On the birational section conjecture with local conditions

JAKOB STIX

Abstract — A birationally liftable Galois section s of a hyperbolic curve X/k over a number field k yields an adelic point $\underline{x}(s) \in \overline{X}(\mathbb{A}_k)_\bullet$ of the smooth completion $X \subseteq \overline{X}$. We show that $\underline{x}(s)$ is X-integral outside a set of places of Dirichlet density 0, or s is cuspidal. The proof relies on $\mathrm{GL}_2(\mathbb{F}_\ell)$-quotients of $\pi_1(U)$ for some open $U \subset X$.

If k is totally real or imaginary quadratic, we prove that all birationally adelic, non-cuspidal Galois sections come from rational points as predicted by the section conjecture of anabelian geometry. As an aside we also obtain a strong approximation result for rational points on hyperbolic curves over $\mathbb{Q}$ or imaginary quadratic fields.

1. Introduction

The section conjecture [Gr83] predicts for a smooth hyperbolic curve X/k over a number field k that every Galois section of the projection $\pi_1(X) \to \pi_1(\mathrm{Spec}(k))$ arises by functoriality from a rational point (possibly of the smooth completion), see [Sti13] for a survey.

For diophantine applications it suffices to describe the set of rational points in terms of sections with additional group theoretic conditions. We impose two kinds of extra conditions in this note:

(1) birational lifting: the section lifts to a section of $\pi_1(\mathrm{Spec}(K)) \to \pi_1(\mathrm{Spec}(k))$ where K is the function field of X, see Section §2.1.

(2) adelic: the section locally belongs to an adelic point of X, see Section §2.2.

Both conditions imply by Koenigsmann [Ko05] that the section is Selmer, i.e., it comes locally from a point or is cuspidal. While (1) allows us to work birationally on the curve and is entirely in terms of groups, condition (2) imposes some kind of discreteness that we rather would like to deduce than to invest in the theory. Nevertheless, the study of (2) is justified by the application to strong approximation, see Theorem C below.

1.1. Results.

We obtain in Corollary 7 the following result.

Theorem A. *Let k be a totally real or an imaginary quadratic number field, and X/k be a hyperbolic curve. Then the set of $\pi_1(X_{\bar{k}})$-conjugacy classes of birationally adelic non-cuspidal sections of $\pi_1(X) \to \pi_1(\mathrm{Spec}(k))$ is in natural bijection with the set of k-rational points of X.*

While Theorem A shows that assuming *birationally adelic* is almost enough (depends on k) to prove the birational section conjecture, Theorem B shows that this hypothesis is almost true.

Theorem B. *Let $s : \mathrm{Gal}_k \to \pi_1(X)$ be a birationally liftable section of a hyperbolic curve X/k with smooth completion $\overline{X}$ over a number field k.*

Then the associated adelic point $(x_v(s)) \in \overline{X}(\mathbb{A}_k)_\bullet$ has

(1) either $x_v(s) \in X(\mathfrak{o}_v)$ is integral for a set of places v of Dirichlet density 1,

(2) or the section s is cuspidal.

The proof of Theorem B, see Corollary 15 and Theorem 20, uses the geometric monodromy of the Legendre family of elliptic curves. This leads to a new GL_2-type description of cuspidal sections in contrast to the characterization via weights due to Nakamura [Na90]. The use of the Legendre family has the flavour of the known reduction of the section conjecture for birationally liftable sections to the special case of $X = \mathbb{P}^1 - \{0, 1, \infty\}$ as observed for example in [EsHa08]

Date: February 27, 2014.

Key words and phrases. section conjecture, anabelian geometry, descent obstruction.

Proposition 7.9. But in fact, we have to exploit many rational maps $X \dashrightarrow \mathbb{P}^1 - \{0,1,\infty\}$ and so the line of thought is different.

1.2. **Outline.** Section §2 contains various notions of sections with (local) conditions and describes these notions for 1-dimensional tori. In Section §3 we make use of Stoll's finite support result in descent theory. Here we prove Theorem A and obtain the following interesting result of strong approximation, see Corollary 6.

Theorem C. *Let X/k be a hyperbolic curve over either $k = \mathbb{Q}$ or k an imaginary quadratic number field such that $\mathcal{O}^*(X) \neq k^*$. Then the natural map*

$$X(k) \xrightarrow{\sim} X(\mathbb{A}_k)_\bullet^{\mathrm{f-desc}}$$

is a bijection from rational points to adelic points that survive any finite descent obstruction.

In Section §4 we start to draw conclusions for Selmer sections from the presence of non-constant families of elliptic curves. We prove a density theorem, Theorem 10, based on the asymptotic of group theory in $\mathrm{GL}_2(\mathbb{F}_\ell)$ for $\ell \to \infty$. The theorem roughly says that the adelic point associated to a section behaves either, up to a set of density 0, like a rational point, or like a cuspidal section. This works over any number field. The precise statement concerning cuspidal sections is obtained in Section §5 by means of the geometric monodromy of the Legendre family.

Acknowledgements.

I would like to express my gratitude towards Olivier Wittenberg and Hélène Esnault for listening to the argument at an early stage and for comments on an earlier version of this manuscript. I am grateful to Leila Schneps for providing the explicit form of monodromy for the Legendre family (actually in 2005 — a long time ago).

1.3. **Notation and terminology.** A **hyperbolic curve** is a smooth relative curve $X \to S$ endowed with a smooth projective compactification $\overline{X} \to S$ such that the following holds. The geometric fibres $\overline{X}_{\bar{s}}$ are connected of constant genus, $Y = \overline{X} \setminus X \to S$ is a finite étale relative divisor, and the fibrewise ℓ-adic Euler characteristic $\chi(X_{\bar{s}}, \mathbb{Q}_\ell)$ is constant and negative ($\ell \in \mathcal{O}_S^*$).

For a number field k we denote its ring of integers by $\mathfrak{o}_k$, the completion at a place v of k is k_v with ring of integers $\mathfrak{o}_v$ if $v \nmid \infty$. The adele ring of k is denoted by $\mathbb{A}_k$. For a not necessarily finite set of places S of k we denote by $\mathfrak{o}_{k,S}$ the ring of S-integers (which are integral outside S).

2. Galois sections with local conditions

2.1. **Sections.** Let X/k be a geometrically irreducible and reduced variety with function field K. Let $K \subset \overline{K}$ be a fixed algebraic closure and set $\mathrm{Gal}_K = \mathrm{Gal}(K^{\mathrm{sep}}/K)$ with K^{sep} the separable closure in $\overline{K}$. The algebraic (resp. separable) closure of k contained in $\overline{K}$ will be denoted by $\bar{k}$ (resp. k^{sep}) and $\mathrm{Gal}_k = \mathrm{Gal}(k^{\mathrm{sep}}/k)$. The fundamental group of X/k forms an extension $\pi_1(X/k)$

$$1 \to \pi_1(X_{\bar{k}}) \to \pi_1(X) \to \mathrm{Gal}_k \to 1,$$

where the geometric generic point $\mathrm{Spec}(\overline{K}) \to X_{\bar{k}} \to X$ is the implicit base point. The space of sections of $\pi_1(X/k)$ up to conjugation by elements from $\pi_1(X_{\bar{k}})$ will be denoted by $\mathscr{S}_{\pi_1(X/k)}$, and its birational analogue, $\mathrm{Gal}_{K\bar{k}}$-conjugacy classes of sections of $\mathrm{Gal}_K \to \mathrm{Gal}_k$, by $\mathscr{S}_{\pi_1(K/k)}$.

To the point $a \in X(k)$ we associate by functoriality a class of sections $s_a : \mathrm{Gal}_k \to \pi_1(X)$. This gives rise to the non-abelian profinite Kummer map $a \mapsto \kappa(a) = s_a$

$$\kappa : X(k) \to \mathscr{S}_{\pi_1(X/k)}.$$

2.1.1. *Birationally liftable sections.* The inclusion of the generic point $j : \operatorname{Spec} K \to X$ induces a map $j_* : \mathrm{Gal}_K \to \pi_1(X)$, a surjection if X is normal, and furthermore a map

$$j_* : \mathscr{S}_{\pi_1(K/k)} \to \mathscr{S}_{\pi_1(X/k)},$$

the image of which by definition is the set of **birationally liftable** sections $\mathscr{S}^{\mathrm{bir}}_{\pi_1(X/k)}$. The property *birationally liftable* is a priori stronger than the notion defined in [Sti13] §18.5.

2.1.2. *The limit argument.* A **neighbourhood** of a section $s : \mathrm{Gal}_k \to \pi_1(X)$ is a finite étale cover $X' \to X$ together with a lift s' of the section, i.e., an open subgroup $H \subseteq \pi_1(X)$ containing the image of the section $s = s'$. The limit over all neighbourhoods yields a pro-étale cover

$$X_s = \varprojlim X' \to X$$

corresponding to $\pi_1(X_s) = s(\mathrm{Gal}_k) \subseteq \pi_1(X)$. It follows that a section s of $\pi_1(X/k)$ comes from a k-rational point of X if and only if $X_s(k)$ is nonempty: we have $s = s_a$ if and only if

$$a \in \operatorname{im}\big(X_s(k) \to X(k)\big).$$

2.1.3. *Cuspidal sections.* For simplicity, we now moreover assume that X/k is a smooth curve with smooth completion $X \subseteq \overline{X}$. Let $a \in \overline{X}(k) \setminus X(k)$ and let w_a be the corresponding discrete k-valuation of K. Denote by I_{w_a} the inertia group and by D_{w_a} the decomposition group of (a prolongation $\bar{w}_a$ to $\overline{K}$ of) the valuation w_a. The short exact sequence

$$1 \to I_{w_a} \to D_{w_a} \to \mathrm{Gal}_k \to 1$$

splits. Composing splittings with the natural map $D_{w_a} \subseteq \mathrm{Gal}_K \to \pi_1(X)$ leads to sections of $\pi_1(X/k)$. These are by definition the **cuspidal sections** of $\pi_1(X/k)$ and naturally form a subset

$$\mathscr{S}^{\mathrm{cusp}}_{\pi_1(X/k)} \subseteq \mathscr{S}^{\mathrm{bir}}_{\pi_1(X/k)}.$$

If the section s comes from a section of $D_{w_a} \to \mathrm{Gal}_k$, then we say that s is centered in $a \in \overline{X} \setminus X$.

For an arbitrary section $s : \mathrm{Gal}_k \to \pi_1(X)$ we consider the pro-(finite branched) cover

$$\overline{X}_s = \varprojlim_{X'} \overline{X'} \to \overline{X}$$

where $X' \to X$ ranges through neighbourhoods of s and $\overline{X'}$ is the normalization of $\overline{X}$ in $X' \to X$. Then s is cuspidal and centered in a if and only if

$$a \in \operatorname{im}\big(\overline{X}_s(k) \to \overline{X}(k)\big) \setminus X(k).$$

2.2. **Local conditions.** Recall the base change map $s \mapsto s \otimes k'$ for a field extension k'/k in characteristic 0, see [Sti13] §3.2, namely the map

$$\mathscr{S}_{\pi_1(X/k)} \to \mathscr{S}_{\pi_1(X \times_k k'/k')}.$$

Note that base change for birational sections exists only if k'/k is algebraic, because in general $\mathrm{Gal}_{Kk'} \to \mathrm{Gal}_K \times_{\mathrm{Gal}_k} \mathrm{Gal}_{k'}$ is not an isomorphism, if k'/k is transcendental.

2.2.1. *Selmer sections.* Let k be a number field. Selmer groups in Galois cohomology classify torsors that become locally trivial because they possess local points everywhere. In analogy, Selmer sections are sections that locally belong to a rational point.

For a place v of k we write $s \otimes k_v = s_v$. The section $s : \mathrm{Gal}_k \to \pi_1(X)$ is a **Selmer section** if for every place v of k the localisation s_v is cuspidal or belongs to a rational point in $X(k_v)$. The set of all Selmer sections we denote by $\mathscr{S}^{\mathrm{Sel}}_{\pi_1(X/k)}$.

Let X/k be a hyperbolic curve with smooth completion $\overline{X}$. The adelic point $\underline{x}(s) = (x_v)_v$ in $\overline{X}(\mathbb{A}_k)_\bullet$ associated to a Selmer section s by $s_v = s_{x_v}$ is unique. Here $\overline{X}(\mathbb{A}_k)_\bullet$ denotes the set of modified adelic points of $\overline{X}$ where the component at an infinite place v is given by $\pi_0(\overline{X}(k_v))$. It

follows form [HSx10] Theorem 11 that $\underline{x}(s) \in \overline{X}(\mathbb{A}_k)_\bullet^{\mathrm{f-desc}}$, the set of adelic points that survive all finite descent obstructions. So we obtain a map

$$\underline{x} \,:\, \mathscr{S}^{\mathrm{Sel}}_{\pi_1(X/k)} \to \overline{X}(\mathbb{A}_k)_\bullet^{\mathrm{f-desc}}. \tag{2.1}$$

If $X = \overline{X}$ and the genus is at least 1, then (2.1) is surjective by [HSx10] Theorem 11.

Proposition 1 (Koenigsmann)**.** *Let X/k be a hyperbolic curve over a number field k with smooth projective completion $X \subseteq \overline{X}$.*

(1) If $\pi_1(X/k)$ admits a birationally liftable section, then $\overline{X}(k_v) \neq \emptyset$ for every completion k_v.
(2) Any birationally liftable section of $\pi_1(X/k)$ is a Selmer section.

Proof. (1) is immediate from [Ko05] Corollary 2.6. To show (2) we apply (1) to all neighbourhoods X' of s as in the proof of [Ko05] Proposition 2.4 (a). As $\overline{X}_{s_v} = \overline{X}_s \times_k k_v$, we find by compactness

$$\overline{X}_s(k_v) = \varprojlim_{X'} \overline{X'}(k_v) \neq \emptyset.$$

We pick $x_v \in \mathrm{im}(\overline{X}_s(k_v) \to \overline{X}(k_v))$, so that $s_v = s_{x_v}$, and the section s is Selmer. □

2.2.2. *Adelic sections.* Let X/k be a hyperbolic curve. An **adelic section** is a Selmer section $s : \mathrm{Gal}_k \to \pi_1(X)$ such that $\underline{x}(s) \in \overline{X}(\mathbb{A}_k)_\bullet$ lies in $X(\mathbb{A}_k)_\bullet$. The set of all adelic sections will be denoted by $\mathscr{S}^{\mathrm{adelic}}_{\pi_1(X/k)}$. We obtain a map

$$\underline{x} \,:\, \mathscr{S}^{\mathrm{adelic}}_{\pi_1(X/k)} \twoheadrightarrow X(\mathbb{A}_k)_\bullet^{\mathrm{f-desc}}$$

that is surjective due to [HSx10] Theorem 11, see also [Sti13] Theorem 144.

2.2.3. *Birationally adelic sections.* Let X/k be a hyperbolic curve with function field K. A **birationally adelic section** is a section $s : \mathrm{Gal}_k \to \pi_1(X)$ that is birationally liftable to a section $\mathrm{Gal}_k \to \mathrm{Gal}_K$ such that for every open $U \subseteq X$ the induced section of $\pi_1(U/k)$ is either adelic for U/k or cuspidal. The set of all birationally adelic sections is denoted by $\mathscr{S}^{\mathrm{ba}}_{\pi_1(X/k)}$.

2.3. **Examples.** We discuss tori of rank 1, since these enter the proof of Theorem A.

Proposition 2. *For a quadratic imaginary number field k or $k = \mathbb{Q}$ we have*

$$k^* = \mathbb{G}_m(k) = \mathscr{S}^{\mathrm{adelic}}_{\pi_1(\mathbb{G}_m/k)}.$$

Proof. The diagonal map $\widehat{k^*} \hookrightarrow \prod_v \widehat{k_v^*}$ is injective, see [NSW08] Theorem 9.1.11(2). The intersection

$$\mathscr{S}^{\mathrm{adelic}}_{\pi_1(\mathbb{G}_m/k)} = \mathscr{S}_{\pi_1(\mathbb{G}_m/k)} \cap \mathbb{G}_m(\mathbb{A}_k)_\bullet = \widehat{k^*} \cap \mathbb{G}_m(\mathbb{A}_k)_\bullet$$

inside the product contains k^*. By finiteness of the class number we can fix a finite set of places S of k containing all infinite places S_∞ with $\mathrm{Pic}(\mathfrak{o}_{k,S}) = 1$. Then we can use elements from k^* to move the support of the divisor of any $(x_v) \in \mathbb{G}_m(\mathbb{A}_k)_\bullet$ into S and thus

$$\begin{aligned}
\widehat{k^*} \cap \mathbb{G}_m(\mathbb{A}_k)_\bullet &= k^* \cdot \Big(\widehat{k^*} \cap \prod_{v \notin S} \mathfrak{o}_v^* \times \prod_{v \in S \setminus S_\infty} k_v^* \times \prod_{v \in S_\infty} \pi_0(k_v^*) \Big) \\
&= k^* \cdot \Big(\widehat{\mathfrak{o}_{k,S}^*} \cap \prod_{v \notin S} \mathfrak{o}_v^* \times \prod_{v \in S \setminus S_\infty} k_v^* \times \prod_{v \in S_\infty} \pi_0(k_v^*) \Big) \\
&= k^* \cdot \ker(v \otimes \hat{\mathbb{Z}} : \mathfrak{o}_{k,S}^* \otimes \hat{\mathbb{Z}} \to \bigoplus_{v \in S \setminus S_\infty} \hat{\mathbb{Z}}/\mathbb{Z}) = k^* \cdot \widehat{\mathfrak{o}_k^*}.
\end{aligned}$$

The assumption on k implies that $\mathfrak{o}_k^*$ is finite, hence $k^* = k^* \cdot \widehat{\mathfrak{o}_k^*}$ and the proof is complete. □

Proposition 3. *Let F be a totally real number field and let E/F be a quadratic extension that is totally imaginary. Then, for the norm 1-torus $T = \ker(N : R_{E|F}\mathbb{G}_m \to \mathbb{G}_m)$ over F we have*

$$T(F) = \ker(N : E^* \to F^*) = \mathscr{S}^{\mathrm{adelic}}_{\pi_1(T/F)}.$$

Proof. We need to compute $\widehat{T(F)} \cap T(\mathbb{A}_F)_\bullet$ which certainly injects by restriction into

$$\ker\left(N : \widehat{E^*} \cap \mathbb{G}_m(\mathbb{A}_E)_\bullet \to \widehat{F^*} \cap \mathbb{G}_m(\mathbb{A}_F)_\bullet\right) = \ker\left(N : E^* \cdot \widehat{\mathfrak{o}_E^*} \to F^* \cdot \widehat{\mathfrak{o}_F^*}\right),$$

where we have used the general computation of Proposition 2. By Dirichtlet's Unit Theorem the map $N : \mathfrak{o}_E^* \to \mathfrak{o}_F^*$ is an isomorphism up to torsion. This is preserved under profinite completion, and furthermore, the map

$$N \ : \ \widehat{\mathfrak{o}_E^*}/\mathfrak{o}_E^* \to \widehat{\mathfrak{o}_F^*}/\mathfrak{o}_F^*$$

is an isomorphism. An application of the snake lemma shows that the natural map

$$T(F) = \ker(N : E^* \to F^*) \xrightarrow{\sim} \ker\left(N : E^* \cdot \widehat{\mathfrak{o}_E^*} \to F^* \cdot \widehat{\mathfrak{o}_F^*}\right)$$

is an isomorphism. This completes the proof. □

3. Finite support

Let X/k be a hyperbolic curve over the number field k with smooth projective completion $\overline{X}$. The **support** of a Selmer section $s : \mathrm{Gal}_k \to \pi_1(X)$ is defined as the Zariski-closed subscheme

$$Z(s) = \overline{\bigcup_v \mathrm{im}(x_v : \mathrm{Spec}(k_v) \to \overline{X})} \subseteq \overline{X}$$

where $\underline{x}(s) = (x_v) \in \overline{X}$ is the adelic point associated to the Selmer section. We say that a Selmer section s has **finite support** if $Z(s)$ is finite over k.

The following important descent result due to Stoll.

Theorem 4 (Stoll [St07] Theorem 8.2)**.** *Let Z be a proper closed subscheme of a smooth projective curve $\overline{X}$ of genus at least 1 over a number field k. Then the diagonal map is a bijection:*

$$Z(k) \xrightarrow{\sim} \left\{(x_v) \in \overline{X}(\mathbb{A}_k)_\bullet^{\mathrm{f-desc}} \ ; \ x_v \in Z(k_v) \text{ for a set of places } v \text{ of density } 1\right\}.$$

Stoll's result is stronger requiring that the adelic point only survives finite descent obstructions with respect to abelian groups. For our application to sections the difference does not matter.

Corollary 5. *Let X/k be a hyperbolic curve over a number field. Then the image of the map*

$$X(k) \to \mathscr{S}^{\mathrm{adelic}}_{\pi_1(X/k)} \subseteq \mathscr{S}^{\mathrm{Selmer}}_{\pi_1(X/k)} \setminus \mathscr{S}^{\mathrm{cusp}}_{\pi_1(X/k)}$$

consists precisely of the non-cuspidal Selmer sections with finite support.

Proof. For $a \in X(k)$ the support of s_a is the subscheme $\{a\} \hookrightarrow \overline{X}$. It remains to conclude the converse: if the support $Z(s)$ is finite and s is not cuspidal, then s belongs to some rational point of X. If we pass to a neighbourhood $h : X' \to X$ of the section s with lift s', then

$$Z(s') \subseteq h^{-1}(Z(s)),$$

so that the property of having finite support is preserved. We may therefore without loss of generality assume that the smooth completion $\overline{X}$ of X has genus ≥ 1. Then by Theorem 4

$$\underline{x}(s) \in Z(s)(\mathbb{A}_k)_\bullet \cap \overline{X}(\mathbb{A}_k)_\bullet^{\mathrm{f-desc}} = Z(k)$$

and so in the limit over all neighbourhoods X' of s

$$X_s(k) \supseteq \varprojlim_{(X',s')} Z(s')(k) \neq \emptyset.$$

The limit argument (Section §2.1.2) implies that $s = s_a$ for any $a \in \mathrm{im}\left(\overline{X}_s(k) \to \overline{X}(k)\right)$. Since we assumed s not to be cuspidal, we may even deduce that $a \in X(k)$. □

Corollary 6. *Let k be $\mathbb{Q}$ or an imaginary quadratic number field. Let X/k be a hyperbolic curve with a global non-constant unit $f \in \mathcal{O}_X^* \setminus k^*$. Then the maps κ and $\underline{x}$ are bijective:*

$$X(k) \xrightarrow{\sim} \mathscr{S}^{\mathrm{adelic}}_{\pi_1(X/k)} \xrightarrow{\sim} X(\mathbb{A}_k)^{\mathrm{f-desc}}_\bullet.$$

Proof. We first treat κ. By Corollary 5 it suffices to show that adelic sections $s : \mathrm{Gal}_k \to \pi_1(X)$ have finite support. The non-constant unit defines a non-constant map $f : X \to \mathbb{G}_m$, and

$$Z(s) \subseteq f^{-1}(Z(f_* s)).$$

But the adelic section $f_* s : \mathrm{Gal}_k \to \pi_1(\mathbb{G}_m)$ comes from a rational point by Proposition 2, hence $f_* s$ and a forteriori s have finite support. This shows κ is bijective.

The map $X(k) \hookrightarrow X(\mathbb{A}_k)^{\mathrm{f-desc}}_\bullet$ is injective and $\underline{x} : \mathscr{S}^{\mathrm{adelic}}_{\pi_1(X/k)} \twoheadrightarrow X(\mathbb{A}_k)^{\mathrm{f-desc}}_\bullet$ is surjective by [HSx10] Theorem 11. In view of $X(k) = \mathscr{S}^{\mathrm{adelic}}_{\pi_1(X/k)}$ we conclude that also $\underline{x}$ must be bijective. □

Corollary 7. *Let k be a totally real number field or an imaginary quadratic number field. Let X/k be a hyperbolic curve. Then the natural map is a bijection:*

$$\mathscr{S}^{\mathrm{cusp}}_{\pi_1(X/k)} \amalg X(k) \xrightarrow{\sim} \mathscr{S}^{\mathrm{ba}}_{\pi_1(X/k)}.$$

Proof. We show that birationally adelic sections have finite support and use Corollary 5. We may replace X by an open $U \subseteq X$. If $k/\mathbb{Q}$ is imaginary quadratic or $k = \mathbb{Q}$ we choose U such that we have a non-constant global unit on U and conclude with Corollary 6.

It remains to treat the case of a totally real number field k. Let $a \in k^*$ be totally negative and set $k' = k(\sqrt{a})$ with $\mathrm{Gal}(k'/k)$ generated by σ. We set

$$T = \ker(N : R_{k'|k}\mathbb{G}_m \to \mathbb{G}_m).$$

A rational map $f : X \dashrightarrow T$ corresponds to an element $f \in k(X) \otimes_k k'$ of norm

$$N(f) = \sigma(f) f = \mathbf{1}.$$

We take $\alpha \in k' \setminus k$ and a non-constant element $g \in k(X)^* \setminus k^*$ and set

$$f = \sigma(g + \alpha)/(g + \alpha) = (g + \sigma(\alpha))/(g + \alpha).$$

Then $N(f) = \mathbf{1}$ and, for $U \subset X$ small enough, f is a non-constant map $f : U \to T$. The argument of Corollary 6 with Proposition 3 instead of Proposition 2 concludes the proof. □

A result in the same spirit but using abelian varieties instead of tori was proven by Stoll [St07] Theorem 8.6 and Remark 8.9. For abelian varieties all Selmer sections are adelic.

4. Density of non-integral places

We now discuss to what extent a Selmer section misses to be an adelic or cuspidal section.

4.1. **Types of adelic points.** Let X/k be a smooth, geometrically connected curve over a number field k and let $\overline{X}$ be its smooth projective completion. Let $U \subseteq \mathrm{Spec}(\mathfrak{o}_k)$ be a dense open such that $X \subseteq \overline{X}$ has good reduction $\mathscr{X} \subseteq \overline{\mathscr{X}}$ over U in the sense of open curves, i.e., $\mathscr{X}$ is an open in the smooth, projective $\overline{\mathscr{X}} \to U$ and the boundary divisor $\overline{\mathscr{X}} \setminus \mathscr{X}$ is relatively étale over U. For an adelic point

$$\underline{x} = (x_v) \in \overline{X}(\mathbb{A}_k)_\bullet$$

we define a partition of all places of k with respect to U and the models $\mathscr{X} \subseteq \overline{\mathscr{X}}$ as follows.

integral : An integral place for $\underline{x}$ is a place $v \in U$ such that the closure of $\{x_v\}$ in $\overline{\mathscr{X}} \times_U \mathfrak{o}_v$ is contained in $\mathscr{X} \times_U \mathfrak{o}_v$.

degenerate : A degenerate place for $\underline{x}$ is a place $v \in U$ such that $x_v \in X(k_v)$ and the closure of $\{x_v\}$ in $\overline{\mathscr{X}} \times_U \mathfrak{o}_v$ meets the boundary $(\overline{\mathscr{X}} \setminus \mathscr{X}) \times_U \mathfrak{o}_v$.

cuspidal : A cuspidal place for $\underline{x}$ is a place $v \in U$ such that $x_v \in (\overline{X} \setminus X)(k_v)$.

bad : A bad place for $\underline{x}$ is a place $v \notin U$. In particular, all infinite places are bad by definition.

Definition 8. With the notation as above, we say that $(x_v) \in \overline{X}(\mathbb{A}_k)_\bullet$ is **asymptotically integral** if the intersection number with the boundary divisor $\overline{\mathscr{X}} \setminus \mathscr{X}$ of the closure of $\{x_v\}$ for degenerate places v tends to 0 in $\hat{\mathbb{Z}}$, i.e., for every $n \geq 1$ there are only finitely many degenerate places v where n does not divide this intersection number.

Remark 9. (1) Since we will be interested in assertions on finiteness or on the Dirichlet density of the partition sets, the choice of U and the models $\mathscr{X} \subseteq \overline{\mathscr{X}}$ are irrelevant.

(2) The subset $X(\mathbb{A}_k)_\bullet \subseteq \overline{X}(\mathbb{A}_k)_\bullet$ contains precisely those adelic points for which all but finitely many places are integral, no place is cuspidal and the components at $v \notin U$ lie in $X(k_v)$.

4.2. **Families of elliptic curves and ℓ-adic representations.** Let X/k be a geometrically connected variety with geometric point $\bar{x} \in X$. We assume that there is a family of elliptic curves $E \to X$ and consider, for every $\ell \neq \mathrm{char}(k)$, the ℓ-adic 2-dimensional representation

$$\rho_{E/X,\ell} : \pi_1(X, \bar{x}) \to \mathrm{GL}(\mathrm{T}_\ell(E_{\bar{x}}))$$

where $E_{\bar{x}}$ is the geometric fibre of E/X in $\bar{x}$. The Weil-pairing induces a canonical isomorphism

$$\det(\rho_{E/X,\ell}) = \varepsilon \circ \mathrm{pr}_*$$

where ε is the corresponding ℓ-adic cyclotomic character and $\mathrm{pr}_* : \pi_1(X, \bar{x}) \to \mathrm{Gal}_k$ is induced by the projection map.

To any section $s : \mathrm{Gal}_k \to \pi_1(X, \bar{x})$ we can thus associate a family of ℓ-adic representations

$$\rho_{s,E/X,\ell} = \rho_{E/X,\ell} \circ s : \mathrm{Gal}_k \to \mathrm{GL}(\mathrm{T}_\ell(E_{\bar{x}}))$$

with cyclotomic determinant

$$\det(\rho_{s,E/X,\ell}) = \varepsilon.$$

By naturality of the construction, if $s = s_a$ for $a \in X(k)$, then $\rho_{s,E/X,\ell}$ is nothing but the Galois representation $\rho_{E_a/k,\ell}$ on $\mathrm{T}_\ell(E_a)$ for the fibre E_a of E/X in a. If the family is constant $E = X \times E_0$, then clearly $\rho_{s,E/X,\ell}$ is independent of s and agrees with $\rho_{E_0/k,\ell}$.

Recall that k is a number field. Strictly speaking, the family $\{\rho_{s,E/X,\ell}\}_\ell$ does not deserve to be called an ℓ-adic representation, because

(i) we lack a conductor N such that $\rho_{s,E/X,\ell}$ is unramified for all places $v \nmid \ell \cdot N$,
(ii) we lack integrality of the characteristic polynomials of Frobenius,
(iii) and we lack independence of ℓ for the characteristic polynomials of Frobenius.

This changes for Selmer sections, well almost.

4.3. **Almost an ℓ-adic representation.** Let now X/k be a smooth, geometrically connected curve, and assume that the family E/X has bad semistable reduction along every point of $\overline{X} \setminus X$. Let $s : \mathrm{Gal}_k \to \pi_1(X)$ be a Selmer section with associated adelic point $\underline{x}(s) = (x_v)$ of the smooth projective completion $\overline{X}$. Let $D_v = \mathrm{Gal}_{k_v} \subset \mathrm{Gal}_k$ be the decomposition subgroup of the place v, and let $I_v \subset D_v$ be the inertia subgroup. We discuss the local behaviour

$$\rho_{s,E/X,\ell}|_{D_v} : \mathrm{Gal}_{k_v} \to \mathrm{GL}(\mathrm{T}_\ell(E_{\bar{x}}))$$

in terms of the type of v with respect to $\underline{x}$. As $\mathscr{X} \to U$ with $U \subseteq \mathrm{Spec}(\mathfrak{o}_k)$ we take a model such that the family E/X has good reduction over $\mathscr{X}$ and bad semistable reduction along $\overline{\mathscr{X}} \setminus \mathscr{X}$. Note that $\overline{X}$ is a surface and that semistable reduction ceases to make sense only in a set of codimension 2, hence a finite set that we may assume to be empty by shrinking U.

integral: For an integral v the local representation belongs to the elliptic curve E_v/k_v which is the fibre of E/X in $x_v \in X(k_v)$ and has good reduction over $\mathrm{Spec}(\mathfrak{o}_v)$. It follows that
(i) the representation $\rho_{s,E/X,\ell}|_{D_v}$ is unramified for $\ell \neq \mathrm{char}(\mathbb{F}_v)$ with $\mathbb{F}_v$ being the residue field of v,

(ii) the characteristic polynomial of Frobenius is integral
$$\det(\mathbf{1} - \mathrm{Frob}_v\, T | \rho_{s,E/X,\ell}) = \mathbf{1} - a_v T + N(v)T^2 \in \mathbb{Z}[T]$$
(here $N(v) = \#\mathbb{F}_v$ is the norm of v),

(iii) and the trace of Frobenius $a_v \in \mathbb{Z}$ is independent of ℓ with $|a_v| \leq 2\sqrt{N(v)}$.

degenerate: For a degenerate v the local representation belongs to the elliptic curve E_v/k_v which is the fibre of E/X in $x_v \in X(k_v)$ and has bad semistable reduction over $\mathrm{Spec}(\mathfrak{o}_v)$. It follows that

(i) there is a quadratic unramified character $\delta_v : \mathrm{Gal}_{k_v} \to \{\pm 1\}$ such that for all $\ell \neq \mathrm{char}(\mathbb{F}_v)$ in a suitable basis
$$\rho_{s,E/X,\ell}|_{D_v} \sim \begin{pmatrix} \delta\varepsilon & \psi \\ & \delta \end{pmatrix} \tag{4.1}$$
where $\psi|_{I_v} = m_v \cdot t_\ell$ is a multiple of the tame ℓ-adic character with $m_v > 0$ integral and independent of ℓ,

(ii) the characteristic polynomial of Frobenius still makes sense (computed on the unramified semisimplification) and is integral
$$\det(\mathbf{1} - \mathrm{Frob}_v\, T | \rho_{s,E/X,\ell}) = \mathbf{1} - a_v T + N(v)T^2$$
$$= (\mathbf{1} - \delta_v(\mathrm{Frob}_v)T)(\mathbf{1} - \delta_v(\mathrm{Frob}_v)N(v)T) \in \mathbb{Z}[T],$$

(iii) and the trace of Frobenius $a_v \in \mathbb{Z}$ is independent of ℓ with
$$a_v = \delta_v(\mathrm{Frob}_v)(N(v) + 1).$$

The character δ describes the 1-dimensional torus in the special fibre of the Néron model of E_v over $\mathrm{Spec}(\mathfrak{o}_v)$. Concerning the claim on ψ we may pass to an unramified extension k_v'/k_v such that E_v attains split multiplicative reduction and therefore admits a Tate uniformization $E_v \times_{k_v} k_v' = \mathbb{G}_m/q_v^{\mathbb{Z}}$, with $q_v \in k_v'$. The cocycle $\psi|_{I_v}$ is the Kummer cocycle associated to q_v and thus agrees with the $m_v = v(q_v) > 0$ multiple of the tame ℓ-adic character.

cuspidal: For a cuspidal v the local section s_v is cuspidal at x_v and thus factors over the decomposition subgroup of x_v in $\pi_1(X \otimes k_v/k_v)$: the absolute Galois group of the fraction field of $\hat{\mathcal{O}}_{\overline{X}_{\otimes k_v}, x_v}$ that is noncanonically isomorphic to $k_v((z))$. It follows that the image of the representation $\rho_{s,E/X,\ell}|_{D_v}$ is contained in the image of the representation of the corresponding Tate elliptic curve which is the fibre $E \times_X \mathrm{Spec}\, k((z))$. We thus can say the same thing about $\rho_{s,E/X,\ell}|_{D_v}$ for $v \nmid \ell$ as for degenerate places v except that we do know nothing on ψ:

(i) There is a quadratic unramified character $\delta_v : \mathrm{Gal}_{k_v} \to \{\pm 1\}$ such that for all $\ell \neq \mathrm{char}(\mathbb{F}_v)$ in a suitable basis
$$\rho_{s,E/X,\ell}|_{D_v} \sim \begin{pmatrix} \delta\varepsilon & * \\ & \delta \end{pmatrix},$$

(ii) the characteristic polynomial of Frobenius still makes sense and is integral
$$\det(\mathbf{1} - \mathrm{Frob}_v\, T | \rho_{s,E/X,\ell}) = \mathbf{1} - a_v T + N(v)T^2$$
$$= (\mathbf{1} - \delta_v(\mathrm{Frob}_v)T)(\mathbf{1} - \delta_v(\mathrm{Frob}_v)N(v)T) \in \mathbb{Z}[T],$$

(iii) and the trace of Frobenius $a_v \in \mathbb{Z}$ is independent of ℓ with
$$a_v = \delta_v(\mathrm{Frob}_v)(N(v) + 1).$$

bad: For the finitely many bad v we say nothing.

For a Selmer section s as above and $\rho = \{\rho_{s,E/X,\ell}\}$ we define the **trace of Frobenius**

$$a_v(\rho) = \mathrm{tr}\big(\rho_{s,E/X,\ell}(\mathrm{Frob}_v)|\,\mathrm{T}_\ell(E_{\bar{x}})\big) \in \mathbb{Z}$$

for any $\ell \neq \mathrm{char}(\mathbb{F}_v)$ and any v that is not bad. By the above discussion this number is indeed a well defined integer.

4.4. **A dichotomoy.** As a consequence of the Chebotarev Density Theorem we will now prove the following result.

Theorem 10. *Let X/k be a hyperbolic curve over a number field with smooth completion $\overline{X}$. Let E/X be a family of elliptic curves with bad and not even potentially good reduction over $\overline{X}\setminus X$. Let $s : \mathrm{Gal}_k \to \pi_1(X)$ be a Selmer section with adelic point $\underline{x}(s) = (x_v) \in \overline{X}(\mathbb{A}_k)_\bullet$. Then $\underline{x}(s)$ is asymptotically integral with respect to X, and exactly one of the following occurs.*

(1) Either the set

$$\{\textit{places } v \textit{ such that } x_v \textit{ is integral with respect to } X\}$$

has Dirichlet density 1,

(2) or the family of ℓ-adic representations $\rho_{s,E/X,\ell}$ factors in a suitable basis through

$$\begin{pmatrix} \delta\varepsilon & * \\ & \delta \end{pmatrix}$$

with a quadratic character $\delta : \mathrm{Gal}_k \to \{\pm 1\}$ that is independent of ℓ and ramified at most in the bad places. Moreover, all but finitely many places are cuspidal or degenerate. The remaining places are bad.

Proof. We may pass to a neighbourhood $h : X' \to X$ of the section s. For every $y' \in \overline{X'}\setminus X'$ above $y \in \overline{X}\setminus X$, the semistable reduction theorem implies that h^*E/X' has semistable reduction at y' if the ramification index $e_{y'/y}$ is divisible by an integer that only depends on the degeneration of E in y. Since X is hyperbolic, among the neighbourhoods of the section s we find universal ramification along $\overline{X}\setminus X$. Hence we may and will assume from the beginning that the family E/X has bad semistable reduction outside X.

Let us first address the claim on asymptotic integrality. Let ℓ be a prime number and let $r \geq 1$. We have to show divisibility by ℓ^r of the intersection number d_v of the closure of $\{x_v\}$ with the boundary for almost all degenerate $v \nmid \ell$.

Let $m_v = v(q_v) > 0$ be the valuation of the local Tate parameter q_v at a degenerate place v for the elliptic curve E_v as in Section §4.3 above. Being essentially a finite quotient of a global Galois group, the mod ℓ^r reduction of the representation $\rho_{s,E/X,\ell}$ is unramified for allmost all v. If $v \nmid \ell$ is degenerate and unramified in the mod ℓ^r representation, then $\ell^r \mid m_v$ by the description of ψ in (4.1).

Let now t be a local parameter on $\overline{\mathscr{X}} \times_U \mathfrak{o}_v$ for the boundary component of $(\overline{\mathscr{X}}\setminus\mathscr{X}) \times_U \mathfrak{o}_v$ that intersects with x_v. The j-function on $\mathscr{X}$ induced by the family E/X (more precisely its extension to $\mathscr{X}$) has a pole along $\{t = 0\}$ of some order e and thus $t^e \sim j^{-1}$ differ by a v-adic unit. Moreover, the local Tate parameter q_v has $v(q_v) = -v(j(x_v))$. This leads to

$$d_v = v(t(x_v)) = -\frac{1}{e}v(j(x_v)) = \frac{1}{e}v(q_v) = \frac{m_v}{e}.$$

Since only finitely many e can occur, we conclude asymptotic integrality for $\underline{x}(s)$.

We now address the claimed dichotomy. Let $G_\ell \subseteq \mathrm{GL}_2(\mathbb{F}_\ell)$ be the image of the mod ℓ reduction of $\rho_{s,E/X,\ell}$. And let $M_\ell \subseteq G_\ell$ be the subset of elements with split characteristic polynomial and at least one eigenvalue ± 1 modulo ℓ. The Frob_v for v cuspidal or degenerate are contained in M_ℓ so that their Dirichlet density is bounded above by

$$\frac{\#M_\ell}{\#G_\ell}.$$

We will show that this ratio can become arbitrarily small for ℓ ranging over all prime numbers or otherwise $\rho_{s,E/X,\ell}$ has the exceptional form (2).

Since the determinant of our representation is the cyclotomic character, we may assume by working with $\ell \gg 0$ that

$$\det\ :\ G_\ell \twoheadrightarrow \mathbb{F}_\ell^*$$

is surjective.

Let PG_ℓ be the image of G_ℓ in $\mathrm{PGL}_2(\mathbb{F}_\ell)$. Then the classification of subgroups $G \subseteq \mathrm{GL}_2(\mathbb{F}_\ell)$ with $\det(G) = \mathbb{F}_\ell^*$ (for $\ell \gg 0$) says that we can have either of the following cases:

(i) The mod ℓ representation is reducible, i.e.,

$$G_\ell \subseteq \begin{pmatrix} * & * \\ & * \end{pmatrix},$$

(ii) $G_\ell = \mathrm{GL}_2(\mathbb{F}_\ell)$,
(iii) G_ℓ is contained in the normalizer of a split torus but not in the torus and $\ell \nmid \#G_\ell$,
(iv) G_ℓ is contained in the normalizer of a non-split torus and $\ell \nmid \#G_\ell$,
(v) PG_ℓ is either A_4, S_4, or S_5 and $\ell \nmid \#G_\ell$.

By Lemmata 11–14 below we are done unless case (i) occurs for all but finitely many places. We therefore now assume that all mod ℓ representations are reducible for $\ell \gg 0$.

Let $\chi_i : G_\ell \to \mathbb{F}_\ell^*$ for $i = 1, 2$ be the projection onto the two diagonal entries. We denote by $H_i \subseteq \mathbb{F}_\ell^*$ the subgroup generated by $\chi_i(M_\ell)$. If the index

$$(\chi(G_\ell) : H_i)$$

is unbounded for ℓ ranging over all prime numbers, then $\#M_\ell/\#G_\ell \leq \#H_i/\#\chi_i(G_\ell)$ becomes arbitrarily small and we are done. We therefore assume that the two indices are bounded.

Let $\overline{G}_\ell$ denote the image of G_ℓ under

$$\mathrm{pr} = (\chi_1, \chi_2) : \begin{pmatrix} * & * \\ & * \end{pmatrix} \to \mathbb{F}_\ell^* \times \mathbb{F}_\ell^*$$

and set $\overline{M}_\ell = \mathrm{pr}(M_\ell)$. We have $(H_1)^2 \times (H_2)^2 \subseteq \overline{G}_\ell$ and therefore the estimate

$$\frac{\#M_\ell}{\#G_\ell} \leq \frac{\#\overline{M}_\ell}{\#\overline{G}_\ell} \leq \frac{2\#H_1 + 2\#H_2}{1/4 \cdot \#H_1 \cdot \#H_2} = \frac{8}{\#H_1} + \frac{8}{\#H_2}$$

so that we can conclude the claim of the theorem if both $\#H_i$ are unbounded when ℓ ranges over all prime numbers.

It remains to discuss the case, where $\min_{i=1,2}\{\#\chi_i(G_\ell)\}$ remains bounded when ℓ tends to infinity. In this case there is an $m \in \mathbb{N}$ independent of ℓ and v such that there is a $\zeta \in \mu_m$ depending on ℓ, v such that

$$a_v(\rho) = \mathrm{tr}(\mathrm{Frob}_v \,|\rho_{s,E/X,\ell}) \equiv \zeta + \zeta^{-1}N(v) \mod \ell.$$

Now there are only finitely many $\zeta \in \mu_m$ and so for a each fixed v there must be one ζ that is good for infinitely many ℓ. With that ζ we find

$$a_v(\rho) = \zeta + \zeta^{-1}N(v)$$

so that ζ satisfies a nontrivial quadratic relation over $\mathbb{Z}$. If $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2$, then this must be irreducible, and $N(v) = N(\zeta) = 1$ which is absurd. Therefore $\zeta \in \mathbb{Q}$ and thus $\zeta = \pm 1$. We conclude that

$$a_v(\rho) = \pm(N(v) + 1)$$

for every finite place v. This contradicts the Hasse–Weil bound $|a_v(\rho)| \leq 2\sqrt{N(v)}$ in case v were integral. We deduce that all but finitely many places are cuspidal or degenerate and the remaining places are bad (the same argument shows that the two scenarios (1) and (2) of the theorem cannot hold simultaneously).

By approximating an arbitrary element $\sigma \in \mathrm{Gal}_k$ by Frobenius elements at places which are unramified in the mod ℓ^n reduction of $\rho_{s,E/X,\ell}$ we deduce that in $\mathbb{Z}_\ell$.

$$\mathrm{tr}(\rho_{s,E/X,\ell}(\sigma)) = \pm(\varepsilon(\sigma)+1).$$

Here the sign is independent of ℓ since we can approximate the mod ℓ^n reduction for two different ℓ simultaneously by Frobenius elements and there the sign is independent of ℓ.

Let $\Gamma_\ell \subset \mathrm{GL}(\mathrm{T}_\ell(E_{\bar{x}}))$ be the image of the representation $\rho_{s,E/X,\ell}$. Then Γ_ℓ is a closed ℓ-adic analytic group and by [La65] contains an open normal subgroup $\Gamma_\ell^0 \lhd \Gamma_\ell$ that consists of squares from Γ_ℓ. Let k_ℓ be the finite extension of k corresponding to the finite quotient $\mathrm{Gal}_k \twoheadrightarrow \Gamma_\ell/\Gamma_\ell^0$. Then for $\sigma \in \mathrm{Gal}_{k_\ell}$ we find $\gamma \in \Gamma_\ell$ with

$$\rho_{s,E/X,\ell}(\sigma) = \gamma^2.$$

Using the identity for $A \in GL_2$

$$\mathrm{tr}(A^2) = \mathrm{tr}(A)^2 - 2\det(A),$$

we compute

$$\begin{aligned}\mathrm{tr}(\rho_{s,E/X,\ell}(\sigma)) &= \mathrm{tr}(\gamma^2) = (\mathrm{tr}(\gamma))^2 - 2\det(\gamma)\\ &= (\pm(\varepsilon(\gamma)+1))^2 - 2\varepsilon(\gamma) = \varepsilon(\gamma^2)+1 = \varepsilon(\sigma)+1.\end{aligned}$$

It follows that the semisimplification of $\rho_{s,E/X,\ell}|_{\mathrm{Gal}_{k_\ell}}$ agrees with $\varepsilon \oplus \mathbf{1}$. Since $\varepsilon \neq \mathbf{1}$ and the trivial representation is preserved by automorphisms we conclude that $\rho_{s,E/X,\ell}$ itself is also reducible. The semisimplification must be $\delta\varepsilon \oplus \delta^{-1}$ with a character δ of finite order. For the Frobenius elements, we find values of these characters

$$\{\pm 1, \pm N(v)\} = \{\delta(\mathrm{Frob}_v)N(v), \delta^{-1}(\mathrm{Frob}_v)\}.$$

As $\pm N(v)$ is never torsion in $\mathbb{Z}_\ell^*$ we must have $\delta(\mathrm{Frob}_v) = \pm 1$ and δ is a quadratic character

$$\delta : \mathrm{Gal}_k \to \{\pm 1\} \subset \mathbb{Z}_\ell^*.$$

Moreover, δ is independent of ℓ, since it is determined by the signs in $a_v(\rho) = \pm(N(v)+1)$ which are independent of ℓ. Furthermore, by comparing with the local form at cuspidal or degenerate places, we see that δ can be ramified at most at the bad places.

It remains to exclude that $\rho_{s,E/X,\ell}$ has the form

$$\begin{pmatrix} \delta & * \\ & \delta\varepsilon \end{pmatrix}$$

in a suitable basis without being the direct sum $\delta \oplus \delta\varepsilon$. Assume that this happens. Then no place can be degenerate since inertia would then act nontrivially unipotently and thereby uniquely determine the fixed $\mathbb{Z}_\ell$-line. However, the description of the local representations then says that the character associated to this submodule must be $\delta\varepsilon$, a contradiction. If now all but finitely many places are cuspidal, we conclude that the adelic point $\underline{x}(s)$ has finite support in $\overline{X} \setminus X$. This allows to use Corollary 5 (or better its proof) to deduce that s is cuspidal. But then it follows from the known structure (as recalled above for cuspidal places) of the Galois representation associated to Tate elliptic curves that $\rho_{s,E/X,\ell}$ has the shape of (2). This finally finishes the proof of the theorem. □

4.5. **Asymptotics in subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$.** We now provide the Lemmas needed in the proof of Theorem 10.

Lemma 11. *If $G_\ell = \mathrm{GL}_2(\mathbb{F}_\ell)$, then*

$$\#M_\ell/\#G_\ell \leq 2/(\ell-1).$$

Proof. The possible Jordan normal forms for elements in M_ℓ are

$$\begin{pmatrix} 1 & \\ & 1 \end{pmatrix}, \begin{pmatrix} -1 & \\ & -1 \end{pmatrix}, \begin{pmatrix} a & \\ & 1 \end{pmatrix}, \begin{pmatrix} b & \\ & -1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ & -1 \end{pmatrix}$$

with $a, b \in \mathbb{F}_\ell^*$ and, to make the list disjoint, the condition $a \neq 1$ and $b \neq \pm 1$. We now have to sum up the reciprocals of the size of the respective centralizer. This leads to

$$\begin{aligned} \frac{\#M_\ell}{\#G_\ell} &= \frac{2}{(\ell^2-1)(\ell^2-\ell)} + \frac{2\ell-5}{(\ell-1)^2} + \frac{2}{\ell(\ell-1)} \\ &= \frac{2\ell}{(\ell^2-1)(\ell-1)} + \frac{2\ell-5}{(\ell-1)^2} \leq \frac{2\ell-3}{(\ell-1)^2} \leq \frac{2}{\ell-1}. \end{aligned}$$

□

Lemma 12. *If $PG_\ell = A_4$, S_4, or A_5 and $\det(G_\ell) = \mathbb{F}_\ell^*$, then*

$$\#M_\ell/\#G_\ell \leq 60/(\ell-1).$$

Proof. We consider an element $A \in M_\ell$ with eigenvalues $a, 1$ or $-a, -1$. The order of the image of A in PG_ℓ is in both cases the order of $a \in \mathbb{F}_\ell^*$. Since the order of an element in A_4, S_4, or A_5 divides 60 we conclude that a must lie in the 60-torsion of $\mathbb{F}_\ell^*$.

Since $\det(A) = a$ we conclude that $\det(M_\ell)$ is also contained in the 60-torsion of $\mathbb{F}_\ell^*$. The estimate

$$\frac{\#M_\ell}{\#G_\ell} \leq \frac{\#\det(M_\ell)}{\ell-1} \leq \frac{60}{\ell-1}$$

finishes the proof. □

Lemma 13. *If G_ℓ is contained in the normalizer of a non-split torus, $\ell \nmid \#G_\ell$ and $\det(G_\ell) = \mathbb{F}_\ell^*$, then*

$$\#M_\ell/\#G_\ell \leq 2/(\ell-1).$$

Proof. The normalizer of a nonsplit torus has the form $\mathbb{F}_{\ell^2}^* \rtimes \mathrm{Gal}(\mathbb{F}_{\ell^2}/\mathbb{F}_\ell)$. We consider an element $A \in M_\ell$ with eigenvalues $a, 1$ or $-a, -1$. Then A^2 is contained in the non-split torus with eigenvalues $a^2, 1$. The eigenvalues of $\lambda \in \mathbb{F}_{\ell^2}$ are $\lambda, \bar{\lambda}$. We deduce that necessarily $a^2 = 1$, and the Jordan normal form of A is one of the following

$$\begin{pmatrix} 1 & \\ & 1 \end{pmatrix}, \begin{pmatrix} -1 & \\ & -1 \end{pmatrix}, \begin{pmatrix} 1 & \\ & -1 \end{pmatrix}.$$

Therefore $\det(M_\ell)$ is contained in the 2-torsion of $\mathbb{F}_\ell^2$ and the estimate

$$\frac{\#M_\ell}{\#G_\ell} \leq \frac{\#\det(M_\ell)}{\ell-1} \leq \frac{2}{\ell-1}$$

finishes the proof. □

Lemma 14. *If G_ℓ is contained in the normalizer of a split torus but not in a torus, $\ell \nmid \#G_\ell$ and $\det(G_\ell) = \mathbb{F}_\ell^*$, then*

$$\#M_\ell/\#G_\ell \leq 6/\sqrt{(\ell-1)}.$$

Proof. The normalizer of the split torus is

$$(\mathbb{F}_\ell^* \times \mathbb{F}_\ell^*) \rtimes \langle \begin{pmatrix} & 1 \\ 1 & \end{pmatrix} \rangle = \left\{ \begin{pmatrix} a & \\ & b \end{pmatrix}, \begin{pmatrix} & b \\ a & \end{pmatrix} \;;\; a, b \in \mathbb{F}_\ell^* \right\}.$$

For $A \in M_\ell$ not in the torus, we have $A = \begin{pmatrix} & b \\ a & \end{pmatrix}$ with characteristic polynomial $X^2 - ab$. As ± 1 must be a root we see that $ab = 1$. Moreover, two such elements differ by an element of

$$D := G_\ell \cap \mathrm{SL}_2(\mathbb{F}_\ell),$$

and their eigenvalues are ± 1.

Let $H \subseteq \mathbb{F}_\ell^*$ be the subgroup generated by all eigenvalues of elements from M_ℓ. Then for every $a \in H^2$ we have

$$\begin{pmatrix} a & \\ & 1 \end{pmatrix} \in G_\ell.$$

Therefore we have $H^2 \times H^2 \subseteq G_\ell$ and the product map $D \times (H^2 \times \{\mathbf{1}\}) \hookrightarrow G_\ell$ is injective. Since H is cyclic, we obtain the estimates

$$(\#H)^2 \leq 4\#G_\ell \qquad \text{and} \qquad \#H \cdot \#D \leq 2\#G_\ell.$$

Now we simply count the elements in M_ℓ by counting those of the form

$$\begin{pmatrix} a & \\ & \pm 1 \end{pmatrix}, \begin{pmatrix} \pm 1 & \\ & a \end{pmatrix}, \begin{pmatrix} & a^{-1} \\ a & \end{pmatrix}$$

so that

$$\#M_\ell \leq 4 \cdot \#H + \#D.$$

As $\det(M_\ell) \subseteq \pm H$ has size $\#\det(M_\ell) \leq 2\#H$, the estimate

$$\left(\frac{\#M_\ell}{\#G_\ell}\right)^2 \leq \frac{4 \cdot \#H + \#D}{\#G_\ell} \cdot \frac{\#\det(M_\ell)}{\ell - 1} \leq \frac{8(\#H)^2 + 2\#D \cdot \#H}{\#G_\ell(\ell-1)} \leq \frac{36}{\ell - 1}$$

finishes the proof. □

Corollary 15. *Let $s : \mathrm{Gal}_k \to \pi_1(X)$ be a birationally liftable section of a hyperbolic curve with smooth completion $\overline{X}$ over a number field k. Then the associated adele $\underline{x}(s) \in \overline{X}(\mathbb{A}_k)_\bullet$ has*

(1) either $x_v \in X(\mathfrak{o}_v)$ is integral for a set of places v of Dirichlet density 1, or
(2) all but finitely many places v are cuspidal or degenerate with respect to $X \subset \overline{X}$.

Proof. The open subsets $U = \beta^{-1}(\mathbb{P}^1 - \{0, 1, \infty\}) \subseteq X$ for finite maps $\beta : \overline{X} \to \mathbb{P}^1$ which map $\overline{X} \setminus X$ to $\{0, 1, \infty\}$ form a basis of the topology of X (even with β étale over $\mathbb{P}^1 - \{0, 1, \infty\}$ due to an improved version of Belyi's Theorem by Mochizuki [Mz04] Corollary 1.1). The Legendre family of elliptic curves

$$E_\lambda = \{Y^2 = X(X-1)(X-\lambda)\} \ \to \ \mathbb{P}^1 - \{0, 1, \infty\}$$

has bad reduction exactly in 0, 1, and ∞. Thus we can apply Theorem 10 to a lift $\mathrm{Gal}_k \to \pi_1(U)$ of s and the pullback family $\beta^* E_\lambda \to U$. It follows that either $x_v \in U(\mathfrak{o}_v)$ is integral for a set of places of density 1, in which case we are done, or secondly that all but finitely many places are cuspidal or degenerate with respect to $U \subseteq \overline{X}$.

We may therefore assume that we are in the second case for all U as above. Let X be covered by $U_1, \ldots, U_n$ for open subsets U_i as above (in fact two such sets suffice). Let $\mathscr{Y}_i$ be the Zariski closure of $X \setminus U_i$ in a suitable common model. The intersection $\bigcap_i \mathscr{Y}_i$ is finite. Thus x_v is actually cuspidal or degenerate also for allmost all places v with respect to $X \subset \overline{X}$. □

5. Cuspidal sections

5.1. **Geometric monodromy of the Legendre family.** For the finer analysis in Theorem 20 below we have to understand the geometric monodromy representation of the Legendre family

$$\rho_{\mathrm{Leg}} = \rho_{E_\lambda/\mathbb{P}^1 - \{0,1,\infty\}} \ : \ \pi_1(\mathbb{P}^1_{\overline{\mathbb{Q}}} - \{0, 1, \infty\}, \overrightarrow{01}) \to \mathrm{GL}_2(\mathbb{Z}_\ell).$$

In fact, the 2-adic representaion turns out to be crucial. Since we are in characteristic 0, this is nothing but the profinite/pro-2 completion of the topological monodromy on the period lattice of the family. The topological fundamental group

$$\pi_1^{\mathrm{top}}(\mathbb{P}^1(\mathbb{C}) - \{0, 1, \infty\}, \overrightarrow{01}) = \langle x, y, z | xyz = 1 \rangle$$

is freely generated by an infinitesimal counterclockwise loop x around 0 starting and ending at the tangential base point $\overrightarrow{01}$, and by the path y which is the image of x under $\lambda \mapsto 1 - \lambda$

conjugated by the path from $\overrightarrow{01}$ to $\overrightarrow{10}$ along the real interval $[0,1]$. The path $z = (xy)^{-1}$ turns out to be a an infinitesimal loop around ∞ conjugated by a path form $\overrightarrow{01}$ to a tangential base point at ∞. In particular, this topological presentation reveals representatives for the inertia groups at the cusps 0, 1, and ∞, namely $I_0 = \langle x\rangle$, $I_1 = \langle y\rangle$, and $I_\infty = \langle z\rangle$.

Lemma 16. *For a suitable basis, the topological monodromy representation*

$$\rho_{\mathrm{Leg}}^{\mathrm{top}} \,:\, \pi_1^{\mathrm{top}}(\mathbb{P}^1(\mathbb{C}) - \{0,1,\infty\}, \overrightarrow{01}) \to \mathrm{GL}_2(\mathbb{Z})$$

for the Legendre family maps the generators as follows:

$$x \mapsto \begin{pmatrix} 1 & 2 \\ & 1 \end{pmatrix}, \qquad y \mapsto \begin{pmatrix} 1 & \\ -2 & 1 \end{pmatrix}, \qquad z \mapsto \begin{pmatrix} 1 & -2 \\ 2 & -3 \end{pmatrix}.$$

Proof. The computation of the monodromy of the Legendre family of elliptic curves is classical, its Picard-Fuchs equation being a hypergeometric equation studied already by Gauß. The concrete matrices above can for example be found in [St81] on page 450. □

Remark 17. Note that the explicit formulae of Lemma 16 allow to conclude that inertia at 0 and 1 acts unipotently, while inertia at ∞ acts quasi-unipotently with Jordan normal form

$$\begin{pmatrix} -1 & 1 \\ & -1 \end{pmatrix}.$$

Indeed, the reduction of the Legendre family is semistable at $0, 1$ and additive at ∞.

5.2. **Unipotent subgroups up to conjugation.** Let $U \subseteq \mathrm{GL}_2(\mathbb{Z}_\ell)$ be a nontrivial unipotent subgroup. Then

$$L_U = \ker(\mathbf{1} - U) \subset \mathbb{Z}_\ell \times \mathbb{Z}_\ell$$

is a free and cotorsion free submodule of rank 1 and as such defines an element $L_U \in \mathbb{P}^1(\mathbb{Z}_\ell)$. Conversely, to a line $L \in \mathbb{P}^1(\mathbb{Z}_\ell)$ we associate the unipotent subgroup

$$U(L) = \{A \in \mathrm{GL}_2(\mathbb{Z}_\ell) \,;\, A|_L = \mathrm{id}_L \text{ and } \det(A) = 1\}.$$

Clearly, $U \subseteq U(L_U)$ and unipotent subgroups of the form U_L are maximal among unipotent subgroups with respect to inclusion.

Lemma 18. *Every nontrivial unipotent subgroup U of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ is contained in a unique maximal unipotent subgroup, namely $U(L_U)$. The map $U \mapsto L_U$ defines a bijection*

$$\{\textit{maximal unipotent subgroups of } \mathrm{GL}_2(\mathbb{Z}_\ell)\} \;\longleftrightarrow\; \mathbb{P}^1(\mathbb{Z}_\ell).$$

Proof. The map $L \mapsto U(L)$ is the inverse map. □

5.3. **Recognizing cusps via unipotent subgroups.** It follows from Lemma 18 that $\mathrm{GL}_2(\mathbb{Z}_\ell)$ acts transitively by conjugation on the set of its maximal unipotent subgroups. However, this changes if we consider only the conjugation action by a suitable subgroup.

Lemma 19. *The maximal unipotent subgroups U_0, U_1, and U_∞ of $\mathrm{GL}_2(\mathbb{Z}_2)$ containing the images of (the square of) inertia in the 2-adic geometric monodromy representation of the Legendre family*

$$\rho_{\mathrm{Leg}}(I_0), \rho_{\mathrm{Leg}}(I_1), \text{ and respectively } \rho_{\mathrm{Leg}}((I_\infty)^2)$$

are mutually not conjugate under the image $\rho_{\mathrm{Leg}}\big(\pi_1(\mathbb{P}^1_{\bar{\mathbb{Q}}} - \{0,1,\infty\}, \overrightarrow{01})\big)$.

Proof. The Legendre family has trivial 2-torsion as is reflected by $\rho_{\mathrm{Leg}}^{\mathrm{top}}$ mapping to the subgroup $\Gamma(2) \subset \mathrm{SL}_2(\mathbb{Z})$ of elements $\equiv \mathbf{1} \bmod 2$. This is inherited by the profinite completion ρ_{Leg}. We deduce that conjugation by elements from $\mathrm{im}(\rho_{\mathrm{Leg}})$ only moves maximal unipotent subgroups within the fibre of the mod 2 reduction

$$\mathbb{P}^1(\mathbb{Z}_2) \twoheadrightarrow \mathbb{P}^1(\mathbb{F}_2) = \{0,1,\infty\}.$$

Now x fixes $\binom{1}{0}$, and y fixes $\binom{0}{1}$ and z^2 fixes $\binom{1}{1}$, so that U_0, U_1, and U_∞ map to three different elements in $\mathbb{P}^1(\mathbb{F}_2)$. □

5.4. **Enough families of elliptic curves.** We are now in a position to treat Selmer sections that behave like cuspidal sections with respect to the dichotomy of Theorem 10.

Theorem 20. *Let $s : \mathrm{Gal}_k \to \pi_1(X)$ be a birational lifting section of a hyperbolic curve X over a number field k with smooth completion $\overline{X}$. If the associated adele $\underline{x}(s) = (x_v)$ is cuspidal or degenerate with respect to $X \subseteq \overline{X}$ at all but finitely many places of k, then s is a cuspidal section.*

Proof. Let $Y = \overline{X} \setminus X$ be the complement. Since the assumptions are inherited by neighbourhoods, it suffices to show that $Y(k) \neq \emptyset$ and apply the limit argument in the version for cuspidal sections, see Section §2.1.3.

We consider the following map defined on almost all places of k:

$$v \mapsto y_v \in Y$$

where we assign to a cuspidal or degenerate place v of k the closed point y_v of Y such that the closure of x_v and y_v in a model over $\mathfrak{o}_v$ intersect in the special fibre.

Let $\beta : U \to \mathbb{P}^1 - \{0, 1, \infty\}$ be a finite map defined on an open $U \subseteq X$. We lift s to a section of $\pi_1(U/k)$ and apply Theorem 10 to this lift and $\beta^* E_\lambda / U$. Since $\underline{x}(s)$ does not change with the lift, we are still in the second case of the conclusion of Theorem 10. The 2-adic representation induced by the section factors through

$$\begin{pmatrix} \delta\varepsilon & * \\ & \delta \end{pmatrix} \subseteq \mathrm{GL}_2(\mathbb{Z}_2),$$

which is a pro-2 group. By passing to a neighbourhood $h : U' \to U$ of s we may assume that

$$\rho_{h^*\beta^* E_\lambda/U',2} : \pi_1(U') \to \mathrm{GL}_2(\mathbb{Z}_2)$$

factors through a pro-2 group. Let S be a finite set of places containing all the bad places for $h^*\beta^* E_\lambda / U'$ and the places dividing 2. Let $\mathscr{U}' / \mathrm{Spec}(\mathfrak{o}_{k,S})$ be a hyperbolic curve model of U'/k. Denote by $\pi_1^{(2)}(-)$ the fibrewise pro-2 fundamental group. Then the representations factor as

$$\begin{array}{ccccc} \pi_1^{(2)}(U') & \xrightarrow{\mathrm{sp}} & \pi_1^{(2)}(\mathscr{U}') & \xrightarrow{\rho_{h^*\beta^* E_\lambda/U',2}} & \mathrm{GL}_2(\mathbb{Z}_2) \\ {\scriptstyle \mathrm{pr}_*}\downarrow \uparrow{\scriptstyle s} & \nearrow{\scriptstyle \mathrm{sp}\circ s} & {\scriptstyle \mathrm{pr}_*}\downarrow & & \\ \mathrm{Gal}_k & \twoheadrightarrow & \pi_1(\mathrm{Spec}(\mathfrak{o}_{k,S})) & & \end{array}$$

The specialisation map $\mathrm{sp} : \pi_1^{(2)}(U') \to \pi_1^{(2)}(\mathscr{U}')$ is an isomorphism on the kernels of the respective projections pr_*. Let $v \nmid 2$ be a cuspidal or degenerate place, and let $D_v \subset \mathrm{Gal}_k$ be a choice of a decomposition subgroup at v. Then, as x_v degenerates into y_v we find that

$$\mathrm{sp} \circ s(D_v) \text{ cyclotomically normalizes } I_{y'_v} \tag{5.1}$$

where $I_{y'}$ denotes the inertia group of $y' \in Y' = \overline{X'} \setminus X'$ in $\pi_1^{(2)}(U'_{\bar{k}}) \subseteq \pi_1^{(2)}(\mathscr{U}')$. Here **cyclotomically normalizing** means that the induced action by conjugation is via the cyclotomic character. Due to neglecting base points and choice of prolongations of places, these inertia and decomposition groups are only well defined up to conjugation and (5.1) has to be considered as holding for suitable choices within the conjugacy classes of these groups. Because of

$$\rho_{s,h^*\beta^* E_\lambda/U',2}(D_v) \subseteq \begin{pmatrix} \delta\varepsilon & * \\ & \delta \end{pmatrix},$$

depending on whether or not $* = 0$ for the restriciton of the representation to D_v, there are two:

$$U_+ = \begin{pmatrix} 1 & * \\ & 1 \end{pmatrix} \text{ and } U_- = \begin{pmatrix} 1 & \\ * & 1 \end{pmatrix},$$

or a unique maximal unipotent subgroup normalized by D_v. But in any case only U_+ is cyclotomically normalized. This maximal unipotent subgroup is independent of v and thus must by (5.1) be conjugate to the image of $I_{y'_v}$. We conclude with Lemma 19 that

$$\beta(y_v) = \beta(h(y'_v)) \in \{0, 1, \infty\}$$

is also independent of v.

By Riemann-Roch, it is easy to find for any partition $Y = Y_0 \amalg Y_\infty$ a suitable $U \subseteq X$ and a finite $\beta : U \to \mathbb{P}^1 - \{0, 1, \infty\}$ with $\beta(Y_0) = \{0\}$ and $\beta(Y_\infty) = \infty$. We conclude that $v \mapsto y_v$ must be a constant function, i.e., all local points x_v degenerate or are cuspidal with the very same point $y \in Y$. This means in particular, that the residue field extension $\kappa(y)/k$ has a split place above almost all places v of k, and this is only possible if $\kappa(y) = k$ by the classical Lemma 21 below. Thus $y \in Y(k)$ and this finishes the proof. □

Lemma 21. *Let F/K be a finite extension of number fields such that for all but finitely many places of v there is a place w of E with the same residue field. Then we have necessarily $E = F$.*

Proof. Let E/K be a Galois hull of F/K and let $G = \mathrm{Gal}(E/K) \supseteq H = \mathrm{Gal}(F/K)$ be the respective Galois groups. The assumption says that for all but finitely many v the conjugacy class of Frobenius elements at places $w \mid v$ meets H nontrivially. But since every element of G is a Frobenius element infinitely often, this implies that G is the union of the conjugates of H. This is only possible if $G = H$ and thus $F = K$ as claimed. □

References

[EsHa08] Esnault, H., Hai, Ph. H., Packets in Grothendieck's Section Conjecture, *Advances in Mathematics* **218** (2008), no. 2, 395–416.

[HSx10] Harari, D., Stix, J., Descent obstruction and fundamental exact sequence, in: *The arithmetic of fundamental groups — PIA 2010*, editor Jakob Stix, Contributions in Mathematical and Computational Science **2**, Springer, 2012, chapter 7, 147–166.

[Gr83] Grothendieck, A., Brief an Faltings (27/06/1983), in: *Geometric Galois Action 1* (ed. L. Schneps, P. Lochak), LMS Lecture Notes **242**, Cambridge, 1997, 49–58.

[Ko05] Koenigsmann, J., On the 'section conjecture' in anabelian geometry, *J. Reine Angew. Math.* **588** (2005), 221–235.

[La65] Lazard, M., Groupes analytiques p-adiques, *Publications mathématiques de l'IHES* **26** (1965), 5–219.

[Mz04] Mochizuki, S., Noncritical Belyi maps, *Math. J. Okayama Univ.* **46** (2004), 105–113.

[Na90] Nakamura, H., Galois rigidity of the étale fundamental groups of punctured projective lines, *J. Reine Angew. Math.* **411** (1990), 205–216.

[NSW08] Neukirch, J., Schmidt, A., Wingberg, K., *Cohomology of number fields*, second edition, Grundlehren der Mathematischen Wissenschaften **323**, Springer, 2008, xvi + 825pp.

[St81] Stiller, P. F., Monodromy and invariants of elliptic surfaces, *Pacific J. Math.* **92** (1981), no. 2, 433–452.

[St07] Stoll, M., Finite descent obstructions and rational points on curves, *Algebra & Number Theory* **1** (2007), 349–391.

[Sti13] Stix, J., *Rational Points and Arithmetic of Fundamental Groups, Evidence for the Section Conjecture*, Springer Lecture Notes in Mathematics **2054**, Springer Verlag, 2013, xx + 249pp.

Jakob Stix, Institut für Mathematik, Goethe–Universität Frankfurt, Robert-Mayer-Str. 6–8, 60325 Frankfurt am Main, Germany

E-mail address: stix@math.uni-frankfurt.de