

Chapter 14

Nilpotent Sections

The next difficult characteristic quotient of a profinite group beyond the maximal abelian quotient might be the maximal pro-nilpotent quotient or its truncated versions of bounded nilpotency. These quotients have been studied in the realm of the section conjecture by Ellenberg around 2000, unpublished, and later by Wickelgren in her thesis [Wg09], and in [Wg10, Wg12a, Wg12b] with special emphasis on the interesting case $\mathbb{P}^1 - \{0, 1, \infty\}$.

The (relative) pro-algebraic version has played an important role in at least two strands of mathematics: (1) on the Hodge theoretic side in the study conducted by Hain of the Teichmüller group and the section conjecture for the generic curve [Hal1b], and (2) on the arithmetic side in the non-abelian Chabauty method of Kim [Ki05] for Diophantine finiteness problems.

We will examine in detail the Lie algebra associated to the maximal pro- ℓ quotient of the geometric fundamental group, see Sect. 14.3, and in particular prove Proposition 207 about the sub Lie algebra of invariants under a finite abelian group action. This will be crucial for counting pro- ℓ sections over a finite field in Sect. 15.3.

The nilpotent section conjecture is known to fail by work of Hoshi [Ho10]. We try to explain that examples for this failure should be seen as *accidents* due to an accidental coincidence of very special properties. In Sect. 14.7, we extend the range of examples, show that in most of these examples the spaces of pro- p sections are in fact uncountable, and suggest a way of reviving the pro- p version of the section conjecture by asking a virtually pro- p section conjecture.

14.1 Primary Decomposition

Let X/k be a geometrically connected variety. We may push the extension $\pi_1(X/k)$ by the maximal pro-nilpotent quotient $\pi_1(\bar{X}) \twoheadrightarrow \pi_1^{\text{nilp}}(\bar{X})$ to obtain the maximal nilpotent extension $\pi_1^{\text{nilp}}(X/k)$. As any finite nilpotent group is canonically the

direct product of its unique p -Sylow groups we obtain in the limit a canonical isomorphism

$$\pi_1^{\text{nilp}}(\overline{X}) = \prod_p \pi_1^{\text{pro-}p}(\overline{X}) \quad (14.1)$$

and also a primary decomposition

$$\pi_1^{\text{nilp}}(X/k) = \prod_p \pi_1^{\text{pro-}p}(X/k) \quad (14.2)$$

that has to be read as a fibre product over Gal_k . For the corresponding section spaces and Kummer maps this leads to

$$\kappa_{\text{nilp}} = (\kappa_p)_p : X(k) \rightarrow \mathcal{S}_{\pi_1^{\text{nilp}}(X/k)} = \prod_p \mathcal{S}_{\pi_1^{\text{pro-}p}(X/k)}. \quad (14.3)$$

If X/k moreover is abelian injective, then because $\pi^{\text{ab}}(X/k)$ is a quotient extension of $\pi_1^{\text{nilp}}(X/k)$ we have

$$X(k) = \kappa_{\text{nilp}}(X(k)) \subset \prod_p \kappa_p(X(k)).$$

Let for the moment k be an algebraic number field and X/k a smooth hyperbolic curve. Then, by Theorem 76, we have $X(k) = \kappa_p(X(k))$, and the section conjecture raises the question whether only diagonal tuples of pro- p sections lift to actual sections along

$$\mathcal{S}_{\pi_1(X/k)} \rightarrow \mathcal{S}_{\pi_1^{\text{nilp}}(X/k)},$$

or better: the section conjecture could be modified to ask for a definition of diagonal tuples as the image and find a Diophantine description of this set. For the section conjecture to hold in its original form it would be desirable if the diagonal tuples would feature a certain independence of p .

14.2 Obstructions from the Descending Central Series

The obstructions against lifting of an abelian section s^{ab} to a nilpotent section form a hierarchy of obstruction classes $\delta_n(s^{\text{ab}})$ with δ_n only being defined if all the previous obstructions δ_i vanish for $i < n$ and also depending on the chosen partial lifts. This study was initiated by Ellenberg and in the thesis of Wickelgren [Wg09].

Definition 194. The *descending central filtration* $C_\bullet \Gamma$ on a profinite group Γ is defined inductively by

$$C_{-1}\Gamma = \Gamma \quad \text{and} \quad C_{-(n+1)}\Gamma = [C_n\Gamma, C_n\Gamma]$$

for $n \geq 2$ where $[A, B]$ is the profinite subgroup generated by the corresponding commutators $[a, b]$ with $a \in A$ and $b \in B$.

The strange numbering takes into account the weight of the associated graded when $\Gamma = \pi_1(\bar{X})$, at least when X is smooth and projective.

Definition 195. Let X/k be a geometrically connected variety and let $\ell \neq \text{char}(k)$ be a prime number. For every $n \in \mathbb{N}$ we have

(1) The *geometrically n -step nilpotent quotient extension* of $\pi_1(X/k)$

$$C_{\geq -n}(\pi_1(X/k))$$

as the pushout by the characteristic quotient

$$\pi_1(\bar{X}) \twoheadrightarrow \pi_1(\bar{X})/C_{-(n+1)}\pi_1(\bar{X}).$$

(2) The *geometrically n -step pro- ℓ nilpotent quotient extension* of $\pi_1(X/k)$

$$C_{\geq -n}(\pi_1^{\text{pro-}\ell}(X/k))$$

as the pushout by the characteristic quotient

$$\pi_1^{\text{pro-}\ell}(\bar{X}) \twoheadrightarrow \pi_1^{\text{pro-}\ell}(\bar{X})/C_{-(n+1)}\pi_1^{\text{pro-}\ell}(\bar{X}).$$

Definition 196. The following commutative diagram defines truncated nilpotent Kummer maps

$$\kappa_{\text{ab}}, \quad \kappa_{\text{nilp}}, \quad \kappa_n, \quad \kappa_\ell, \quad \text{and} \quad \kappa_{\ell,n},$$

the abelian, nilpotent, n -step nilpotent, pro- ℓ , n -step nilpotent pro- ℓ Kummer map respectively. The diagram moreover shows how these Kummer maps factorize each other:

$$\begin{array}{ccccccc}
 X(k) & \xrightarrow{\quad \quad \quad} & \text{Pic}_X^1(k) & & & & \\
 \downarrow \kappa & \searrow \kappa_{\text{nilp}} & \searrow \kappa_n & \searrow \kappa_{\text{ab}} & & & \downarrow \kappa_{\text{Pic}_X^1} \\
 \mathcal{S}_{\pi_1(X/k)} & \xrightarrow{\quad \quad} & \mathcal{S}_{\pi_1^{\text{nilp}}(X/k)} & \xrightarrow{\quad \quad} & \mathcal{S}_{C_{\geq -n}(\pi_1(X/k))} & \xrightarrow{\quad \quad} & \mathcal{S}_{\pi_1^{\text{ab}}(X/k)} \\
 & \searrow \kappa_\ell & \downarrow \text{pr} & \searrow \kappa_{\ell,n} & \downarrow \text{pr} & & \downarrow \text{pr} \\
 & & \mathcal{S}_{\pi_1^{\text{pro-}\ell}(X/k)} & \xrightarrow{\quad \quad} & \mathcal{S}_{C_{\geq -n}(\pi_1^{\text{pro-}\ell}(X/k))} & \xrightarrow{\quad \quad} & \mathcal{S}_{\pi_1^{\text{ab,}\ell}(X/k)}.
 \end{array}$$

Dévissage for truncated nilpotent sections. We abbreviate $\bar{\pi} = \pi_1(\bar{X})$ and for the maximal pro- ℓ quotient $\bar{\pi}^\ell = \pi_1^{\text{pro-}\ell}(\bar{X})$. The central extension

$$1 \rightarrow \text{gr}_{-n}^C \bar{\pi} \rightarrow \bar{\pi}/C_{-(n+1)}\bar{\pi} \xrightarrow{\text{pr}} \bar{\pi}/C_{-n}\bar{\pi} \rightarrow 1 \quad (14.4)$$

describes a pullback of extensions, see [Sx05] Proposition 2.6. By Proposition 91 any section s of $\pi_1^{\text{pro-}\ell}(X/k)$ is unramified at points $b \in B$ of codimension 1, and thus by Zariski–Nagata purity, see [SGA1] X Theorem 3.1, every pro- ℓ section is unramified on B and descends uniquely to a section

$$s_B : \pi_1(B) \rightarrow \pi_1(\mathcal{X}) / \ker(\pi_1(\bar{X}) \rightarrow \pi_1^{\text{pro-}\ell}(\bar{X})).$$

The map $s \mapsto s_B$ yields an inverse to the pullback map

$$j^* : \mathcal{S}_{\pi_1^{\text{pro-}\ell}(\mathcal{X}/B)} \xrightarrow{\sim} \mathcal{S}_{\pi_1^{\text{pro-}\ell}(X/k)}.$$

The central extension

$$1 \rightarrow \text{gr}_{-n}^C \bar{\pi}^\ell \rightarrow \bar{\pi}^\ell / C_{-(n+1)} \bar{\pi}^\ell \xrightarrow{\text{pr}} \bar{\pi}^\ell / C_{-n} \bar{\pi}^\ell \rightarrow 1 \quad (14.5)$$

yields as an application of Sect. 1.3 the following pro- ℓ version.

Proposition 199. *Let X/k have good reduction over the base B with function field k . Then we have an exact sequence*

$$1 \rightarrow H^1(B_{\text{ét}}, \text{gr}_{-n}^C \bar{\pi}^\ell) \rightarrow \mathcal{S}_{C_{\geq -n} \pi_1^{\text{pro-}\ell}(X/k)} \xrightarrow{\text{pr}_*} \mathcal{S}_{C_{\geq -(n-1)} \pi_1^{\text{pro-}\ell}(X/k)} \xrightarrow{\delta_n} H^2(B_{\text{ét}}, \text{gr}_{-n}^C \bar{\pi}^\ell).$$

In particular, the obstruction to lifting a section s_{n-1} of $C_{\geq -(n-1)} \pi_1^{\text{pro-}\ell}(X/k)$ to a section of $C_{\geq -n} \pi_1^{\text{pro-}\ell}(X/k)$ is given by the class $\delta_n(s_{n-1})$.

Proof. Étale cohomology of $B_{\text{ét}}$ and group cohomology of $\pi_1(B)$ compare as follows. We have

$$H^1(\pi_1(B), \text{gr}_{-n}^C \bar{\pi}^\ell) = H^1(B_{\text{ét}}, \text{gr}_{-n}^C \bar{\pi}^\ell)$$

and an inclusion

$$H^2(\pi_1(B), \text{gr}_{-n}^C \bar{\pi}^\ell) \subseteq H^2(B_{\text{ét}}, \text{gr}_{-n}^C \bar{\pi}^\ell).$$

Now the proof is essentially the same as for Proposition 197. □

Remark 200. Hain considers in [Hai11a] a fully pro-algebraic analogue of non-abelian cohomology as discussed in Sect. 14.2. He replaces the base group Gal_k by an ℓ -adic representation

$$\rho : \text{Gal}_k \rightarrow R(\mathbb{Q}_\ell)$$

in a reductive algebraic group R and considers the relative algebraic unipotent completion

$$\tilde{\rho} : \pi_1(X) \rightarrow G(\mathbb{Q}_\ell)$$

of $\pi_1(X)$ relative ρ that takes values in the universal (in some sense) unipotent extension G of R . This makes non-abelian cohomology somewhat computable since

we can now work with Lie algebras, more precisely Lie algebras in the Tannaka category of R -modules. Hain's result on the section conjecture for the generic curve in [Hal1b] builds on this pro-algebraic version of non-abelian cohomology.

14.3 The Lie Algebra

Following Magnus and Lazard, see [La94], we associate to the descending central series $C_\bullet \Gamma$ of a pro- ℓ group Γ the graded \mathbb{Z}_ℓ -Lie-algebra

$$\mathrm{Lie}(\Gamma) = \bigoplus_{n \geq 1} \mathrm{Lie}_n(\Gamma) = \bigoplus_{n \geq 1} \mathrm{gr}_{-n}^C (C_{-n} \Gamma / C_{-(n+1)} \Gamma) \quad (14.6)$$

with the Lie bracket being induced by the commutator in the group Γ .

From now on let X/k be a smooth, projective curve of genus at least 2. For a prime number ℓ different from the characteristic of k , the group $\bar{\pi}^\ell = \pi_1(\bar{X})^{\mathrm{pro-}\ell}$ is a Poincaré duality group and coincides with the pro- ℓ completion of the surface group

$$\Pi = \Pi_g = \langle x_1, \dots, x_{2g} | [x_1, x_2] \dots [x_{2g-1}, x_{2g}] \rangle.$$

In this case we set

$$\mathfrak{p} = \mathrm{Lie}(\bar{\pi}^\ell). \quad (14.7)$$

The graded piece $\mathfrak{p}_n = \mathrm{Lie}_n(\bar{\pi}^\ell)$ in degree $-n$ is a free \mathbb{Z}_ℓ -module of finite rank, see [La66] Proposition 1. We set

$$\mathfrak{p}_K = \mathfrak{p} \otimes_{\mathbb{Z}_\ell} K \quad (14.8)$$

for the change of coefficients to a field extension K/\mathbb{Q}_ℓ . The conjugation action by $\pi_1(X)$ descends to a Gal_k action on the graded Lie algebra \mathfrak{p}_K over K .

The Poincaré series. We are interested to compute the Poincaré series of \mathfrak{p} as a power series

$$[\mathfrak{p}] = \sum_{n \geq 1} [\mathfrak{p}_n] T^n \quad (14.9)$$

with coefficients in the Grothendieck ring of $\mathbb{Z}_\ell[\mathrm{Gal}_k]$ -modules which are free of finite rank as \mathbb{Z}_ℓ -modules. For the free Lie algebra this was achieved in characteristic 0 by Brandt [Br44] Theorem III, and rediscovered more conceptually by many, e.g. [By03] Theorem 5.4. We follow the same path, especially we argue in strong analogy with the computation of the generating function

$$\sum_{n \geq 1} \dim_K \mathfrak{p}_{K,n} T^n$$

by Labute [La67] Theorem 2.

Let L_H be the free \mathbb{Z}_ℓ -Lie algebra generated by the $\mathbb{Z}_\ell[\text{Gal}_k]$ -module

$$H = \overline{\pi}^{\text{ab}, \ell} = \text{gr}_{-1}^C \overline{\pi}^\ell = \bigoplus_{i=1}^{2g} \mathbb{Z}_\ell x_i.$$

There is a natural short exact sequence of graded \mathbb{Z}_ℓ -Lie algebras

$$0 \rightarrow \mathfrak{r} \rightarrow L_H \rightarrow \mathfrak{p} \rightarrow 0.$$

Let $\rho \in \mathfrak{r}_2$ be the image of the relation $[x_1, x_2] \dots [x_{2g-1}, x_{2g}]$. We have the following special case of Labute's results on one-relator groups.

Theorem 201 (Labute [La67]).

- (1) *As a module under the universal enveloping algebra $U(\mathfrak{p})$ the module $\mathfrak{r}/[\mathfrak{r}, \mathfrak{r}]$ is free of rank 1 and generated by ρ in degree 2.*
- (2) *We have a short exact sequence*

$$0 \rightarrow \mathfrak{r}/[\mathfrak{r}, \mathfrak{r}] \rightarrow U(\mathfrak{p})^{2g} \rightarrow U(\mathfrak{p}) \rightarrow \mathbb{Z}_\ell \rightarrow 0$$

which is a free resolution of \mathbb{Z}_ℓ with trivial action by free $U(\mathfrak{p})$ -modules of finite rank. \square

By Theorem 201 and Poincaré–Birkhoff–Witt we have the following identifications of graded Gal_k -modules.

$$\mathfrak{r}/[\mathfrak{r}, \mathfrak{r}] \cong U(\mathfrak{p}) \otimes \mathbb{Z}_\ell(-1) \quad (14.10)$$

$$U(\mathfrak{r}) \cong \text{Ass}_{\mathfrak{r}/[\mathfrak{r}, \mathfrak{r}]} \quad (14.11)$$

$$U(\mathfrak{r}) \otimes U(\mathfrak{p}) \cong U(L_H) \cong \text{Ass}_H \quad (14.12)$$

Here Ass_V is the free associative algebra on the \mathbb{Z}_ℓ -module V , and we have made use of the fact, that \mathfrak{r} as a subalgebra of a free Lie algebra is again free on $\mathfrak{r}/[\mathfrak{r}, \mathfrak{r}]$ after [La67] Proposition 2.

The Poincaré series of \mathfrak{p} will be computed through the Poincaré series of $U(\mathfrak{p})$ which is as follows.

$$\begin{aligned} \frac{1}{1 - [H] \cdot T} &= [\text{Ass}_H] = [U(L_H)] = [U(\mathfrak{r})] \cdot [U(\mathfrak{p})] = [\text{Ass}_{\mathfrak{r}/[\mathfrak{r}, \mathfrak{r}]}] \cdot [U(\mathfrak{p})] \\ &= \frac{1}{1 - [\mathfrak{r}/[\mathfrak{r}, \mathfrak{r}]]} \cdot [U(\mathfrak{p})] = \frac{[U(\mathfrak{p})]}{1 - [U(\mathfrak{p})] \cdot [\mathbb{Z}_\ell(-1)] \cdot T^2} \end{aligned}$$

This solves for $[U(\mathfrak{p})]$ as

$$[U(\mathfrak{p})] = \frac{1}{1 - [H] \cdot T + [\mathbb{Z}_\ell(-1)] \cdot T^2} \quad (14.13)$$

Adams operations. The formula for $[\mathfrak{p}_n]$ which can be extracted from (14.13) requires Adams operations Ψ^d on the corresponding Grothendieck ring of $\mathbb{Z}_\ell[\text{Gal}_k]$ -modules which are free of finite rank as \mathbb{Z}_ℓ -modules, see [Be84, Se77]. In particular, for any V in the Grothendieck ring which we put in degree d we have

$$[\text{Sym}^\bullet(V)] = \exp \left(\sum_{m \geq 1} \Psi^m([V]) \frac{T^{dm}}{m} \right)$$

and

$$T \frac{d \log}{dT} [\text{Sym}^\bullet(V)] = \sum_{m \geq 1} \Psi^m(d[V]) \cdot T^{dm}$$

The Poincaré–Birkhoff–Witt Theorem shows

$$[U(\mathfrak{p})] = \prod_d [\text{Sym}^\bullet \mathfrak{p}_d]$$

and thus for the logarithmic derivative

$$\sum_{n \geq 1} \sum_{d|n} \Psi^{n/d}(d[\mathfrak{p}_d]) \cdot T^n = \frac{[H] \cdot T - 2[\mathbb{Z}_\ell(-1)] \cdot T^2}{1 - [H] \cdot T + [\mathbb{Z}_\ell(-1)] \cdot T^2} =: \sum_{n \geq 1} S_n T^n.$$

Working with formal roots of the denominator

$$1 - [H] \cdot T + [\mathbb{Z}_\ell(-1)] \cdot T^2 = (1 - \alpha T)(1 - \beta T)$$

we easily deduce a linear recursion formula for the $S_n = \alpha^n + \beta^n$ as follows:

$$S_{n+2} = [H] \cdot S_{n+1} - [\mathbb{Z}_\ell] \cdot S_n$$

and $S_1 = [H]$ while $S_0 = 2[\mathbf{1}]$ is twice the trivial 1-dimensional representation.

The Möbius inversion formula in this case reads

$$\sum_{d|n} \mu(d) \Psi^d(S_{n/d}) = \sum_{d|n} \mu(d) \Psi^d \left(\sum_{e| \frac{n}{d}} \Psi^{n/ed} (e \cdot [\mathfrak{p}_e]) \right) = \sum_{ed|n} \mu(d) \Psi^{n/e} (e \cdot [\mathfrak{p}_e]) \quad (14.14)$$

$$= \sum_{e|n} \Psi^{n/e} (e \cdot [\mathfrak{p}_e]) \sum_{d| \frac{n}{e}} \mu(d) = n[\mathfrak{p}_n]. \quad (14.15)$$

The analogue of [La70] Theorem (1), requires an explicit formula for the S_n which can be proven by induction via an informed Ansatz mimicking the formula [La70] Theorem (1). We obtain

$$S_m = \sum_{i=0}^{\lfloor m/2 \rfloor} (-1)^i \frac{m}{m-i} \binom{m-i}{i} [H]^{2m-i} \cdot [\mathbb{Z}_\ell(-i)]$$

and thus

$$[\mathfrak{p}_n] = \frac{1}{n} \sum_{d|n} \mu(n/d) \Psi^{n/d} \left(\sum_{i=0}^{\lfloor d/2 \rfloor} (-1)^i \frac{d}{d-i} \binom{d-i}{i} [H]^{2d-i} \cdot [\mathbb{Z}_\ell(-i)] \right). \quad (14.16)$$

Remark 202. (1) It is unclear to me whether this description of $[\mathfrak{p}_n]$ is of any use. For example, it seems impossible to decide by means of (14.16) whether $H^0(G, \mathfrak{p}) \neq 0$ if G is a finite cyclic group acting on \mathfrak{p} via graded Lie algebra automorphisms.

(2) A slight generalization of (14.16) and the use of Adams operations occurs in §2.3 and in particular formula (2.3.3) of [AN95].

14.4 Finite Dimensional Subalgebras and Invariants

The key property of \mathfrak{p}_K that forces $\dim_K H^0(G, \mathfrak{p}_K)$ to be infinite for a finite group G acting on \mathfrak{p}_K is the following bound on cohomological dimension.

Lemma 203. *Let K/\mathbb{Q}_ℓ be a field. The cohomological dimension of a sub-Lie algebra $\mathfrak{g} \subset \mathfrak{p}_K$ is at most 2.*

Proof. By the Poincaré–Birkhoff–Witt Theorem $U(\mathfrak{p}_K)$ is a free $U(\mathfrak{g})$ -module. Thus the resolution

$$0 \rightarrow \tau/[\tau, \tau] \otimes K \rightarrow U(\mathfrak{p}_K)^{2g} \rightarrow U(\mathfrak{p}_K) \rightarrow K \rightarrow 0$$

derived from Theorem 201 (2) shows that K with trivial \mathfrak{g} -action has projective dimension at most 2. Hence $H^q(\mathfrak{g}, M) = \text{Ext}_{U(\mathfrak{g})}^q(K, M)$ vanishes for $q \geq 3$. \square

Lemma 204. *Let $\mathfrak{g} = \bigoplus_{n \geq 1} \mathfrak{g}_n$ be a graded Lie algebra over the field K of dimension $4 \leq \dim_K \mathfrak{g} < \infty$. Then there is a graded abelian Lie algebra $\mathfrak{a} \subset \mathfrak{g}$ with $\dim_K \mathfrak{a} \geq 3$, i.e., we have $[\mathfrak{a}, \mathfrak{a}] = 0$.*

Proof. Let N be maximal with $\mathfrak{g}_N \neq 0$. It follows that the piece \mathfrak{g}_N is central in \mathfrak{g} and we are done if $\dim_K \mathfrak{g}_N \geq 2$. So we assume now $\dim_K \mathfrak{g}_N = 1$.

Let m be maximal with $m < N$ and $\mathfrak{g}_m \neq 0$. We set $\mathfrak{g}_{<m} = \bigoplus_{i < m} \mathfrak{g}_i$ and note that

$$[\cdot, \cdot] : \mathfrak{g}_{<m} \otimes \mathfrak{g}_m \rightarrow \mathfrak{g}$$

describes a bilinear pairing with values in \mathfrak{g}_N . If $\mathfrak{g}_{<m} \neq 0$, then because by assumption either $\dim_K \mathfrak{g}_{<m} \geq 2$ or $\dim_K \mathfrak{g}_m \geq 2$ we find homogeneous lines $\mathfrak{a}_{<m} \subseteq \mathfrak{g}_{<m}$, and $\mathfrak{a}_m \subseteq \mathfrak{g}_m$ with $[\mathfrak{a}_{<m}, \mathfrak{a}_m] = 0$. Hence

$$\mathfrak{a} = \mathfrak{a}_{<m} \oplus \mathfrak{a}_m \oplus \mathfrak{g}_N$$

is abelian of dimension 3.

It remains to discuss the case $\mathfrak{g}_{<m} = 0$. We then argue with the alternating pairing

$$[\cdot, \cdot] : \mathfrak{g}_m \otimes \mathfrak{g}_m \rightarrow \mathfrak{g}_N.$$

As by assumption $\dim_K \mathfrak{g}_m \geq 3$ we can find an isotropic subspace $\mathfrak{a}_m \subset \mathfrak{g}_m$ of dimension 2. Then $\mathfrak{a} = \mathfrak{a}_m \oplus \mathfrak{g}_N$ is abelian of dimension 3. This settles the claim in all cases. \square

Proposition 205. *Let $\mathfrak{g} \subset \mathfrak{p}_K$ be a graded sub-Lie algebra of finite K -dimension. Then $\dim_K \mathfrak{g} \leq 3$ and $\dim_K \mathfrak{g}_n \leq 2$ for all $n \geq 1$.*

Proof. We argue by contradiction. If $\dim_K \mathfrak{g} \geq 4$, then by Lemma 204 we find an abelian Lie algebra $\mathfrak{a} \subseteq \mathfrak{g} \subset \mathfrak{p}$ with $\dim_K \mathfrak{a} = 3$. But as $H^3(\mathfrak{a}, K) = K$ does not vanish, this contradicts Lemma 203.

The assertion $\dim_K \mathfrak{g}_n \leq 2$ follows because the only potential exception would be a graded sub-Lie algebra $\mathfrak{g} \subseteq \mathfrak{p}_K$ with $\mathfrak{g} = \mathfrak{g}_n$ of dimension 3 for some n . But such a \mathfrak{g} were abelian and thus leads to the same contradiction. \square

Corollary 206. *The Lie algebra \mathfrak{g} generated by a subspace $\mathfrak{g}_n \subseteq \mathfrak{p}_{K,n}$ with dimension $\dim_K \mathfrak{g}_n \geq 3$ is infinite dimensional and $\mathfrak{g}_{dn} \neq 0$ for all $d \geq 1$.* \square

The Lie algebra of invariants. Instead of Gal_k we now discuss the case of a finite abelian group G acting on \mathfrak{p} by graded Lie algebra automorphisms.

Proposition 207. *Let G be a finite abelian group of order invertible in K which acts on \mathfrak{p}_K by graded Lie algebra automorphisms. Then the G -invariants $H^0(G, \mathfrak{p}_K)$ form a graded sub-Lie algebra of infinite K -dimension.*

Proof. It is clear that $H^0(G, \mathfrak{p}_K)$ forms a graded sub-Lie algebra. Let N be the exponent of G . In order to determine the dimension of $H^0(G, \mathfrak{p}_K)$ we can assume that K contains all N th roots of unity.

Let V_χ be the χ -isotypical component of a G -representation V with respect to the character χ . If for some n and some character χ we have $\dim_K \mathfrak{p}_{n,\chi} \geq 3$, then by Corollary 206 the Lie algebra $\langle \mathfrak{p}_{n,\chi} \rangle \subseteq \mathfrak{p}_K$ generated by $\mathfrak{p}_{n,\chi}$ is infinite dimensional and nontrivial in every degree which is a multiple of n . But G acts on $\langle \mathfrak{p}_{n,\chi} \rangle_{dn}$ by χ^d so that for every $r \in \mathbb{N}$ we have

$$0 \neq \langle \mathfrak{p}_{n,\chi} \rangle_{rNn} \subset H^0(G, \mathfrak{p}_K).$$

That there is a character χ and $n \in \mathbb{N}$ with $\dim_K \mathfrak{p}_{n,\chi} \geq 3$ follows from the pigeon hole principle and the estimate for $\dim_K \mathfrak{p}_n$ in the following lemma. \square

Lemma 208. *We have the following estimate*

$$\left| \text{rk}_{\mathbb{Z}_\ell} \mathfrak{p}_n - \frac{\alpha^n}{n} \right| \leq \frac{\alpha}{n(\alpha - 1)} \alpha^{n/p} + 1$$

where p is the smallest prime factor of n and $\alpha = g + \sqrt{g^2 - 1} \approx 2g$. In particular, we have $\mathrm{rk}_{\mathbb{Z}_\ell} \mathfrak{p}_n \rightarrow \infty$ for $n \rightarrow \infty$.

Proof. We remind that we are working under the hypothesis that $g \geq 2$. We define $\beta = g - \sqrt{g^2 - 1}$ so that $(1 - \alpha T)(1 - \beta T) = 1 - 2gT + T^2$ and $\mathrm{rk}_{\mathbb{Z}_\ell} S_n = \alpha^n + \beta^n$. It follows from (14.15) that

$$\mathrm{rk}_{\mathbb{Z}_\ell} \mathfrak{p}_n = \frac{1}{n} \cdot \sum_{d|n} \mu(d) (\alpha^{n/d} + \beta^{n/d}).$$

By the triangle inequality and because $|\beta| < 1$ we have

$$\begin{aligned} \left| \mathrm{rk}_{\mathbb{Z}_\ell} \mathfrak{p}_n - \frac{\alpha^n}{n} \right| &\leq \frac{1}{n} \cdot \left(\sum_{d|n, d < n} \alpha^d + \sum_{d|n} \beta^d \right) \\ &< \frac{1}{n} \left(\sum_{i=1}^{n/p} \alpha^i + \sum_{i=1}^n 1 \right) < \frac{\alpha}{n(\alpha - 1)} \alpha^{n/p} + 1. \quad \square \end{aligned}$$

For an application of Proposition 207 see Theorem 226 in Sect. 15.3. This application was the main stimulus behind our discussion of the Lie algebra \mathfrak{p} in Sect. 14.3.

14.5 Nilpotent Sections in the Arithmetic Case

In the remaining sections of this chapter we examine the space of nilpotent sections for a smooth projective curve X/k over an algebraic number field k , or over a finite extension k/\mathbb{Q}_p . The behaviour is fundamentally different for the maximal geometrically pro- ℓ quotient for $\ell \neq p$ and for the maximal geometrically pro- p quotient.

The maximal pro- ℓ quotient with good reduction. Let k/\mathbb{Q}_p be a finite extension with ring of integers \mathfrak{o}_k and residue field \mathbb{F} . Let X/k be a smooth, projective curve with good reduction $\mathcal{X}/\mathrm{Spec}(\mathfrak{o}_k)$ and special fibre $Y = \mathcal{X}_{\mathbb{F}}$ over \mathbb{F} .

For $\ell \neq p$, every section of $\pi_1^{\mathrm{pro-}\ell}(X/k)$ is unramified over \mathfrak{o}_k by a pro- ℓ version of Proposition 91. For sections associated to rational points this was noted in [KiTa08] Theorem 0.1, see Sect. 8.5. Moreover, the specialisation map

$$\mathcal{S}_{\pi_1^{\mathrm{pro-}\ell}(X/k)} \rightarrow \mathcal{S}_{\pi_1^{\mathrm{pro-}\ell}(Y/\mathbb{F})}$$

is bijective. The pro- ℓ Kummer map sits in a diagram

$$\begin{array}{ccc}
X(k) & \xrightarrow{\kappa_\ell} & \mathcal{S}_{\pi_1^{\text{pro-}\ell}}(X/k) \\
\downarrow & & \parallel \\
Y(\mathbb{F}) & \xrightarrow{\kappa_\ell} & \mathcal{S}_{\pi_1^{\text{pro-}\ell}}(Y/\mathbb{F})
\end{array}$$

and thus factors over the finite set. On the other hand, by Theorem 226 below, we know that $\mathcal{S}_{\pi_1^{\text{pro-}\ell}}(Y/\mathbb{F})$ is uncountable. We conclude that the pro- ℓ section conjecture fails badly for proper smooth p -adic curves of good reduction with $\ell \neq p$.

Remark 209. It has been observed¹ by Tamagawa, see [Ho09] Remark 10 (i), that the pro- ℓ Kummer map

$$\kappa_\ell : Y(\mathbb{F}_q) \rightarrow \mathcal{S}_{\pi_1^{\text{pro-}\ell}}(Y/\mathbb{F}_q)$$

may fail to be injective for hyperbolic curves Y over a finite field \mathbb{F}_q .

14.6 Pro- p Counter-Examples After Hoshi

We are going to explain the counter-examples to a pro- p version of the section conjecture over algebraic number fields found by Hoshi, see [Ho10].

Theorem 210 (Hoshi, [Ho10] Theorem A). *Let $p \geq 3$ be a regular prime and let $k/\mathbb{Q}(\zeta_p)$ be a Galois extension unramified outside p with Galois group a finite p -group.*

Let $\beta : X \rightarrow \mathbb{P}_k^1$ be a finite map of connected proper smooth curves such that

- (i) *the genus of X is ≥ 2 ,*
- (ii) *$X(k)$ is nonempty,*
- (iii) *$\bar{\beta} : \bar{X} \rightarrow \mathbb{P}_{\bar{k}}^1$ is Galois of p -power degree and unramified outside $0, 1$, and ∞ ,*
- (iv) *and the hyperbolic curve $X \setminus \beta^{-1}(\{0, 1, \infty\})$ has good reduction outside p .*

Then there exists a finite extension k'/k unramified outside p with pro- p Galois hull, such that the pro- p Kummer map

$$\kappa_p : X(k') \rightarrow \mathcal{S}_{\pi_1^{\text{pro-}p}}(X/k)(k')$$

is not surjective, i.e., there are non-Diophantine pro- p sections after a finite pro- p extension unramified outside p . Moreover, if $v|p$ is a place of k' with completion k'_v , then also the local pro- p Kummer map

¹I thank Yuichiro Hoshi for bringing Tamagawa's observation to my attention.

$$\kappa_p : X(k'_v) \rightarrow \mathcal{S}_{\pi_1^{\text{pro-}p}(X/k)}(k'_v)$$

is not surjective.

Remark 211. Hoshi also constructs an explicit series of examples. Let $p \geq 11$ be a regular prime and let $k/Q(\zeta_p)$ be as in Theorem 210. Let $X_{\text{Fermat},p}/k$ be the Fermat curve

$$\{A^p + B^p = C^p\} \subset \mathbb{P}_k^2.$$

Then as a consequence of [Ho10] Theorem B, we obtain even that $\mathcal{S}_{\pi_1^{\text{pro-}p}(X_{\text{Fermat},p}/k)}$ is at least countable infinite.

We develop, complement and generalize the ideas of [Ho10] in the sequel.

Lemma 212. *Let k be an algebraic number field, and let $S \subseteq \text{Spec}(\mathfrak{o}_k[\frac{1}{p}])$ be a dense open arithmetic curve with a geometric point $\bar{s} \in S$.*

Let X/k be a smooth, projective geometrically connected curve of genus ≥ 2 with

- (i) *good reduction over S ,*
- (ii) *and Gal_k acts on $\pi_1^{\text{ab}}(\bar{X}, \bar{x}) \otimes \mathbb{F}_p = H_1(\bar{X}, \mathbb{F}_p)$ through a p -group.*

Then the pro- p outer Galois action

$$\rho_{X/k} : \text{Gal}_k \rightarrow \text{Out}(\pi_1^{\text{pro-}p}(\bar{X}))$$

factors over $\pi_1^{\text{pro-}p}(S, \bar{s})$.

Proof. That $\rho_{X/k}$ is unramified above S , i.e., factors over $\pi_1(S, \bar{s})$ follows from [Sx05] Propositions 2.6 and 2.7. By a profinite version of a theorem of Hall, see [Ha59] Theorem 12.2.2., the kernel of

$$\text{Out}(\pi_1^{\text{pro-}p}(\bar{X})) \rightarrow \text{Aut}(H_1(\bar{X}, \mathbb{F}_p))$$

is a pro- p group. Hence (ii) implies that the image of $\rho_{X/k}$ is a pro- p group. \square

In the situation of Lemma 212 the extension $\pi_1^{\text{pro-}p}(X/k)$ is the pullback of the extension

$$1 \rightarrow \pi_1^{\text{pro-}p}(\bar{X}) \rightarrow \text{Aut}(\pi_1^{\text{pro-}p}(\bar{X})) \times_{\text{Out}(\pi_1^{\text{pro-}p}(\bar{X}))} \pi_1^{\text{pro-}p}(S, \bar{s}) \rightarrow \pi_1^{\text{pro-}p}(S, \bar{s}) \rightarrow 1. \quad (14.17)$$

Let \mathcal{S} denote the $\pi_1^{\text{pro-}p}(\bar{X})$ -conjugacy classes of sections of (14.17). As in the context of base change, we obtain a natural map

$$\mathcal{S} \rightarrow \mathcal{S}_{\pi_1^{\text{pro-}p}(X/k)}.$$

Lemma 213. *With X/k as in Lemma 212, the map $\mathcal{S} \rightarrow \mathcal{S}_{\pi_1^{\text{pro-}p}(X/k)}$ is bijective.*

Proof. Since p is invertible in S , it follows that all ramification at places $v \in S$ is at most tame. We conclude by Proposition 91 that every pro- p section of $\pi_1^{\text{pro-}p}(X/k)$ is unramified above S . As (14.17) is a sequence of pro- p groups, every section further descends to \mathcal{S} . \square

Lemma 214. *Let p be an odd prime number, and let $S \subseteq \text{Spec}(\mathfrak{o}_k[\frac{1}{p}])$ be a dense open arithmetic curve with function field $k/\mathbb{Q}(\zeta_p)$ and geometric point $\bar{s} \in S$. Then $\pi_1^{\text{pro-}p}(S, \bar{s})$ is a free pro- p group if and only if the following conditions all hold:*

- (i) $S = \text{Spec}(\mathfrak{o}_k[\frac{1}{p}])$,
- (ii) p is inert in k/\mathbb{Q} ,
- (iii) $\text{Pic}(\mathfrak{o}_k) \otimes \mathbb{Z}_p$ is generated by the only prime $\mathfrak{p}|p$.

Proof. This is well known. We give a proof for the convenience of the reader. The group $\pi_1^{\text{pro-}p}(S, \bar{s})$ is free pro- p if and only if

$$H^2(\pi_1^{\text{pro-}p}(S, \bar{s}), \mathbb{Z}/p\mathbb{Z}) = H^2(S, \mathbb{Z}/p\mathbb{Z}) \cong H^2(S, \mu_p)$$

vanishes. From the Kummer sequence we obtain an exact sequence

$$0 \rightarrow \text{Pic}(S) \otimes \mathbb{F}_p \rightarrow H^2(S, \mu_p) \rightarrow \text{Br}(S)[p] \rightarrow 0.$$

As $\text{Br}(S)[p]$ is isomorphic to the elements in $\bigoplus_{v \notin S} \mathbb{Q}/\mathbb{Z}$ of sum 0 where v ranges over all finite places of k outside S , the Brauer term vanishes if and only if (i) and (ii) hold. Clearly then (iii) is equivalent to the vanishing of the Picard term. \square

Theorem 215. *Let p be an odd prime number, and let $k/\mathbb{Q}(\zeta_p)$ be an algebraic number field, such that*

- (i) p is inert in k/\mathbb{Q} ,
- (ii) $\text{Pic}(\mathfrak{o}_k) \otimes \mathbb{Z}_p$ is generated by the only prime $\mathfrak{p}|p$.

Let X/k be a smooth, projective geometrically connected curve of genus ≥ 2 with

- (iii) *good reduction over $S = \text{Spec}(\mathfrak{o}_k[\frac{1}{p}])$,*
- (iv) *Gal_k acts on $\pi_1^{\text{ab}}(\bar{X}, \bar{x}) \otimes \mathbb{F}_p = H_1(\bar{X}, \mathbb{F}_p)$ through a p -group,*
- (v) *and positive Mordell-Weil rank, i.e., $\text{Pic}_X^0(k)$ is infinite.*

Then the set $\mathcal{S}_{\pi_1^{\text{pro-}p}(X/k)}$ is uncountably infinite and the pro- p Kummer map

$$\kappa_p : X(k) \rightarrow \mathcal{S}_{\pi_1^{\text{pro-}p}(X/k)}$$

is not surjective, i.e., there are non-Diophantine pro- p sections.

Proof. The extension (14.17) can be pushed to the geometrically maximal abelian quotient and gives an extension

$$1 \rightarrow \pi_1^{\text{ab, pro-}p}(\bar{X}) \rightarrow \frac{\text{Aut}(\pi_1^{\text{pro-}p}(\bar{X})) \times_{\text{Out}(\pi_1^{\text{pro-}p}(\bar{X}))} \pi_1^{\text{pro-}p}(S, \bar{s})}{\ker(\pi_1^{\text{pro-}p}(\bar{X}) \twoheadrightarrow \pi_1^{\text{ab, pro-}p}(\bar{X}))} \rightarrow \pi_1^{\text{pro-}p}(S, \bar{s}) \rightarrow 1 \quad (14.18)$$

the $\pi_1^{\text{ab,pro-}p}(\overline{X})$ -conjugacy classes of which we denote by \mathcal{S}^{ab} . The analogue of Lemma 213 holds and yields a natural bijective map

$$\mathcal{S}^{\text{ab}} \rightarrow \mathcal{S}_{\pi_1^{\text{ab,pro-}p}(X/k)} = \mathcal{S}_{\pi_1^{\text{pro-}p}(\text{Pic}_X^1/k)}.$$

The Albanese torsor map $\alpha : X \hookrightarrow \text{Pic}_X^1$ provides a commutative diagram

$$\begin{array}{ccccc} X(k) & \xrightarrow{\kappa_{X,p}} & \mathcal{S}_{\pi_1^{\text{pro-}p}(X/k)} & \xleftarrow{\sim} & \mathcal{S} \\ \downarrow \alpha & & \downarrow \alpha_* & & \downarrow \alpha_* \\ \text{Pic}_X^1(k) & \longrightarrow & \mathcal{S}_{\pi_1^{\text{pro-}p}(\text{Pic}_X^1/k)} & \xleftarrow{\sim} & \mathcal{S}^{\text{ab}} \end{array} \quad (14.19)$$

With (i) and (ii) we deduce from Lemma 214 that $\pi_1^{\text{pro-}p}(S, \bar{s})$ is a free pro- p group, hence the map

$$\alpha_* : \mathcal{S} \twoheadrightarrow \mathcal{S}^{\text{ab}}$$

is surjective and a fortiori, by Lemma 213 and its abelianized analogue, the map

$$\alpha_* : \mathcal{S}_{\pi_1^{\text{pro-}p}(X/k)} \twoheadrightarrow \mathcal{S}_{\pi_1^{\text{pro-}p}(\text{Pic}_X^1/k)}$$

is surjective. Moreover, the spaces of sections in (14.19) are in fact non-empty. The cohomological description in the abelian case now shows a bijection

$$\mathcal{S}_{\pi_1^{\text{pro-}p}(\text{Pic}_X^1/k)} \cong H^1(k, \pi_1^{\text{ab,pro-}p}(\overline{X})) = H^1(k, T_p(\text{Pic}_X^0))$$

which via the Kummer sequence contains $\text{Pic}_X^0(k) \otimes \mathbb{Z}_p$ and thus by assumption (v) is uncountably infinite. Consequently, also the space of pro- p sections $\mathcal{S}_{\pi_1^{\text{pro-}p}(X/k)}$ is uncountably infinite, which shows in particular the presence of non-Diophantine pro- p sections. \square

In [Ho10] Hoshi finds an ingenious anabelian way to ensure property (iv) of Theorem 215 that we are going to explain now.

Proposition 216 (Hoshi, [Ho10] Lemma 2.1). *Let $\beta : X \rightarrow Y$ be a finite map of geometrically connected proper smooth curves over an algebraic number field k such that*

- (i) *there is a hyperbolic dense open $V \subset Y$ such that $\beta|_U : U = \beta^{-1}(V) \rightarrow V$ is finite étale,*
- (ii) *Gal_k acts on $H_1(\overline{V}, \mathbb{F}_p)$ through a p -group,*
- (iii) *and, geometrically, the map $\overline{\beta} : \overline{U} \rightarrow \overline{V}$ is Galois of p -power degree.*

Then Gal_k acts on $H_1(\overline{X}, \mathbb{F}_p)$ via a finite p -group.

Proof. Since $H_1(\overline{X}, \mathbb{F}_p)$ is a quotient module of $H_1(\overline{U}, \mathbb{F}_p)$ it suffices to show that the action of Gal_k on the latter is via a p -group. As above, this is equivalent to the outer pro- p Galois action

$$\rho_{U/k} : \text{Gal}_k \rightarrow \text{Out}(\pi_1^{\text{pro-}p}(\overline{U}))$$

factoring over a pro- p group.

By (i) and (iii) there is a finite p -group G and the following diagram with exact rows and column.

$$\begin{array}{ccccccc}
 & & 1 & & & & \\
 & & \uparrow & & & & \\
 & & G & & & & \\
 & & \uparrow & & & & \\
 1 & \longrightarrow & \pi_1^{\text{pro-}p}(\overline{V}) & \longrightarrow & \pi_1^{(\text{pro-}p)}(V) & \longrightarrow & \text{Gal}_k \longrightarrow 1 \\
 & & \uparrow & & \uparrow \beta_* & & \parallel \\
 1 & \longrightarrow & \pi_1^{\text{pro-}p}(\overline{U}) & \longrightarrow & \pi_1^{(\text{pro-}p)}(U) & \longrightarrow & \text{Gal}_k \longrightarrow 1 \\
 & & \uparrow & & & & \\
 & & 1 & & & &
 \end{array}$$

(14.20)

Let Z_U (resp. Z_V) be the centraliser of $\pi_1^{\text{pro-}p}(\overline{U})$ in $\pi_1^{(\text{pro-}p)}(U)$ (resp. of $\pi_1^{\text{pro-}p}(\overline{V})$ in $\pi_1^{(\text{pro-}p)}(V)$). Since U and V are hyperbolic, $\pi_1^{\text{pro-}p}(\overline{U})$ and $\pi_1^{\text{pro-}p}(\overline{V})$ have trivial center, Z_U and Z_V inject as normal closed subgroups in Gal_k , and we have

$$\text{im}(\rho_{U/k}) = \text{Gal}_k / Z_U \quad \text{and} \quad \text{im}(\rho_{V/k}) = \text{Gal}_k / Z_V.$$

To the exact column of (14.20) belongs an outer action

$$\rho : G \rightarrow \text{Out}(\pi_1^{\text{pro-}p}(\overline{U}))$$

and a natural isomorphism

$$\pi_1^{\text{pro-}p}(\overline{V}) = \text{Aut}(\pi_1^{\text{pro-}p}(\overline{U})) \times_{\text{Out}(\pi_1^{\text{pro-}p}(\overline{U}), \rho)} G.$$

It follows that an automorphism of $\pi_1^{\text{pro-}p}(\overline{U})$ extends in at most one way to an automorphism of $\pi_1^{\text{pro-}p}(\overline{V})$, see [Sx02] Lemma 4.2.9 for another case of this argument. Consequently, we have an inclusion $Z_U \subseteq Z_V$ and an exact sequence

$$1 \rightarrow Z_V/Z_U \rightarrow \text{im}(\rho_{U/k}) \rightarrow \text{im}(\rho_{V/k}) \rightarrow 1.$$

By assumption (ii) and the profinite version of [Ha59] Theorem 12.2.2, the image $\text{im}(\rho_{V/k})$ is pro- p , so that it suffices to analyse Z_V/Z_U . We define a map

$$\psi : Z_V \rightarrow G$$

which sends $a \in Z_V$ of the form $a = \gamma u$ with $\gamma \in \pi_1^{\text{pro-}p}(\overline{V})$ and $u \in \pi_1^{(\text{pro-}p)}(U)$ to

$$\psi(a) = \gamma \cdot \pi_1^{\text{pro-}p}(\overline{U}).$$

The map ψ is well defined, as with another decomposition $a = \gamma' u'$ we have

$$\gamma^{-1} \gamma' = u(u')^{-1} \in \pi_1^{\text{pro-}p}(\overline{V}) \cap \pi_1^{(\text{pro-}p)}(U) = \pi_1^{\text{pro-}p}(\overline{U})$$

and so

$$\gamma \cdot \pi_1^{\text{pro-}p}(\overline{U}) = \gamma' \cdot \pi_1^{\text{pro-}p}(\overline{U}).$$

If $b \in Z_V$ is another element with decomposition $b = \delta v$ with $\delta \in \pi_1^{\text{pro-}p}(\overline{V})$ and $v \in \pi_1^{(\text{pro-}p)}(U)$, then

$$ab = a(\delta v) = \delta av = \delta(\gamma u)v = (\delta\gamma)(uv),$$

so that

$$\psi(ab) = \psi(b)\psi(a).$$

Hence, the map ψ is a homomorphism $Z_V \rightarrow G^{\text{opp}}$ to G with the opposite group law, which is still a p -group by assumption (iii). Since

$$\ker(\psi) = Z_V \cap (\pi_1^{(\text{pro-}p)}(U)) = Z_U,$$

the quotient Z_V/Z_U is a finite p -group. □

Remark 217. (1) Theorem 210 now is deduced as follows. The assumptions on k implies that

$$\pi_1^{\text{pro-}p}(\text{Spec}(\mathfrak{o}_k[\frac{1}{p}])) \subseteq \pi_1^{\text{pro-}p}(\text{Spec}(\mathbb{Z}[\zeta_p, \frac{1}{p}]))$$

is an open subgroup, which is a free pro- p group due to $p \geq 3$ being a regular prime, see Lemma 214. This guarantees properties (i) and (ii) of Theorem 215, while property (iii) is also assumed from the start in Theorem 210. In order to assure (iv) we apply Proposition 216 with

$$V = \mathbb{P}_k^1 - \{0, 1, \infty\} \subset Y = \mathbb{P}_k^1,$$

and the map $\beta : X \rightarrow \mathbb{P}_k^1$ of Theorem 210. This allows to conclude as in the proof of Theorem 215 that for the Albanese torsor map $\alpha : X \hookrightarrow \text{Pic}_X^1$ the induced abelianization map on sections

$$\alpha_* : \mathcal{S}_{\pi_1^{\text{pro-}p}(X/k)} \twoheadrightarrow \mathcal{S}_{\pi_1^{\text{pro-}p}(\text{Pic}_X^1/k)}$$

is surjective with both sets non-empty. Here Hoshi resorts to another argument to ensure that there are non-Diophantine sections in case property (v) of Theorem 215, the positive Mordell–Weil rank, fails. It is this step that requires to replace k by a finite pro- p extension k'/k which is unramified outside p . For details on the latter argument see [Ho10] §4.

(2) For a regular prime $p \geq 11$ and $k = \mathbb{Q}(\zeta_p)$, the p th Fermat curve

$$X_{\text{Fermat},p} = \{A^p + B^p = C^p\} \subset \mathbb{P}_k^2$$

actually satisfies all assumptions of Theorem 215, with (v) following by [GrRo78] and with Belyi map given by

$$(A, B, C) \mapsto (A^p, B^p, C^p) \in \{(u, v, w) ; u + v = w\} \cong \mathbb{P}_k^1.$$

Hence we have also explained part of [Ho10] Theorem B.

(3) We cannot help but think that the above counter-examples to the pro- p version of the section conjecture come to life due to a coincidence of a number of *accidents*. For example, the freeness of the pro- p fundamental group of the arithmetic base curve $S \subset \text{Spec}(\mathfrak{o}_k[\frac{1}{p}])$ forces S to be almost all of $\text{Spec}(\mathfrak{o}_k)$. On the other hand, having good reduction almost everywhere is a rare commodity among smooth projective curves. We could artificially force the Galois action on $H_1(\bar{X}, \mathbb{F}_p)$ to be unipotent, or even trivial, but only at the expense of enlarging k in an uncontrolled manner with respect to the pro- p freeness condition.

Nevertheless, the hope to prove the section conjecture immediately via a pro- p approach is destroyed. In light of the above described accidents, we might ask, whether still pro- p methods can prove the section conjecture, if we do not apply them directly to a given curve X/k but to an auxiliary finite, maybe even cyclic, étale cover $X' \rightarrow X$ such that we leave the realm of the accidental failure of the pro- p section conjecture.

14.7 Variations on Pro- p Counter-Examples After Hoshi

We aim at a generalization of Hoshi's approach to counter-examples for the pro- p section conjecture which makes use of more precise knowledge of pro- p arithmetic fundamental groups.

Theorem 218. *Let p be a prime number, and let k be an algebraic number field. Let B be a dense open in $\text{Spec}(\mathfrak{o}_k)$ with complement S , such that p is invertible on B . We moreover assume that there is a subset $S_0 \subseteq S$ of the places of k above p with*

- (i) $\sum_{v \in S_0} \frac{1 - \#\mu_p(k_v)}{1 - p} = \frac{1 - \#\mu_p(k)}{1 - p}$,
- (ii) *and the map $H^1(B, \mu_p) \rightarrow \prod_{v \in S_0} H^1(k_v, \mu_p)$ is injective.*

Let X/k be a smooth, projective geometrically connected curve of genus ≥ 2 with

- (iii) *good reduction over B ,*
- (iv) *and Gal_k acts on $\pi_1^{\text{ab}}(\bar{X}, \bar{x}) \otimes \mathbb{F}_p = H_1(\bar{X}, \mathbb{F}_p)$ through a p -group.*

Let us furthermore assume that

- (v) $X(k_v) \neq \emptyset$ for all $v \in S \setminus S_0$,
- (vi) *and S_0 misses at least one place $\mathfrak{p} | p$ of k or the auxiliary set T below in the proof is bigger than S .*

Then the set $\mathcal{S}_{\pi_1^{\text{pro-}p}(X/k)}$ is uncountably infinite and the pro- p Kummer map

$$\kappa_p : X(k) \rightarrow \mathcal{S}_{\pi_1^{\text{pro-}p}(X/k)}$$

is not surjective, i.e., there are non-Diophantine pro- p sections.

Proof. According to [NSW08] Theorem 10.9.1, properties (i) and (ii) are the precise criterion to put us in the *degenerate case* as defined in [NSW08] Definition 10.9.3, which means that there is a finite set of places T containing S and a natural isomorphism

$$\bigstar_{v \in S \setminus S_0} \text{Gal}_{k_v}^{\text{pro-}p} \bigstar_{T \setminus S} \mathbb{Z}_p \xrightarrow{\sim} \pi_1^{\text{pro-}p}(B), \quad (14.21)$$

which sends $\text{Gal}_{k_v}^{\text{pro-}p}$ (resp. $1 \in \mathbb{Z}_p$) for $v \in S \setminus S_0$ (resp. for $v \in T \setminus S$) to the decomposition group in $\pi_1^{\text{pro-}p}(B)$ (resp. to the Frobenius) of a place above v .

Properties (iii) and (iv) imply by Lemma 212 that the outer pro- p Galois representation

$$\rho_{X/k} : \text{Gal}_k \rightarrow \text{Out}(\pi_1^{\text{pro-}p}(\bar{X}))$$

factors through $\pi_1^{\text{pro-}p}(B)$. We denote again by \mathcal{S} the $\pi_1^{\text{pro-}p}(\bar{X})$ -conjugacy classes of sections of the extension

$$1 \rightarrow \pi_1^{\text{pro-}p}(\bar{X}) \rightarrow \text{Aut}(\pi_1^{\text{pro-}p}(\bar{X})) \times_{\text{Out}(\pi_1^{\text{pro-}p}(\bar{X}))} \pi_1^{\text{pro-}p}(B) \rightarrow \pi_1^{\text{pro-}p}(B) \rightarrow 1 \quad (14.22)$$

which again pulls back to the extension $\pi_1^{\text{pro-}p}(X/k)$ to yield a base change map

$$\mathcal{S} \rightarrow \mathcal{S}_{\pi_1^{\text{pro-}p}(X/k)}$$

whose bijectivity is assured by property (iii) and Lemma 213.

The same conclusion holds for the following local analogues. First, for a place v of k , the local outer pro- p Galois representation of $X \otimes k_v/k_v$ still has a pro- p group as its image, so that the extension $\pi_1^{\text{pro-}p}(X \otimes k_v/k_v)$ is the pullback of the extension

$$1 \rightarrow \pi_1^{\text{pro-}p}(\overline{X}) \rightarrow \text{Aut}(\pi_1^{\text{pro-}p}(\overline{X})) \times_{\text{Out}(\pi_1^{\text{pro-}p}(\overline{X}))} \text{Gal}_{k_v}^{\text{pro-}p} \rightarrow \text{Gal}_{k_v}^{\text{pro-}p} \rightarrow 1. \quad (14.23)$$

Let \mathcal{S}_v denote the $\pi_1^{\text{pro-}p}(\overline{X})$ -conjugacy classes of sections of (14.23). Then there is again a base change map

$$\mathcal{S}_v \rightarrow \mathcal{S}_{\pi_1^{\text{pro-}p}(X/k)}(k_v)$$

which is clearly bijective. Secondly, for a place $v \in B$ where X has good reduction and $v \nmid p$, the local outer pro- p Galois representation is even unramified and thus factors over

$$\text{Gal}_{k_v}^{\text{pro-}p, \text{nr}} = \mathbb{Z}_p.$$

The extension $\pi_1^{\text{pro-}p}(X \otimes k_v/k_v)$ then is even a pullback of the extension

$$1 \rightarrow \pi_1^{\text{pro-}p}(\overline{X}) \rightarrow \text{Aut}(\pi_1^{\text{pro-}p}(\overline{X})) \times_{\text{Out}(\pi_1^{\text{pro-}p}(\overline{X}))} \mathbb{Z}_p \rightarrow \mathbb{Z}_p \rightarrow 1 \quad (14.24)$$

describing the situation for the special fibre of the good reduction at v . Let $\mathcal{S}_v^{\text{nr}}$ denote the $\pi_1^{\text{pro-}p}(\overline{X})$ -conjugacy classes of sections of (14.24). There is again a base change map

$$\mathcal{S}_v^{\text{nr}} \rightarrow \mathcal{S}_{\pi_1^{\text{pro-}p}(X/k)}(k_v)$$

which is bijective by Proposition 91. We obtain the following commutative diagram

$$\begin{array}{ccccc} X(k) & \xhookrightarrow{\kappa_{X,p}} & \mathcal{S}_{\pi_1^{\text{pro-}p}(X/k)} & \xleftarrow{\sim} & \mathcal{S} \\ \downarrow & & \downarrow & & \downarrow \\ \prod_{v \in T \setminus S_0} X(k_v) & \xrightarrow{\kappa_{X \otimes k_v, p}} & \prod_{v \in T \setminus S_0} \mathcal{S}_{\pi_1^{\text{pro-}p}(X/k)}(k_v) & \xleftarrow{\sim} & \prod_{v \in S \setminus S_0} \mathcal{S}_v \times \prod_{v \in T \setminus S} \mathcal{S}_v^{\text{nr}} \end{array}$$

where by the degenerate structure (14.21) of $\pi_1^{\text{pro-}p}(B)$ the localisation map

$$\mathcal{S} \twoheadrightarrow \prod_{v \in S \setminus S_0} \mathcal{S}_v \times \prod_{v \in T \setminus S} \mathcal{S}_v^{\text{nr}}$$

is surjective. Property (v) prevents $\prod_{v \in S \setminus S_0} \mathcal{S}_v$ from being empty, while

$$\prod_{v \in T \setminus S} \mathcal{S}_v^{\text{nr}}$$

is always nonempty. If there is a place $\mathfrak{p}|p$ in $S \setminus S_0$, then by Theorem 76 the map

$$\kappa_p : X(k_{\mathfrak{p}}) \hookrightarrow \mathcal{S}_{\pi_1^{\text{pro-}p}(X/k)}(k_{\mathfrak{p}})$$

is injective, and a consequently $\mathcal{S}_{\mathfrak{p}}$ is uncountable. If on the other hand we have $v \in T \setminus S$, then $\mathcal{S}_v^{\text{nr}}$ is uncountable by Theorem 226. By property (vi) at least one of these places exists and in any case \mathcal{S} is uncountable. We deduce that again $\mathcal{S}_{\pi_1^{\text{pro-}p}(X/k)}$ is uncountable, so that there must be in particular non-Diophantine pro- p sections for X/k . \square

Remark 219. (1) If k in Theorem 218 contains ζ_p , then by [NSW08] Theorem 10.9.1 we have necessarily $S_0 = \{\mathfrak{p}\}$ with $\mathfrak{p}|p$.

(2) In Theorem 210, the conditions imposed on the number field k imply by Lemma 214 that there is a unique place \mathfrak{p} of k with $\mathfrak{p}|p$ and that for

$$B = \text{Spec}(\mathfrak{o}_k[\frac{1}{p}])$$

property (i) and (ii) of Theorem 218 holds with respect to $S_0 = \{\mathfrak{p}\} = S$. The auxiliary set T contains S properly. Hence also property (vi) holds. Theorem 210 is in fact a special case of Theorem 218.

Nevertheless, although Theorem 218 provides more flexibility in the construction of counter-examples with regard to the number field and the locus of good reduction, however, I see no other method than Hoshi's to establish the key property (iv), see Proposition 216.

Example 220. Here is a concrete example for the failure of the pro-3 section conjecture that lies beyond Theorem 210. In the notation of Theorem 218, we set $k = \mathbb{Q}(\zeta_3)$ and

$$B = \text{Spec}(\mathbb{Z}[\zeta_3, \frac{1}{6}])$$

with $S_0 = \{3\}$ and $S = \{2, 3, \infty\}$. Then (i) holds and (ii) is equivalent to the restriction

$$\text{res}_3 : \mathcal{O}^*(B)/(\mathcal{O}^*(B))^3 \rightarrow \mathbb{Q}_3(\zeta_3)^*/(\mathbb{Q}_3(\zeta_3)^*)^3$$

being injective. Since 2 is inert in $\mathbb{Q}(\zeta_3)/\mathbb{Q}$ and

$$3 = -\zeta_3^2 \cdot (1 - \zeta_3)^2$$

we find that the classes of $\zeta_3, 2, 3$ form a basis of the left hand side. If we look at the filtration of the right hand side given by the subspaces

$$\ker(N : \mathbb{Z}_3[\zeta_3]^*/(\mathbb{Z}_3[\zeta_3]^*)^3 \rightarrow \mathbb{Z}_3^*/(\mathbb{Z}_3^*)^3) \subset \mathbb{Z}_3[\zeta_3]^*/(\mathbb{Z}_3[\zeta_3]^*)^3$$

then res_3 becomes upper triangular with $\zeta_3, 2, 3$ being nontrivial in the respective filtration quotients. It follows as in the proof of Theorem 218 from [NSW08]

Theorem 10.9.1 that we are in the degenerate case. Moreover we have $\#(T \setminus S) = 1$, and formula (14.21) in this particular case reads

$$(\mathbb{Z}_3(1) \rtimes_4 \mathbb{Z}_3) * \mathbb{Z}_3 = \mathrm{Gal}_{\mathbb{Q}_2(\zeta_3)}^{\mathrm{pro-3}} * \mathbb{Z}_3 \xrightarrow{\sim} \pi_1^{\mathrm{pro-3}}(\mathrm{Spec}(\mathbb{Z}[\zeta_3, \frac{1}{6}])).$$

Here $\mathbb{Z}_3(1) \rtimes_4 \mathbb{Z}_3$ is the semidirect product, where the generator of \mathbb{Z}_3 acts via the 3-adic automorphism of multiplication by $4 = 1 + 3$ on $\mathbb{Z}_3(1) = \mathbb{Z}_3$.

The example is now provided by the smooth projective curve $C = C_0 \times_{\mathbb{Q}} \mathbb{Q}(\zeta_3)$ of genus 3 given by

$$C_0 = \{Y^3Z = X(X - Z)(X - 3Z)(X - 9Z)\} \subset \mathbb{P}_{\mathbb{Q}}^2.$$

Indeed, the curve C_0 has a \mathbb{Q} -rational point, namely $[0 : 1 : 0]$, and good reduction outside $2 \cdot 3$ as can be seen easily from the jacobian criterion applied to the integral curve $\mathcal{C}_0 \subset \mathbb{P}_{\mathbb{Z}}^2$ given by the same equation. The example at this point relies on the *accident* that the only primes which divide differences of the numbers 0, 1, 3, 9 are 2 and 3. Moreover, the curve C_0 is a μ_3 torsor over $\mathbb{P}_{\mathbb{Q}}^1$ described by taking a cube root of

$$T(T - 1)(T - 3)(T - 9)$$

hence finite étale over $U = \mathbb{P}_{\mathbb{Q}}^1 - \{0, 1, 3, 9\}$ with geometric monodromy a 3-group. Because the ramification points are rational, we find

$$H_1(\overline{U}, \mathbb{F}_3) = \mathbb{Z}/3\mathbb{Z}(1) \oplus \mathbb{Z}/3\mathbb{Z}(1) \oplus \mathbb{Z}/3\mathbb{Z}(1).$$

In particular, Gal_k acts through a 3-group and property (iv) of Theorem 218 holds. We may conclude that the pro-3 Kummer map

$$\kappa_3 : C(\mathbb{Q}(\zeta_3)) \rightarrow \mathcal{S}_{\pi_1^{\mathrm{pro-3}}(C/\mathbb{Q}(\zeta_3))}$$

is injective with finite image in an uncountable space of pro-3 sections.

We end this chapter by posing a question which might revitalize work on the pro- p analogue of the section conjecture.

Question 221. Does every smooth projective geometrically connected curve X/k over an algebraic number field k admit a finite étale cover $h : X' \rightarrow X$ with X'/k geometrically connected, such that the pro- p Kummer map

$$\kappa_p : X'(k) \rightarrow \mathcal{S}_{\pi_1^{\mathrm{pro-p}}(X'/k)}$$

is bijective for X'/k ?

<http://www.springer.com/978-3-642-30673-0>

Rational Points and Arithmetic of Fundamental Groups
Evidence for the Section Conjecture

Stix, J.

2013, XX, 249 p., Softcover

ISBN: 978-3-642-30673-0