PARAMETRIZATION AND LOCAL–GLOBAL PRINCIPLE FOR p-EXTENSIONS IN CHARACTERISTIC p

NOTES FOR A TALK GIVEN IN BORDEAUX (2025/09/19), GRENOBLE (2025/10/02), CAEN (2025/10/03), BESANÇON (2025/10/14), TOULOUSE (2025/10/16), PADERBORN (2025/11/12), LYON (2025/11/27).

BÉRANGER SEGUIN

Abstract. One of the main themes of number theory is the description of extensions of a fixed (local or global) field. For abelian extensions, this is accomplished by class field theory, which has the distinctive property that local and global extensions are tightly connected. When restricted to abelian p-extensions in characteristic p, this theory takes an explicit form: this is Artin-Schreier(-Witt) theory. In this talk, we shall venture beyond the well-trodden path of abelian extensions, and explore non-abelian generalizations of Artin-Schreier theory.

A key feature of p-extensions in characteristic p is wild ramification, which will enable us to formulate a local-global principle in the spirit of class field theory for certain non-abelian p-extensions. This principle relies on a new phenomenon: the invariance of the last jump of minimal solutions to local embedding problems when modifying only the unramified part of the problem.

All results are joint with Fabian Gundlach.

Conventions for the whole talk:

- p is a fixed prime number (2 is allowed), and all fields will have characteristic p
- if K is a field, $\Gamma_K := \mathrm{Gal}(K^{\mathrm{sep}}|K)$ is its absolute Galois group, with the profinite topology
- G will always denote a finite p-group
  To simplify things, we assume that $g^p = 1$ for all $g \in G$ (G is trivial or has exponent p). Getting rid of this hypothesis is a small exercise if you know about Witt vectors.
- except if stated otherwise, $\rho\colon \Gamma_K \to G$ means that ρ is a continuous group homomorphism
- a *G-extension of K* will be a conjugacy class (up to left-composition by inner automorphisms of G) of continuous group homomorphisms $\Gamma_K \to G$, i.e., an element of $H^1(K, G)$.[1]

1. Abelian p-extensions: Artin–Schreier theory and class field theory

There are not many abelian p-groups of exponent $\leq p$: only $G = (\mathbb{Z}/p\mathbb{Z})^r$ for some $r \geq 0$. Because of the equality $H^1(K, (\mathbb{Z}/p\mathbb{Z})^r) = H^1(K, \mathbb{Z}/p\mathbb{Z})^r$, we reduce to the cyclic case $G = \mathbb{Z}/p\mathbb{Z}$. It is dealt with by the following classical theorem:

Theorem 1.1 (Artin–Schreier theory)**.** *We have* $\mathrm{Hom}(\Gamma_K, \mathbb{Z}/p\mathbb{Z}) = H^1(K, \mathbb{F}_p) = K/\wp(K)$, *where* $\wp\colon K^{\mathrm{sep}} \to K^{\mathrm{sep}}$ *is the* Artin–Schreier map $x \mapsto x^p - x$.

Proof. That $\mathrm{Hom}(\Gamma_K, \mathbb{Z}/p\mathbb{Z}) = H^1(K, \mathbb{F}_p)$ is clear (Γ_K acts trivially on $\mathbb{F}_p$ since $\mathbb{F}_p \subseteq K$). The map $\wp$ is surjective with kernel $\mathbb{F}_p$, so we have the short exact sequence $0 \to \mathbb{F}_p \to K^{\mathrm{sep}} \xrightarrow{\wp} K^{\mathrm{sep}} \to 0$. Taking Galois cohomology yields the short exact sequence $K \xrightarrow{\wp} K \to H^1(K, \mathbb{F}_p) \to H^1(K, K^{\mathrm{sep}})$. By "additive Hilbert 90" (normal basis theorem), we have $H^1(K, K^{\mathrm{sep}}) = 0$, concluding the proof. (The same proof shows $H^i(K, \mathbb{F}_p) = 0$ for $i \geq 2$.) □

[1]We think of G-extensions as Galois extensions $L|K$ with an isomorphism $\mathrm{Gal}(L|K) \simeq G$, but since we do not require surjectivity this also includes étale K-algebras that are not fields. For instance, the trivial homomorphism $\Gamma_K \to G$ corresponds to the trivial extension (the product of $|G|$ copies of K, where G acts by permutation), which is not a field if $G \neq 1$. Observe that, just like in a Galois field extension, the points fixed by the action of G correspond to the diagonal embedding, so the "fixed subfield" is K. If we want to count only fields, i.e., conjugacy classes of surjective homomorphisms, we can proceed by inclusion-exclusion, sieving homorphisms depending on their image, and using the Möbius function associated with the lattice of subgroups of G.

Concretely, if $x \in K$, then the $\rho\colon \Gamma_K \to \mathbb{Z}/p\mathbb{Z}$ corresponding to $x \bmod \wp(K)$ is $\tau \mapsto \tau(y) - y$, where $y \in \wp^{-1}(x)$ is arbitrary (any two y differ by an element of $\mathbb{F}_p$ so induce the same ρ).

Now, assume that K is a local or global field, and let $K^{\mathrm{ur}} \subseteq K^{\mathrm{sep}}$ be its maximal unramified extension (for global fields, this means: unramified at all primes). We let $\mathrm{Hom}_{\mathrm{ur}}(\Gamma_K, G) := \mathrm{Hom}(\mathrm{Gal}(K^{\mathrm{ur}}|K), G)$, which is identified with the subset of $\mathrm{Hom}(\Gamma_K, G)$ consisting of morphisms that vanish on $\Gamma_{K^{\mathrm{ur}}}$. If G is an abelian group, then $\mathrm{Hom}(\Gamma_K, G)$ is an abelian group, and $\mathrm{Hom}_{\mathrm{ur}}(\Gamma_K, G)$ is a subgroup. We define the quotient

$$\mathcal{I}(K, G) := \mathrm{Hom}(\Gamma_K, G) / \mathrm{Hom}_{\mathrm{ur}}(\Gamma_K, G).$$

For any $\rho\colon \Gamma_K \to G$, we say that its projection in $\mathcal{I}(K, G)$ is its *inertial type.*

Class field theory implies the following local–global principle for inertial types of abelian p-extensions:

Theorem 1.2 (A consequence of class field theory)**.** *Let $K = \mathbb{F}_q(T)$ with $q = p^d$, let G be an abelian p-group.*[2] *Then:*

$$\mathcal{I}(K, G) \simeq \bigoplus_{\mathfrak{p} \text{ prime of } K} \mathcal{I}(K_{\mathfrak{p}}, G)$$

Today's goal: give non-abelian generalizations of Theorems 1.1 and 1.2.

2. Parametrization of p-extensions: beyond the abelian case

2.1. **The Lazard correspondence.** Let $\mathfrak{g}$ be a Lie $\mathbb{F}_p$-algebra of nilpotency class $< p$ (i.e., $[x_1, [x_2, [\ldots, [x_{p-1}, x_p] \cdots]]] = 0$). Then, we can equip $\mathfrak{g}$ with a binary operation $\circ$ defined by truncating the Baker–Campbell–Hausdorff formula (the one expressing $\log(\exp(x)\exp(y))$ in terms of commutators):

$$x \circ y := x + y + \frac{1}{2}[x, y] + \frac{1}{12}\left([x, [x, y]] + [y, [y, x]]\right) + \ldots$$

Here, we truncate the formula as soon as p appears in the denominator, which is also the moment where we see p-fold commutators (in other words, we take $\frac{0}{0} = 0$...).

Theorem 2.1 (Lazard correspondence)**.** *When equipped with $\circ$, $(\mathfrak{g}, \circ)$ is a group. In fact, the relationship between $\mathfrak{g}$ and $(\mathfrak{g}, \circ)$ defines an equivalence of categories*

$$\left\{ \begin{array}{c} \text{Lie } \mathbb{F}_p\text{-algebras} \\ \text{of nilpotency class} < p \end{array} \right\} \overset{\sim}{\longleftrightarrow} \left\{ \begin{array}{c} \text{groups of exponent 1 or } p, \\ \text{of nilpotency class} < p \end{array} \right\}.$$

2.2. **σ-conjugacy classes and G-extensions.** If G has nilpotency class $< p$, we can "extend scalars" to any field K of characteristic p: via the Lazard correspondence, we have $G = (\mathfrak{g}, \circ)$ for some Lie $\mathbb{F}_p$-algebra $\mathfrak{g}$; we can then consider the Lie algebra $\mathfrak{g} \otimes_{\mathbb{F}_p} K$ (the Lie bracket is extended bilinearly),[3] and use the Lazard correspondence again to obtain a group

$$G_K := (\mathfrak{g} \otimes_{\mathbb{F}_p} K, \circ).$$

(If you prefer geometric language: we have a *canonical* algebraic group over $\mathbb{F}_p$, defined via its functor of points $R \mapsto (\mathfrak{g} \otimes_{\mathbb{F}_p} R, \circ)$, which is unipotent [hence connected] and has G as its group of $\mathbb{F}_p$-points. Realizing a given group as the $\mathbb{F}_p$-points of a connected algebraic group seems hard in general, cf. `https://mathoverflow.net/questions/498176/extending-scalars-of-p-groups`.)

The natural action of the absolute Frobenius $\sigma\colon K \to K, x \mapsto x^p$ on K induces an endomorphism of G_K. The group G_K acts on itself via *σ-conjugation*:

$$g.m = \sigma(g) \circ m \circ (-g).$$

(Note that $-g$ is the inverse of g for both $+$ and $\circ$.) We denote by $G_K /\!/ G_K$ the set of the orbits for this action (the σ-conjugacy classes).

[2] We could replace the hypotheses "the base field is rational" and "G is p-group" by "G has order coprime both to $|\mathbb{F}_q^\times| = q - 1$ and to the order of Pic^0 of K" . In more general situations, the statement is incorrect.

[3] For groups of exponent p^r, one should instead consider Lie $\mathbb{Z}/p^r\mathbb{Z}$-algebras, and tensor them with the ring $W_r(K)$ of truncated Witt vectors of length r over K.

Remark 2.2 (Abelian case). If G is abelian, then $\circ = +$ and we simply have $g.m = m + \wp(g)$, so $G_K//G_K = G_K/\wp(G_K)$.

We obtain a non-abelian form of Theorem 1.1, known to Victor Abrashkin (and probably known before him):

Theorem 2.3 (Nilpotent Artin–Schreier theory)**.** $H^1(K, G) \simeq G_K//G_K$

Sketch of proof. Just like the proof of Theorem 1.1, the proof follows "formally" from the two following facts:

(i) the "non-abelian $\wp$", i.e., the map $G_{K^{\mathrm{sep}}} \to G_{K^{\mathrm{sep}}}$, $x \mapsto \sigma(x) \circ (-x)$, is surjective
(ii) the non-abelian cohomology set $H^1(\Gamma_K, G_{K^{\mathrm{sep}}})$ is trivial (a singleton)

Both of these facts are proved by induction on the nilpotency class, reducing to the abelian case. □

Remark 2.4. Facts (i) and (ii) (and hence Theorem 2.3) also hold in other settings, e.g., when $G = \mathrm{GL}_n(\mathbb{F}_p)$ and $G_K = \mathrm{GL}_n(K)$: in these cases, Theorem 2.3 becomes a principle for parametrizing modulo p Galois representations of K: this is the theory of étale φ-modules.

3. Last jumps, and the non-abelian local–global principle

3.1. **Ramification filtration and last jump.** If K is a local field, then Γ_K is equipped with a *ramification filtration* (in the upper numbering) by normal subgroups Γ_K^v for $v \in \mathbb{R}_{\geq -1}$. For instance:

$$\Gamma_K^{-1} = \Gamma_K \qquad \Gamma_K^0 = \text{inertia} \qquad \bigcup_{v>0} \Gamma_K^v = \text{wild inertia (pro-}p\text{-Sylow of inertia)} \qquad \bigcap_{v \geq -1} \Gamma_K^v = 1$$

This filtration encodes information about extensions of K (Artin conductors, discriminant, etc.).

Definition 3.1. If K is a local field and $\rho\colon \Gamma_K \to G$ is a (local) homomorphism, we define

$$\operatorname{lastjump} \rho := \inf \left\{ v \in \mathbb{Q}_{\geq 0} \;\middle|\; \rho(\Gamma_K^v) = 1 \right\} \in \mathbb{Q}_{\geq 0}.$$

If K is a global field, $\rho\colon \Gamma_K \to G$ is a (global) homomorphism, and $\mathfrak{p}$ is a prime of K, we define

$$\operatorname{lastjump}_{\mathfrak{p}} \rho := \operatorname{lastjump} \rho|_{\Gamma_{K_{\mathfrak{p}}}}.$$

(This has the same value for all the (conjugate) embeddings $\Gamma_{K_{\mathfrak{p}}} \hookrightarrow \Gamma_K$ via the identification $\Gamma_{K_{\mathfrak{p}}} \simeq D_{\mathfrak{P}|\mathfrak{p}}$ for primes $\mathfrak{P}$ above $\mathfrak{p}$ in K^{sep} .)

If G is abelian, then the last jump is an integer by the Hasse–Arf theorem, and it compares to the conductor as follows:

$$\operatorname{lastjump} \rho = \begin{cases} 0 & \text{if } \operatorname{cond} \rho = 0 \quad \text{(unramified case)} \\ \operatorname{cond} \rho - 1 & \text{if } \operatorname{cond} \rho \geq 1 \quad \text{(ramified case).} \end{cases}$$

Hence, the last jump can be seen as a "generalized conductor", vanishing exactly for extensions that are at most tamely ramified.

3.2. **Local–global principle.** Consider an exact sequence

$$1 \longrightarrow N \longrightarrow G \longrightarrow Q \longrightarrow 1$$

where $N \subseteq Z(G)$, and N and Q are both finite abelian p-groups. (G is then a finite p-group of nilpotency class ≤ 2.)

Theorem 3.2. *Let $K = \mathbb{F}_q(T)$ with $q = p^d$. Fix for each prime $\mathfrak{p}$ of K a number $v_{\mathfrak{p}} \in \mathbb{Q}_{\geq 0}$, such that $\left\{ \mathfrak{p} \;\middle|\; v_{\mathfrak{p}} \neq 0 \right\}$ is finite. Then:*

$$\frac{1}{|G|} \left| \left\{ \rho\colon \Gamma_K \to G \;\middle|\; \forall \mathfrak{p},\ \operatorname{lastjump}_{\mathfrak{p}} \rho = v_{\mathfrak{p}} \right\} \right| = \prod_{\mathfrak{p} \in \mathcal{P}} \frac{1}{|G|} \left| \left\{ \rho_{\mathfrak{p}}\colon \Gamma_{K_{\mathfrak{p}}} \to G \;\middle|\; \operatorname{lastjump} \rho_{\mathfrak{p}} = v_{\mathfrak{p}} \right\} \right|$$

This is a direct (quantitative) link between local and global extensions!

Remark 3.3 (Abelian case). When G is abelian, Theorem 3.2 follows immediately from Theorem 1.2. Indeed, $\frac{1}{|G|}\left|\{\rho \mid \ldots\}\right|$ is simply counting inertial types, for which we have a local–global bijection. Note that in this case the last jump can be replaced by basically any height (as long as it vanishes exactly for unramified G-extensions, and makes the counts finite).

Remark 3.4. When G is non-abelian, the interpretation of the factor $\frac{1}{|G|}$ is not as easy as for abelian extensions. It cannot be interpreted as a number of equivalence classes identifying homomorphisms having the same restriction to inertia (a natural generalization of inertial types), as the size of the class of a given ρ is not necessarily $|G|$, but $\left|\mathrm{Cent}_G(\rho(\Gamma_K^0))\right|$ (Frobenius elements cannot be picked arbitrarily). In fact, to get "orbits of size $|G|$", we will have to define a subtler notion of "unramified twist" (change of Frobenius element), explained later. This will end up affecting not only the unramified part of extensions, but also the "first few" ramification subgroups. The last jump is unchanged when altering the first few ramification subgroups, so this twisting operation will be last-jump-preserving; it will not, however, be discriminant-preserving: this explains the special role of the last jump when dealing with non-abelian extensions.

3.3. **Reduction to a local phenomenon.** The proof of Theorem 3.2 relies on Theorem 1.2 and on the following purely local phenomenon:

$$\begin{gathered}\text{For any } \overline{\rho}\colon \Gamma_{K_\mathfrak{p}} \to Q, \text{ the following number}\\ \text{depends only on the inertial type of } \overline{\rho}\text{:}\\ \operatorname{minembed}\overline{\rho} := \min\left\{\operatorname{lastjump}\rho \;\middle|\; \begin{matrix}\rho\colon \Gamma_{K_\mathfrak{p}} \to G\\ \rho \bmod N = \overline{\rho}\end{matrix}\right\}\end{gathered} \tag{$\star$}$$

(In other words, $\operatorname{minembed}\overline{\rho} = \operatorname{minembed}(\overline{\rho}+\overline{\delta})$ for any $\overline{\delta} \in \mathrm{Hom}_{\mathrm{ur}}(\Gamma_{K_\mathfrak{p}}, Q)$.)

Remark 3.5. The set of solutions $\left\{\rho\colon \Gamma_{K_\mathfrak{p}} \to G \;\middle|\; \rho \bmod N = \overline{\rho}\right\}$ is indeed non-empty because $H^2(K,N) = 0$ (cf. Theorem 1.1), so the corresponding embedding problems are solvable.

We first explain how to derive Theorem 3.2 from ($\star$).

Lemma 3.6. *Assume* ($\star$). *Then, the following property holds:*

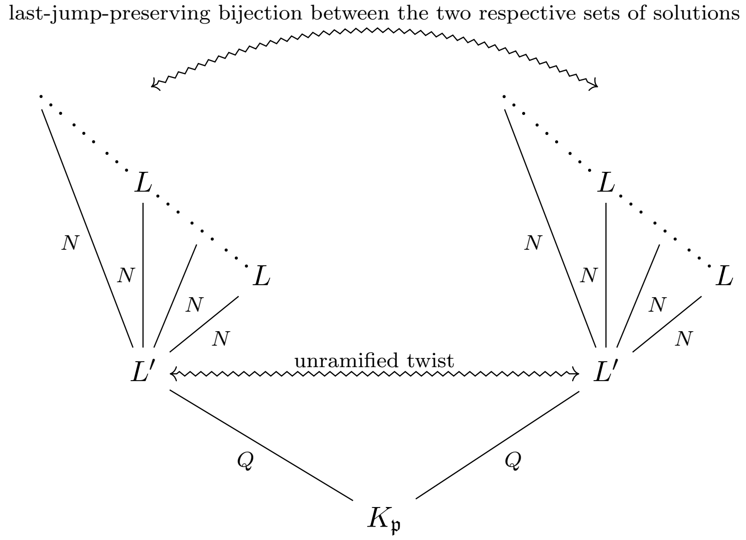
$$\begin{gathered}\textit{For any } \overline{\rho}\colon \Gamma_{K_\mathfrak{p}} \to Q \textit{ and for any } v \geq 0, \textit{ the following number}\\ \textit{depends only on the inertial type of } \overline{\rho}\textit{:}\\ \left|\left\{\rho\colon \Gamma_{K_\mathfrak{p}} \to G \;\middle|\; \begin{matrix}\rho \bmod N = \overline{\rho}\\ \operatorname{lastjump}\rho = v\end{matrix}\right\}\right|\end{gathered} \tag{$\star'$}$$

Proof. Pick a minimal solution $\rho_0\colon \Gamma_{K_\mathfrak{p}} \to G$, such that $\rho_0 \bmod N = \overline{\rho}$ and $\operatorname{lastjump}\rho_0 = \operatorname{minembed}\overline{\rho}$. All lifts of $\overline{\rho}$ are twists of ρ_0 by some $\delta\colon \Gamma_{K_\mathfrak{p}} \to N$. Computing the last jump of $\delta \cdot \rho_0$, we obtain

$$\left|\left\{\rho\colon \Gamma_{K_\mathfrak{p}} \to G \;\middle|\; \begin{matrix}\rho \bmod N = \overline{\rho}\\ \operatorname{lastjump}\rho \leq v\end{matrix}\right\}\right| = \begin{cases} 0 & \text{if } v < \operatorname{minembed}\overline{\rho}\\ \left|\left\{\delta\colon \Gamma_{K_\mathfrak{p}} \to N \;\middle|\; \operatorname{lastjump}\delta \leq v\right\}\right| & \text{otherwise.}\end{cases}$$

The right-hand side depends on $\overline{\rho}$ only through $\operatorname{minembed}\overline{\rho}$, which depends only on the inertial class by ($\star$), proving the claim (that $\leq v$ can be replaced by $= v$ is obvious). □

A visual representation of $(\star')$ is given by the following diagram:



Proof of Theorem 3.2, assuming $(\star)$. Pick for each $\overline{\rho}\colon \Gamma_K \to Q$ a solution $\widetilde{\overline{\rho}}\colon \Gamma_K \to G$ to the embedding problem. We have

$$\begin{aligned}
&\frac{1}{|G|}\left|\left\{\rho\colon \Gamma_K \to G \;\middle|\; \forall \mathfrak{p},\ \operatorname{lastjump}_{\mathfrak{p}} \rho = v_{\mathfrak{p}}\right\}\right| \\
&= \frac{1}{|Q|}\sum_{\overline{\rho}\colon \Gamma_K \to Q} \frac{1}{|N|}\left|\left\{\rho\colon \Gamma_K \to G \;\middle|\; \begin{matrix} \rho \bmod N = \overline{\rho} \\ \forall \mathfrak{p},\ \operatorname{lastjump}_{\mathfrak{p}} \rho = v_{\mathfrak{p}} \end{matrix}\right\}\right| \\
&= \frac{1}{|Q|}\sum_{\overline{\rho}\colon \Gamma_K \to Q} \frac{1}{|N|}\left|\left\{\delta\colon \Gamma_K \to N \;\middle|\; \forall \mathfrak{p},\ \operatorname{lastjump}_{\mathfrak{p}}(\delta\cdot\widetilde{\overline{\rho}}) = v_{\mathfrak{p}}\right\}\right| \\
&= \frac{1}{|Q|}\sum_{\overline{\rho}\colon \Gamma_K \to Q} \prod_{\mathfrak{p}} \frac{1}{|N|}\left|\left\{\delta_{\mathfrak{p}}\colon \Gamma_{K_{\mathfrak{p}}} \to N \;\middle|\; \operatorname{lastjump}(\delta_{\mathfrak{p}}\cdot\widetilde{\overline{\rho}}|_{\Gamma_{K_{\mathfrak{p}}}}) = v_{\mathfrak{p}}\right\}\right| \quad \text{by Theorem 1.2 for } N \\
&= \frac{1}{|Q|}\sum_{\overline{\rho}\colon \Gamma_K \to Q} \underbrace{\prod_{\mathfrak{p}} \frac{1}{|N|}\left|\left\{\rho_{\mathfrak{p}}\colon \Gamma_{K_{\mathfrak{p}}} \to G \;\middle|\; \begin{matrix} \rho_{\mathfrak{p}} \bmod N = \overline{\rho}|_{\Gamma_{K_{\mathfrak{p}}}} \\ \operatorname{lastjump} \rho_{\mathfrak{p}} = v_{\mathfrak{p}} \end{matrix}\right\}\right|}_{\text{depends only on the inertial class of } \overline{\rho} \text{ by } (\star')} \\
&= \prod_{\mathfrak{p}} \frac{1}{|Q|}\sum_{\overline{\rho}_{\mathfrak{p}}\colon \Gamma_{K_{\mathfrak{p}}} \to Q} \frac{1}{|N|}\left|\left\{\rho_{\mathfrak{p}}\colon \Gamma_{K_{\mathfrak{p}}} \to G \;\middle|\; \begin{matrix} \rho_{\mathfrak{p}} \bmod N = \overline{\rho}|_{\Gamma_{K_{\mathfrak{p}}}} \\ \operatorname{lastjump} \rho_{\mathfrak{p}} = v_{\mathfrak{p}} \end{matrix}\right\}\right| \quad \text{by Theorem 1.2 for } Q \\
&= \prod_{\mathfrak{p}} \frac{1}{|G|}\left|\left\{\rho_{\mathfrak{p}}\colon \Gamma_{K_{\mathfrak{p}}} \to G \;\middle|\; \operatorname{lastjump} \rho_{\mathfrak{p}} = v_{\mathfrak{p}}\right\}\right|. \qquad \square
\end{aligned}$$

3.4. **Proof of** $(\star)$ **(sketch).** Let $\rho \in \operatorname{Hom}(\Gamma_{K_{\mathfrak{p}}}, G)$, $\delta \in \operatorname{Hom}_{\mathrm{ur}}(\Gamma_{K_{\mathfrak{p}}}, G)$, let $\overline{\rho} := \rho \bmod N$ and $\overline{\delta} := \delta \bmod N$. Assume that ρ is a minimal solution, i.e., $\operatorname{lastjump}\rho = \operatorname{minembed}\overline{\rho}$. By symmetry, we simply have to show $\operatorname{minembed}(\overline{\rho}+\overline{\delta}) \leq \operatorname{minembed}\overline{\rho}$, i.e., to construct a lift ρ' of $\overline{\rho}+\overline{\delta}$ such that $\operatorname{lastjump}\rho' \leq \operatorname{lastjump}\rho$. There is an obvious *map* lifting $\overline{\rho}+\overline{\delta}$ with last jump $\operatorname{lastjump}\rho$, namely the pointwise product $\rho\cdot\delta$. However, it is not a homomorphism! In order to "fix it", we look for a map $\varepsilon\colon \Gamma_{K_{\mathfrak{p}}} \to N$ such that

(i) $\varepsilon\cdot\rho\cdot\delta$ is a homomorphism (it is then a lift of $\overline{\rho}+\overline{\delta}$)
(ii) $\operatorname{lastjump}\varepsilon \leq \operatorname{lastjump}\rho$ (in fact we will have $\leq \operatorname{lastjump}\overline{\rho}$)

This then implies that $\rho' := \varepsilon\cdot\rho\cdot\delta$ works, proving the claim.

Point (ii) makes precise the claim that "only the first few ramification subgroups need to be modified" from Remark 3.4. At the price of this modification, we can extend "unramified twisting" to non-abelian settings.

For any map $\varepsilon\colon \Gamma_{K_\mathfrak{p}} \to N$, we define the 2-coboundary $\partial\varepsilon(\tau_1,\tau_2) := \varepsilon(\tau_1)+\varepsilon(\tau_2)-\varepsilon(\tau_1\tau_2)$. A straightforward computation shows that property (i) is equivalent to $\partial\varepsilon(\tau_1,\tau_2) = [\overline{\rho}_2(\tau_2),\overline{\rho}_1(\tau_1)]$ (here, $[-,-]\colon Q^2 \to N$ is the commutator in G, which is a biadditive map).

Define $N_K = N\otimes_{\mathbb{F}_p}K$, $Q_K = Q\otimes_{\mathbb{F}_p}K$, and extend $[-,-]$ bilinearly to a K-bilinear alternating map $Q_K^2 \to N_K$.

By Artin–Schreier theory, there exists $m_1 \in Q_{K_\mathfrak{p}}$ such that $\overline{\rho}(\tau) = \tau(g_1) - g_1$ for $g_1 \in \wp^{-1}(m_1)$, and such that $\operatorname{lastjump}\overline{\rho} = -v(m_1)$ (v is the valuation in $K_\mathfrak{p}$).

Similarly, letting $\kappa_\mathfrak{p}$ be the residue field of $K_\mathfrak{p}$ (a finite field), the theory of unramified extensions shows that there exists $m_2 \in Q_{\kappa_\mathfrak{p}}$ such that $\overline{\delta}(\tau) = \tau(g_2) - g_2$ for $g_2 \in \wp^{-1}(m_2) \subseteq \overline{\mathbb{F}}_p$.

We let $m_3 := [m_1, g_2] \in N_{K_\mathfrak{p}^{\mathrm{sep}}}$, we pick an arbitrary $g_3 \in \wp^{-1}(m_3) \subseteq N_{K_\mathfrak{p}^{\mathrm{sep}}}$, and we define

$$\varepsilon(\tau) := \tau(g_3) - g_3 + [\overline{\delta}(\tau), g_1].$$

Claim 1: ε is valued in N. Indeed:

$$\begin{aligned}\wp(\tau(g_3) - g_3) &= \tau(m_3) - m_3 \\ &= [m_1, \tau(g_2)] - [m_1, g_2] && \text{as } m_1 \in Q_{K_\mathfrak{p}} \\ &= [\wp(g_1), \overline{\delta}(\tau)] && \text{as } \overline{\delta}(\tau) = \tau(g_2) - g_2 \\ &= \wp([g_1, \overline{\delta}(\tau)]) && \text{as } \overline{\delta}(\tau) \in N.\end{aligned}$$

Claim 2: ε satisfies (i). This is a computation...

Claim 3: We have $\operatorname{lastjump}\varepsilon \leq \operatorname{lastjump}\overline{\rho}$, so ε satisfies (ii). Indeed, we can ignore the term $[\overline{\delta}(\tau), g_1]$ as it vanishes on inertia (unramified terms do not change the last jump). What is left is the Artin–Schreier homomorphism associated to m_3, so $\operatorname{lastjump}\varepsilon \leq -v(m_3)$. Picking a uniformizer π of $K_\mathfrak{p}$ and writing

$$m_1 = \sum_{i=0}^{\operatorname{lastjump}\overline{\rho}} x_i\pi^{-i} \qquad \text{with } x_i \in Q_{\kappa_\mathfrak{p}}$$

we have

$$m_3 = [m_1, g_2] = \sum_{i=0}^{\operatorname{lastjump}\overline{\rho}} [x_i, g_2]\pi^{-i}$$

so $-v(m_3) = \max\{i \mid [x_i, g_2] \neq 0\} \leq \operatorname{lastjump}\overline{\rho}$.

Together, Claims 1–3 conclude the proof.

4. An application: counting D_4-extensions

Let $p = 2$, and $G = D_4$, fitting in the short exact sequence $1 \to \mathbb{F}_2 \to D_4 \to \mathbb{F}_2^2 \to 1$. Locally, over $K = \mathbb{F}_q((T))$ we have

$$\left|\{\rho\colon \Gamma_K \to D_4 \mid \operatorname{lastjump}\rho \leq v\}\right| = \underbrace{\left|\{\delta\colon \Gamma_K \to \mathbb{F}_2 \mid \operatorname{lastjump}\delta \leq v\}\right|}_{=2q^{\lceil v/2\rceil}} \cdot \left|\{\overline{\rho}\colon \Gamma_K \to \mathbb{F}_2^2 \mid \operatorname{minembed}\overline{\rho} \leq v\}\right|$$

with

$$\left|\{\overline{\rho}\colon \Gamma_K \to \mathbb{F}_2^2 \mid \operatorname{minembed}\overline{\rho} = v\}\right| = \begin{cases} 1 & \text{if } v = 0 \\ 2q^{\frac{v-1}{2}}(q-1) & \text{if } v \in 2\mathbb{N} - 1 \\ \frac{v}{2}q^{\frac{v}{2}-1}(q-1)^2 & \text{if } v \in 2\mathbb{N} \end{cases}$$

(all jumps are integers for D_4-extensions!)

Let $K = \mathbb{F}_q(T)$ with $q = 2^d$. The local–global principle (the generating function factors as an Euler product) together with an analytic lemma (comparing the Euler product with Hasse-Weil zeta functions) then implies the following global asymptotics, for some $C > 0$:

$$\left|\{\rho\colon \Gamma_K \to D_4 \mid \textstyle\sum_\mathfrak{p} \deg\mathfrak{p} \cdot \operatorname{lastjump}_\mathfrak{p}\rho = X\}\right| \sim_{X\to\infty} Cq^{3X}X.$$