consider the natural arrow, given by inflation,

$$H^i(\widehat{\Gamma}, M) \xrightarrow{\theta^i} H^i(\Gamma, M)\,,$$

where cohomology used at the source is that of a profinite group, with discrete coefficients (it is $\varinjlim H^i(\Gamma/\Gamma_0, M)$, where $\Gamma_0 \subset \Gamma$ runs through normal subgroups of finite index, acting trivially on M) and cohomology at the target is usual group cohomology. Then, θ^i is an isomorphism.

Proof. To prove (1), it is convenient to use the classical presentation of Γ by generators and relations:

$$\Gamma = \langle X_1, Y_1, \ldots, X_g, Y_g \,|\, [X_1, Y_1] \ldots [X_g, Y_g] = 1 \rangle.$$

From there, the result is obvious. Let us prove (2). The fact that $H^i(\Gamma, M) \longrightarrow H^i_{sing}(S, M)$ is an isomorphism, is a general fact that holds because the universal cover of S is contractible. The second assertion is classical, from the assumptions made on S. With the help of (1), item (3) is a direct consequence of Poincaré duality.

It remains to deal with (4). It is clear that θ^0 is an isomorphism. Let $\Gamma_0 \subset \Gamma$ be a normal subgroup of finite index, acting trivially on M. There is the inflation-restriction sequence

$$0 \longrightarrow H^1(\Gamma/\Gamma_0, M) \xrightarrow{\mathrm{Inf}} H^1(\Gamma, M) \xrightarrow{\mathrm{Res}} H^1(\Gamma_0, M) = \mathrm{Hom}(\Gamma_0, M).$$

It follows from the same exact sequence for any finite index normal subgroup Γ_1 of Γ that θ^1 is injective. Given a class $c \in H^1(\Gamma, M)$, let $\Gamma_1 \subset \Gamma$ be a normal subgroup of finite index, contained in $\mathrm{Ker}(\mathrm{Res}(c)) \subset \Gamma_0$. Using the inflation-restriction sequence for Γ_1, one sees that c is inflated from $H^1(\Gamma/\Gamma_1, M)$. This proves surjectivity of θ^1. For $i = 2$, and for any Γ_0 as above, there is an exact sequence

$$H^0(\Gamma/\Gamma_0, H^1(\Gamma_0, M)) \xrightarrow{e} H^2(\Gamma/\Gamma_0, M) \xrightarrow{\mathrm{Inf}} H^2(\Gamma, M).$$

Pick $x \in H^2(\Gamma/\Gamma_0, M)$, with $\mathrm{Inf}(x) = 0$. Pick an invariant class $c \in H^1(\Gamma_0, M) = \mathrm{Hom}(\Gamma_0, M)$, such that $e(c) = x$. As above, let $\Gamma_1 \subset \Gamma$ be any normal subgroup of finite index, contained in $\mathrm{Ker}(\mathrm{Res}(c))$. By a little diagram chase, using the exact sequence above and its analogue for Γ_1, one concludes that the inflation of

x in $H^2(\Gamma/\Gamma_1, M)$ vanishes. This proves injectivity of θ^2. It remains to prove surjectivity. Pick some $c \in H^2(\Gamma, M)$.
Let us first prove that its restriction to some subgroup of finite index vanishes. For Γ_0 as above, considering $\mathrm{Res}(c) \in H^2(\Gamma_0, M)$, one first reduces to the case where the action of Γ on M is trivial. By dévissage on the finite abelian group M, one reduces further, to $M = \mathbb{F}_p$. By Poincaré duality, $H^2(\Gamma, \mathbb{F}_p) \simeq \mathbb{F}_p$ has a generator of the shape $x_1 \cup x_2$, for $x_1, x_2 \in H^1(\Gamma, \mathbb{F}_p)$, so that $\mathrm{Ker}(x_1) \subset \Gamma$ does the job. Thus, there exists a normal subgroup of finite index $\Gamma_1 \subset \Gamma$, acting trivially on M, and such that $\mathrm{Res}_{\Gamma_1}(c) = 0 \in H^2(\Gamma_1, M)$. Introduce the extension of finite (Γ/Γ_1)-modules

$$(E) : 0 \longrightarrow M \xrightarrow{\iota} M[\Gamma/\Gamma_1] \longrightarrow N \longrightarrow 0,$$

where ι is the natural map. By Shapiro's Lemma,

$$\iota_*(c) = 0 \in H^2(\Gamma, M[\Gamma/\Gamma_1]) \simeq H^2(\Gamma_1, M).$$

Hence, c is of the form $(E) \cup x$, for some $x \in H^1(\Gamma, N)$. Let $\Gamma_2 \subset \Gamma_1$ be a subgroup of finite index, normal in Γ, and such that $x \in H^1(\Gamma/\Gamma_2, N)$. As the cup-product of two extensions of finite (Γ/Γ_2)-modules, c is then inflated from $H^2(\Gamma/\Gamma_2, M)$, proving surjectivity of θ^2. □

Remark 4.2. A representation $\Gamma \longrightarrow \mathbf{GL}_d(\mathbb{Z}/p^r)$ is the same as a continuous representation $\widehat{\Gamma} \longrightarrow \mathbf{GL}_d(\mathbb{Z}/p^r)$. Thus, the lifting problems considered in this text are the same for Γ and $\widehat{\Gamma}$. Point (4) of the preceding Lemma states they also share the same cohomology groups. [Note that $H^i(\widehat{\Gamma}, M) = H^i(\Gamma, M) = 0$, for $i \geq 3$.] All this is a particular case of "cohomological goodness" (in the sense of [10], I.2.6, exercise 2) for surface groups, see for instance [8], Proposition 3.7.

Proposition 4.3. *Let $(\Gamma, \mathbb{Z}_p(1))$ be one of the following.*

1. *The absolute Galois group $\Gamma = \mathrm{Gal}(F^{sep}/F)$, of a local field F ($\mathbb{R}$, $\mathbb{C}$, a finite extension of $\mathbb{Q}_\ell$, or a finite extension of $\mathbb{F}_\ell((t))$, for a prime ℓ possibly equal to p). Define the module $\mathbb{Z}_p(1)$ to be $\mathbb{Z}_p$ if $\mathrm{char}(F) = p$, or the Tate module of roots of unity of p-primary order in $\overline{F}$, if $\mathrm{char}(F) \neq p$.*
2. *The profinite completion Γ of the topological fundamental group $\Gamma_{g,top}$ of a closed connected orientable surface S_g, of genus $g \geq 1$. Take $\mathbb{Z}_p(1)$ to be the trivial module $\mathbb{Z}_p$.*

Then the group Γ is p-manageable, and $(\Gamma, \mathbb{Z}_p(1))$ satisfies W90.

Proof. Let us deal with item (1). The case $F = \mathbb{C}$ is trivial, and $F = \mathbb{R}$ is an exercise. If $\mathrm{char}(F) = p$, then F is of p-cohomological dimension 1 by Artin-Schreier theory (see [10], II, Proposition 3). This is a much stronger property than p-manageability and W90. In the remaining cases, $\mathrm{char}(F) \neq p$. The fact that Γ is p-manageable is then a straighforward consequence of local class field theory, stating in particular that $H^2(E, \mathbb{F}_p(1)) \simeq \mathbb{F}_p$, for every finite extension E/F. The property W90 is deduced from Hilbert's Theorem 90 for $\mathbf{G}_m$, namely $H^1(F, F^{sep\times}) = 0$. Let us deal with item (2). The W90 property follows from item (1) of Proposition 4.1, which also holds for every subgroup of finite index of $\Gamma_{g,top}$. By item (2) of this Proposition, one has $H^2(\Gamma'_{g',top}, \mathbb{F}_p) = \mathbb{F}_p$, for every subgroup of finite index $\Gamma'_{g',top} \subset \Gamma_{g,top}$ (since such a subgroup is of the same geometric origin). If this index is prime-to-p, using restriction/corestriction, one sees that the restriction $H^2(\Gamma_{g,top}, \mathbb{F}_p) \longrightarrow H^2(\Gamma'_{g',top}, \mathbb{F}_p)$ is injective – hence an isomorphism of one-dimensional $\mathbb{F}_p$-vector spaces. By a straightforward limit argument, condition (1) of the definition of p-manageable is thus satisfied. Condition (2) holds by item (3) of Proposition 4.1. □

Remark 4.4. In the Proposition above, $H^1(\Gamma, \mathbb{F}_p)$ is finite-dimensional. However, this is not required for our method to work.

Remark 4.5. Let E/F be an infinite algebraic extension of a local field F, of degree divisible by p^∞, as a supernatural number. This means here that $E = \varinjlim_{i\in\mathbb{N}} E_i$, where $F \subset E_i \subset E_{i+1}$ are finite extensions, whose degrees $[E_{i+1} : E_i]$ are all divisible by p. Local class field theory identifies the restriction

$$\mathrm{Br}(E_i) \longrightarrow \mathrm{Br}(E_{i+1})$$

to

$$\mathbb{Q}/\mathbb{Z} \xrightarrow{[E_{i+1}:E_i]\mathrm{Id}} \mathbb{Q}/\mathbb{Z}.$$

Since

$$\mathrm{Br}(E) = \varinjlim_{i\in\mathbb{N}} \mathrm{Br}(E_i),$$

One infers that $\mathrm{Br}(E)[p] = 0$, so that the p-cohomological dimension of E is ≤ 1. [In particular, this applies to $E = \varinjlim F(\mu_{p^i})$, the cyclotomic p-extension of F.] Therefore, all lifting problems considered in this text (for Γ_E) can easily be solved.

5. When $H^1(\Gamma, \mathbb{F}_p)$ is finite

In this paper, all lifting theorems hold for a profinite group Γ, which is both p-manageable and satisfies Property W90. The first condition is actually much stronger than the second. One can thus naively raise the following question.
Let Γ be a p-manageable profinite group. Does there exist a $\mathbb{Z}_p$-module of rank one $\mathbb{Z}_p(1)$, with a continuous Γ-action, such that the pair $(\Gamma, \mathbb{Z}_p(1))$ satisfies W90?
As the question is stated, the answer is most likely negative. However, it is positive if Γ is Demuškin (i.e. Γ is p-manageable, pro-p, and $H^1(\Gamma, \mathbb{F}_p)$ is finite). This result is found in [11], 9.3. The next Proposition is slightly more general: there, Γ is not required to be a pro-p-group. The proof we provide is constructive.

Proposition 5.1. *Let Γ be a profinite group, of cohomological dimension 2. Assume that $\dim_{\mathbb{F}_p}(H^2(\Gamma, \mathbb{F}_p)) = 1$, and that the cup-product pairing*

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

is a perfect pairing of finite abelian groups. Set $\mathbb{F}_p(1) := \mathbb{F}_p$. The following holds.

1. *There exists a lift of $\mathbb{F}_p(1)$ to a $\mathbb{Z}_p$-module of rank one, equipped with a continuous Γ-action, and denoted by $\mathbb{Z}_p(1)$, such that the natural arrow*
$$H^1(\Gamma, \mathbb{Z}/p^r(1)) \longrightarrow H^1(\Gamma, \mathbb{F}_p(1))$$
is surjective for every $r \geq 1$. This $\mathbb{Z}_p(1)$ is unique up to iso.
2. *(Poincaré duality mod p^r) For every $r \geq 1$, $H^2(\Gamma, \mathbb{Z}/p^r(1))$ is a free $\mathbb{Z}/p^r$-module of rank one, and the cup-product pairing*
$$H^1(\Gamma, \mathbb{Z}/p^r) \times H^1(\Gamma, \mathbb{Z}/p^r(1)) \longrightarrow H^2(\Gamma, \mathbb{Z}/p^r(1))$$
is a perfect pairing of finite abelian groups.

Proof. By induction on r, assume built a lift of $\mathbb{F}_p(1)$ to a (Γ, r)-bundle $\mathbb{Z}/p^r(1)$, satisfying the properties in items (1) and (2). Let us explain how to build $\mathbb{Z}/p^{r+1}(1)$. To do so, it is very convenient to use the ring scheme of truncated Witt vectors of length two, $\mathbf{W}_2$. Consider the natural surjection of rings

$$\pi : \mathbf{W}_2(\mathbb{Z}/p^r) \longrightarrow \mathbb{Z}/p^r,$$
$$(x_0, x_1) \mapsto x_0.$$

Recall that the Teichmüller lift for line bundles exists in full generality (see e.g. [6], 4.1). Denote by $\mathbf{W}_2(\mathbb{Z}/p^r(1))$ the Teichmüller lift of $\mathbb{Z}/p^r(1)$: it is a free $\mathbf{W}_2(\mathbb{Z}/p^r)$-module of rank one, equipped with a Γ-action. It lifts $\mathbb{Z}/p^r(1)$ via π. Consider the natural reduction sequence (of $(\mathbf{W}_2(\mathbb{Z}/p^r),\Gamma)$-modules)

$$(\mathcal{W}_r): 0 \longrightarrow \mathbb{Z}/p^r(1) \longrightarrow \mathbf{W}_2(\mathbb{Z}/p^r(1)) \xrightarrow{\pi(1)} \mathbb{Z}/p^r(1) \longrightarrow 0.$$

By Poincaré duality mod p^r, its connecting map in cohomology is of the shape

$$\beta : H^1(\Gamma,\mathbb{Z}/p^r(1)) \longrightarrow H^2(\Gamma,\mathbb{Z}/p^r(1)) \simeq \mathbb{Z}/p^r,$$

$$x \mapsto x \cup e_r,$$

for some (unique) $e_r \in H^1(\Gamma,\mathbb{Z}/p^r)$. Denote by

$$(\mathcal{E}_r): 0 \longrightarrow \mathbb{Z}/p^r \longrightarrow E_r \longrightarrow \mathbb{Z}/p^r \longrightarrow 0$$

the extension of (Γ,r)-bundles corresponding to e_r. Regard it as an extension of $(\mathbf{W}_2(\mathbb{Z}/p^r),\Gamma)$-modules, via π. Upon twisting by $\mathbb{Z}/p^r(1)$, its connecting homomorphism is β as well (i.e. the cup-product by e_r). Form the Baer difference

$$\mathcal{D}_r := (\mathcal{W}_r - \mathcal{E}_r(1)) : 0 \longrightarrow \mathbb{Z}/p^r(1) \longrightarrow L_r \xrightarrow{\lambda} \mathbb{Z}/p^r(1) \longrightarrow 0.$$

It is an extension of $(\mathbf{W}_2(\mathbb{Z}/p^r),\Gamma)$-modules. Since $\mathcal{E}_r$ is geometrically trivial (=trivial as an extension of $\mathbf{W}_2(\mathbb{Z}/p^r)$-modules), $\mathcal{D}_r$ is geometrically isomorphic to $\mathcal{W}_r$. Consequently, its middle term L_r, as a $\mathbf{W}_2(\mathbb{Z}/p^r)$-module, is free of rank one. By compatibility of connecting maps to Baer sum, one sees that the connecting map of $\mathcal{D}_r$ vanishes. Equivalently, the induced arrow

$$H^1(\Gamma,L_r) \xrightarrow{H^1(\lambda)} H^1(\Gamma,\mathbb{Z}/p^r(1))$$

is surjective. Introduce the homomorphism Φ of Lemma 5.4, and set

$$\mathbb{Z}/p^{r+1}(1) := L_r \otimes_\Phi \mathbb{Z}/p^{r+1}.$$

As a $\mathbb{Z}/p^{r+1}$-module, $\mathbb{Z}/p^{r+1}(1)$ is free of rank one. Observe that $\mathbb{Z}/p^{r+1}(1)\otimes_{\mathbb{Z}/p^{r+1}} \mathbb{F}_p$ is isomorphic to $\mathbb{F}_p(1)$ (given at the very start). However, a priori,

$$\mathbb{Z}/p^r(1)' := \mathbb{Z}/p^{r+1}(1) \otimes_{\mathbb{Z}/p^{r+1}} \mathbb{Z}/p^r$$

need not be isomorphic to $\mathbb{Z}/p^r(1)$ (constructed in the previous step). Consider the natural reduction sequence of $(\Gamma,r+1)$-modules

$$\mathcal{K}_{r+1}: 0 \longrightarrow \mathbb{Z}/p^r(1)' \longrightarrow \mathbb{Z}/p^{r+1}(1) \longrightarrow \mathbb{F}_p(1) \longrightarrow 0.$$

Using the commutative diagram of Lemma 5.4, one gets a commutative diagram of $(\Gamma,r+1)$-modules

$$\begin{array}{ccc} L_r & \xrightarrow{x\mapsto x\otimes 1} & \mathbb{Z}/p^{r+1}(1) \\ \downarrow{\scriptstyle \lambda} & & \downarrow{\scriptstyle \mathrm{nat}_{r+1}} \\ \mathbb{Z}/p^r(1) & \xrightarrow{\mathrm{nat}_r} & \mathbb{F}_p(1). \end{array}$$

Since $H^1(\lambda)$ and $H^1(\mathrm{nat}_r)$ are surjective, so is

$$H^1(\mathrm{nat}_{r+1}) : H^1(\Gamma,\mathbb{Z}/p^{r+1}(1)) \longrightarrow H^1(\Gamma,\mathbb{F}_p(1)).$$

By uniqueness of $\mathbb{Z}/p^r(1)$, this shows that $\mathbb{Z}/p^r(1)'$ is actually isomorphic to $\mathbb{Z}/p^r(1)$. Observe that, as in Lemma 3.12, the arrow

$$H^1(\Gamma,\mathbb{Z}/p^{r+1}(1)) \longrightarrow H^1(\Gamma,\mathbb{Z}/p^r(1))$$

is then surjective as well.

Let us prove uniqueness of $\mathbb{Z}/p^{r+1}(1)$. Denote by $\chi_r : \Gamma \longrightarrow (\mathbb{Z}/p^r)^\times$ the character

corresponding to $\mathbb{Z}/p^r(1)$. Assume that $\mathbb{Z}/p^{r+1}(1)'$ is some other choice for a suitable lift of $\mathbb{Z}/p^r(1)$. Its character is then of the shape

$$\chi'_{r+1} = \chi_{r+1} + \epsilon,$$

where

$$\epsilon : \Gamma \longrightarrow (1 + p^r\mathbb{Z}/p^{r+1}\mathbb{Z})^\times \simeq \mathbb{Z}/p$$

is simply a mod p character, corresponding to an extension of (Γ, r)-modules

$$(\epsilon) : 0 \longrightarrow \mathbb{F}_p \longrightarrow * \longrightarrow \mathbb{Z}/p^r \longrightarrow 0.$$

Consider the reduction sequences of $(\Gamma, r+1)$-modules

$$0 \longrightarrow \mathbb{F}_p(1) \longrightarrow \mathbb{Z}/p^{r+1}(1) \longrightarrow \mathbb{Z}/p^r(1) \longrightarrow 0$$

and

$$0 \longrightarrow \mathbb{F}_p(1) \longrightarrow \mathbb{Z}/p^{r+1}(1)' \longrightarrow \mathbb{Z}/p^r(1) \longrightarrow 0.$$

Since $\mathbb{Z}/p^{r+1}(1)$ and $\mathbb{Z}/p^{r+1}(1)'$ satisfy item (1), the connecting maps $H^1(\Gamma, \mathbb{Z}/p^r(1)) \longrightarrow H^2(\Gamma, \mathbb{F}_p(1))$ of both extensions vanish. Also, the Baer difference of these extensions is $(\epsilon)(1)$, i.e. $(\epsilon)\otimes_{\mathbb{Z}/p^r}\mathbb{Z}/p^r(1)$. Using compatibility of Baer sum to connecting maps, and surjectivity of $H^1(\Gamma, \mathbb{Z}/p^r(1)) \longrightarrow H^1(\Gamma, \mathbb{F}_p(1))$, a small chase reveals that $\epsilon \in H^1(\Gamma, \mathbb{F}_p)$ lies in the (left) kernel of the perfect cup-product pairing

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

Hence ϵ vanishes, proving uniqueness of $\mathbb{Z}/p^r(1)$.
The next step is to upgrade Poincaré duality, mod p^{r+1}. First, observe that applying $H^2(\Gamma, .)$ to $\mathcal{K}_{r+1}$ yields an exact sequence

$$0 \longrightarrow \mathbb{Z}/p^r \simeq H^2(\Gamma, \mathbb{Z}/p^r(1)) \xrightarrow{i} H^2(\Gamma, \mathbb{Z}/p^{r+1}(1)) \xrightarrow{s} \mathbb{Z}/p \simeq H^2(\Gamma, \mathbb{F}_p(1)) \longrightarrow 0.$$

Indeed, i is injective because the arrow $H^1(\mathrm{nat}_{r+1})$ above is surjective, and s is surjective because Γ is of cohomological dimension two. Next, observe that the natural composite

$$\mathbb{Z}/p^{r+1}(1) \twoheadrightarrow \mathbb{Z}/p^r(1) \hookrightarrow \mathbb{Z}/p^{r+1}(1)$$

equals $p\mathrm{Id}$. Applying $H^2(\Gamma, .)$, after a straightforward chase, one sees that the p-torsion of the group $H^2(\Gamma, \mathbb{Z}/p^{r+1}(1))$ is isomorphic to $H^2(\Gamma, \mathbb{F}_p(1)) \simeq \mathbb{F}_p$. Therefore, $H^2(\Gamma, \mathbb{Z}/p^{r+1}(1))$ must be a free $\mathbb{Z}/p^{r+1}$-module of rank one. It remains to prove that the duality arrow

$$\phi : H^1(G, \mathbb{Z}/p^{r+1}) \longrightarrow H^1(G, \mathbb{Z}/p^{r+1}(1))^\vee$$

is an iso. A little chase, using the two exact sequences

$$0 \longrightarrow \mathbb{F}_p \longrightarrow \mathbb{Z}/p^{r+1} \longrightarrow \mathbb{Z}/p^r \longrightarrow 0$$

$$0 \longrightarrow \mathbb{Z}/p^r(1) \longrightarrow \mathbb{Z}/p^{r+1}(1) \longrightarrow \mathbb{F}_p(1) \longrightarrow 0,$$

reveals that ϕ is injective. If $\mathbb{Z}/p^{r+1}(1) \simeq \mathbb{Z}/p^{r+1}$, it is hence an iso. Otherwise, observe that the long exact sequences in cohomology arising from extensions above, respectively give

$$0 \longrightarrow H^1(G, \mathbb{F}_p) \longrightarrow H^1(G, \mathbb{Z}/p^{r+1}) \longrightarrow H^1(G, \mathbb{Z}/p^r) \longrightarrow H^2(G, \mathbb{F}_p) \simeq \mathbb{F}_p$$

and

$$0 \longrightarrow H^0(G, \mathbb{F}_p) \longrightarrow H^1(G, \mathbb{Z}/p^r(1)) \longrightarrow H^1(G, \mathbb{Z}/p^{r+1}(1)) \longrightarrow H^1(G, \mathbb{F}_p) \longrightarrow 0.$$

Computing alternating products of cardinals of the finite groups involved, one gets

$$|H^1(G, \mathbb{Z}/p^{r+1})| \geq |H^1(G, \mathbb{Z}/p^{r+1}(1))|.$$

Thus, ϕ is an iso as well.
The recursive construction of $\mathbb{Z}_p(1)$ is over, and (1),(2) are proved. □

Remark 5.2. Observe that the case $p = 2$, $\Gamma_p = \mathbb{Z}/2$, though excluded from the statement of Proposition 5, is easily dealt with. For in that case, $\Gamma = \Gamma' \rtimes \mathbb{Z}/2$, for some unique open normal subgroup $\Gamma' \subset \Gamma$ of odd order. Set $\mathbb{Z}_2(1) := \mathbb{Z}_2$, on which Γ acts via the sign character $\Gamma \longrightarrow \mathbb{Z}/2 = \{1, -1\}$. Then (1) and (2) hold. Via a restriction/corestriction argument, this follows from the case of $\mathbb{Z}/2$.

Remark 5.3. Assume that the premises of Proposition 5.1 also hold for every open subgroup $\Gamma' \subset \Gamma$, in place of Γ. [This holds in the Demuškin case, i.e. when Γ is a pro-p-group.] Then, it is not hard to prove that (1) and (2) are also true for every open subgroup Γ' (for the same coefficients $\mathbb{Z}_p(1)$, restricted to Γ'). This means that the pair $(\Gamma, \mathbb{Z}_p(1))$ is $(1, \infty)$-cyclotomic, in the sense of [5].

To conclude, we deal with the Lemma that was used in the previous proof.

LEMMA 5.4. *For each $r \geq 1$, there exists a ring homomorphism*

$$\Phi : \mathbf{W}_2(\mathbb{Z}/p^r) \longrightarrow \mathbb{Z}/p^{r+1},$$

such that the diagram of ring homomorphisms

$$\begin{array}{ccc} \mathbf{W}_2(\mathbb{Z}/p^r) & \xrightarrow{\Phi} & \mathbb{Z}/p^{r+1} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \text{nat}} \\ \mathbb{Z}/p^r & \xrightarrow{\text{nat}} & \mathbb{F}_p \end{array}$$

commutes, where $\pi(x_0, x_1) = x_0$ is the natural surjection.

PROOF.
Consider the Witt vector Frobenius of the ring $\mathbb{Z}/p^{r+1}$, given by the first Witt polynomial:

$$\mathbf{W}_2(\mathbb{Z}/p^{r+1}) \xrightarrow{\text{Frob}} \mathbb{Z}/p^{r+1},$$
$$(x_0, x_1) \mapsto x_0^p + p x_1.$$

As in [6], Lemma 5.5 (to which we refer for details), one proves that Frob factors through the natural arrow $\mathbf{W}_2(\mathbb{Z}/p^{r+1}) \longrightarrow \mathbf{W}_2(\mathbb{Z}/p^r)$, giving rise to the promised ring homomorphism. The commutativity of the diagram is readily checked.

□

Exercise 5.5. Show that the ring $\mathbf{W}_2(\mathbb{Z}/p^r)$ is a $(\mathbb{Z}/p^{r+1})$-algebra.

6. Gluing, lifting and gluifting extensions of (Γ, r)-bundles

In this section, Γ is any group, or profinite group. In the latter case, all representations are assumed to be continuous.

DEFINITION 6.1. *(Gluing)*
Assume given two extensions of (Γ, r)-bundles,

$$\mathcal{E}_{d,r} : 0 \longrightarrow V_{1,r} \longrightarrow V_{d,r} \longrightarrow V_{d/1,r} \longrightarrow 0$$

and

$$\mathcal{F}_{d,r} : 0 \longrightarrow V_{d/1,r} \longrightarrow W_{d,r} \longrightarrow L_{d+1,r} \longrightarrow 0,$$

where $V_{1,r}$ and $L_{d+1,r}$ are invertible, and $V_{d,r}$, $W_{d,r}$ are d-dimensional.
A gluing of $\mathcal{E}_{d,r}$ and $\mathcal{F}_{d,r}$ is a pair $(\mathcal{E}_{d+1,r}, \phi_r)$, consisting of an extension of (Γ, r)-bundles

$$\mathcal{E}_{d+1,r} : 0 \longrightarrow V_{d,r} \longrightarrow V_{d+1,r} \longrightarrow L_{d+1,r} \longrightarrow 0,$$

and an isomorphism of extensions of (Γ, r)*-bundles*

$$\phi_r : \pi_*(\mathcal{E}_{d+1,r}) \xrightarrow{\sim} \mathcal{F}_{d+1,r},$$

where $\pi : V_{d,r} \longrightarrow V_{d/1,r}$ *is the natural surjection introduced earlier, and* $\pi_*(.)$ *denotes the induced push-forward operation, at the level of extensions.*
Isomorphisms of gluings are defined in the obvious way.

The obstruction to gluing $\mathcal{E}_{d,r}$ and $\mathcal{F}_{d,r}$ is the cup-product

$$\mathrm{obs}(\mathcal{E}_{d+1,r}) := \mathcal{E}_{d,r} \cup \mathcal{F}_{d,r} : 0 \longrightarrow V_{1,r} \longrightarrow V_{d,r} \longrightarrow W_{d,r} \longrightarrow L_{d+1,r} \longrightarrow 0.$$

It is a 2-extension of (Γ, r)-bundles, whose Yoneda class in

$$\mathrm{Ext}^2_{(\Gamma,r)-Mod}(L_{d+1,r}, V_{1,r}) = H^2(\Gamma, L^\vee_{d+1,r} \otimes V_{1,r})$$

vanishes if, and only if, a pair $(\mathcal{E}_{d+1,r}, \phi_r)$ as above exists.

Definition 6.2. *(Lifting).*
Assume given an extension of (Γ, r)*-bundles*

$$\mathcal{E}_r : 0 \longrightarrow V_{j,r} \longrightarrow V_{k,r} \longrightarrow V_{k/j,r} \longrightarrow 0.$$

A lifting of $\mathcal{E}_r$ *(mod* p^{r+1}*) is a pair* $(\mathcal{E}_{r+1}, \psi_r)$*, where*

$$\mathcal{E}_{r+1} : 0 \longrightarrow V_{j,r+1} \longrightarrow V_{k,r+1} \longrightarrow V_{k/j,r+1} \longrightarrow 0$$

is an extension of $(\Gamma, r+1)$*-bundles, and where*

$$\psi_r : q(\mathcal{E}_{r+1}) \xrightarrow{\sim} \mathcal{E}_r$$

is an isomorphism of extensions of (Γ, r)*-bundles.*
[Recall the notation $q(.) = (.) \otimes_{\mathbb{Z}/p^{r+1}} (\mathbb{Z}/p^r)$*.]*
Isomorphisms of liftings are defined in the obvious way.

Definition 6.3. *Define*

$$\mathbf{GL}(V_{j,r} \subset V_{k,r}) \subset \mathbf{GL}(V_{k,r}),$$

resp.

$$\mathbf{End}(V_{j,1} \subset V_{k,1}) \subset \mathbf{End}(V_{k,1}),$$

as the subgroup, resp. $\mathbb{F}_p$*-subspace, of automorphisms, resp. endomorphisms, preserving* $V_{j,r}$*, resp.* $V_{j,1}$*. In block form, it is given by*

$$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \subset \begin{pmatrix} * & * \\ * & * \end{pmatrix},$$

where blocks are of sizes j *and* $k - j$*. There is a natural reduction sequence*

$$0 \longrightarrow \mathbf{End}(V_{j,1} \subset V_{k,1}) \xrightarrow{i} \mathbf{GL}(V_{j,r+1} \subset V_{k,r+1}) \xrightarrow{q} \mathbf{GL}(V_{j,r} \subset V_{k,r}) \longrightarrow 1,$$

where q *is the natural reduction, and*

$$i(\epsilon) = \mathrm{Id} + p^r \epsilon,$$

for $\epsilon \in \mathbf{End}(V_{j,1} \subset V_{k,1})$*.*

Let $\mathcal{E}_r$ be an extension of (Γ, r)-bundles. Via a classical construction in non-abelian cohomology (see [10] chapter 1, 5.6), the obstruction to lifting $\mathcal{E}_r$ mod p^{r+1} is a natural class

$$\mathrm{obs}(\mathcal{E}_{r+1}) \in H^2(\Gamma, \mathbf{End}(V_{j,1} \subset V_{k,1})).$$

DEFINITION 6.4. *(Gluifting)*
Assume given two extensions of $(\Gamma, r+1)$*-bundles,*

$$\mathcal{E}_{d,r+1} : 0 \longrightarrow V_{1,r+1} \longrightarrow V_{d,r+1} \longrightarrow V_{d/1,r+1} \longrightarrow 0$$

and

$$\mathcal{F}_{d,r+1} : 0 \longrightarrow V_{d/1,r+1} \longrightarrow W_{d,r+1} \longrightarrow L_{d+1,r+1} \longrightarrow 0,$$

and a gluing

$$(\mathcal{E}_{d+1,r}, \phi_r)$$

of the extensions of (Γ, r)*-bundles* $\mathcal{E}_{d,r} := q(\mathcal{E}_{d,r+1})$ *and* $\mathcal{F}_{d,r} := q(\mathcal{F}_{d,r+1})$.
A lifting of the gluing $(\mathcal{E}_{d+1,r}, \phi_r)$*, is the data of a gluing* $(\mathcal{E}_{d+1,r+1}, \phi_{r+1})$ *of* $\mathcal{E}_{d,r+1}$ *and* $\mathcal{F}_{d,r+1}$*, together with an isomorphism*

$$\theta_r : q(\mathcal{E}_{d+1,r+1}, \phi_{r+1}) \xrightarrow{\sim} (\mathcal{E}_{d+1,r}, \phi_r),$$

as gluings of $\mathcal{E}_{d,r}$ *and* $\mathcal{F}_{d,r}$.
Altogether, the data of $(\mathcal{E}_{d+1,r+1}, \phi_{r+1}, \theta_r)$ *is called a gluifting of* $(\mathcal{E}_{d,r+1}, \mathcal{F}_{d,r+1}, \mathcal{E}_{d+1,r}, \phi_r)$.

Gluifting is related to Grothendieck's "extensions panachées", and makes sense in a much more general stacky setting, worth investigation. However, we stick here to an elementary concrete approach. Let us now explain how the obstruction to gluifting is a natural reduction of $\mathrm{obs}(\mathcal{E}_{d+1,r+1})$ to a mod p cohomology class.

LEMMA 6.5. *The obstruction to gluifting as above, is a natural class*

$$c_1 \in \mathrm{Ext}^2_{(\Gamma,1)}(L_{d+1,1}, L_{1,1}) = H^2(\Gamma, L^\vee_{d+1,1} \otimes_{\mathbb{F}_p} L_{1,1}),$$

such that

$$i_*(c_1) = \mathrm{obs}(\mathcal{E}_{d+1,r+1}) \in H^2(\Gamma, L^\vee_{d+1,r+1} \otimes_{\mathbb{Z}} L_{1,r+1}).$$

PROOF.
To simplify, assume first that $L_{d+1,r+1} = \mathbb{Z}/p^{r+1}$ is trivial.
Consider the natural surjection of $(\Gamma, r+1)$-modules

$$V_{d,r} \oplus (V_{d,r+1}/L_{1,r+1}) \xrightarrow{f} V_{d/1,r} \longrightarrow 0,$$

given by

$$f(v, l) := \pi(v) - q(l).$$

It fits into an extension of $(\Gamma, r+1)$-modules

$$\mathcal{Q} : 0 \longrightarrow N \longrightarrow V_{d,r} \oplus V_{d/1,r+1} \xrightarrow{f} V_{d/1,r} \longrightarrow 0,$$

whose kernel N naturally fits into the exact sequence

$$\mathcal{N} : 0 \longrightarrow L_{1,1} \longrightarrow V_{d,r+1} \xrightarrow{s} N \longrightarrow 0,$$

where

$$s(v) := (q(v), \pi(v)) \in N \subset V_{d,r} \oplus V_{d/1,r+1}.$$

The injection in $\mathcal{N}$ is given by the composite inclusion

$$L_{1,1} \xhookrightarrow{\iota} V_{d,1} \xhookrightarrow{i} V_{d,r+1}.$$

Since $L_{d+1,r+1} = \mathbb{Z}/p^{r+1}$, we can consider $\mathcal{E}_{d+1,r}$, resp. $\mathcal{F}_{d,r+1}$, as a torsor under the $(\Gamma, r+1)$-module $V_{d,r}$, resp. $(V_{d,r+1}/L_{d,r+1})$. Taking their direct product, one gets a torsor X, under the $(\Gamma, r+1)$-module $V_{d,r} \oplus (V_{d,r+1}/L_{1,r+1})$. The data of the gluing $(\mathcal{E}_{d+1,r}, \phi_r)$ then yields a natural trivialization of $q_*(X)$, which is a Γ-torsor under $V_{d/1,r}$. Using the extension $\mathcal{Q}$, we get a natural torsor Y, under N, together with a natural isomorphism $X \xrightarrow{\sim} \iota_*(Y)$. Lifting the gluing $(\mathcal{E}_{d+1,r}, \phi_1)$ is then

equivalent to lifting Y, to a Γ-torsor under $V_{d,r+1}$, via s. Using the connecting map associated to $\mathcal{N}$, one sees this is obstructed by a class

$$c_1 \in H^2(\Gamma, L_{1,1}).$$

It is left to the reader, to check that $i_*(c_1) = \mathrm{obs}(\mathcal{E}_{d+1,r+1})$.
The general case, where $L_{d+1,r+1}$ is not assumed to be trivial, reduces to the previous one by applying $(. \otimes L^\vee_{d+1,r+1})$, the tensor product of $(\Gamma, r+1)$-modules. In other words, replacing all $(\Gamma, r+1)$-modules M by $M \otimes L^\vee_{d+1,r+1}$, we are sent back to the case $L_{d+1,r+1} = \mathbb{Z}/p^{r+1}$. The proof is complete. □

7. Lifting (wound) Kummer flags

In this section, Γ is a p-manageable profinite group, and $\mathbb{Z}_p(1)$ is an invertible $\mathbb{Z}_p$-module, with a continuous action of Γ, such that $(\Gamma, \mathbb{Z}_p(1))$ satisfies W90.
For instance, one may take one of the two pairs of Proposition 4.3. More generally, by Proposition 5.1, lifting theorems of this section apply to all profinite groups satisfying mod p Poincaré duality in dimension 2.

Let $\nabla_r = (V_{d,r})$ be a d-dimensional complete (Γ, r)-flag. Under suitable assumptions, we prove that ∇_r lifts to a complete $(\Gamma, r+1)$-flag ∇_{r+1} – in a very strong "step-by-step" sense.

7.1. Wound Kummer flags.

Definition 7.1. *(wound flag)*
A complete (Γ, r)-flag $\nabla = (V_{i,r})$ is said to be wound *(*ployé *in French), if for all $1 \leq i \leq d-1$, the extension of $(\Gamma, 1)$-modules*

$$0 \longrightarrow L_{i,1} \longrightarrow P_{i,1} := V_{i+1,1}/V_{i-1,1} \longrightarrow L_{i+1,1} \longrightarrow 0$$

does not split.

Remark 7.2. The flag ∇ is wound if and only if its mod p reduction is wound, as a complete $(\Gamma, 1)$-flag.

Remark 7.3. A complete $(\Gamma, 1)$-flag $\nabla = (V_{i,1})$ is wound, if and only if it is the only complete flag, with which the $(\Gamma, 1)$-bundle $V_{d,1}$ can be equipped. The proof is left as an instructive exercise, for the interested reader.

Definition 7.4. *(wound Kummer flag)*
Let $\nabla_{d,r}$ be a wound complete (Γ, r)-flag. We say that $\nabla_{d,r}$ is a wound Kummer flag if there exists $N \in \mathbb{Z}$, such that, for all $i = 1, \ldots, d$,

$$L_{i,r} \simeq \mathbf{W}_r(L_{i,1}(i))(N-i). \tag{1}$$

Remark 7.5. Assume that $r = 1$. Taking $N = 0$ in definition above, one sees that $\mathbf{W}_1(L_{i,1}(i))(-i) = L_{i,1}(i)(-i) = L_{i,1}$.
Hence, every wound $(\Gamma, 1)$-flag is wound Kummer.

Remark 7.6. The integer N in the definition above is secondary. Its purpose is to make the notion of a Kummer flag invariant by "global" (in the sense of independent of i) cyclotomic twists, and by dualizing (Exercise below).

Exercise 7.7. Let $\nabla_{d,r} = (V_{i,r})$ be a wound Kummer (Γ, r)-flag. Show that its dual flag $\nabla^\vee_{d,r} = (V^\vee_{d+1-i,r})$ is a wound Kummer (Γ, r)-flag, as well.

Remark 7.8. The last line of Definition above essentially says that $L_{i,r} = L_{i+1,r}(1)$, after restriction to a subgroup of Γ of prime-to-p index and up to a global "cyclotomic" twist. Here are details. Denote by $\chi_L : \Gamma \longrightarrow (\mathbb{Z}/p^r)^\times$ the character associated to a one-dimensional (Γ, r)-bundle L. Recall that $(\mathbb{Z}/p^r)^\times = \mathbb{F}_p^\times \times U_r$, where $U_r = (1 + p\mathbb{Z}/p^r\mathbb{Z})$. [Note that $U_r = \mathbb{Z}/2 \times (\mathbb{Z}/2^{r-2})$ if $p = 2$, and $U_r = (\mathbb{Z}/p^{r-1})$ if $p > 2$.]
Denote by

$$\chi'_L : \Gamma \longrightarrow U_r$$

the second component of χ_L, with respect to this decomposition.
Then $\chi'_L = 1$, if and only if $L = \mathbf{W}_r(L/p)$ (i.e. L is the Teichmüller lift of its mod p reduction). We thus see that $L_{i,r} \simeq \mathbf{W}_r(L_{i,1}(i))(-i)$, if and only if $\chi'_{L_{i,r}} = \chi'_{\mathbb{Z}/p^r(-i)}$. Equivalently, there exists a finite extension E/F, of degree prime to p, such that $L_{i,r} \simeq \mathbb{Z}/p^r(-i)$, as (Γ_E, r)-bundles.

Example 7.9. Denote by

$$\chi(1) : \Gamma \longrightarrow \mathbb{Z}_p^\times$$

the character associated to $\mathbb{Z}_p(1)$. As a triangular representation, a 3-dimensional wound Kummer (Γ, r)-flag reads as

$$\Gamma \xrightarrow{\rho} \begin{pmatrix} \chi(-2) \cdot \mathbf{W}_r(\overline{\chi}(2)\varepsilon_2) & \alpha_1 & \alpha_3 \\ 0 & \chi(-1) \cdot \mathbf{W}_r(\overline{\chi}(1)\varepsilon_1) & \alpha_2 \\ 0 & 0 & \mathbf{W}_r(\varepsilon_0) \end{pmatrix} \in \mathbf{B}_3(\mathbb{Z}/p^r)$$

for characters $\varepsilon_i \colon \Gamma \longrightarrow \mathbb{F}_p^\times$, and suitable functions $\alpha_i : \Gamma \longrightarrow \mathbb{Z}/p^r$, such that both induced mod p representations

$$\Gamma \longrightarrow \begin{pmatrix} \varepsilon_2 & \overline{\alpha}_1 \\ 0 & \varepsilon_1 \end{pmatrix} \in \mathbf{B}_2(\mathbb{F}_p)$$

and

$$\Gamma \longrightarrow \begin{pmatrix} \varepsilon_1 & \overline{\alpha}_2 \\ 0 & \varepsilon_0 \end{pmatrix} \in \mathbf{B}_2(\mathbb{F}_p)$$

correspond to non-split line bundle extensions. In case $\varepsilon_i = 1$ for $i = 0, 1, 2$, this means that $\overline{\alpha}_1$ and $\overline{\alpha}_2$ are non-zero characters $\Gamma \longrightarrow (\mathbb{F}_p, +)$.

The next Proposition states that wound Kummer flags can be lifted, in a very strong sense. This means they can be lifted step-by-step, regarding both torsion (i.e. lifting from mod p^r to mod p^{r+1}) and dimension (i.e. extending a lifting of a truncation of the flag, to a lifting of the whole flag).

PROPOSITION 7.10. *(step-by-step liftability of wound Kummer flags)*
Let $\nabla_{d,r}$ be a wound Kummer (Γ, r)-flag.
Assume given a wound Kummer flag $\nabla^\flat_{d-1,r+1} = (V^\flat_{i,r+1})_{1 \leq i \leq d-1}$, together with an isomorphism $\nabla_{d-1,r} \overset{\phi}{\cong} \nabla^\flat_{d-1,r}$. Then, there exists a lift of $\nabla_{d,r}$, to a wound Kummer flag $\nabla_{d,r+1}$, and an isomorphism $\nabla_{d-1,r+1} \cong \nabla^\flat_{d-1,r+1}$, whose reduction mod p^r equals ϕ.

Before giving the proof, here is a corollary, straightforward by induction on d.

COROLLARY 7.11. *Assume that $\nabla_{d,r}$ is a wound Kummer (Γ, r)-flag. Then it admits a lift to a wound Kummer $(\Gamma, r+1)$-flag.*

Proof. We prove the Proposition, by induction on $d = \dim(\nabla_{d,r})$. If $d = 1$, there is nothing to prove, since $\mathbf{W}_{r+1}(L_{1,1})$ is a lift of $\mathbf{W}_r(L_{1,1})$.
If $d = 2$, then $\mathcal{V}_{1,r+1}$ consists of the single piece $L_{1,r+1} = \mathbf{W}_{r+1}(L_{1,1}(1))(-1)$. Our job is to lift $[V_{2,r}] \in \mathrm{Ext}^1_\Gamma(L_{2,r}, L_{1,r})$ to a class in $\mathrm{Ext}^1_\Gamma(L_{2,r+1}, L_{1,r+1})$. Note that, for all $s \geq 0$,

$$\mathrm{Ext}^1_\Gamma(L_{2,s}, L_{1,s}) = H^1(\Gamma, (L^\vee_{2,s} \otimes L_{1,s}) = H^1(\Gamma, \mathbf{W}_s(L^\vee_{2,1} \otimes L_{1,1})(1)).$$

The map $\mathrm{Ext}^1_\Gamma(L_{2,r+1}, L_{1,r+1}) \longrightarrow \mathrm{Ext}^1_\Gamma(L_{2,r}, L_{1,r})$ can thus be identified to

$$H^1(\Gamma, \mathbf{W}_{r+1}(L^\vee_{2,1} \otimes L_{1,1})(1)) \longrightarrow H^1(\Gamma, \mathbf{W}_r(L^\vee_{2,1} \otimes L_{1,1})(1)),$$

which is surjective by Lemma 3.12 (consequence of the (W90) property), concluding the proof.
It remains to treat the case $d > 2$, assuming that the Proposition holds for all flags of dimension $< d$. We introduce the $(d-1)$-dimensional wound Kummer flag

$$\nabla_{d/1,r} := \nabla_{d,r}/L_{1,r} : 0 \subset V_{2/1,r} \subset V_{3/1,r} \subset \ldots \subset V_{d/1,r}.$$

Similarly, we introduce the $(d-2)$-dimensional wound Kummer flag

$$\nabla^\flat_{d-1/1,r+1} := \nabla^\flat_{d-1,r+1}/L_{1,r+1} : 0 \subset V^\flat_{2/1,r+1} \subset V^\flat_{3/1,r+1} \subset \ldots \subset V^\flat_{d-1/1,r+1}\,.$$

By the induction hypothesis, there exists a wound Kummer lift $\nabla^\sharp_{d-1,r+1}$ of $\nabla_{d/1,r}$, compatible with $\nabla^\flat_{d-1/1,r+1}$. The obstruction to gluift $\nabla^\flat_{d/1,r+1}$ and $\nabla^\sharp_{d-1,r+1}$, along $\nabla_{d,r}$, to a flag $\nabla_{d,r+1}$, is a class

$$c_1 \in H^2(\Gamma, L^\vee_{d,1} \otimes L_{1,1})$$

(see Definition 6.4, and the discussion thereafter). If $c_1 = 0$, then gluifting can be done, and $\nabla_{d,r+1}$ is automatically a wound Kummer flag, compatible with $\nabla^\flat_{d-1,r+1}$ (i.e. with ϕ).
Assume that $c_1 \neq 0$. We are going to modify (=adjust) $\nabla^\sharp_{d-1,r+1}$, so that gluifting becomes possible. Since $\nabla_{d,r}$ is wound, the extension

$$0 \longrightarrow L_{1,1} \longrightarrow V_{2,1} \longrightarrow L_{2,1} \longrightarrow 0$$

does not split, nor its twist by $L^\vee_{d,1}$. Denote its class by

$$p_1 \in \mathrm{Ext}^1_\Gamma(L_{2,1}, L_{1,1}) \simeq H^1(\Gamma, L^\vee_{2,1} \otimes L_{1,1}).$$

Since $p_1 \neq 0$, Lemma 3.8 implies that there exists a class

$$\epsilon^\sharp \in \mathrm{Ext}^1_\Gamma(L_{d,1}, L_{2,1}) = H^1(\Gamma, L^\vee_{d,1} \otimes L_{2,1}),$$

such that $p_1 \cup \epsilon^\sharp = c_1$.
There are natural Γ-equivariant injections

$$\iota : L^\vee_{d,1} \otimes L_{2,1} \hookrightarrow \mathbf{End}(\nabla^\sharp_{d-1,1}) \hookrightarrow \mathbf{Aut}(\nabla^\sharp_{d-1,r+1}),$$

where the second one is given by the formula

$$f \mapsto \mathrm{Id} + p^r f.$$

It is a disguise of the embedding of triangular subgroups of $\mathbf{GL}_{d-1}(\mathbb{Z}/p^{r+1})$,

$$\begin{pmatrix} 1 & 0 & 0 & p^r* \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \subset \begin{pmatrix} \times & * & * & * \\ 0 & \times & * & * \\ 0 & 0 & \times & * \\ 0 & 0 & 0 & \times \end{pmatrix}.$$

Since $\iota(L_{d,1}^\vee \otimes L_{2,1})$ is *central* in $\mathbf{Aut}(\nabla^\sharp_{d-1,r+1})$, we can define the flag

$$\nabla^{\sharp\mathrm{ad}}_{d-1,r+1} := \nabla^\sharp_{d-1,r+1} - \iota_*(\epsilon^\sharp).$$

It is a new lift of $\nabla^\sharp_{d-1,r}$, arising as a very small (actually as small as possible) deformation of $\nabla^\sharp_{d-1,r+1}$. Denote by

$$c_1^{\mathrm{ad}} \in H^2(\Gamma, L_{d,1}^\vee \otimes L_{1,1})$$

the obstruction to glue $\nabla^\flat_{d-1,r+1}$ and $\nabla^{\sharp\mathrm{ad}}_{d-1,r+1}$, to a lift $\nabla_{d,r+1}$ of $\nabla_{d,r}$. Using naturality of cup-product, one computes:

$$c_1^{\mathrm{ad}} = c_1 - p_1 \cup \epsilon^\sharp = 0.$$

Therefore, $\nabla^{\sharp\mathrm{ad}}_{d-1,r+1}$ and $\nabla^\flat_{d/1,r+1}$ glue, to the desired $\nabla_{d,r+1}$.

□

7.2. Generalisation to a larger class of coefficients. Let k be a (not necessarily perfect) field of characteristic p. Then, Proposition 7.10, as well as all results so far, hold for representations over the ring of Witt vectors $\mathbf{W}_r(k)$, in place of $\mathbb{Z}/p^r(= \mathbf{W}_r(\mathbb{F}_p))$. Indeed, $\mathbb{F}_p$-linearity can everywhere be upgraded to k-linearity. For instance, Lemma 3.8 generalizes to finite-dimensional representations of Γ over k (in place of $\mathbb{F}_p$). The proof is the same.

7.3. Kummer flags, in the presence of enough roots of unity. In this section, we assume that $\mathbb{Z}/p^{r+1}(1) \simeq \mathbb{Z}/p^{r+1}$. This assumption is satisfied in the topological case. In the arithmetic case where $\Gamma = \Gamma_F$ for a local field F, it is equivalent to assuming that F contains a primitive p^{r+1}-th root of unity.

Definition 7.12. *Let $\nabla_{d,r}$ be a complete (Γ, r)-flag.*
For all $1 \leq k \leq d$, define $i_r(k)$ to be the smallest integer $0 \leq i \leq k-1$ such that the extension of (Γ, r)-modules

$$0 \longrightarrow V_{k-1,r}/V_{i,r} \longrightarrow V_{k,r}/V_{i,r} \longrightarrow L_{k,r} \longrightarrow 0$$

splits.

To state a general lifting theorem, we need the following notion of Kummer flag, defined by induction. Recall that to any flag $\nabla_{d,r}$ of rank d, we can attach two flags: its truncation $\nabla_{d-1,r}$, and its quotient $\nabla_{d/1,r} := \nabla_{d,r}/V_{1,r}$.

Definition 7.13. *A complete (Γ, r)-flag $\nabla_{d,r}$ is a Kummer flag if the following conditions hold.*

1. *For all $1 \leq k \leq d$, $i_r(k) = i_1(k)$.*
2. *For all $k = 1, \ldots, d$, $L_{k,r} = \mathbb{Z}/p^r$. In other words, all one-dimensional graded pieces are trivial.*
3. *$\nabla_{d-1,r}$ and $\nabla_{d/1,r}$ are Kummer.*
4. *For all $2 \leq k \leq d$, if $i_r(k) = 0$, then for any splitting $s : L_{k,r} \longrightarrow V_{k,r}$, the flag $\nabla^{q,s}_{d-1,r} := \nabla_{d,r}/s(L_{k,r})$ is Kummer.*

Several remarks are in order, to illustrate this Definition.

Remark 7.14. Consider the condition:

(ii) For all $k = 1, \ldots, d$, $L_{k,r} = \mathbf{W}_r(L_{k,1})$.

It is less restrictive than Condition (2) above. The main results, Theorem 7.21 and its corollary, remain valid if (2) is replaced by (ii), in Definition 7.13. Since this makes no significant difference, we've chosen to work with (2).

Remark 7.15. If $d = 1$, a flag $\nabla_{1,r} (= L_{1,r})$ is Kummer if and only if it is attached to the trivial character $\Gamma \longrightarrow (\mathbb{Z}/p^r)^\times$.
If $d = 2$, a flag $\nabla_{2,r}$ is Kummer if and only if it is attached to an extension of the trivial character by itself, that is either split, or is non-split modulo p.

Remark 7.16. If $r = 1$, then $\nabla_{d,1}$ is a Kummer flag if and only if all its graded pieces are trivial.

Remark 7.17. Condition (1) in Definition 7.13 is equivalent to:

(i) Consider an extension of (Γ, r)-modules of the shape

$$(E_r) : 0 \longrightarrow V_{j/i,r} \longrightarrow V_{k/i,r} \longrightarrow V_{k/j,r} \longrightarrow 0,$$

for some integers $0 \leq i \leq j \leq k \leq d$. If (E_1) splits, then (E_r) splits.

Actually, in combination with conditions (3) and (4), it would suffice to demand (i) for $j = i + 1 = k - 1$. [Thus, as stated, the formulation of the Definition is slightly redundant. It is nonetheless convenient in practice.]
Checking these facts is left to the interested reader.

Remark 7.18. A wound Kummer (Γ, r)-flag (in the sense of Definition 7.4) is a Kummer (Γ, r)-flag (in the sense of Definition 7.13), if and only if $L_{i,1}$ is trivial for every $i = 1, \dots, d$. Indeed, the wound condition implies that $i_r(k) = i_1(k) = k - 1$ for every $k = 1, \dots, d$, and the fact that $L_{i,1}$ is trivial and $\mathbb{Z}/p^r \cong \mathbb{Z}/p^r(1)$ as (Γ, r)-modules implies that $L_{i,r}$ is trivial for every $i = 1, \dots, d$.
On the other hand, a Kummer (Γ, r)-flag is wound if and only if $i_r(k) = i_1(k) = k - 1$ for every $k = 1, \dots, d$. One can easily construct an example of a Kummer flag not satisfying this condition, so that not all Kummer flags are wound.

The following two lemmas will be useful in the proof of the main Theorem.

LEMMA 7.19. *Let $\nabla_{d,r+1}$ be a complete $(\Gamma, r + 1)$-flag. Let $2 \leq k \leq d - 1$ and $s : L_{k,r+1} \longrightarrow V_{k,r+1}$ be a section of $V_{k,r+1} \longrightarrow L_{k,r+1}$.*
If $\nabla_{d,r}$, $\nabla_{d/1,r+1}$ and $\nabla_{d,r+1}/s(L_{k,r+1})$ are Kummer, then $\nabla_{d,r+1}$ is Kummer.

Proof. The only non-obvious case to check condition (1) in the definition of Kummer flag for $\nabla_{d,r+1}$ is when $k = d$ and $i_1(d) = i_r(d)$ (since $\nabla_{d,r}$ is Kummer) is 0 or 1. Then $i_{r+1}(d) = 0$ or 1 since $\nabla_{d/1,r+1}$ is Kummer. If $i_1(d) = i_r(d)$ is 1, then $i_{r+1}(d) = 1$. If $i_1(d) = i_r(d) = 0$, then $i_{r+1}(d) = 0$ since $\nabla_{d,r+1}/s(L_{k,r+1})$ is Kummer.
Condition (2) in the definition is obvious.
Condition (3) is obvious for $\nabla_{d/1,r+1}$ and follows by induction on the dimension for $\nabla_{d-1,r+1}$.
Condition (4) holds by induction on d. □

LEMMA 7.20. *Let $\nabla_{d,r+1}$ be a complete $(\Gamma, r + 1)$-flag such that $i_1(k) \geq 1$ for all $2 \leq k \leq d - 1$ and $i_1(d) \geq 2$.*
If $\nabla_{d/1,r+1}$ and $\nabla_{d-1,r+1}$ are Kummer, then $\nabla_{d,r+1}$ is Kummer.

Proof. Condition (1) is obvious for all $k \leq d - 1$ since $\nabla_{d-1,r+1}$ is Kummer, and for $k = n$ since $i_1(d) \geq 2$ and $\nabla_{d/1,r+1}$ is Kummer.
Conditions (2) and (3) are obvious.
Condition (4) is clear because of the assumption on the $i_1(k)$'s. □

We can now state and prove the main result of this section.

THEOREM 7.21. *Assume that $\mathbb{Z}/p^{r+1}(1) \simeq \mathbb{Z}/p^{r+1}$.*
Let $\nabla_{d,r}$ be a complete Kummer (Γ, r)-flag.

- *Consider a Kummer flag* $\nabla^\sharp_{d-1,r+1}$*, together with an isomorphism* $\nabla_{d/1,r} \overset{\phi_r}{\cong} \nabla^\sharp_{d-1,r}$*. Then, there exists a Kummer lift* $\nabla_{d,r+1}$ *of* $\nabla_{d,r}$*, together with an isomorphism* $\nabla_{d/1,r+1} \overset{\phi_{r+1}}{\cong} \nabla^\sharp_{d-1,r+1}$*, which lifts* ϕ_r*.*
- *Consider a Kummer flag* $\nabla^\flat_{d-1,r+1}$*, together with an isomorphism* $\nabla_{d-1,r} \overset{\phi_r}{\cong} \nabla^\flat_{d-1,r}$*. Then, there exists a Kummer lift* $\nabla_{d,r+1}$ *of* $\nabla_{d,r}$*, together with an isomorphism* $\nabla_{d-1,r+1} \overset{\phi_{r+1}}{\cong} \nabla^\flat_{d-1,r+1}$*, which lifts* ϕ_r*.*

In particular, $\nabla_{d,r}$ *lifts to a complete Kummer* $(\Gamma, r+1)$*-flag* $\nabla_{d,r+1}$*.*

Before the proof, we give a straightforward corollary.
Let

$$\nabla_{d,r} = V_{1,r} \subset V_{2,r} \subset \ldots \subset V_{d,r}$$

be a Kummer flag of (Γ, r)-bundles, for some $r \geq 2$. Then, every $c \in H^1(\Gamma, V_{d,1})$ can be seen as the class of an extension of $(\Gamma, 1)$-bundles

$$0 \longrightarrow V_{d,1} \longrightarrow V_{d+1,1} \longrightarrow \mathbb{Z}/p \longrightarrow 0,$$

which determines a $(d+1)$-dimensional Kummer flag of $(\Gamma, 1)$-bundles

$$\nabla_{d+1,1} := V_{1,1} \subset V_{2,1} \subset \ldots \subset V_{d,1} \subset V_{d+1,1}.$$

Thus, Theorem 7.21 implies the following.

Corollary 7.22. *Let* $r \geq 2$ *be an integer. Assume that* $\mathbb{Z}/p^r(1) \simeq \mathbb{Z}/p^r$*. Let* V *be a* (Γ, r)*-bundle, which fits into a Kummer* (Γ, r)*-flag*

$$\nabla_{d,r} = V_{1,r} \subset V_{2,r} \subset \ldots \subset V_{d,r} = V.$$

Then, the natural map

$$H^1(\Gamma, V) \longrightarrow H^1(\Gamma, V/p)$$

is surjective.

We go back to the proof of Theorem 7.21.

Proof. It is enough to prove the first statement of the Theorem: the second one follows by duality, given that the dual of a Kummer flag is again a Kummer flag, and taking duals swaps subobjects and quotients.
We proceed by induction on d. If $d = 1$ or $d = 2$, the proof is identical to that of Proposition 7.10.
Assume that $d > 2$ and that the result holds for all Kummer flags of dimension $< d$. Let $\nabla_{d,r} = (V_{i,r})_{1 \leq i \leq d}$ be a d-dimensional Kummer flag, and let $\nabla^\sharp_{d-1,r+1}$ be as in the statement of the first part of the Theorem.
Consider the natural $(d-1)$-dimensional Kummer flags $\nabla_{d-1,r} \subset \nabla_{d,r}$ and $\nabla_{d/1,r} := \nabla_{d,r}/V_{1,r}$ associated to $\nabla_{d,r}$.
By induction, there exists a Kummer lift $\nabla^\flat_{d-1,r+1}$ of $\nabla_{d-1,r}$ compatible with $\nabla^\sharp_{d-2,r+1}$.

- Assume first that there exists $2 \leq k \leq d-1$ such that $i_1(k) = 0$, i.e. that the modulo p extension

  $$0 \longrightarrow V_{k-1,1} \longrightarrow V_{k,1} \longrightarrow L_{k,1} \longrightarrow 0$$

  splits. Since $\nabla^\flat_{d-1,r+1}$ is Kummer, the modulo p^{r+1} extension

  $$0 \longrightarrow V_{k-1,r+1} \longrightarrow V_{k,r+1} \longrightarrow L_{k,r+1} \longrightarrow 0$$

splits. The choice of a section $s : L_{k,r+1} \longrightarrow V_{k,r+1}$ determines a 1-dimensional direct factor $s(L_{k,r+1})$ of $\nabla^\flat_{k,r+1}$, hence 1-dimensional $(\Gamma, r+1)$-submodules of $\nabla^\sharp_{d-1,r}$ and of $\nabla_{d,r}$. In particular, we have a cartesian commutative diagram modulo p^r:

$$\begin{array}{ccc} \nabla_{d,r} & \longrightarrow & \nabla^\sharp_{d-1,r} \\ \downarrow & & \downarrow \\ \nabla^s_{d-1,r} := \nabla_{d,r}/s(L_{k,r}) & \longrightarrow & \nabla^{\sharp,s}_{d-2,r} := \nabla^\sharp_{d-1,r}/s(L_{k,r})\,. \end{array}$$

By induction, there exists a lift $\nabla^s_{d-1,r+1}$ of $\nabla^s_{d-1,r}$ compatible with $\nabla^{\sharp,s}_{d-2,r+1} := \nabla^\sharp_{d-1,r+1}/s(L_{k,r+1})$.
Then one defines a lift $\nabla_{d,r+1}$ of $\nabla_{d,r}$ as the following cartesian diagram

$$\begin{array}{ccc} \nabla_{d,r+1} & \longrightarrow & \nabla^\sharp_{d-1,r+1} \\ \downarrow & & \downarrow \\ \nabla^s_{d-1,r+1} & \longrightarrow & \nabla^{\sharp,s}_{d-2,r+1}\,. \end{array}$$

Then by Lemma 7.19, $\nabla_{d,r+1}$ is a Kummer lift of $\nabla_{d,r}$, extending $\nabla^\sharp_{d-1,r+1}$ (and $\nabla^\flat_{d-1,r+1}$).

- Assume now that $i_1(d) = 0$, i.e. that the extension
$$0 \longrightarrow V_{d-1,1} \longrightarrow V_{d,1} \longrightarrow L_{d,1} \longrightarrow 0$$
splits. Since $\nabla_{d,r}$ is Kummer, then the analogous extension splits modulo p^r. Then we define $\nabla_{d,r+1}$ as the direct sum $\nabla^\flat_{d-1,r+1} \oplus L_{d,r+1}$. Then $\nabla_{d,r+1}$ is the required Kummer lift of $\nabla_{d,r}$.
- Assume now that $i_1(d) = 1$, i.e. that the extension
$$0 \longrightarrow V_{d-1/1,1} \longrightarrow V_{d/1,1} \longrightarrow L_{d,1} \longrightarrow 0$$
splits. Since $\nabla^\sharp_{d-1,r+1}$ is Kummer, the analogous extension splits modulo p^{r+1}. The choice of a splitting defines a 2-dimensional subflag $\nabla^!_{2,r}$ of $\nabla_{d,r}$, and $\nabla_{d,r}$ appears in the following pushout diagram of inclusions
$$\begin{array}{ccc} \nabla_{1,r} & \longrightarrow & \nabla_{d-1,r} \\ \downarrow & & \downarrow \\ \nabla^!_{2,r} & \longrightarrow & \nabla_{d,r}\,. \end{array}$$
By the 2-dimensional case, the flag $\nabla^!_{2,r}$ lifts to a flag $\nabla^!_{2,r+1}$ compatible with both $\nabla^\flat_{1,r+1} = L_{1,r+1}$ and $L_{d,r+1}$, and one can define the required lift $\nabla_{d,r+1}$ by the following pushout diagram of inclusions
$$\begin{array}{ccc} \nabla^\flat_{1,r+1} & \longrightarrow & \nabla^\flat_{d-1,r+1} \\ \downarrow & & \downarrow \\ \nabla^!_{2,r+1} & \longrightarrow & \nabla_{d,r+1}\,. \end{array}$$
Finally, one checks that the flag $\nabla_{d,r+1}$ we just defined is Kummer and satisfies the statement of the Theorem.

- Assume finally that $i := i_1(d) \geq 2$ (and that we are not in the previous cases).
  Then the modulo p extension

$$0 \longrightarrow V_{d-1/i-1,1} \longrightarrow V_{d/i-1,1} \longrightarrow L_{d,1} \longrightarrow 0$$

does not split, while the extension

$$0 \longrightarrow V_{d-1/i,1} \longrightarrow V_{d/i,1} \longrightarrow L_{d,1} \longrightarrow 0$$

does split. In particular, the choice of a splitting of the second one defines a non-split extension

$$0 \longrightarrow L_{i,1} \longrightarrow P_{i,d,1} \longrightarrow L_{d,1} \longrightarrow 0\,.$$

By assumption $i_1(i) \neq 0$, so that the following extension does not split:

$$0 \longrightarrow V_{i-1,1} \longrightarrow V_{i,1} \longrightarrow L_{i,1} \longrightarrow 0.$$

The argument is now very similar to the proof of Proposition 7.10.
The obstruction to glue $\nabla^\flat_{d-1,r+1}$ and $\nabla^\sharp_{d-1,r+1}$ to a lift $\nabla_{d,r+1}$ of $\nabla_{d,r}$, is a class

$$c_1 \in H^2(\Gamma, L^\vee_{d,1} \otimes L_{1,1})$$

(see the discussion after Definition 6.4). If $c_1 = 0$, then gluifting can be done, and $\nabla_{d,r+1}$ is automatically a Kummer flag, compatible with $\nabla^\sharp_{d-1,r+1}$.
Assume that $c_1 \neq 0$. We are going to modify $\nabla^\flat_{d-1,r+1}$, so that gluifting becomes possible.

By assumption, the extension

$$0 \longrightarrow V_{d-1/i-1,1} \longrightarrow V_{d/i-1,1} \longrightarrow L_{d,1} \longrightarrow 0$$

does not split, nor the twist of its dual by $L_{1,1}$:

$$0 \longrightarrow L^\vee_{d,1} \otimes L_{1,1} \longrightarrow V^\vee_{d/i-1,1} \otimes L_{1,1} \longrightarrow V^\vee_{d-1/i-1,1} \otimes L_{1,1} \longrightarrow 0\,.$$

Denote its class by

$$p_1 \in \mathrm{Ext}^1_\Gamma(V^\vee_{d-1/i-1,1}, L^\vee_{d,1}) \simeq H^1(\Gamma, L^\vee_{d,1} \otimes \big(V_{d-1/i-1,1}\big))\,.$$

Since $p_1 \neq 0$, Lemma 3.8 implies that there exists a class

$$\epsilon^\flat \in H^1(\Gamma, V^\vee_{d-1/i-1,1} \otimes L_{1,1}) = \mathrm{Ext}^1_\Gamma(V_{d-1/i-1,1}, L_{1,1})\,,$$

such that $p_1 \cup \epsilon^\flat = c_1$.

There is a natural Γ-equivariant injection

$$\iota : \big(V_{d-1/i-1,1}\big)^\vee \otimes L_{1,1} \hookrightarrow \mathbf{Aut}(\nabla^\flat_{d-1,r+1}).$$

Since $\iota(\big(V_{d-1/i-1,1}\big)^\vee \otimes L_{1,1})$ is *central* in $\mathbf{Aut}(\nabla^\flat_{d-1,r+1})$, we can define the flag

$$\nabla^{\flat,\mathrm{ad}}_{d-1,r+1} := \nabla^\flat_{d-1,r+1} - \iota_*(\epsilon^\flat).$$

It is a new lift of $\nabla^\flat_{d-1,r}$, arising as a very small deformation of $\nabla^\flat_{d-1,r+1}$. Note that $\nabla^{\flat,\mathrm{ad}}_{d-1,r+1}$ is Kummer since none of the $i_1(k)$ are zero, for $2 \leq k \leq d-1$. Denote by

$$c_1^{\mathrm{ad}} \in H^2(\Gamma, L^\vee_{d,1} \otimes L_{1,1})$$

the obstruction to gluing $\nabla^\sharp_{d-1,r+1}$ and $\nabla^{\flat,\mathrm{ad}}_{d-1,r+1}$ to a lift $\nabla_{d,r+1}$ of $\nabla_{d,r}$. Using the naturality of the cup-product, one computes:

$$c_1^{\mathrm{ad}} = c_1 - p_1 \cup \epsilon^\flat = 0.$$

Therefore, $\nabla^{\flat,\mathrm{ad}}_{d-1,r+1}$ and $\nabla^{\sharp}_{d-1,r+1}$ glue, to the desired $\nabla_{d,r+1}$, that is Kummer by Lemma 7.20.

□

One could hope for a statement generalizing both Proposition 7.10 and Theorem 7.21, with no assumptions on roots of unity in the arithmetic case and with a suitable notion of Kummer flag. This cannot be achieved using only cyclotomic twists for the L_k's, as shown in the following example.

Example 7.23. Let $K = \mathbb{Q}_2$ (resp. $\mathbb{Q}_\ell$, with $\ell \equiv 3\,[4]$) and $p = 2$. The map

$$\alpha : H^1(K, \mathbb{Z}/4\mathbb{Z}) \longrightarrow H^1(K, \mathbb{Z}/2\mathbb{Z}),$$

induced by reduction modulo 2, is not surjective: its image is a subgroup of index 2. More precisely, identifying $H^1(K, \mathbb{Z}/2\mathbb{Z})$ with $K^\times/(K^\times)^2$, it is classical that for all $x \in K^\times$, $(x) \in H^1(K, \mathbb{Z}/2\mathbb{Z})$ lifts to $H^1(K, \mathbb{Z}/4\mathbb{Z})$ if and only if

$$(x) \cup (x) = (x) \cup (-1) = 0 \in H^2(K, \mathbb{Z}/2\mathbb{Z}).$$

Hence $H^1(K, \mathbb{Z}/2\mathbb{Z}) \setminus \mathrm{im}(\alpha) = \{(-1), (-2), (-5), (-10)\}$ (resp. $H^1(K, \mathbb{Z}/2\mathbb{Z}) \setminus \mathrm{im}(\alpha) = \{(-\ell), (\ell)\}$).
Let $\varepsilon := (-2)$ and $\varepsilon' := (-5)$ in $H^1(K, \mathbb{Z}/2\mathbb{Z})$ (resp. $\varepsilon := (-\ell)$ and $\varepsilon' := (\ell)$). Then $\varepsilon, \varepsilon' \notin \mathrm{im}(\alpha)$ and $\varepsilon \cup \varepsilon' = 0$.
The relation $\varepsilon \cup \varepsilon' = 0$ implies that the representations of Γ_K defined by $\rho_1 := \begin{pmatrix} 1 & \varepsilon & \varepsilon \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ and $\rho_2 := \begin{pmatrix} 1 & 0 & \varepsilon' \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ glue to a four-dimensional representation $\rho_3 := \begin{pmatrix} 1 & \varepsilon & \varepsilon & * \\ 0 & 1 & 0 & \varepsilon' \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$. Similarly, the representations ρ_2 and $\rho_4 := \begin{pmatrix} 1 & 0 & \varepsilon' \\ 0 & 1 & \varepsilon \\ 0 & 0 & 1 \end{pmatrix}$ glue to a four-dimensional representation $\rho_5 := \begin{pmatrix} 1 & 0 & \varepsilon' & * \\ 0 & 1 & 0 & \varepsilon' \\ 0 & 0 & 1 & \varepsilon \\ 0 & 0 & 0 & 1 \end{pmatrix}$.
Finally, the obstruction to glue ρ_3 and ρ_5 (along ρ_2) to a five-dimensional representation lies in $H^2(K, \mathbb{Z}/2\mathbb{Z})$. Up to modifying the top right hand side coefficient of ρ_3 by an element in $H^1(K, \mathbb{Z}/2\mathbb{Z})$, one can assume that this obstruction is trivial, hence ρ_3 and ρ_5 glue to a representation $\bar\rho : \Gamma_K \longrightarrow \mathbf{GL}_5(\mathbb{F}_2)$ defined by

$$\bar\rho := \begin{pmatrix} 1 & \varepsilon & \varepsilon & * & * \\ 0 & 1 & 0 & \varepsilon' & * \\ 0 & 0 & 1 & 0 & \varepsilon' \\ 0 & 0 & 0 & 1 & \varepsilon \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

and we denote by $\nabla_{5,1}$ the associated flag.
Then $\bar\rho$ does not lift to a representation $\rho : \Gamma_K \longrightarrow \mathbf{GL}_5(\mathbb{Z}/4\mathbb{Z})$ of the shape:

$$\rho = \begin{pmatrix} \chi_1 & * & * & * & * \\ 0 & \chi_2 & 0 & * & * \\ 0 & 0 & \chi_3 & 0 & * \\ 0 & 0 & 0 & \chi_4 & * \\ 0 & 0 & 0 & 0 & \chi_5 \end{pmatrix}$$

such that χ_i are powers of the cyclotomic character. Equivalently, $\nabla_{5,1}$ does not lift to a $(\Gamma_K, 2)$-flag $\nabla_{5,2}$, such that $L_{k,2}$ are powers of the cyclotomic character

and the extensions $V_{3/2,2}$ and $V_{4/3,2}$ split.
Indeed, assume the contrary and denote χ_i by χ^{ξ_i} where χ is the cyclotomic character modulo 4 and $\xi_i \in \mathbb{Z}/2\mathbb{Z}$. One sees that $\varepsilon, \varepsilon' \in H^1(K, \mathbb{Z}/2\mathbb{Z})$ then lift to

$$H^1(K, \chi_j^\vee \otimes \chi_i) = H^1(K, L_{j,2}^\vee \otimes L_{i,2}) = H^1(K, \mathbb{Z}/4\mathbb{Z}(\xi_i + \xi_j)),$$

for all $(i,j) \in \{(1,2),(1,3),(2,4),(3,5),(4,5)\}$, hence for all such (i,j), one has $\xi_i + \xi_j = 1$, i.e. $\xi_i \neq \xi_j$. Therefore $\xi_1 \neq \xi_2$, $\xi_2 \neq \xi_4$, $\xi_4 \neq \xi_5$, hence $\xi_1 \neq \xi_5$, and $\xi_1 \neq \xi_3$, $\xi_3 \neq \xi_5$, hence $\xi_1 = \xi_5$. So we get the contradiction $\xi_5 \neq \xi_5$.

Remark 7.24. It follows from [7, Theorem 6.4.4] that, in the case $\ell = p = 2$, $\overline{\rho}$ as in Example 7.23 admits a lift to a completely reducible representation $\rho\colon \Gamma_F \longrightarrow \mathbf{GL}_5(\mathbb{Z}/4\mathbb{Z})$. However, it is important to the Emerton-Gee method to allow the characters on the diagonal to be arbitrary crystalline characters. For instance if $F = \mathbb{Q}_p$, crystalline characters are unramified twists of powers of the cyclotomic character, and the images of Frobenius under the unramified twists appearing on the diagonal give distinct variables on the Emerton-Gee stack, that provide the necessary freedom to construct lifts for all possible $\overline{\rho}$.
In the case when $\ell \neq p$, one can deduce from [3, Section 2.4.4] that $\overline{\rho}$ admits a lift $\rho\colon \Gamma_F \longrightarrow \mathbf{GL}_5(\mathbb{Z}/4\mathbb{Z})$ equipped with a complete flag, and such that the inertia subgroup of Γ_F acts unipotently. Then a simple argument shows that the flag for ρ cannot satisfy condition (1) of Definition 7.13, in view of the example above.

From Proposition 7.10 and Theorem 7.21, one derives the following much weaker

Corollary 7.25. *Let Γ be one of the following groups:*

- *the absolute Galois group of a local field F (a finite extension of $\mathbb{Q}_\ell$ or $\mathbb{F}_\ell((t))$, with $\ell = p$ allowed.)*
- *the topological fundamental group of a closed connected orientable surface.*

Let $d \geq 1$ be an integer, and let

$$\rho_1 : \Gamma \longrightarrow \mathbf{GL}_d(\mathbb{F}_p)$$

be a mod p representation. The following holds.

(1) Assume that the representation ρ_1 has a unique complete Γ-invariant flag. Together with this complete flag, it then lifts for all $r \geq 2$ to a representation

$$\rho_r : \Gamma \longrightarrow \mathbf{GL}_d(\mathbb{Z}/p^r\mathbb{Z}),$$

and these lifts can be chosen in such a way that ρ_{r+1} reduces to ρ_r mod p^r for every r.

(2) In the arithmetic case, assume that F contains all p^2-th roots of unity. Then ρ_1 lifts to a representation

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

Proof. In the topological case, we first extend ρ_1 to a continuous representation $\widehat{\rho}_1 : \widehat{\Gamma} \longrightarrow \mathbf{GL}_d(\mathbb{F}_p)$. Lifting $\widehat{\rho}_1$ to continuous representations of $\widehat{\Gamma}$ implies lifting ρ_1 to representations of Γ (see Remark 4.2). From now on, Γ denotes the profinite completion $\widehat{\Gamma}$.
In Item (1), observe that the unique flag for ρ_1 is necessarily wound (see Remark 7.3). The result then follows from the step-by-step liftability statement of Corollary 7.11. Let us prove Item (2), using a standard technique from group cohomology. Denote by $\Gamma_0 \subset \Gamma$ the open subgroup $\mathrm{Ker}(\rho_1)$. Set $\Gamma^0 := \Gamma/\Gamma_0$. Let $S \subset \Gamma^0$ be a p-Sylow subgroup and $\Gamma_S \subset \Gamma$ be the pullback of S in Γ (it is a prime-to-p finite index subgroup). By passing to the quotient and restriction, ρ_1 gives

rise to a representation $\Gamma_S \longrightarrow \mathbf{GL}_d(\mathbb{F}_p)$. Since S is a p-group, this representation is conjugate to a strictly upper triangular representation $\Gamma_S \longrightarrow \mathbf{U}_d(\mathbb{F}_p)$. Define $V_d := \mathbb{F}_p^d$, viewed as a $(\Gamma_S, 1)$-module via $\rho_{1|\Gamma_S} : \Gamma_S \longrightarrow \mathbf{GL}_d(\mathbb{F}_p)$. By Remark 7.16, it follows that V_d can be equipped with a Kummer flag $\nabla_{d,1}$. Applying Theorem 7.21 (to Γ_S and $r = 1$) one gets that $\nabla_{d,1}$ lifts mod p^2. One then concludes using [4], Lemmas 3.2 and 3.4. □

Remark 7.26. No assumption on roots of unity is required in Corollary 7.25(1), thanks to the (strong) assumption that ρ_1 admits a unique complete Γ-invariant flag. Also, in Corollary 7.25(2), one can replace the assumption on roots of unity, by the weaker condition $F(\mu_p) = F(\mu_{p^2})$, see Remark 7.14.

Remark 7.27. In the topological case, it would be interesting to provide an alternative elementary proof of item (2) of the Corollary, using the presentation of $\pi_1(S)$ by $2g$ generators X_i, Y_i, with the single relation $[X_1, Y_1] \dots [X_g, Y_g] = 1$. To our knowledge, such a proof is not available in the literature. Note that, in genus $g = 1$, item (2) boils down to a nice exercise: prove that two commuting elements of $\mathbf{GL}_d(\mathbb{F}_p)$ admit lifts, to commuting elements of $\mathbf{GL}_d(\mathbb{Z}_p)$. Note also that item (2), in the arithmetic case, is proved in [1] using the presentation of Γ by generators and relations. This approach is much more involved than ours, but works without assumptions on roots of unity.

Remark 7.28. As already mentioned in Section 7.2, the preceding Corollary is still true upon replacing $\mathbb{F}_p$ by a field k of characteristic p, and $\mathbb{Z}/p^2$ (resp. $\mathbb{Z}_p$) by $\mathbf{W}_2(k)$ (resp. $\mathbf{W}(k)$). The proof adapts, with minor modifications.

Remark 7.29. For Galois groups of local fields, the proof of Corollary 7.25 is altogether extremely short. By [7] or [2], item (1) actually holds unconditionally (dismissing flags). We hope this can be done by an elementary treatment, as well.

Acknowledgments

We are grateful to Julien Marché, who brought to our attention that the method we initially designed to study liftability of Galois representations of local fields, applies verbatim to representations of fundamental groups of surfaces. Our thanks go to the anonymous referee, and to Gebhard Böckle, Pierre Colmez, Hélène Esnault, Jean-Pierre Serre and Olivier Wittenberg. They made meaningful remarks and helped improve the exposition.
This work was completed while Mathieu Florence was visiting Nesin Mathematics Village, in Şirince. He warmly thanks the staff for their kindness and excellent working conditions.

Bibliography

[1] G. Böckle, *Lifting mod p representations to characteristics p^2,* J. Number Theory 101 (2003), no. 2, 310–337.
[2] G. Böckle, A. Iyengar, V. Paškūnas, *On local Galois deformation rings,* Forum of Math. Pi, 2023.
[3] L. Clozel, M. Harris, R. Taylor, *Automorphy for some l-adic lifts of automorphic mod l Galois representations.* With Appendix A, summarizing unpublished work of Russ Mann, and Appendix B by Marie-France Vignéras. Publ. Math. Inst. Hautes Études Sci. No. 108, 2008, 1–181.
[4] C. De Clercq, M. Florence, *Lifting low-dimensional local systems,* Math. Zeitschrift, 2021.
[5] C. De Clercq, M. Florence, *Smooth profinite groups, I: geometrizing Kummer theory,* available on the arXiv at https://arxiv.org/abs/2009.11130.

[6] C. De Clercq, M. Florence, G. Lucchini-Arteche, *Lifting vector bundles to Witt vector bundles,* to appear in Israel J. Math.
[7] M. Emerton, T. Gee, *Moduli stacks of étale (ϕ, Γ)-modules and the existence of crystalline lifts,* Annals of Math. Studies, 2023.
[8] F. Grunewald, A. Jaikin-Zapirain, P. A. Zalesskii, *Cohomological goodness and the profinite completion of Bianchi groups,* Duke Math. J., Tome 141 (2008) no. 1, p. 53-72.
[9] C. B. Khare, M. Larsen, *Liftable groups, negligible cohomology and Heisenberg representations,* available on the arXiv at https://arxiv.org/pdf/2009.01301.pdf.
[10] J.-P. Serre, *Cohomologie galoisienne*, Springer Lecture Notes in Math., 1997.
[11] J.-P. Serre, *Structure de certains pro-p-groupes*, Sém. Bourbaki, exp. 252 (1964), p. 145-155.

Andrea Conti, Department of Mathematics, University of Luxembourg, 6 Av. de la Fonte, 4364 Esch-sur-Alzette, Luxembourg, Cyril Demarche and Mathieu Florence, Sorbonne Université and Université Paris Cité, CNRS, IMJ-PRG, F-75005 Paris, France.