Notes on the Iwasawa theory for elliptic curves

Samy Mkhinini

PhD in Mathematics

Iwasawa theory & p-adic Hodge theory

October 14, 2026

1 Selmer groups

Let E be an elliptic curve over a number field F.

Theorem 1.1 (Mordell–Weil)**.** *$E(F)$ is a finitely generated abelian group.*

Theorem 1.2 (Weak Mordell–Weil)**.** *For any integer $m \geq 2$, the group*

$$E(F)/mE(F)$$

is finite.

Proof. Let $P \in E(F)$ be a point and choose $Q \in E(\overline{F})$ such that $mQ = P$. The map

$$\begin{aligned} \varphi_Q \colon G_F &\longrightarrow E[m] \\ \sigma &\longmapsto \sigma(Q) - Q \end{aligned}$$

is a 1-cocycle. Let $c_P = [\varphi_Q]$ be the class of φ_Q in $H^1(F, E[m])$. Let Q' be another point such that $mQ' = P$. Then

$$\varphi_Q - \varphi_{Q'}$$

is a 1-coboundary, so c_P depends only on P. Indeed, $\varphi_Q - \varphi_{Q'} \in B^1(G_F, E[m])$, and hence $[\varphi_Q] = [\varphi_{Q'}]$. Thus, the map

$$\begin{aligned} k \colon E(F) &\longrightarrow H^1(F, E[m]) \\ P &\longmapsto c_P \end{aligned}$$

is clearly a homomorphism. Then,

$$\begin{aligned} P \in \ker(k) &\iff c_P = 0 \text{ in } H^1(F, E[m]) \\ &\iff c_P \text{ is a 1-coboundary} \\ &\iff \exists R \in E[m],\ \forall \sigma \in G_F,\ \sigma(Q) - Q = \sigma(R) - R \\ &\iff \exists R \in E[m],\ \forall \sigma \in G_F,\ \sigma(Q - R) = Q - R \\ &\iff \exists R \in E[m],\ Q - R \in E(F). \end{aligned}$$

Let $P \in \ker(k)$. There exists $R \in E[m]$ such that $Q - R \in E(F)$. Then,

$$P = mQ = mQ - mR = m(Q - R) \in mE(F),$$

since $mR = O$. Thus, $\ker(k) = mE(F)$. Then, the induced map

$$\begin{aligned} k \colon E(F)/mE(F) &\hookrightarrow H^1(F, E[m]) \\ P &\longmapsto c_P \end{aligned}$$

is injective. This is the Kummer map for the $[m]$-endomorphism of E. Let v be a finite place of F not dividing m and such that E has good reduction at v. This excludes only finitely many places of F, which we denote by Σ. Let k_v be the residue field of v, and let $\ell = \mathrm{char}(k_v)$. Let $\widetilde{E}$ be the reduction of E modulo v, which is an elliptic curve over k_v. As $\ell \nmid m$, the reduction map

$$E[m] \xrightarrow{\sim} \widetilde{E}[m]$$

is an isomorphism on m-torsion. Let $\sigma \in I_v$. Then σ acts trivially on $\widetilde{E}$, and so $\sigma(Q)$ and Q have the same image in $\widetilde{E}$. In particular,

$$\sigma(Q) - Q$$

reduces to the origin in $\widetilde{E}$. But $\sigma(Q) - Q \in E[m]$, and so, by injectivity of the reduction map on $E[m]$,

$$\sigma(Q) - Q = O.$$

The restriction of φ_Q to I_v is a 1-coboundary. This means that

$$\begin{aligned} \mathrm{im}(k) &\subseteq \ker\left(H^1(F, E[m]) \xrightarrow{\mathrm{res}} \prod_{v \notin \Sigma} H^1(I_v, E[m]) \right) \\ &= H^1(G_{F,\Sigma}, E[m]), \end{aligned}$$

and we obtain:

$$\begin{aligned} k \colon E(F)/mE(F) &\hookrightarrow H^1(G_{F,\Sigma}, E[m]) \\ P &\longmapsto c_P. \end{aligned}$$

The key point is that $H^1(G_{F,\Sigma}, E[m])$ is finite. Indeed, let $L = F(E[m]) \subseteq F_\Sigma$ be the finite Galois extension of F obtained by adjoining the coordinates of points in $E[m]$. We have an exact sequence

$$1 \longrightarrow \mathrm{Gal}(F_\Sigma/L) \longrightarrow G_{F,\Sigma} \longrightarrow \mathrm{Gal}(L/F) \longrightarrow 1,$$

and the inflation-restriction sequence gives

$$0 \longrightarrow H^1\big(\mathrm{Gal}(L/F), E[m]^{\mathrm{Gal}(F_\Sigma/L)}\big) \longrightarrow H^1(G_{F,\Sigma}, E[m]) \longrightarrow H^1\big(\mathrm{Gal}(F_\Sigma/L), E[m]\big)^{\mathrm{Gal}(L/F)}.$$

Then, we obtain:

$$0 \longrightarrow H^1\big(\mathrm{Gal}(L/F), E[m]^{\mathrm{Gal}(F_\Sigma/L)}\big) \longrightarrow H^1(G_{F,\Sigma}, E[m]) \longrightarrow H^1\big(\mathrm{Gal}(F_\Sigma/L), E[m]\big).$$

The group $H^1\big(\mathrm{Gal}(L/F), E[m]^{\mathrm{Gal}(F_\Sigma/L)}\big)$ is finite, as both $\mathrm{Gal}(L/F)$ and $E[m]$ are finite. Since $\mathrm{Gal}(F_\Sigma/L)$ acts trivially on $E[m]$, we have

$$H^1\big(\mathrm{Gal}(F_\Sigma/L), E[m]\big) = \mathrm{Hom}\big(\mathrm{Gal}(F_\Sigma/L), E[m]\big).$$

Any homomorphism

$$\mathrm{Gal}(F_\Sigma/L) \longrightarrow E[m]$$

factors through the Galois group over L of the maximal abelian extension M of L of exponent m that is unramified outside the finitely many places of L dividing a place in Σ. By class field theory, M/L is finite. But,

$$\mathrm{Hom}\big(\mathrm{Gal}(F_\Sigma/L), E[m]\big) \simeq \mathrm{Hom}\big(\mathrm{Gal}(M/L), E[m]\big),$$

so $\mathrm{Hom}\big(\mathrm{Gal}(F_\Sigma/L), E[m]\big)$ is finite. Thus, $H^1(G_{F,\Sigma}, E[m])$ lies between two finite groups, and is therefore finite. Finally, we have an inclusion $E(F)/mE(F) \hookrightarrow H^1(G_{F,\Sigma}, E[m])$, and $E(F)/mE(F)$ is finite. □

The Kummer map $P \xmapsto{k} c_P$ is defined for elliptic curves over any field, in particular over each completion F_v of F. For each place v of F, the natural inclusion $F \hookrightarrow F_v$ induces the following commutative diagram

$$\begin{array}{ccc} E(F)/mE(F) & \xrightarrow{\quad k \quad} & H^1(F, E[m]) \\ \downarrow & & \downarrow{\scriptstyle \mathrm{res}_v^m} \\ E(F_v)/mE(F_v) & \xrightarrow[k_v]{} & H^1(F_v, E[m]). \end{array}$$

We define the Selmer group for the multiplication by m map on E

$$\mathrm{Sel}_m(E/F) := \left\{ c \in H^1(F, E[m]) : \mathrm{res}_v^m(c) \in \mathrm{im}(k_v), \forall v \right\}.$$

Since the diagram commutes, we obtain $\mathrm{im}(k) \subset \mathrm{Sel}_m(E/F)$. Moreover, if $v \nmid m$ and E has good reduction at v, then:

$$\mathrm{im}(k_v) \subset \ker\left(H^1(F_v, E[m]) \xrightarrow{\mathrm{res}} H^1(I_v, E[m]) \right),$$

and $\mathrm{Sel}_m(E/F) \subset H^1(G_{F,\Sigma}, E[m])$. From the short exact sequence

$$0 \longrightarrow E[m] \longrightarrow E \xrightarrow{m} E \longrightarrow 0,$$

we also have:

$$0 \longrightarrow E(F)/mE(F) \xrightarrow{k} H^1(F, E[m]) \xrightarrow{\alpha} H^1(F, E)[m] \longrightarrow 0$$

and

$$0 \longrightarrow E(F_v)/mE(F_v) \xrightarrow{k_v} H^1(F_v, E[m]) \xrightarrow{\alpha_v} H^1(F_v, E)[m] \longrightarrow 0.$$

Exactness at $H^1(F_v, E[m])$ implies

$$\begin{aligned} \mathrm{im}(k_v) &= \ker\left(H^1(F_v, E[m]) \xrightarrow{\alpha_v} H^1(F_v, E)[m] \right) \\ &= \ker\left(H^1(F_v, E[m]) \xrightarrow{\alpha_v} H^1(F_v, E) \right). \end{aligned}$$

Thus, we can rewrite the Selmer group as

$$\mathrm{Sel}_m(E/F) := \ker\left(H^1(F, E[m]) \xrightarrow{\mathrm{res}} \prod_v H^1(F_v, E) \right).$$

Moreover, we have:

$$\begin{aligned} \mathrm{im}(k) &= \ker\left(H^1(F, E[m]) \xrightarrow{\alpha} H^1(F, E) \right) \\ &= \ker\left(\mathrm{Sel}_m(E/F) \xrightarrow{\alpha} H^1(F, E) \right). \end{aligned}$$

Proposition 1.3. *There is a fundamental exact sequence*

$$0 \longrightarrow E(F)/mE(F) \xrightarrow{k} \mathrm{Sel}_m(E/F) \xrightarrow{\alpha^{\mathrm{Ш}}} Ш(E/F)[m] \longrightarrow 0,$$

where $Ш(E/F) := \ker\left(H^1(F, E) \xrightarrow{\mathrm{res}^E} \prod_v H^1(F_v, E) \right)$ *is the Shafarevich–Tate group of E over F.*

Proof. We first show that $\alpha^{\mathrm{Ш}} := \alpha|_{\mathrm{Sel}_m(E/F)}$ is well-defined. Let $c \in \mathrm{Sel}_m(E/F)$. We have $\alpha^{\mathrm{Ш}}(c) = \alpha(c)$. Let v be a place of F. Then,

$$\mathrm{res}_v^E(\alpha(c)) = \alpha_v(\mathrm{res}_v^m(c)) = 0,$$

since $\mathrm{res}_v^m(c) \in \mathrm{im}(k_v) = \ker(\alpha_v)$. But $\alpha^{\mathrm{Ш}}(c)$ is also killed by m, so we deduce that $\alpha^{\mathrm{Ш}}(c) \in Ш(E/F)[m]$. Exactness at $\mathrm{Sel}_m(E/F)$ is clear, since changing the codomain does not change the kernel. It remains to show that $\mathrm{Sel}_m(E/F) \longrightarrow Ш(E/F)[m]$ is surjective. Let $s \in Ш(E/F)[m]$. In particular, s is in $H^1(F, E)[m]$. Since $H^1(F, E[m]) \xrightarrow{\alpha} H^1(F, E)[m]$ is surjective, there exists $c \in H^1(F, E[m])$ such that $s = \alpha(c)$. But $\mathrm{res}^E(s) = 0$, so we obtain:

$$\begin{aligned} 0 &= \mathrm{res}_v^E(s), \ \forall v \\ &= \mathrm{res}_v^E(\alpha(c)), \ \forall v \\ &= \alpha_v(\mathrm{res}_v^m(c)), \ \forall v \end{aligned}$$

and $\mathrm{res}_v^m(c) \in \ker(\alpha_v) = \mathrm{im}(k_v)$. Hence, $c \in \mathrm{Sel}_m(E/F)$ by definition, and

$$s = \alpha(c) = \alpha|_{\mathrm{Sel}_m(E/F)}(c) = \alpha^{Ш}(c).$$

So, we are done. □

The Selmer groups behave compatibly as m varies and under extensions of the base field F. Indeed, if $m \mid m'$, then $E[m] \subset E[m']$, and $H^1(F, E[m]) \twoheadrightarrow H^1(F, E[m'])[m]$. So, there is a surjection

$$\mathrm{Sel}_m(E/F) \twoheadrightarrow \mathrm{Sel}_{m'}(E/F)[m].$$

Moreover,

$$\begin{aligned}\ker\left(\mathrm{Sel}_m(E/F) \longrightarrow \mathrm{Sel}_{m'}(E/F)[m]\right) &= \ker\Big(H^1(F, E[m]) \longrightarrow H^1(F, E[m'])[m]\Big) \\ &= \frac{E[m'/m](F)}{mE[m'](F)}.\end{aligned}$$

If F'/F is a finite extension, then $H^1(F, E[m]) \longrightarrow H^1(F', E[m])$ induces a homomorphism $\mathrm{Sel}_m(E/F) \longrightarrow \mathrm{Sel}_m(E/F')$. Furthermore, if F'/F is Galois, then the Galois group $\mathrm{Gal}(F'/F)$ acts on $H^1(F', E[m])$ and defines an action on $\mathrm{Sel}_m(E/F')$, and the subgroup of $\mathrm{Gal}(F'/F)$-invariants contains the image of $\mathrm{Sel}_m(E/F)$.

We define the p^∞-Selmer group of E by taking the direct limit over n of the p-power Selmer groups $\mathrm{Sel}_{p^n}(E/F)$, i.e.

$$\mathrm{Sel}_{p^\infty}(E/F) := \varinjlim_n \mathrm{Sel}_{p^n}(E/F).$$

Since $\varinjlim_n H^1(F, E[p^n]) = H^1(F, E[p^\infty])$, the p^∞-Selmer group of E can be defined as:

$$\begin{aligned}\mathrm{Sel}_{p^\infty}(E/F) &= \Big\{c \in H^1(F, E[p^\infty]) : \mathrm{res}_v(c) \in \mathrm{im}(k_v), \forall v\Big\} \\ &= \ker\left(H^1(F, E[p^\infty]) \xrightarrow{\mathrm{res}} \prod_v H^1(F_v, E)\right).\end{aligned}$$

There is a natural surjection $H^1(F, E[p^n]) \twoheadrightarrow H^1(F, E[p^\infty])[p^n]$, which induces a surjection

$$\mathrm{Sel}_{p^n}(E/F) \twoheadrightarrow \mathrm{Sel}_{p^\infty}(E/F)[p^n]$$

whose kernel is $E[p^\infty](F)/p^nE[p^\infty](F)$. Taking the direct limit of the fundamental exact sequences associated with multiplication by p^n, we obtain:

$$0 \longrightarrow E(F) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \mathrm{Sel}_{p^\infty}(E/F) \longrightarrow Ш(E/F)[p^\infty] \longrightarrow 0.$$

In what follows, our goal will be to describe $\mathrm{Sel}_{p^\infty}(E/F)$ solely in terms of $E[p^\infty]$, i.e. without any reference to the full curve E.

Let v be a place of F such that $v \nmid p$. We first consider the case where $v \nmid p\infty$. If $\ell = \mathrm{char}(k_v)$, then $E(F_v)$ contains a pro-ℓ-subgroup of finite index, denoted by $E_1(F_v)$. In particular, we have a short exact sequence

$$0 \longrightarrow E_1(F_v) \longrightarrow E(F_v) \longrightarrow E(F_v)/E_1(F_v) \longrightarrow 0.$$

Since $\ell \neq p$, the multiplication-by- p map is an automorphism of $E_1(F_v)$. Then,

$$E_1(F_v)/p^nE_1(F_v) = 0,$$

for all $n \geq 1$. Moreover, we have $E(F_v)/E_1(F_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0$, since $E(F_v)/E_1(F_v)$ is finite and $\mathbb{Q}_p/\mathbb{Z}_p$ is divisible. Tensoring the previous short exact sequence with $\mathbb{Q}_p/\mathbb{Z}_p$, we obtain:

$$E_1(F_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow E(F_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow E(F_v)/E_1(F_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow 0,$$

which gives the following short exact sequence:

$$0 \longrightarrow E(F_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow 0 \longrightarrow 0.$$

It follows that $E(F_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0$. In the second case, suppose $v \mid \infty$. Then, F_v is either to $\mathbb{C}$ or $\mathbb{R}$. If $F_v = \mathbb{C}$, $E(\mathbb{C})$ is divisible and $E(\mathbb{C}) \otimes \mathbb{Z}/p^n\mathbb{Z} = 0$. It follows that $E(\mathbb{C}) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0$. If $F_v = \mathbb{R}$, we have a short exact sequence

$$0 \longrightarrow E(\mathbb{R})^0 \longrightarrow E(\mathbb{R}) \longrightarrow E(\mathbb{R})/E(\mathbb{R})^0 \longrightarrow 0,$$

where $E(\mathbb{R})^0$ is divisible (since it is isomorphic to $\mathbb{R}/\mathbb{Z}$) and $E(\mathbb{R})/E(\mathbb{R})^0$ is finite. By the same reasoning as before, we obtain:

$$E(\mathbb{R}) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0.$$

Taking the direct limit of the short exact sequences associated with k_v, we have:

$$0 \longrightarrow E(F_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0 \xrightarrow{k_v} H^1(F_v, E[p^\infty]) \xrightarrow{\alpha_v} H^1(F_v, E)[p^\infty] \longrightarrow 0.$$

Thus, $\mathrm{im}(k_v) = 0$, and the local condition at v defining $\mathrm{Sel}_{p^\infty}(E/F)$ reduces to $\mathrm{res}_v(\cdot) = 0$ in $H^1(F_v, E[p^\infty])$. Now assume that E has good reduction at v. Consider the map $H^1(F_v, E[p^\infty]) \longrightarrow H^1(I_v, E[p^\infty])$. We have

$$\begin{aligned}
\ker\left(H^1(F_v, E[p^\infty]) \to H^1(I_v, E[p^\infty])\right) &= \ker\left(H^1(F_v, E[p^\infty]) \to H^1(I_v, E[p^\infty])^{G_{F_v}/I_v}\right) \\
&= \ker\left(H^1(F_v, E[p^\infty]) \to H^1(I_v, E[p^\infty])\right) \\
&= H^1\left(G_{F_v}/I_v, E[p^\infty]^{I_v}\right) \\
&= H^1\left(G_{F_v}/I_v, E[p^\infty]\right),
\end{aligned}$$

where the first equality follows from the inclusion $H^1(I_v, E[p^\infty])^{G_{F_v}/I_v} \hookrightarrow H^1(I_v, E[p^\infty])$ and the last equality follows from the fact that I_v acts trivially on $E[p^\infty]$ since E has good reduction at v.

Lemma 1.4. *Let G be the profinite group $\widehat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z}$.*

1. *Let A be a discrete G-module. Denote by F the automorphism of A induced by the action of the canonical topological generator s of G, and let A' be a subgroup of A defined by*

$$A' = \left\{a \in A : \exists n \geq 1,\ (1 + F + ... + F^{n-1})(a) = 0\right\}.$$

Then, $(F-1)A$ is a subgroup of A' and

$$H^1(G, A) = A'/(F-1)A.$$

2. *If A is a torsion group, then $A' = A$.*

Proof. 1. $\underline{(F-1)A \text{ is a subgroup of } A'}$: Let $a \in A$ and $m \geq 1$. We have:

$$\begin{aligned}
(1 + F + ... + F^{m-1})(F(a) - a) &= F(a) - a + F(F(a) - a) + ... + F^{m-1}(F(a) - a) \\
&= F(a) - a + F^2(a) - F(a) + ... + F^m(a) - F^{m-1}(a) \\
&= F^m(a) - a.
\end{aligned}$$

For every $a \in A$, the stabilizer G_a of a is an open subgroup of G. Hence, there exists $n \geq 1$ such that

$$n\widehat{\mathbb{Z}} \subset G_a.$$

In particular, $n.1 = n.s = s^n \in G_a$ and

$$s^n \cdot a = F^n(a) = a,$$

i.e. $F^n(a) - a = 0$. Thus, $F(a) - a \in A'$ and $(F-1)A \subset A'$. Moreover, the image of A under $F - 1$ is a subgroup of A. Since A' is a subgroup of A, it follows that $(F-1)A$ is a subgroup of A'.

$Z^1(G, A)$ is isomorphic to A': Consider the map

$$\begin{array}{rccc} \varphi : Z^1(G,A) & \longrightarrow & A' \\ c & \longmapsto & c(s) \end{array}.$$

We first verify that φ is well-defined, i.e. that $\mathrm{im}(\varphi) \subset A'$. Let $c \in Z^1(G, A)$. Since c is a 1-cocycle, we have:

$$c(s^2) = c(s) + s \cdot c(s) = c(s) + F(c(s)).$$

Similarly, $c(s^3) = c(s^2) + s^2 \cdot c(s) = c(s) + F(c(s)) + F^2(c(s))$. By iteration, we obtain:

$$c(s^m) = (1 + F + ... + F^{m-1})(c(s)),$$

for all $m \geq 1$. Since A is discrete, $\{0\}$ is open in A. By continuity of c, the set $U = c^{-1}(\{0\})$ is open in G. Moreover, U is an open neighbourhood of 1_G, since $c(1_G) = 0$. We deduce that:

$$\exists n \geq 1,\ n\widehat{\mathbb{Z}} \subset U.$$

In particular, $s^n \in U$ and $c(s^n) = 0$. By our previous computation, we obtain $c(s) \in A'$ and φ is well-defined. Now, let $c \in Z^1(G, A)$ such that $\varphi(c) = 0$. It remains to show that $c \equiv 0$. By assumption, we have:

$$c(s^n) = 0,$$

for all $n \geq 1$. We also have $c(1_G) = 0$, so we obtain:

$$0 = c(1_G) = c(s^n.s^{-n}) = c(s^n) + s^n \cdot c(s^{-n}) = s^n \cdot c(s^{-n}).$$

But the action of s^n is an automorphism, so it follows that $c(s^{-n}) = 0$, and finally

$$c(s^n) = 0,$$

for all $n \in \mathbb{Z}$. Since $\langle s \rangle$ is dense in $\widehat{\mathbb{Z}}$, c is continuous, and A is Hausdorff, it follows that $c = 0$. Hence φ is injective. Now, let $a \in A'$. We have to construct a continuous 1-cocycle

$$\hat{c} : \widehat{\mathbb{Z}} \longrightarrow A$$

such that $\hat{c}(s) = a$. Since $a \in A'$, there exists $n \geq 1$ such that

$$(1 + F + ... + F^{n-1})(a) = 0.$$

So we consider the map

$$c : \mathbb{Z} \longrightarrow A$$

defined by $c(0) = 0, c(1) = a$, and for all $k \geq 1$,

$$c(k) = \sum_{j=0}^{k-1} F^j(a) \quad \text{and} \quad c(-k) = -\sum_{j=1}^{k} F^{-j}(a).$$

Let $k, l \geq 1$. We have:

$$\begin{aligned} c(k+l) &= \sum_{j=0}^{k+l-1} F^j(a) \\ &= \sum_{j=0}^{k-1} F^j(a) + \sum_{j=k}^{k+l-1} F^j(a) \\ &= c(k) + \sum_{j=0}^{l-1} F^{j+k}(a) \\ &= c(k) + F^k\left(\sum_{j=0}^{l-1} F^j(a)\right) \\ &= c(k) + k \cdot c(l), \end{aligned}$$

and c is a 1-cocycle. Moreover, c is n-periodic. Indeed, for all $k \in \mathbb{Z}$,

$$c(k+n) = c(k) + k \cdot c(n) = c(k) + k \cdot 0 = c(k),$$

since $c(n) = 0$ by construction. Thus, c factors through $\mathbb{Z}/n\mathbb{Z}$; denote the induced map by $\bar{c}$. But we still need to check that $\bar{c}$ is a 1-cocycle on $\mathbb{Z}/n\mathbb{Z}$, i.e. we need the following identity

$$\bar{c}(\bar{k} + \bar{l}) = \bar{c}(\bar{k}) + \bar{k} \cdot \bar{c}(\bar{l}) = c(k) + \bar{k} \cdot c(l),$$

where $\bar{k} \cdot c(l)$ should be equal to $F^k(c(l))$. We also need the action to factor through $\mathbb{Z}/n\mathbb{Z}$. Let $k \in \mathbb{Z}$ such that $\overline{k+n} = \bar{k}$ and let $x \in A$. We have:

$$\overline{k+n} \cdot x = F^{k+n}(x) \quad \text{and} \quad \bar{k} \cdot x = F^k(x).$$

So we need to have $F^{k+n}(x) = F^k(x)$, which is equivalent to $F^n(x) = x$ for all $x \in A$. However, this need not hold in general; at this stage, we know it only for elements of the form $x = F^j(a)$. So let us introduce the subgroup of A generated by the $F^j(a)$, i.e.

$$M := \langle F^j(a) : j \in \mathbb{Z} \rangle.$$

Actually, this doesn't change anything because the image of c was already in M by construction. Then, we have $F^n|_M = \mathrm{id}_M$ and the action of $\mathbb{Z}$ on M factors through $\mathbb{Z}/n\mathbb{Z}$. The preceding computations show that $\bar{c} \in Z^1(\mathbb{Z}/n\mathbb{Z}, M)$. Now define $\hat{c} : \widehat{\mathbb{Z}} \longrightarrow A$ by:

$$\hat{c}(g) = \bar{c}(\pi_n(g)),$$

for all $g \in \widehat{\mathbb{Z}}$, and where π_n denotes the canonical projection. Let $g, h \in G$. We have:

$$\begin{aligned} \hat{c}(gh) &= \bar{c}(\pi_n(gh)) \\ &= \bar{c}(\pi_n(g)\pi_n(h)) \\ &= \bar{c}(\pi_n(g)) + \pi_n(g) \cdot \bar{c}(\pi_n(h)) \\ &= \hat{c}(g) + \pi_n(g) \cdot \hat{c}(h). \end{aligned}$$

Then, $\pi_n(g) \cdot \hat{c}(h)$ must be equal to $g \cdot \hat{c}(h)$. By construction, s^n acts trivially on M, and so does every element of $\langle s^{nk} : k \in \mathbb{Z} \rangle$. Then, the set $\langle s^{nk} : k \in \mathbb{Z} \rangle$ is contained in G_x, for all $x \in M$. But G_x is also closed, so it contains the closure $\overline{\langle s^{nk} : k \in \mathbb{Z} \rangle} = n\widehat{\mathbb{Z}}$, and $n\widehat{\mathbb{Z}}$ acts trivially on M. Let $g, g' \in G$ such that $\pi_n(g) = \pi_n(g')$. Then, g and g' also have the same reduction in $\widehat{\mathbb{Z}}/n\widehat{\mathbb{Z}}$, since we have the isomorphism $\widehat{\mathbb{Z}}/n\widehat{\mathbb{Z}} \cong \mathbb{Z}/n\mathbb{Z}$. Hence, g and g' act in the same way on M. Then, we can define the action of $\pi_n(g)$ on M by

$$\pi_n(g) \cdot x := g \cdot x,$$

for all $x \in M$. It follows $\hat{c}$ is indeed a 1-cocycle. This action agrees with the previously defined action of $\mathbb{Z}/n\mathbb{Z}$. Indeed, let $g = s^k$ for some $k \in \mathbb{Z}$. We have:

$$\pi_n(s^k) \cdot x = \bar{k} \cdot x = F^k(x) = s^k \cdot x.$$

Moreover, $\hat{c}$ is continuous as a composition of continuous maps and we have:

$$\hat{c}(s) = \bar{c}(\pi_n(s)) = \bar{c}(\bar{1}) = c(1) = a.$$

Finally, for every $a \in A'$, we have constructed a continuous 1-cocycle $\hat{c} : G \longrightarrow A$ (since $M \hookrightarrow A$) such that

$$\varphi(\hat{c}) = \hat{c}(s) = a.$$

Then, φ is surjective.

$\underline{B^1(G,A) \text{ is isomorphic to } (F-1)A}$: By our previous work, we know that $B^1(G,A)$ is isomorphic to $\varphi(B^1(G,A))$. Let $c_b \in B^1(G,A)$ be a 1-coboundary defined by

$$c_b(g) = g \cdot b - b,$$

for some $b \in A$. It follows that $\varphi(c_b) = F(b) - b \in (F-1)A$. Let $x \in (F-1)A$. There exists $a \in A$ such that $x = (F-1)(a)$. So consider $c_a : G \longrightarrow A$ defined by $c_a(g) = g \cdot a - a$. Then, we obtain:

$$\varphi(c_a) = F(a) - a = x,$$

and $x \in \varphi(B^1(G,A))$.

2. Suppose that A is a torsion group. We have to show that $A' = A$. One inclusion is immediate. To prove the reserve inclusion, let $a \in A$. Since A is a discrete G-module, there exists (as noted at the beginning of the proof) $m \geq 1$ such that $F^m(a) = a$. Since A is a torsion group, there also exists $r \geq 1$ such that $ra = 0$. Set $n = mr$, we have:

$$\begin{aligned}(1 + F + ... + F^{mr-1})(a) &= (1 + F + ... + F^{mr-m} + F^{mr-(m-1)} ... + F^{mr-1})(a) \\ &= \sum_{j=0}^{r-1} F^{jm} \left(\sum_{k=0}^{m-1} F^k(a) \right).\end{aligned}$$

But, we also have $F^{jm}(F^k(a)) = F^k((F^m \circ ... \circ F^m)(a)) = F^k(a)$. Then, we obtain:

$$\sum_{j=0}^{r-1} F^{jm} \left(\sum_{k=0}^{m-1} F^k(a) \right) = \sum_{j=0}^{r-1} \sum_{k=0}^{m-1} F^{jm}(F^k(a)) = r \sum_{k=0}^{m-1} F^k(a) = \sum_{k=0}^{m-1} F^k(ra) = 0$$

and finally $a \in A'$.

□

Applying the lemma yields:

$$H^1\left(G_{F_v}/I_v, E[p^\infty]\right) = E[p^\infty]/(\text{Frob}_v - 1)E[p^\infty].$$

But $E[p^\infty]$ is divisible and 1 is not an eigenvalue of the action of Frob_v on $T_p\widetilde{E} \cong T_pE$, so $\text{Frob}_v - 1$ is surjective on $E[p^\infty]$ and $E[p^\infty]/(\text{Frob}_v - 1)E[p^\infty] = 0$. Thus, we obtain:

$$\ker\left(H^1(F_v, E[p^\infty]) \to H^1(I_v, E[p^\infty])\right) = 0.$$

Then, for any $c_v \in H^1(F_v, E[p^\infty])$, we have:

$$c_v = 0 \iff c_v|_{I_v} = 0 \iff c_v \text{ is unramified at } v.$$

Hence, we can rewrite the p^∞-Selmer group as

$$\begin{aligned}\mathrm{Sel}_{p^\infty}(E/F) &= \ker\left(H^1(F,E[p^\infty]) \xrightarrow{\mathrm{res}} \prod_{v\nmid p} H^1(F_v,E[p^\infty]) \times \prod_{v\mid p} H^1(F_v,E)\right)\\ &= \ker\left(H^1(G_{F,\Sigma},E[p^\infty]) \xrightarrow{\mathrm{res}} \prod_{\substack{v\in\Sigma\\ v\nmid p}} H^1(F_v,E[p^\infty]) \times \prod_{v\mid p} H^1(F_v,E)\right)\\ &= \ker\left(H^1(G_{F,\Sigma},E[p^\infty]) \xrightarrow{\mathrm{res}} \prod_{\substack{v\in\Sigma\\ v\nmid p}} H^1(F_v,E[p^\infty]) \times \prod_{v\mid p} H^1(F_v,E[p^\infty])/\operatorname{im}(k_v)\right).\end{aligned}$$

Let $v \mid p$. To complete our description, it remains to describe $\operatorname{im}(k_v)$ solely in terms of $E[p^\infty]$. Recall that there is a canonical isomorphism

$$T_pE \otimes \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{\sim} E[p^\infty].$$

Suppose that E has either good ordinary reduction or multiplicative reduction at v. There is a G_{F_v}-filtration of T_pE:

$$0 \longrightarrow T_v^+ \longrightarrow T_pE \longrightarrow T_pE/T_v^+ \longrightarrow 0,$$

such that T_pE/T_v^+ is unramified. Hence, the representation $\rho : G_{F_v} \longrightarrow \mathrm{Aut}_{\mathbb{Z}_p}(T_pE/T_v^+)$ factors through G_{F_v}/I_v. Moreover, the action of Frob_v on T_pE/T_v^+ is well-defined and is given by

$$\rho(\mathrm{Frob}_v) = \begin{cases} \times\ \alpha_p, & \text{if } E \text{ has good (ordinary) reduction,}\\ \times\ a_v(E), & \text{if } E \text{ has multiplicative reduction,}\end{cases}$$

where $\alpha_p \in \mathbb{Z}_p^\times$ is a root of $x^2 - a_v(E)x + p$. This leads to the following proposition:

Proposition 1.5. $\operatorname{im}(k_v) = \operatorname{im}\left(H^1\left(F_v, T_v^+ \otimes \mathbb{Q}_p/\mathbb{Z}_p\right) \longrightarrow H^1\left(F_v, E[p^\infty]\right)\right)_{\mathrm{div}}$

Proof. See [Gre98, Proposition 2.2]. □

References

[Gre98] Ralph Greenberg. "Iwasawa theory for elliptic curves". In: *arXiv preprint math/9809206* (1998).

[Ski18] Christopher Skinner. "Lectures on the Iwasawa theory of elliptic curves". In: *Lecture Notes for the Arizona Winter School*. 2018.