Contents

Euler systems and Kolyvagin systems

Karl Rubin

IAS/Park City Mathematics Series
Volume XX, XXXX

Euler systems and Kolyvagin systems

Karl Rubin

Department of Mathematics, UC Irvine, Irvine CA 92617 USA
E-mail address: krubin@math.uci.edu

LECTURE 1

Galois cohomology

We begin with a *very* quick and selective introduction to the facts from group cohomology and Galois cohomology that will be needed for the following lectures. For basic details see [**AW, Gr, Se2**], and for some of the more advanced results see [**Se1, Mi**]. For another quick overview see the lectures of Tate [**Ta3**] from PCMI 1999. We omit most proofs, although accessible ones are often given as exercises.

1.1. G-modules.

Suppose G is a group. A *G-module* is an abelian group A with an action of G on A that respects the group operation on A. That is, there is a map

$$G \times A \longrightarrow A$$

such that, if we let ga (or sometimes a^g) denote the image of (g, a) in A, then

$$(gh)a = g(ha), \qquad g(a + b) = ga + gb$$

for $g, h \in G$ and $a, b \in A$. Define the fixed subgroup

$$A^G = \{a \in A : ga = a \text{ for every } g \in G\}.$$

Example 1.1.1. If X is an abelian group we can view X as a G-module with trivial G action, and then $X^G = X$.

Example 1.1.2. If F/K is a Galois extension of fields and $G = \mathrm{Gal}(F/K)$, then F and $F^\times$ are G-modules. More generally, if $\mathcal{H}$ is an algebraic group defined over K, then the group of F-points $\mathcal{H}(F)$ is a G-module and $\mathcal{H}(F)^G = \mathcal{H}(K)$.

Example 1.1.3. If A and B are G-modules and $\varphi : A \to B$ is a group homomorphism, we define a new group homomorphism $g\varphi$ for $g \in G$ by $(g\varphi)(a) = g(\varphi(g^{-1}a))$. This makes $\mathrm{Hom}(A, B)$ into a G-module, and $\mathrm{Hom}(A, B)^G$ is the group of G-module homomorphisms from A to B.

We say that a G module A is *co-induced* if $A \cong \mathrm{Hom}(\mathbf{Z}[G], X)$ for some abelian group X.

Exercise 1.1.4. Suppose A is a G-module, and A_0 is the G-module whose underlying abelian group is A, but whose G action is trivial. Show that the map $a \mapsto \varphi_a$, where $\varphi_a(g) = g^{-1}a$, is an injection from A to the co-induced module $\mathrm{Hom}(\mathbf{Z}[G], A_0)$.

1.2. Characterization of the cohomology groups.

For this section suppose that the group G is finite. For every G-module A, there are abelian (cohomology) groups $H^i(G, A)$ for $i \geq 0$. For an explicit definition using cocycles and coboundaries, see [**AW, Se2**]. We will omit the definition, and just make use of the following properties.

Theorem 1.2.1. *There is a unique collection of functors $H^i(G, \,\cdot\,)$ from G-modules to abelian groups, for $i \geq 0$, satisfying the following properties:*

1. *$H^0(G, A) = A^G$ for every G-module A.*
2. *If $0 \to A \to B \to C \to 0$ is a short exact sequence of G-modules, then there is a (functorial) long exact sequence*

$$0 \to H^0(G,A) \to H^0(G,B) \to H^0(G,C) \to H^1(G,A) \to H^1(G,B) \to \cdots$$
$$\cdots \to H^i(G,A) \to H^i(G,B) \to H^i(G,C) \to H^{i+1}(G,A) \to \cdots$$

3. *If A is co-induced, then $H^i(G, A) = 0$ for all $i \geq 1$.*

Exercise 1.2.2. Show that the three properties above determine the cohomology groups $H^i(G, A)$ uniquely (assuming they exist). Hint: use induction and the fact (Exercise 1.1.4) that for every G-module A there is a short exact sequence $0 \to A \to B \to C \to 0$ with B co-induced.

In these lectures we will only make use of $H^i(G, A)$ for $i \leq 2$ (and mostly $i \leq 1$). When $i = 0$ the groups are described explicitly by condition (1) of Theorem 1.2.1; when $i = 1$ we have the following explicit description.

Define $C^1(G, A)$ (the 1-cochains) to be the group of (set) maps from G to A. Define subgroups of cocycles and coboundaries $B^1(G, A) \subset Z^1(G, A) \subset C^1(G, A)$ by

$$Z^1(G,A) = \{f \in C^1(G,A) : f(gh) = f(g) + g(f(h))\}$$
$$B^1(G,A) = \{f \in C^1(G,A) : \text{for some } a \in A,\ f(g) = ga - a \text{ for every } g \in G\}.$$

Proposition 1.2.3. *$H^1(G, A) = Z^1(G, A)/B^1(G, A)$.*

There is a similar definition of $H^i(G, A)$ for every i, where the cochains $C^i(G, A)$ (are) set maps from G^i to A, and $B^i(G, A) \subset Z^i(G, A) \subset C^i(G, A)$ are defined appropriately.

Example 1.2.4. Suppose that G acts trivially on A. Then $Z^1(G, A) = \mathrm{Hom}(G, A)$ and $B^1(G, A) = 0$, so in this case we conclude from Proposition 1.2.3 that

$$H^1(G, A) = \mathrm{Hom}(G, A).$$

Exercise 1.2.5. Suppose that G is a finite cyclic group. For every G-module A, let $A_N := \{a \in A : \sum_{g\in G} ga = 0\}$ (here "N" stands for "norm"; A_N is the kernel of the norm map $a \mapsto \sum_{g\in G} ga$).

Show that if g is a generator of G, then the map $f \mapsto f(g)$ is an injective homomorphism from $Z^1(G, A)$ to A with image A_N. Deduce that in this case

$$H^1(G, A) \cong A_N/(g - 1)A.$$

(Warning: note that this isomorphism depends on the choice of generator g.)

Exercise 1.2.6. Suppose $0 \to A \to B \to C \to 0$ is an exact sequence of G-modules, and suppose $c \in C^G$. Fix an element $b \in B$ that maps to c.

Show that the map $g \mapsto gb - b$ defines a 1-cocycle $f_c \in Z^1(G, A)$ (that depends on the choice of b). Show that $c \mapsto f_c$ induces a well-defined homomorphism $H^0(G, C) \to H^1(G, A)$ and check that with this homomorphism, the beginning of the long exact sequence of Theorem 1.2.1(2) is in fact exact.

1.3. Continuous cohomology.

Now suppose that G is a *profinite group* (see for example [**Gr**]), i.e., there is an isomorphism

$$G = \varprojlim G/U \tag{1.1}$$

where U runs over open subgroups of G of finite index. This isomorphism gives G natural topology, where we view each finite quotient G/U as a discrete topological space, so the product $\prod(G/U)$ is a compact group with the product topology, and then (1.1) identifies G with a closed (and hence compact) subset of $\prod(G/U)$.

Note that a finite group G is profinite, with the discrete topology.

If A is a G-module, we will view A as a topological group with the discrete topology, and we call A a continuous G-module if the action of G on A (i.e., the map $G \times A \to A$) is continuous.

Exercise 1.3.1. Suppose A is a G-module. Show that the following are equivalent:

(1) A is a continuous G-module,
(2) for every $a \in A$, the stabilizer of a in G is open,
(3) $A = \cup A^U$, union over open subgroups $U \subset G$.

Example 1.3.2. If F/K is an infinite Galois extension of fields, and we put $G := \mathrm{Gal}(F/K)$, then there is a natural isomorphism

$$G = \varprojlim \mathrm{Gal}(L/K)$$

inverse limit over finite Galois extensions L of K in F. Thus G is a profinite group.

If $\mathcal{H}$ is an algebraic group over K as in Example 1.1.2, then

$$\mathcal{H}(F) = \cup\mathcal{H}(L) = \cup\mathcal{H}(F)^{\mathrm{Gal}(L/K)},$$

union over finite extensions L of K in F. Therefore G acts continuously on $\mathcal{H}(F)$ by Exercise 1.3.1.

It follows (for example) that when $F = K^{\mathrm{sep}}$ is a separable closure of K, the following G-modules are continuous: K^{sep}, $(K^{\mathrm{sep}})^\times$, $\boldsymbol{\mu}_{p^\infty}$ (the p-power roots of unity in K^{sep}), $E(K^{\mathrm{sep}})$ for an elliptic curve E, and $E[p^\infty]$ (the p-power torsion in $E(K^{\mathrm{sep}})$).

If A is a continuous G-module, we can define *continuous* cohomology groups $H^i(G, A)$, defined similarly to the case of finite groups G but with *continuous* cochains (that is, $C^i(G, A)$ consists of continuous maps from G^i to A). Theorem 1.2.1(1) and (2) also hold for continuous cohomology groups.

If G is finite, then all relevant maps are continuous and the continuous cohomology groups agree with the cohomology groups described in §1.2.

In the next section we will see (Proposition 1.4.7) how to describe the continuous cohomology groups in terms of the cohomology of finite groups.

Until further notice we will always assume that the group G is profinite, and G-module will mean continuous G-module, a discrete abelian group with a continuous action of G.

1.4. Change of group.

Suppose H is a closed subgroup of a profinite group G, and A is a G-module. Then A is an H-module, and $A^G \subset A^H$. For every i there is a restriction map on cochains

$\mathrm{Res} : C^i(G,A) \to C^i(H,A)$, and these maps induce *restriction maps*

$$\mathrm{Res} : H^i(G,A) \to H^i(H,A).$$

If $[G : H]$ is finite, then there is also a norm map $A^H \to A^G$, defined by $a \mapsto \sum_g ga$, summing over a set of left coset representatives of G/H. This map extends in a less obvious way to a *corestriction map*

$$\mathrm{Cor} : H^i(H,A) \to H^i(G,A)$$

for every i.

Proposition 1.4.1. *If $[G : H]$ is finite, then* $\mathrm{Cor} \circ \mathrm{Res} : H^i(G,A) \to H^i(G,A)$ *is multiplication by $[G : H]$.*

Corollary 1.4.2. *If G is finite, then for every G-module A and every $i \geq 1$, we have*

$$|G| \cdot H^i(G,A) = 0.$$

Proof. Take $H = \{1\}$ in Proposition 1.4.1. □

Exercise 1.4.3. Suppose $m \in \mathbf{Z}$. Show that if $mA = 0$, then $mH^i(G,A) = 0$ for every i. Show that if $m : A \to A$ is an isomorphism, then $mH^i(G,A) = H^i(G,A)$ for every i. Deduce that if $|G| : A \to A$ is an isomorphism, then $H^i(G,A) = 0$.

Exercise 1.4.4. Suppose G is finite. Using Exercise 1.1.4, show that for $i \geq 1$, $H^i(G,A)$ can be expressed in terms of $H^{i-1}(G,C)$ for some G-module C. Use this fact, the norm map on H^0, and induction to define the corestriction map on H^i.

Using this definition, prove Proposition 1.4.1.

Now suppose that H is a closed normal subgroup of G. Then A^H is a G/H-module, and for every i there is an inflation map on cochains $\mathrm{Inf} : C^i(G/H, A^H) \to C^i(G,A)$. These maps induce *inflation maps*

$$\mathrm{Inf} : H^i(G/H, A^H) \to H^i(G,A).$$

Theorem 1.4.5. *If H is a normal subgroup of G and A is a G-module, then there is an natural exact sequence*

$$\begin{aligned} 0 \to H^1(G/H, A^H) \xrightarrow{\mathrm{Inf}} H^1(G,A) \xrightarrow{\mathrm{Res}} H^1(H,A)^{G/H} \\ \to H^2(G/H, A^H) \to H^2(G,A). \end{aligned}$$

Corollary 1.4.6. *Suppose H acts trivially on A, and*

$$H^1(G/H, A) = H^2(G/H, A) = 0.$$

Then $H^1(G,A) \cong \mathrm{Hom}(H,A)^{G/H}$.

Proposition 1.4.7. *If A is a G-module, then*

$$H^i(G,A) = \varinjlim H^i(G/U, A^U)$$

direct limit over open subgroups $U \subset G$, with respect to the inflation maps.

Exercise 1.4.8. Prove Proposition 1.4.7 when $i = 1$, using the description (Proposition 1.2.3) of $H^1(G,A)$ in terms of cocycles.

Exercise 1.4.9. Use Proposition 1.4.7 to show that if A is a G-module, then $H^i(G,A)$ is a torsion group for $i \geq 1$.

Proposition 1.4.10. *Suppose $G \cong \hat{\mathbf{Z}} := \varprojlim \mathbf{Z}/n\mathbf{Z}$, and A is a torsion G-module.*

1. *If γ is a topological generator of G, then evaluation of cocycles at γ induces an isomorphism $H^1(G, A) \cong A/(\gamma - 1)A$.*
2. *$H^i(G, A) = 0$ for $i \geq 2$.*

Proof. See [**Se2**, §XIII.1]. Assertion (1) is the following exercise. □

Exercise 1.4.11. Prove Proposition 1.4.10(1) using Exercise 1.2.5 and Proposition 1.4.7.

From now on, if F/K is a Galois extension and A is a $\mathrm{Gal}(F/K)$-module, we will write $H^i(F/K, A)$ in place of $H^i(\mathrm{Gal}(F/K), A)$, and when F is a separable closure K^{sep} of K we write simply $G_K := \mathrm{Gal}(K^{\mathrm{sep}}/K)$ and $H^i(K, A)$ in place of $H^i(K^{\mathrm{sep}}/K, A) = H^i(G_K, A)$.

Definition 1.4.12. Suppose K is a nonarchimedean local field K of characteristic zero, i.e., a finite extension of some $\mathbf{Q}_p$. Let $I_K \subset G_K$ denote the inertia group, $K^{\mathrm{ur}} = \bar{K}^{I_K}$ the maximal unramified extension of K, and $\varphi \in \mathrm{Gal}(K^{\mathrm{ur}}/K)$ the Frobenius automorphism. Then $\mathrm{Gal}(K^{\mathrm{ur}}/K) = G_K/I_K \cong \hat{\mathbf{Z}}$, generated by φ.

If A is a G_K-module, define the *unramified cohomology group* $H^1_{\mathrm{u}}(K, A) \subset H^1(K, A)$ by

$$H^1_{\mathrm{u}}(K, A) := \ker\bigl[H^1(K, A) \xrightarrow{\mathrm{Res}} H^1(K^{\mathrm{ur}}, A)\bigr].$$

The inflation-restriction exact sequence (Theorem 1.4.5) shows that

$$H^1_{\mathrm{u}}(K, A) = H^1(K^{\mathrm{ur}}/K, A^{I_K}). \tag{1.2}$$

If A is a G_K-module, we will say that A is *unramified* if I_K acts trivially on A.

Proposition 1.4.13. *If A is a finite unramified G_K-module, then:*

1. $H^1_{\mathrm{u}}(K, A) = H^1(K^{\mathrm{ur}}/K, A) = A/(\varphi - 1)A$,
2. $H^1(K, A)/H^1_{\mathrm{u}}(K, A) \cong \mathrm{Hom}(I_K, A)^{G_K}$.

Proof. This follows from Theorem 1.4.5 and Proposition 1.4.10. □

1.5. Selmer groups.

Suppose for this section that K is a number field, and A is a G_K-module. For every place v of K, we can view the decomposition group G_{K_v} as a subgroup of G_K, so we have restriction maps

$$\mathrm{Res}_v : H^i(K, A) \longrightarrow H^i(K_v, A).$$

Definition 1.5.1. A *Selmer structure* $\mathcal{F}$ for A is a collection of distinguished subgroups

$$H^1_{\mathcal{F}}(K_v, A) \subset H^1(K_v, A)$$

for every place v of K, such that $H^1_{\mathcal{F}}(K_v, A) = H^1_{\mathrm{u}}(K_v, A)$ for all but finitely many v.

If $\mathcal{F}$ is a Selmer structure for A, we define the *Selmer group* $H^1_{\mathcal{F}}(K, A)$ by

$$H^1_{\mathcal{F}}(K, A) = \ker\Bigl[H^1(K, A) \xrightarrow{\oplus \mathrm{Res}_v} \bigoplus_v (H^1(K_v, A)/H^1_{\mathcal{F}}(K_v, A))\Bigr].$$

In other words, $H^1_{\mathcal{F}}(K, A)$ is the subgroup of all classes in $H^1(K, A)$ whose localization lies in $H^1_{\mathcal{F}}(K_v, A)$ for every v.

Exercise 1.5.2. Suppose $\mathcal{F}$ is a Selmer structure, and suppose Σ is a finite set of places of K containing all archimedean places, all places where A is ramified, and all v such that $H^1_{\mathcal{F}}(K_v, A) \neq H^1_{\mathrm{u}}(K_v, A)$. Let K_Σ be the maximal extension of K unramified outside of Σ. Show that

$$H^1_{\mathcal{F}}(K, A) = \ker\big[H^1(K_\Sigma/K, A) \xrightarrow{\oplus \mathrm{Res}_v} \bigoplus_{v \in \Sigma} (H^1(K_v, A)/H^1_{\mathcal{F}}(K_v, A))\big]$$

Proposition 1.5.3. *If A is finite and $\mathcal{F}$ is a Selmer structure for A, then $H^1_{\mathcal{F}}(K, A)$ is finite.*

Proof. With notation as in Exercise 1.5.2, a standard result (for example [**Mi**, Corollary I.4.15]) shows that $H^1(K_\Sigma/K, A)$ is finite. Thus $H^1_{\mathcal{F}}(K, A)$ is finite by Exercise 1.5.2. □

In what follows, Selmer groups will be arithmetically interesting objects (ideal class groups, Selmer groups of elliptic curves, . . .) and their orders should be related to values of L-functions. We will see examples of Selmer groups in the next section.

Exercise 1.5.4. If B is a G_K-quotient of A, show that a Selmer structure $\mathcal{F}$ for A induces a Selmer structure for B (which we also denote by $\mathcal{F}$), where we define $H^1_{\mathcal{F}}(K_v, B)$ to be the image of $H^1_{\mathcal{F}}(K_v, A)$ under the canonical map $H^1(K_v, A) \to H^1(K_v, B)$.

Similarly, show that if C is a G_K-submodule of A, show that a Selmer structure $\mathcal{F}$ for A induces one for C, where $H^1_{\mathcal{F}}(K_v, C)$ is defined to be the inverse image of $H^1_{\mathcal{F}}(K_v, A)$ under the canonical map $H^1(K_v, C) \to H^1(K_v, A)$.

1.6. Kummer theory.

Proposition 1.6.1. *Suppose F/K is a Galois extension. Then*

$$H^i(F/K, F) = \begin{cases} K & \text{if } i = 0 \\ 0 & \text{if } i > 0, \end{cases} \qquad H^i(F/K, F^\times) = \begin{cases} K^\times & \text{if } i = 0 \\ 0 & \text{if } i = 1. \end{cases}$$

Exercise 1.6.2. Use Proposition 1.4.7 to reduce the proof of Proposition 1.6.1 to the case where F/K is finite.

Theorem 1.6.3. *For every $m > 0$ prime to the characteristic of K, there is a natural isomorphism*

$$K^\times/(K^\times)^m \cong H^1(K, \boldsymbol{\mu}_m).$$

Proof. The long exact cohomology sequence coming from the short exact sequence

$$0 \longrightarrow \boldsymbol{\mu}_m \longrightarrow (K^{\mathrm{sep}})^\times \xrightarrow{m} (K^{\mathrm{sep}})^\times \longrightarrow 0$$

begins

$$0 \longrightarrow \boldsymbol{\mu}_m(K) \longrightarrow K^\times \xrightarrow{m} K^\times \longrightarrow H^1(K, \boldsymbol{\mu}_m) \longrightarrow H^1(K, (K^{\mathrm{sep}})^\times).$$

Now the theorem follows from Proposition 1.6.1. □

Exercise 1.6.4. Show using the description from Exercise 1.2.6 that the isomorphism of Theorem 1.6.3 is given by sending $x \in K^\times$ to the cocycle $g \mapsto g(\sqrt[m]{x})/\sqrt[m]{x}$ for $g \in G_K$.

Corollary 1.6.5. *If $\boldsymbol{\mu}_m \subset K$ then $K^\times/(K^\times)^m \cong \mathrm{Hom}(G_K, \boldsymbol{\mu}_m)$.*

Exercise 1.6.6. Suppose $\boldsymbol{\mu}_m \subset K$ and X is a finite subgroup of $K^\times/(K^\times)^m$. Show that the isomorphism of Corollary 1.6.5 identifies

$$X \cong \mathrm{Hom}(\mathrm{Gal}(K(\sqrt[m]{X})/K), \boldsymbol{\mu}_m),$$

where $K(\sqrt[m]{X})$ is the extension of K generated by m-th roots of all elements of X. Show that the isomorphism of Corollary 1.6.5 induces a bijection between finite subgroups of $K^\times/(K^\times)^m$ and finite abelian extensions of K of exponent dividing m.

Definition 1.6.7. If K is a nonarchimedean local field of characteristic zero, define

$$H^1_{\mathrm{f}}(K, \boldsymbol{\mu}_m) \subset H^1(K, \boldsymbol{\mu}_m)$$

to be the image under the Kummer map of Theorem 1.6.3

$$\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^m \hookrightarrow K^\times/(K^\times)^m \cong H^1(K, \boldsymbol{\mu}_m)$$

where $\mathcal{O}_K$ is the ring of integers of K. If K is $\mathbf{R}$ or $\mathbf{C}$, let $H^1_{\mathrm{f}}(K, \boldsymbol{\mu}_m) = H^1(K, \boldsymbol{\mu}_m)$.

Exercise 1.6.8. Show that if K is a number field, then the collection of subgroups $\{H^1_{\mathrm{f}}(K_v, \boldsymbol{\mu}_m)\}$ is a Selmer structure (i.e., show that $H^1_{\mathrm{f}}(K_v, \boldsymbol{\mu}_m) = H^1_{\mathrm{u}}(K_v, \boldsymbol{\mu}_m)$ for all $v \nmid m\infty$).

Proposition 1.6.9. *The Selmer group $H^1_{\mathrm{f}}(K, \boldsymbol{\mu}_m)$ defined with the Selmer structure above satisfies*

$$0 \longrightarrow \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^m \longrightarrow H^1_{\mathrm{f}}(K, \boldsymbol{\mu}_m) \longrightarrow \mathcal{C}_K[m] \longrightarrow 0$$

where $\mathcal{C}_K[m]$ is the m-torsion subgroup of the ideal class group of K.

Exercise 1.6.10. Prove Proposition 1.6.9 as follows. Viewing $H^1_{\mathrm{f}}(K, \boldsymbol{\mu}_m) \subset K^\times/(K^\times)^m$, show that if $x \in K^\times$ projects to an element of $H^1_{\mathrm{f}}(K, \boldsymbol{\mu}_m)$, then the fractional principal ideal $x\mathcal{O}_K$ is $\mathfrak{a}^m$ for some fractional ideal $\mathfrak{a}$. Show that sending x to the class of $\mathfrak{a}$ induces a surjective map $H^1_{\mathrm{f}}(K, \boldsymbol{\mu}_m) \twoheadrightarrow \mathcal{C}_K[m]$ with kernel $\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^m$.

Theorem 1.6.3 has the following analogue for elliptic curves.

Theorem 1.6.11. *Suppose E is an elliptic curve defined over K and $m > 0$ is prime to the characteristic of K. There is an exact sequence*

$$0 \longrightarrow E(K)/mE(K) \longrightarrow H^1(K, E[m]) \longrightarrow H^1(K, E(K^{\mathrm{sep}}))[m] \longrightarrow 0.$$

Exercise 1.6.12. Prove Theorem 1.6.11 using the short exact sequence

$$0 \longrightarrow E[m] \longrightarrow E(K^{\mathrm{sep}}) \xrightarrow{\ m\ } E(K^{\mathrm{sep}}) \longrightarrow 0.$$

Show that the injection $E(K)/mE(K) \hookrightarrow H^1(K, E[m])$ is given by sending $x \in E(K)$ to the cocycle $g \mapsto gy - y$, where $y \in E(K^{\mathrm{sep}})$ satisfies $my = x$ (and the same y is used for all g).

Definition 1.6.13. If K is a nonarchimedean local field of characteristic zero, E is an elliptic curve over K, and $m > 0$, define

$$H^1_{\mathrm{f}}(K, E[m]) \subset H^1(K, E[m])$$

to be the image of the Kummer map of Theorem 1.6.11

$$E(K)/mE(K) \hookrightarrow H^1(K, E[m]).$$

If K is $\mathbf{R}$ or $\mathbf{C}$, let $H^1_{\mathrm{f}}(K, E[m]) = H^1(K, E[m])$.

Suppose now that K is a number field and E is an elliptic curve over K. If $v \nmid m\infty$ and E has good reduction at v, then $H^1_{\mathrm{f}}(K_v, E[m]) = H^1_{\mathrm{u}}(K_v, E[m])$ by [**Ca**], so the collection of subgroups $\{H^1_{\mathrm{f}}(K_v, E[m])\}$ is a Selmer structure. The corresponding Selmer group is the classical m-Selmer group of E/K, $H^1_{\mathrm{f}}(K, E[m]) = \mathrm{Sel}_m(E/K)$ sitting in an exact sequence

$$0 \longrightarrow E(K)/mE(K) \longrightarrow \mathrm{Sel}_m(E/K) \longrightarrow Ш(E/K)[m] \longrightarrow 0 \tag{1.3}$$

where $Ш(E/K)$ is the Shafarevich-Tate group of E/K.

1.7. The Brauer group.

If K is a field, $\boldsymbol{\mu}_\infty$ will denote the roots of unity in K^{sep}.

Exercise 1.7.1. Suppose K is a field. Show that for every $m > 0$ prime to the characteristic of K, there is a natural isomorphism $H^2(K, \boldsymbol{\mu}_m) \cong H^2(K, (K^{\mathrm{sep}})^\times)[m]$. Deduce that if K has characteristic zero, then $H^2(K, \boldsymbol{\mu}_\infty) \cong H^2(K, (K^{\mathrm{sep}})^\times)$.

Theorem 1.7.2. *If K is a nonarchimedean local field of characteristic zero (i.e., a finite extension of some $\mathbf{Q}_p$), then there is a canonical isomorphism*

$$\mathrm{inv}_K : H^2(K, \boldsymbol{\mu}_\infty) \xrightarrow{\sim} \mathbf{Q}/\mathbf{Z}.$$

If $K = \mathbf{R}$, there is a canonical isomorphism

$$\mathrm{inv}_{\mathbf{R}} : H^2(\mathbf{R}, \boldsymbol{\mu}_\infty) \xrightarrow{\sim} \tfrac{1}{2}\mathbf{Z}/\mathbf{Z} \subset \mathbf{Q}/\mathbf{Z}.$$

Proof. See [**Se2**, §XIII.3]. □

Theorem 1.7.3. *Suppose K is a number field. For every $m \le \infty$ there is an exact sequence*

$$0 \longrightarrow H^2(K, \boldsymbol{\mu}_m) \xrightarrow{\oplus \mathrm{Res}_v} \bigoplus_v H^2(K_v, \boldsymbol{\mu}_m) \xrightarrow{\sum \mathrm{inv}_{K_v}} \mathbf{Q}/\mathbf{Z} \longrightarrow 0$$

where K_v is the completion of K at v, and Res_v is the restriction map with respect to the subgroup $G_{K_v} \subset G_K$.

Proof. See [**AT**, Chapter 7, Theorem 8]. □

1.8. Local fields and duality.

Suppose A and B are G-modules. There is a cup product homomorphism

$$H^i(G, A) \otimes H^j(G, B) \longrightarrow H^{i+j}(G, A \otimes B).$$

We view this as a bilinear pairing on $H^i(G, A) \times H^j(G, B)$, written $(a, b) \mapsto a \cup b$. The cup product pairing has numerous properties [**AW, Se2**]; here we mention only that it commutes with restriction maps: if $H \subset G$, then $\mathrm{Res}(a) \cup \mathrm{Res}(b) = \mathrm{Res}(a \cup b)$.

Suppose now that K is a field, A is a finite G_K module, and $\boldsymbol{\mu}_\infty$ is the G_K-module of roots of unity in K^{sep}. Define the Cartier dual $A^* = \mathrm{Hom}(A, \boldsymbol{\mu}_\infty)$. Then A^* is also a (continuous) G_K-module, and there is a natural pairing

$$A \otimes A^* \longrightarrow \boldsymbol{\mu}_\infty.$$

We can compose the cup product with this pairing to get a pairing

$$H^i(K, A) \otimes H^j(K, A^*) \longrightarrow H^{i+j}(K, \boldsymbol{\mu}_\infty). \tag{1.4}$$

If K is a local field of characteristic zero, and $i+j=2$, we can compose the pairing (1.4) with the isomorphism of Proposition 1.7.2 to get a new pairing

$$H^i(K,A)\times H^j(K,A^*)\xrightarrow{\ \cup\ } H^2(K,\boldsymbol{\mu}_\infty)\xrightarrow{\mathrm{inv}_K}\mathbf{Q}/\mathbf{Z}. \tag{1.5}$$

Theorem 1.8.1 (Tate local duality)**.** *Suppose K is a local field of characteristic zero, A is a finite G_K-module, and $0\le i\le 2$. Then* (1.5) *is a perfect pairing of finite groups.*

Proof. See [**Mi**, Corollary I.2.3]. □

In the following examples and exercise, K is a local field of characteristic zero and $\mathcal{O}_K$ is its ring of integers.

Example 1.8.2. Fix $m\ge 0$, and let $A=\boldsymbol{\mu}_m$. Then $A^*=\mathbf{Z}/m\mathbf{Z}$ (with trivial G_K-action), and we have

$$H^1(K,\boldsymbol{\mu}_m)\cong K^\times/(K^\times)^m,\quad H^1(K,\mathbf{Z}/m\mathbf{Z})=\mathrm{Hom}(G_K,\mathbf{Z}/m\mathbf{Z}).$$

By Theorem 1.8.1, the pairing (1.5) gives an isomorphism (for every m)

$$\begin{aligned}K^\times/(K^\times)^m\xrightarrow{\sim}H^1(K,\boldsymbol{\mu}_m)&\xrightarrow{\sim}\mathrm{Hom}(H^1(K,\mathbf{Z}/m\mathbf{Z}),\mathbf{Q}/\mathbf{Z})\\&\xrightarrow{\sim}\mathrm{Hom}(\mathrm{Hom}(G_K,\mathbf{Z}/m\mathbf{Z}),\mathbf{Q}/\mathbf{Z})\xrightarrow{\sim}G_K^{\mathrm{ab}}/(G_K^{\mathrm{ab}})^m.\end{aligned}$$

The inverse limit of these maps over m gives the Artin map $K^\times\to G_K^{\mathrm{ab}}$ of local class field theory.

Exercise 1.8.3. Recall that $H^1_{\mathrm{f}}(K,\boldsymbol{\mu}_m)\subset H^1(K,\boldsymbol{\mu}_m)$ is the image of the Kummer map $\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^m\hookrightarrow H^1(K,\boldsymbol{\mu}_m)$. Define

$$H^1_{\mathrm{f}}(K,\mathbf{Z}/m\mathbf{Z}):=H^1_{\mathrm{u}}(K,\mathbf{Z}/m\mathbf{Z})=\mathrm{Hom}(G_K/I_K,\mathbf{Z}/m\mathbf{Z})\subset H^1(K,\mathbf{Z}/m\mathbf{Z}),$$

where $I_K\subset G_K$ is the inertia group. Show, using the local class field theory description of the isomorphism in Example 1.8.2, that $H^1_{\mathrm{f}}(K,\boldsymbol{\mu}_m)$ and $H^1_{\mathrm{f}}(K,\mathbf{Z}/m\mathbf{Z})$ are orthogonal complements of each other under the Tate pairing

$$H^1(K,\boldsymbol{\mu}_m)\times H^1(K,\mathbf{Z}/m\mathbf{Z})\to\mathbf{Q}/\mathbf{Z}.$$

Example 1.8.4. Suppose E is an elliptic curve over K, $m>0$, and $A=E[m]$. The Weil pairing $E[m]\times E[m]\to\boldsymbol{\mu}_m$ gives a canonical isomorphism $A^*\cong E[m]$. By Theorem 1.8.1, the pairing (1.5) gives a perfect pairing

$$H^1(K,E[m])\times H^1(K,E[m])\longrightarrow\mathbf{Z}/m\mathbf{Z}.$$

The subgroup $H^1_{\mathrm{f}}(K,E[m])\subset H^1(K,E[m])$ given by Definition 1.6.13 is its own orthogonal complement under this pairing [**Ta1**].

1.9. Unramified and transverse cohomology groups.

Fix for this section a nonarchimedean local field K of characteristic zero, and let $\mathcal{O}_K$ be its ring of integers. As in Definition 1.4.12, we let $I_K\subset G_K$ denote the inertia group, $K^{\mathrm{ur}}=\bar{K}^{I_K}$ the maximal unramified extension of K, and $\varphi\in\mathrm{Gal}(K^{\mathrm{ur}}/K)$ the Frobenius automorphism. Then $\mathrm{Gal}(K^{\mathrm{ur}}/K)=G_K/I_K\cong\hat{\mathbf{Z}}$, generated by φ. Recall that a G_K-module A is *unramified* if I_K acts trivially on A.

Proposition 1.9.1. *Suppose A is a finite unramified G_K-module of order prime to the residue characteristic of K. Then $H^1_{\mathrm{u}}(K,A)$ and $H^1_{\mathrm{u}}(K,A^*)$ are orthogonal complements of each other under the pairing* (1.5)*.*

Proof. See for example [**Mi**, Theorem I.2.6], or combine the following two exercises. □

Exercise 1.9.2. Show using Proposition 1.4.13 that if A is a finite unramified G_K-module of order prime to the residue characteristic of K, then

$$|H^1_{\mathrm{u}}(K,A)| = [H^1(K,A^*) : H^1_{\mathrm{u}}(K,A^*)].$$

You will need to use that the tame quotient of I_K is isomorphic (as a G_K-module) to $\prod_{\ell\neq p}\boldsymbol{\mu}_{\ell^\infty}$, where p is the residue characteristic of K.

Exercise 1.9.3. Assuming that the cup product commutes with inflation, show that $H^1_{\mathrm{u}}(K,A)$ and $H^1_{\mathrm{u}}(K,A^*)$ are orthogonal because the following diagram commutes:

$$\begin{tikzcd}
H^1(K,A)\times H^1(K,A^*) \arrow[r, "\cup"] & H^2(K,\boldsymbol{\mu}_\infty) \\
H^1_{\mathrm{u}}(K,A)\times H^1_{\mathrm{u}}(K,A^*) \arrow[r, "\cup"] \arrow[u, "\mathrm{Inf}"] & H^2(K^{\mathrm{ur}}/K,\boldsymbol{\mu}_\infty) \arrow[u, "\mathrm{Inf}"']
\end{tikzcd}$$

and the lower right corner is zero by Proposition 1.4.10(2).

Let $\Bbbk$ denote the residue field of K, and $q := |\Bbbk|$.

Definition 1.9.4. Suppose L/K is a totally tamely ramified extension of degree $q-1$; then there is a canonical isomorphism $\mathrm{Gal}(L/K)\cong\Bbbk^\times$. (When $K=\mathbf{Q}_\ell$ we can take $L=\mathbf{Q}_\ell(\boldsymbol{\mu}_\ell)$.) We define the L-transverse subgroup $H^1_{\mathrm{t}}(K,A)\subset H^1(K,A)$ by

$$H^1_{\mathrm{t}}(K,A) := \ker\bigl[H^1(K,A)\to H^1(L,A)\bigr] = H^1(L/K,A^{G_L}).$$

Proposition 1.9.5. *Suppose A is a finite unramified G_K-module and $(q-1)A=0$. Then:*

1. $H^1_{\mathrm{t}}(K,A)\cong\mathrm{Hom}(\mathrm{Gal}(L/K),A^{\varphi=1})$.
2. $H^1_{\mathrm{t}}(K,A)\otimes\mathrm{Gal}(L/K)\cong A^{\varphi=1}$.
3. *There is a direct sum decomposition $H^1(K,A)=H^1_{\mathrm{u}}(K,A)\oplus H^1_{\mathrm{t}}(K,A)$.*
4. *$H^1_{\mathrm{t}}(K,A)$ and $H^1_{\mathrm{t}}(K,A^*)$ are orthogonal complements of each other under the pairing* (1.5).

Proof. See [**MR1**, Lemmas 1.2.1, 1.2.4 and Proposition 1.3.2]. Since A is unramified and I_K and G_L generate G_K, we have $A^{G_L}=A^{G_K}=A^{\varphi=1}$. This proves (1) and (2). By (1) and Proposition 1.4.13(2), $|H^1(K,A)|=|H^1_{\mathrm{u}}(K,A)|\cdot|H^1_{\mathrm{t}}(K,A)|$, so to prove (3) it is enough to show that $H^1_{\mathrm{u}}(K,A)\cap H^1_{\mathrm{t}}(K,A)=0$, and then to prove (4) it is enough to show that $H^1_{\mathrm{t}}(K,A)$ and $H^1_{\mathrm{t}}(K,A^*)$ are orthogonal. These are left as an exercises, or see [**MR1**]. □

Definition 1.9.6. Suppose $m\mid q-1$, and let $R=\mathbf{Z}/m\mathbf{Z}$. Suppose that A is an unramified G-module that is free of finite rank over R, and that $\det(1-\varphi|A)=0$. Consider the characteristic polynomial

$$P(x) := \det(1-\varphi x|A)\in R[x].$$

Since $P(1)=\det(1-\varphi|A)=0$, we have $P(x)=(x-1)Q(x)$ for some $Q(x)\in R[x]$. By the Cayley-Hamilton theorem, $P(\varphi^{-1})$ annihilates A, so $Q(\varphi^{-1})\subset A^{\varphi=1}$. Define the *unramified-transverse comparison map* ϕ^{ut} to be the composition

$$H^1_{\mathrm{u}}(K,A)\xrightarrow{\sim}A/(\varphi-1)A\xrightarrow{Q(\varphi^{-1})}A^{\varphi=1}\xrightarrow{\sim}H^1_{\mathrm{t}}(K,A)\otimes\mathrm{Gal}(L/K)$$

using the isomorphisms of Proposition 1.4.13(1) and 1.9.5(2).

Exercise 1.9.7 (Lemma 1.2.3 of [**MR1**])**.** Suppose $m \mid q-1$ and A is an unramified G-module that is free of finite rank over $\mathbf{Z}/m\mathbf{Z}$. Show that $A^{\varphi=1}$ is free of rank one over $\mathbf{Z}/m\mathbf{Z}$ if and only if $A/(\varphi-1)A$ is free of rank one over $\mathbf{Z}/m\mathbf{Z}$. If these conditions are satisfied, show that the map ϕ^{ut} of Definition 1.9.6 is an isomorphism and $H^1_{\mathrm{u}}(K,A)$, $H^1_{\mathrm{t}}(K,A)$, $H^1_{\mathrm{u}}(K,A^*)$, $H^1_{\mathrm{t}}(K,A^*)$, are all free of rank 1 over $\mathbf{Z}/m\mathbf{Z}$.

1.10. Comparing Selmer groups.

Suppose K is a number field and A is a finite G_K-module.

Definition 1.10.1. If $\mathcal{F}$ is a Selmer structure for A, define a Selmer structure $\mathcal{F}^*$ for the Cartier dual $A^* := \mathrm{Hom}(A, \boldsymbol{\mu}_\infty)$ by

$$H^1_{\mathcal{F}^*}(K_v, A^*) := H^1_{\mathcal{F}}(K_v, A)^\perp \subset H^1(K_v, A^*)$$

for every v, where $H^1_{\mathcal{F}}(K_v, A)^\perp$ is the orthogonal complement of $H^1_{\mathcal{F}}(K_v, A)$ in $H^1(K_v, A^*)$ under the local Tate pairing (1.5). By Proposition 1.9.1, $\mathcal{F}^*$ is a Selmer structure.

If $\mathcal{F}, \mathcal{G}$ are Selmer structures for A, we will say $\mathcal{G} \subset \mathcal{F}$ if $H^1_{\mathcal{G}}(K_v, A) \subset H^1_{\mathcal{F}}(K_v, A)$ for every v. Note that if $\mathcal{G} \subset \mathcal{F}$, then

- $H^1_{\mathcal{G}}(K, A) \subset H^1_{\mathcal{F}}(K, A)$,
- $\mathcal{F}^* \subset \mathcal{G}^*$.

Theorem 1.10.2 (Global duality)**.** *Suppose $\mathcal{G}_1, \mathcal{G}_2$ are Selmer structures for A, and $\mathcal{G}_1 \subset \mathcal{G}_2$. There are exact sequences*

$$\begin{tikzcd} 0 \arrow[r] & H^1_{\mathcal{G}_1}(K, A) \arrow[r] & H^1_{\mathcal{G}_2}(K, A) \arrow[r, "\oplus \mathrm{Res}_v"] & \bigoplus_v H^1_{\mathcal{G}_2}(K_v, A)/H^1_{\mathcal{G}_1}(K_v, A), \end{tikzcd}$$

$$\begin{tikzcd} 0 \arrow[r] & H^1_{\mathcal{G}_2^*}(K, A^*) \arrow[r] & H^1_{\mathcal{G}_1^*}(K, A^*) \arrow[r, "\oplus \mathrm{Res}_v"] & \bigoplus_v H^1_{\mathcal{G}_1^*}(K_v, A^*)/H^1_{\mathcal{G}_2^*}(K_v, A^*), \end{tikzcd}$$

summing over v such that $H^1_{\mathcal{G}_1}(K_v, A) \neq H^1_{\mathcal{G}_2}(K_v, A)$. The images of the two right-hand maps are orthogonal complements of each other under the sum of the local Tate pairings (1.5)*.*

Proof. See [**R2**, Theorem 1.7.3] to derive this statement from the usual statement of Poitou-Tate duality ([**Ta2**, Theorem 3.1] or [**Mi**, Theorem I.4.10]). □

Exercise 1.10.3. Show that the two sequences of Theorem 1.10.2 are exact. Show that the images of the two right-hand maps are orthogonal, using Theorem 1.7.3.

The following corollary of Theorem 1.10.2 will be used to bound the size of $H^1_{\mathcal{F}}(K, A)$. Note that given $\mathcal{F}$, there will exist $\mathcal{G} \subset \mathcal{F}$ "small enough" that $H^1_{\mathcal{G}}(K, A) = 0$.

Corollary 1.10.4. *Suppose $\mathcal{G} \subset \mathcal{F}$ are Selmer structures for A, and $H^1_{\mathcal{G}}(K, A) = 0$. Then*

$$|H^1_{\mathcal{F}}(K, A)| \leq \left|\mathrm{coker}\big[H^1_{\mathcal{G}^*}(K, A^*) \xrightarrow{\oplus \mathrm{Res}_v} \bigoplus_v H^1_{\mathcal{G}^*}(K_v, A^*)/H^1_{\mathcal{F}^*}(K_v, A^*)\big]\right|.$$

Exercise 1.10.5. Prove Corollary 1.10.4.

LECTURE 2

Kolyvagin systems

From now on, to simplify things we will only consider $K = \mathbf{Q}$. Much of what we do can be extended easily to arbitrary number fields.

Fix a prime p and a positive integer m, and let $R = \mathbf{Z}/p^m\mathbf{Z}$. Fix a $G_{\mathbf{Q}}$-module A that is free of finite rank over R, and a Selmer structure $\mathcal{F}$ for A.

The letter ℓ will always denote a rational prime.

2.1. Varying the Selmer structure.

As in Exercise 1.5.2, let Σ be a finite set of places of $\mathbf{Q}$ containing ∞, p, all primes where A is ramified, and all ℓ such that $H^1_{\mathcal{F}}(\mathbf{Q}_\ell, A) \neq H^1_{\mathrm{u}}(\mathbf{Q}_\ell, A)$.

Definition 2.1.1. Suppose a, b, c are pairwise relatively prime positive integers, and c is not divisible by any primes in Σ. Define a new Selmer structure $\mathcal{F}_a^b(c)$ for A by

$$H^1_{\mathcal{F}_a^b(c)}(\mathbf{Q}_v, A) = \begin{cases} H^1_{\mathcal{F}}(\mathbf{Q}_v, A) & \text{if } v \nmid abc \\ 0 & \text{if } v \mid a, \\ H^1(\mathbf{Q}_v, A) & \text{if } v \mid b, \\ H^1_{\mathrm{t}}(\mathbf{Q}_v, A) & \text{if } v \mid c. \end{cases}$$

In other words, $\mathcal{F}_a^b(c)$ is constructed by modifying $\mathcal{F}$ at the primes dividing abc, with the "strict" condition at ℓ if $\ell \mid a$, the "relaxed" condition at ℓ if $\ell \mid b$, and the transverse condition at ℓ if $\ell \mid c$. (Here the transverse subgroup $H^1_{\mathrm{t}}(\mathbf{Q}_\ell, A)$ is defined with respect to the extension $\mathbf{Q}_\ell(\boldsymbol{\mu}_\ell)/\mathbf{Q}_\ell$ in Definition 1.9.4.)

If any of a, b, or c are equal to 1, we will suppress them from the notation.

Exercise 2.1.2. Show that the dual Selmer structure $(\mathcal{F}_a^b(c))^*$ (in the sense of Definition 1.10.1) is $(\mathcal{F}^*)_b^a(c)$.

Definition 2.1.3. Let

$$\mathcal{P} = \{\ell \notin \Sigma : \ell \equiv 1 \pmod{p^m} \text{ and } A/(\mathrm{Fr}_\ell - 1)A \text{ is free of rank 1 over } R\}.$$

Let $\mathcal{N} = \mathcal{N}(\mathcal{P}) \subset \mathbf{Z}^+$ denote the set of squarefree products of primes in $\mathcal{P}$ (with the convention that $1 \in \mathcal{N}$). If $n \in \mathcal{N}$ let

$$G_n = \bigotimes_{\ell \mid n} \mathbf{F}_\ell^\times = \bigotimes_{\ell \mid n} \mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_\ell)/\mathbf{Q}).$$

Since each $\mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_\ell)/\mathbf{Q})$ is cyclic of order divisible by p^m, we see that $G_n \otimes R$ is free of rank one over R. By convention, we set $G_1 = R$.

If $\ell \mid n \in \mathcal{N}$, then $\ell - 1 = \det(1 - \mathrm{Fr}_\ell | A) = 0$ in R, so we can apply Proposition 1.9.5, Definition 1.9.6, and Exercise 1.9.7 to $H^1(\mathbf{Q}_\ell, A)$. In particular we will write

$$\phi_\ell^{\mathrm{ut}} : H^1_{\mathrm{u}}(\mathbf{Q}_\ell, A) \xrightarrow{\sim} H^1_{\mathrm{t}}(\mathbf{Q}_\ell, A) \otimes G_\ell$$

for the unramified-transverse isomorphism of Definition 1.9.6.

If $n\ell \in \mathcal{N}$, we can compare $H^1_{\mathcal{F}(n)}(\mathbf{Q}, A) \otimes G_n$ and $H^1_{\mathcal{F}(n\ell)}(\mathbf{Q}, A) \otimes G_{n\ell}$ by localizing at ℓ and using the ϕ_ℓ^{ut}:

(2.1)
$$\begin{tikzcd}
 & H^1_{\mathcal{F}(n)}(\mathbf{Q}, A) \otimes G_n \arrow[d, "\mathrm{Res}_\ell \otimes 1"'] \\
 & H^1_{\mathrm{u}}(\mathbf{Q}_\ell, A) \otimes G_n \arrow[d, "\phi_\ell^{\mathrm{ut}} \otimes 1"'] \\
H^1_{\mathcal{F}(n\ell)}(\mathbf{Q}, A) \otimes G_{n\ell} \arrow[r, "\mathrm{Res}_\ell \otimes 1"] & H^1_{\mathrm{t}}(\mathbf{Q}_\ell, A) \otimes G_{n\ell}.
\end{tikzcd}$$

Exercise 2.1.4 (Corollary 2.3.6 of [**MR1**]). If $n \in \mathcal{N}$, show that

$$\begin{aligned}\mathrm{length}(H^1_{\mathcal{F}}(\mathbf{Q}, A)) - \mathrm{length}(H^1_{\mathcal{F}^*}(\mathbf{Q}, A^*))&\\ = \mathrm{length}(H^1_{\mathcal{F}(n)}(\mathbf{Q}, A)) - \mathrm{length}(H^1_{\mathcal{F}(n)^*}(\mathbf{Q}, A^*)).&\end{aligned}$$

where length means length as an R-module, so $|M| = p^{\mathrm{length}(M)}$ for every finite R-module M. Hint: apply Theorem 1.10.2 with $(\mathcal{G}_1, \mathcal{G}_2) = (\mathcal{F}, \mathcal{F}^n)$ and with $(\mathcal{G}_1, \mathcal{G}_2) = (\mathcal{F}(n), \mathcal{F}^n)$, and use Exercise 1.9.7.

2.2. Kolyvagin systems.

Keep the notation of the previous section.

Definition 2.2.1. A *Kolyvagin system* for $(A, \mathcal{F})$ is a collection

$$\{\kappa_n \in H^1_{\mathcal{F}(n)}(\mathbf{Q}, A) \otimes G_n : n \in \mathcal{N}\}$$

such that if $n\ell \in \mathcal{N}$, then the images of κ_n and $\kappa_{n\ell}$ in $H^1_{\mathrm{t}}(\mathbf{Q}_\ell, A) \otimes G_{n\ell}$ in (2.1) are equal. We let $\mathbf{KS}(A, \mathcal{F})$ (or simply $\mathbf{KS}(A)$, if $\mathcal{F}$ is understood) denote the R-module of Kolyvagin systems.

We next reformulate this definition.

Definition 2.2.2. Suppose X is a graph, with vertex set V and edge set E. By a *sheaf* $\mathcal{S}$ of R-modules on X, we mean a rule assigning

- to each vertex v an R-module $\mathcal{S}(v)$,
- to each edge e an R-module $\mathcal{S}(e)$,
- to each pair (v, e) such that the vertex v is an endpoint of the edge e, an R-module homomorphism $\psi_v^e : \mathcal{S}(v) \to \mathcal{S}(e)$.

We call $\mathcal{S}(v)$ the *stalk* of $\mathcal{S}$ at v.

A *global section* of $\mathcal{S}$ is a collection $\{\kappa_v \in \mathcal{S}(v) : v \in V\}$ such that for every edge e, if v, v' are the endpoints of e, then $\psi_v^e(\kappa_v) = \psi_{v'}^e(\kappa_{v'})$. We let $\Gamma(\mathcal{S})$ denote the R-module of global sections of $\mathcal{S}$.

Definition 2.2.3. Define a graph $\mathcal{X}$ associated to $(A, \mathcal{F})$ by taking the set of vertices to be $\mathcal{N}$, and whenever $n, n\ell \in \mathcal{N}$ we join n and $n\ell$ by an edge. Define the *Selmer sheaf* $\mathcal{H} = \mathcal{H}_{(A,\mathcal{F})}$ on $\mathcal{X}$ by

- $\mathcal{H}(n) = H^1_{\mathcal{F}(n)}(\mathbf{Q}, A) \otimes G_n$ for $n \in \mathcal{N}$,

and if e is the edge joining n and $n\ell$,

- $\mathcal{H}(e) = H^1_{\mathrm{t}}(\mathbf{Q}_\ell, A) \otimes G_{n\ell}$,
- ψ^e_n is the composition of the vertical maps of (2.1),
- $\psi^e_{n\ell}$ is the horizontal map of (2.1).

Definition 2.2.1′. A *Kolyvagin system* for $(A, \mathcal{F})$ is a global section of the Selmer sheaf $\mathcal{H}_{(A,\mathcal{F})}$, and so $\mathbf{KS}(A, \mathcal{F}) = \Gamma(\mathcal{H}_{(A,\mathcal{F})})$.

Exercise 2.2.4. Suppose $H^1_{\mathcal{F}}(\mathbf{Q}, A) = 0$. Show that every Kolyvagin system is identically zero.

Exercise 2.2.5. Suppose $\boldsymbol{\kappa} \in \mathbf{KS}(A, \mathcal{F})$ and $\ell \in \mathcal{P}$. Fix a surjection $\xi : G_\ell \to R$. Show that the collection

$$\{(1 \otimes \xi)(\kappa_{n\ell}) : n \in \mathcal{N}, \ell \nmid n\}$$

is a Kolyvagin system for $(A, \mathcal{F}(\ell))$.

We postpone until later any discussion of how one can find Kolyvagin systems, and instead we discuss consequences of the existence of Kolyvagin systems.

2.3. Sheaves and monodromy.

Suppose for this section that $\mathcal{S}$ is a sheaf on a graph X, as in Definition 2.2.2.

Definition 2.3.1. If v and w are vertices of X, a *path* in X from v to w is a sequence of vertices and edges $(v = v_0, e_1, v_1, e_2, \ldots, e_n, v_n = w)$ in X such that for each i, e_i is an edge joining v_{i-1} and v_i. A *loop* in X (at v) is a path from v to v.

We say that $\mathcal{S}$ is *locally cyclic* if all the R-modules $\mathcal{S}(v)$, $\mathcal{S}(e)$ are cyclic and all the maps ψ^e_v are surjective.

If $\mathcal{S}$ is locally cyclic then a *surjective path* (relative to $\mathcal{S}$) from v to w is a path $(v = v_0, e_1, v_1, e_2, \ldots, e_n, v_n = w)$ in X such that for each i, the map $\psi^{e_i}_{v_i}$ is an isomorphism. We say that the vertex v is a *hub* of $\mathcal{S}$ if for every vertex w there is an $\mathcal{S}$-surjective path from v to w.

Suppose now that the sheaf $\mathcal{S}$ is locally cyclic. If P is a surjective path in X:

$$\begin{tikzcd}
\mathcal{S}(v_0) \arrow[r, two heads] & \mathcal{S}(e_1) & \mathcal{S}(v_1) \arrow[l, "\sim"'] \arrow[r, two heads] & \mathcal{S}(e_2) & \mathcal{S}(v_2) \arrow[l, "\sim"'] \arrow[r, two heads] & \cdots & \mathcal{S}(v_{n-1}) \arrow[l, "\sim"'] \arrow[r, two heads] & \mathcal{S}(e_n) & \mathcal{S}(v_n) \arrow[l, "\sim"'] \\
v_0 \arrow[rr, dash, "e_1"'] & & v_1 \arrow[rr, dash, "e_2"'] & & v_2 \arrow[r, dash] & \cdots \arrow[r, dash] & v_{n-1} \arrow[rr, dash, "e_n"'] & & v_n
\end{tikzcd}$$

we can define a surjective map $\psi_P : \mathcal{S}(v_0) \to \mathcal{S}(v_n)$ by

$$\psi_P = (\psi^{e_k}_{v_k})^{-1} \circ \psi^{e_k}_{v_{k-1}} \circ (\psi^{e_{k-1}}_{v_{k-1}})^{-1} \circ \cdots \circ (\psi^{e_1}_{v_1})^{-1} \circ \psi^{e_1}_{v_0} \tag{2.2}$$

since all the inverted maps are isomorphisms. We will say that $\mathcal{S}$ has *trivial monodromy* if whenever v, w, w' are vertices, P, P' are surjective paths $(v, \ldots, w)$ and $(v, \ldots, w')$, and w, w' are joined by an edge e, then $\psi^e_w \circ \psi_P = \psi^e_{w'} \circ \psi_{P'} \in \mathrm{Hom}(\mathcal{S}(v), \mathcal{S}(e))$. In particular for every pair v, w of vertices and and every pair P, P' of surjective paths from v to w, we require that $\psi_P = \psi_{P'} \in \mathrm{Hom}(\mathcal{S}(v), \mathcal{S}(w))$.

Recall that $\Gamma(\mathcal{S})$ is the set of global sections of $\mathcal{S}$.

Proposition 2.3.2. *Suppose $\mathcal{S}$ is locally cyclic and v is a hub of $\mathcal{S}$.*

1. *The map $f_v : \Gamma(\mathcal{S}) \to \mathcal{S}(v)$ defined by $\boldsymbol{\kappa} \mapsto \kappa_v$ is injective, and is surjective if and only if $\mathcal{S}$ has trivial monodromy.*
2. *If $\boldsymbol{\kappa} \in \Gamma(\mathcal{S})$, and if u is a vertex such that $\kappa_u \neq 0$ and κ_u generates $p^k\mathcal{S}(u)$ for some $k \in \mathbf{Z}^+$, then κ_w generates $p^k\mathcal{S}(w)$ for every vertex w.*

Exercise 2.3.3. Prove Proposition 2.3.2

Definition 2.3.4. A global section $\kappa \in \Gamma(\mathcal{S})$ will be called *primitive* if for every vertex v, $\kappa(v) \in \mathcal{S}(v)$ is a generator of the R-module $\mathcal{S}(v)$.

It follows from Proposition 2.3.2 that a locally cyclic sheaf $\mathcal{S}$ with a hub has a primitive global section if and only if $\mathcal{S}$ has trivial monodromy.

The Selmer sheaf will not in general be locally cyclic. However, we will see later that under suitable hypotheses, there is a natural subsheaf $\mathcal{H}'$ of the Selmer sheaf $\mathcal{H}$ such that $\mathcal{H}'$ is locally cyclic with trivial monodromy, $\mathcal{H}'$ has hub vertices, and every global section of $\mathcal{H}$ is a global section of $\mathcal{H}'$, i.e.,

$$\mathbf{KS}(A, \mathcal{F}) = \Gamma(\mathcal{H}) = \Gamma(\mathcal{H}').$$

2.4. Hypotheses on A and $\mathcal{F}$.

From now on we will assume that all of the following hypotheses hold. Let $\bar{A} = A \otimes_R \mathbf{F}_p$. We will assume that in addition to being free of finite rank over R, A satisfies:

(H.1) $\bar{A}$ is an absolutely simple $\mathbf{F}_p[G_{\mathbf{Q}}]$-module, not isomorphic (as a $G_{\mathbf{Q}}$-module) to $\mathbf{F}_p$ or to $\boldsymbol{\mu}_p$.

(H.2) There is a $\tau \in G_{\mathbf{Q}}$ such that $\tau = 1$ on $\boldsymbol{\mu}_{p^\infty}$ and $A/(\tau - 1)A$ is free of rank one over R.

(H.3) $H^1(\mathbf{Q}(A)/\mathbf{Q}, \bar{A}) = H^1(\mathbf{Q}(A^*)/\mathbf{Q}, \bar{A}^*) = 0$, where $\mathbf{Q}(A)$ is the fixed field of the kernel of the map $G_{\mathbf{Q}} \to \mathrm{Aut}(A)$, and similarly for $\mathbf{Q}(A^*)$.

(H.4) Either $\bar{A} \not\cong \bar{A}^*$, or $p \geq 5$.

We will also assume that for every k, $0 \leq k \leq m$, the quotient Selmer structure induced by $\mathcal{F}$ on A/p^kA (via the map $A \twoheadrightarrow A/p^kA$) is the same as the subgroup Selmer structure induced by $\mathcal{F}$ on A/p^kA (via the map $p^{m-k} : A/p^kA \hookrightarrow A$), where the induced Selmer structures are defined in Exercise 1.5.4. In other words, for every v,

(H.5) (image of $H^1_{\mathcal{F}}(\mathbf{Q}_v, A)$ under $H^1(\mathbf{Q}_v, A) \to H^1(\mathbf{Q}_v, A/p^kA)$)
= (inverse image of $H^1_{\mathcal{F}}(\mathbf{Q}_v, A)$ under $H^1(\mathbf{Q}_v, A/p^kA) \to H^1(\mathbf{Q}_v, A)$).

Remark 2.4.1. Hypotheses (H.1), (H.2), and (H.3) are generally requiring that the image of $G_{\mathbf{Q}}$ in $\mathrm{Aut}(A)$ is sufficiently large. For a discussion of the condition on $\mathcal{F}$, and some sufficient conditions for it to be satisfied, see [**MR1**, §3.7]. (Note that the condition on $\mathcal{F}$ is vacuous if $m = 1$, $R = \mathbf{F}_p$.)

If $(A, \mathcal{F})$ satisfy the conditions above, then so do $(A/p^kA, \mathcal{F})$ for $0 \leq k \leq m$.

Exercise 2.4.2. Show that under the assumptions above, $\mathcal{P}$ has positive density. Hint: check that if $\ell \notin \Sigma$ and the Frobenius of ℓ in $\mathrm{Gal}(\mathbf{Q}(A, \boldsymbol{\mu}_{p^m})$ is in the conjugacy class of the element τ of (H.2), then $\ell \in \mathcal{P}$.

Exercise 2.4.3. Show that (H.5) is automatically satisfied for $v \notin \Sigma$.

Exercise 2.4.4 (Lemma 3.7.4 of [**MR1**])**.** Show that if A and $\mathcal{F}$ satisfy the assumptions above, and $n \in \mathcal{N}$, then so do $(A, \mathcal{F}(n))$.

Proposition 2.4.5. *Under the assumptions above, if* $n \in \mathcal{N}$ *and* $0 \leq k \leq m$, *there are isomorphisms*

(1) $H^1_{\mathcal{F}(n)}(\mathbf{Q}, A/p^kA) \xrightarrow{\sim} H^1_{\mathcal{F}(n)}(\mathbf{Q}, A[p^k]) \xrightarrow{\sim} H^1_{\mathcal{F}(n)}(\mathbf{Q}, A)[p^k]$ *induced by* $A/p^kA \xrightarrow{\sim} A[p^k] \hookrightarrow A$,

(2) $H^1_{\mathcal{F}(n)}(\mathbf{Q}, A)[p^k] = \ker\big[H^1_{\mathcal{F}(n)}(\mathbf{Q}, A) \to H^1_{\mathcal{F}(n)}(\mathbf{Q}, A/p^{m-k}A)\big]$,

(3) $H^1_{\mathcal{F}(n)^*}(\mathbf{Q}, A^*[p^k]) \xrightarrow{\sim} H^1_{\mathcal{F}(n)^*}(\mathbf{Q}, A^*)[p^k]$ *induced by* $A^*[p^k] \hookrightarrow A^*$.

Exercise 2.4.6 (Lemma 3.5.3, 3.5.4 of [**MR1**])**.** Prove Lemma 2.4.5. (By Exercise 2.4.4, it is enough to do this for $n = 1$.)

Exercise 2.4.7. Show that the composition $A/p^kA \xrightarrow{\sim} A[p^k] \hookrightarrow A$ induces an inclusion $\mathbf{KS}(A/p^kA) \hookrightarrow \mathbf{KS}(A)[p^k]$. Why is not obvious that this inclusion is an isomorphism?

2.5. The core Selmer group.

Recall that $\bar{A} = A \otimes \mathbf{F}_p$.

Definition 2.5.1. If $n \in \mathcal{N}$, define

$$\lambda(n, A) = \mathrm{length}(H^1_{\mathcal{F}(n)}(\mathbf{Q}, A)) = \mathrm{length}(\mathcal{H}(n)),$$
$$\lambda(n, A^*) = \mathrm{length}(H^1_{\mathcal{F}(n)^*}(\mathbf{Q}, A^*)),$$

and similarly with A replaced by A/p^kA. Note that by Proposition 2.4.5,

$$\lambda(n, A) = 0 \Longleftrightarrow \lambda(n, \bar{A}) = 0, \quad \lambda(n, A^*) = 0 \Longleftrightarrow \lambda(n, \bar{A}^*) = 0.$$

Theorem 2.5.2. *There are integers $r, s \geq 0$, with one of them equal to zero, such that for every $n \in \mathcal{N}$ there is a noncanonical isomorphism*

$$H^1_{\mathcal{F}(n)}(\mathbf{Q}, A) \oplus R^r \cong H^1_{\mathcal{F}(n)^*}(\mathbf{Q}, A^*) \oplus R^s.$$

Proof. To prove the existence of such an isomorphism, it is enough to show that for $1 \leq k \leq m$, the kernels of p^k on the left-hand side and on the right-hand side have the same order. In other words, we need to show that there is a $t \in \mathbf{Z}$ such that for every n,

$$\mathrm{length}(H^1_{\mathcal{F}(n)}(\mathbf{Q}, A)[p^k]) - \mathrm{length}(H^1_{\mathcal{F}(n)^*}(\mathbf{Q}, A^*)[p^k]) = kt.$$

By Proposition 2.4.5, this is equivalent to

$$\lambda(n, A/p^kA) - \lambda(n, A^*[p^k]) = kt.$$

By Exercise 2.1.4, the left-hand side is independent of n, so we only need to consider $n = 1$. In this case what we need follows from [**Wi**, Proposition 1.6] (see also [**MR1**, Proposition 2.3.5]) and [**MR1**, Proposition 1.1.5]. □

Definition 2.5.3. Define the *core rank* $\chi(A)$ of A (suppressing $\mathcal{F}$ from the notation) to be the nonnegative integer s of Theorem 2.5.2. We call $n \in \mathcal{N}$ a *core vertex* if either $\lambda(n, A) = 0$ or $\lambda(n, A^*) = 0$.

Exercise 2.5.4. Show the following:

(1) If $\chi(A) > 0$, then $H^1_{\mathcal{F}(n)}(\mathbf{Q}, A) \cong H^1_{\mathcal{F}(n)^*}(\mathbf{Q}, A^*) \oplus R^{\chi(A)}$ for every $n \in \mathcal{N}$.

(2) If n is a core vertex, then $H^1_{\mathcal{F}(n)}(\mathbf{Q}, A)$ is free over R of rank $\chi(A)$,

(3) If n is a core vertex and $\chi(A) > 0$ then $H^1_{\mathcal{F}(n)^*}(\mathbf{Q}, A^*) = 0$.

(4) If n is a core vertex and $\chi(A) = 0$ then $H^1_{\mathcal{F}(n)}(\mathbf{Q}, A) = 0$.

2.6. Stepping along the Selmer graph.

The next lemma is an application of the global duality (Theorem 1.10.2), and is crucial in many of the calculations that follow.

Proposition 2.6.1. *Suppose $n\ell \in \mathcal{N}$. We have the following diagrams of inclusions, in which the labels on the arrows are the lengths of the corresponding cyclic cokernels.*

$$\begin{tikzcd}
 & H^1_{\mathcal{F}^\ell(n)}(\mathbf{Q},A) & \\
H^1_{\mathcal{F}(n)}(\mathbf{Q},A) \arrow[ur, hook, "a"] & & H^1_{\mathcal{F}(n\ell)}(\mathbf{Q},A) \arrow[ul, hook', "b"'] \\
 & H^1_{\mathcal{F}_\ell(n)}(\mathbf{Q},A) \arrow[ul, hook', "c"] \arrow[ur, hook, "d"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & H^1_{\mathcal{F}_\ell(n)^*}(\mathbf{Q},A^*) & \\
H^1_{\mathcal{F}(n)^*}(\mathbf{Q},A^*) \arrow[ur, hook, "c^*"] & & H^1_{\mathcal{F}(n\ell)^*}(\mathbf{Q},A^*) \arrow[ul, hook', "d^*"'] \\
 & H^1_{\mathcal{F}^\ell(n)^*}(\mathbf{Q},A^*) \arrow[ul, hook', "a^*"] \arrow[ur, hook, "b^*"'] &
\end{tikzcd}$$

These lengths satisfy

(1) $0 \le a, b, c, d, a^*, b^*, c^*, d^* \le m$,
(2) $a + c = b + d$, $a^* + c^* = b^* + d^*$,
(3) $a + a^* = b + b^* = c + c^* = d + d^* = m$,
(4) $a \ge d$, $b \ge c$, $c^* \ge b^*$, $d^* \ge a^*$.

Proof. By definition

$$H^1_{\mathcal{F}(n)}(\mathbf{Q},A) = \ker[H^1_{\mathcal{F}^\ell(n)}(\mathbf{Q},A) \to H^1(\mathbf{Q}_\ell,A)/H^1_{\mathrm{u}}(\mathbf{Q}_\ell,A)],$$
$$H^1_{\mathcal{F}_\ell(n)}(\mathbf{Q},A) = \ker[H^1_{\mathcal{F}(n)}(\mathbf{Q},A) \to H^1_{\mathrm{u}}(\mathbf{Q}_\ell,A)],$$

and similarly for A^*. The two diagrams come from the definitions in this way. Since $H^1_{\mathrm{u}}(\mathbf{Q}_\ell,A)$, $H^1_{\mathrm{t}}(\mathbf{Q}_\ell,A)$, $H^1_{\mathrm{u}}(\mathbf{Q}_\ell,A^*)$, and $H^1_{\mathrm{t}}(\mathbf{Q}_\ell,A^*)$ are all free of rank one over R by Exercise 1.9.7, the inequalities (1) hold. The equalities (2) are immediate from the diagrams.

The equality $a + a^* = m$ follows from global duality (apply Theorem 1.10.2 with $\mathcal{G}_1 = \mathcal{F}(n)$ and $\mathcal{G}_2 = \mathcal{F}^\ell(n)$), and similarly for the other three equalities of (3). Finally, we have

$$H^1_{\mathcal{F}(n)}(\mathbf{Q},A) \cap H^1_{\mathcal{F}(n\ell)}(\mathbf{Q},A) = H^1_{\mathcal{F}_\ell(n)}(\mathbf{Q},A).$$

The first two inequalities of (4) follow from this, and the other two similarly with $(A,\mathcal{F})$ replaced by $(A^*,\mathcal{F}^*)$. □

Corollary 2.6.2. *Suppose $n\ell \in \mathcal{N}$.*

(1) $|\lambda(n\ell,A) - \lambda(n,A)| \le m$ *and* $|\lambda(n\ell,A^*) - \lambda(n,A^*)| \le m$.
(2) *If the localization map $H^1_{\mathcal{F}(n)}(\mathbf{Q},A) \to H^1_{\mathrm{u}}(\mathbf{Q}_\ell,A)$ is surjective, then*

$$H^1_{\mathcal{F}(n\ell)^*}(\mathbf{Q},A^*) = H^1_{\mathcal{F}^\ell(n)^*}(\mathbf{Q},A^*) \subset H^1_{\mathcal{F}(n)^*}(\mathbf{Q},A^*).$$

(3) *The image of the composition*

$$p^{\lambda(n,A^*)}H^1_{\mathcal{F}(n)}(\mathbf{Q},A) \xrightarrow{\mathrm{loc}_\ell} H^1_{\mathrm{u}}(\mathbf{Q}_\ell,A) \xrightarrow{\phi_\ell^{\mathrm{ut}}} H^1_{\mathrm{t}}(\mathbf{Q}_\ell,A) \otimes G_\ell$$

is equal to the image of $p^{\lambda(n\ell,A^*)}H^1_{\mathcal{F}(n\ell)}(\mathbf{Q},A) \otimes G_\ell \xrightarrow{\mathrm{loc}_\ell} H^1_{\mathrm{t}}(\mathbf{Q}_\ell,A) \otimes G_\ell$.

(4) *If both localization maps*

$$H^1_{\mathcal{F}(n)}(\mathbf{Q},A)[p] \to H^1_{\mathrm{u}}(\mathbf{Q}_\ell,A), \qquad H^1_{\mathcal{F}(n)^*}(\mathbf{Q},A^*)[p] \to H^1_{\mathrm{u}}(\mathbf{Q}_\ell,A^*)$$

are nonzero, then $\lambda(n\ell,\bar{A}) = \lambda(n,\bar{A}) - 1$ *and* $\lambda(n\ell,\bar{A}^*) = \lambda(n,\bar{A}^*) - 1$.

Proof. Consider the diagrams of Proposition 2.6.1. Assertion (1) is immediate. Recall (Exercise 1.9.7) that $H^1_{\mathrm{u}}(\mathbf{Q}_\ell,A)$, $H^1_{\mathrm{t}}(\mathbf{Q}_\ell,A)$, $H^1_{\mathrm{u}}(\mathbf{Q}_\ell,A^*)$, and $H^1_{\mathrm{t}}(\mathbf{Q}_\ell,A^*)$ are free of rank one over R, and ϕ_ℓ^{ut} is an isomorphism.

If the localization map in (2) is surjective, then $c = m$ in the left-hand diagram of Proposition 2.6.1. Therefore by (3) and (4) of that lemma, $b^* = 0$, which proves (2).

To prove (3) it is enough to show that $\mathrm{length}(C_n) = \mathrm{length}(C_{n\ell})$ where C_n and $C_{n\ell}$ are the images of $p^{\lambda(n,A^*)}H^1_{\mathcal{F}(n)}(\mathbf{Q},A)$ and $p^{\lambda(n\ell,A^*)}H^1_{\mathcal{F}(n\ell)}(\mathbf{Q},A)$, respectively, under localization at ℓ. The left-hand diagram of Proposition 2.6.1 shows that

$$\mathrm{length}(C_n) = \max\{0, c - \lambda(n,A^*)\}, \qquad \mathrm{length}(C_{n\ell}) = \max\{0, d - \lambda(n\ell,A^*)\}.$$

The right-hand diagram shows that

$$\lambda(n,A^*) - \lambda(n\ell,A^*) = d^* - c^* = c - d,$$

so $\mathrm{length}(C_n) = \mathrm{length}(C_{n\ell})$.

For (4), if the localization maps in question are nonzero, then using Proposition 2.4.5 (with $k = 1$) we see that the localization maps

$$H^1_{\mathcal{F}(n)}(\mathbf{Q},\bar{A}) \to H^1_{\mathrm{u}}(\mathbf{Q}_\ell,\bar{A}), \quad H^1_{\mathcal{F}(n)^*}(\mathbf{Q},\bar{A}^*) \to H^1_{\mathrm{u}}(\mathbf{Q}_\ell,\bar{A}^*)$$

are surjective. Applying Proposition 2.6.1 with A replaced by $\bar{A}$ (and $m = 1$) we have $c = a^* = 1$, so $b^* \le c^* = 0$ and $d \le a = 0$, so $\lambda(n\ell,\bar{A}^*) = \lambda(n,\bar{A}^*) - 1$ and $\lambda(n\ell,\bar{A}) = \lambda(n,\bar{A}) - 1$. □

2.7. Choosing useful primes.

Proposition 2.7.1. *Suppose* $c \in H^1_{\mathcal{F}(n)}(\mathbf{Q},A)$ *and* $d \in H^1_{\mathcal{F}(n)^*}(\mathbf{Q},A^*)$ *are both nonzero. Then* $\{\ell \in \mathcal{P} : \mathrm{Res}_\ell(c) \ne 0$ *and* $\mathrm{Res}_\ell(d) \ne 0\}$ *has positive density.*

Sketch of proof. (For details, see [**MR1**, Proposition 3.6.1].) First, find $\gamma \in G_{\mathbf{Q}}$ such that

(1) $\gamma = \tau$ on $\mathbf{Q}(A,\boldsymbol{\mu}_{p^k})$, where τ is as in (H.2) of §2.4,
(2) $c(\gamma) \notin (\tau - 1)A$,
(3) $d(\gamma) \notin (\tau - 1)A^*$.

where $c(\gamma)$ means the image of γ under any cocycle representing c, which is well-defined modulo $(\gamma - 1)A = (\tau - 1)A$, and similarly for $d(\gamma)$. (One needs to check that these three conditions can be satisfied simultaneously; this uses our hypotheses on A).

If $\ell \notin \Sigma$, $\ell \nmid n$, is a prime whose Frobenius (in a suitably large extension of $\mathbf{Q}$) is γ, then it follows from the first condition implies that $\ell \in \mathcal{P}$ (Exercise 2.4.2), from the second condition that $\mathrm{Res}_\ell(c) \in H^1_{\mathrm{u}}(\mathbf{Q}_\ell,A) \cong A/(\tau - 1)A$ is nonzero, and from the third condition that $\mathrm{Res}_\ell(d) \in H^1_{\mathrm{u}}(\mathbf{Q}_\ell,A^*) \cong A^*/(\tau - 1)A^*$ is nonzero. Thus ℓ belongs to the set in question. □

Corollary 2.7.2. *Suppose* $n \in \mathcal{N}$ *is not a core vertex. Then there is an* $\ell \in \mathcal{P}$ *such that* $\lambda(n\ell,\bar{A}) = \lambda(n,\bar{A}) - 1$ *and* $\lambda(n\ell,\bar{A}^*) = \lambda(n,\bar{A}^*) - 1$.

If in addition $\boldsymbol{\kappa} \in \mathbf{KS}(A)$ *and* $\kappa_n \ne 0$, *then* ℓ *can be chosen so* $\kappa_{n\ell} \ne 0$.

Proof. Since n is not a core vertex, $H^1_{\mathcal{F}(n)}(\mathbf{Q}, A)$ and $H^1_{\mathcal{F}(n)^*}(\mathbf{Q}, A^*)$ are both nonzero. Apply Proposition 2.7.1 with a nonzero $c \in H^1_{\mathcal{F}(n)}(\mathbf{Q}, A)[p]$ and a nonzero $d \in H^1_{\mathcal{F}(n)^*}(\mathbf{Q}, A^*)[p]$, and let $\ell \in \mathcal{P}$ be such that $\mathrm{Res}_\ell(c) \neq 0$ and $\mathrm{Res}_\ell(d) \neq 0$. For this ℓ, Corollary 2.6.2(4) shows that $\lambda(n\ell, \bar{A}) = \lambda(n, \bar{A}) - 1$ and $\lambda(n\ell, \bar{A}^*) = \lambda(n, \bar{A}^*) - 1$.

If we take c to be a multiple of κ_n, then $\mathrm{Res}_\ell(\kappa_n) \neq 0$, so $\mathrm{Res}_\ell(\kappa_{n\ell}) \neq 0$ (by definition of a Kolyvagin system), so $\kappa_{n\ell} \neq 0$. □

Corollary 2.7.3. *Suppose $n \in \mathcal{N}$. Then there is a core vertex n' and a path of length $\min\{\lambda(n, \bar{A}), \lambda(n, \bar{A}^*)\}$ from n to n'.*

If in addition $\boldsymbol{\kappa} \in \mathbf{KS}(A)$ and $\kappa_n \neq 0$, then n' can be chosen so $\kappa_{n'} \neq 0$.

If $n \in \mathcal{N}$, let $\omega(n)$ denote the number of prime factors of n.

Corollary 2.7.4. *Let $r = \min\{\dim_{\mathbf{F}_p} H^1_{\mathcal{F}}(\mathbf{Q}, \bar{A}), \dim_{\mathbf{F}_p} H^1_{\mathcal{F}^*}(\mathbf{Q}, \bar{A}^*)\}$. If n is a core vertex, then $\omega(n) \geq r$. There are core vertices n with $\omega(n) = r$.*

Exercise 2.7.5. Prove Corollaries 2.7.3 and 2.7.4.

Theorem 2.7.6. *If $\chi(A) = 0$, then $\mathbf{KS}(A) = 0$.*

Proof. Suppose $\boldsymbol{\kappa} \in \mathbf{KS}(A)$ and $n \in \mathcal{N}$. If $\kappa_n \neq 0$, then by Corollary 2.7.3 there is a core vertex n' such that $\kappa_{n'} \in H^1_{\mathcal{F}(n')}(\mathbf{Q}, A)$ is nonzero. But since $\chi(A) = 0$, we have $H^1_{\mathcal{F}(n')}(\mathbf{Q}, A) = 0$ by Exercise 2.5.4(4), so this is impossible. □

Remark 2.7.7. Theorem 2.7.6 gives another proof of Exercise 2.2.4, because if $H^1_{\mathcal{F}}(\mathbf{Q}, A) = 0$ then Theorem 2.5.2 shows that $\chi(A) = 0$.

2.8. The stub subsheaf.

We define a subsheaf of the Selmer sheaf $\mathcal{H} = \mathcal{H}_{(A,\mathcal{F})}$ of Definition 2.2.3 as follows.

Definition 2.8.1. The *sheaf of stub Selmer modules* $\mathcal{H}' = \mathcal{H}'_{(A,\mathcal{F})}$ is the subsheaf of $\mathcal{H}$ defined by

- $\mathcal{H}'(n) = p^{\lambda(n,A^*)}\mathcal{H}(n) = p^{\lambda(n,A^*)}H^1_{\mathcal{F}(n)}(\mathbf{Q}, A) \otimes G_n \subset \mathcal{H}(n)$ if $n \in \mathcal{N}$,
- $\mathcal{H}'(e) = \psi^e_n(\mathcal{H}'(n)) \subset \mathcal{H}(e)$ if e is an edge joining n and $n\ell$,

and the vertex-to-edge maps $\psi^e_n, \psi^e_{n\ell}$ are the restrictions of those of $\mathcal{H}$.

By Corollary 2.6.2, $\psi^e_{n\ell}(\mathcal{H}'(n\ell)) = \psi^e_n(\mathcal{H}'(n))$, so $\mathcal{H}'$ is a well-defined sheaf and all vertex-to-edge maps are surjective.

Exercise 2.8.2. Show that for every n, $\mathcal{H}'(n)$ is free of rank $\chi(A)$ over $\mathbf{Z}/p^k\mathbf{Z}$, where $k = \max\{m - \lambda(n, A^*), 0\}$. Deduce that if $\chi(A) = 1$, then $\mathcal{H}'$ is locally cyclic.

Exercise 2.8.3. Show that if $\chi(A) = 1$, then Corollary 2.7.3 can be strengthened to say that for every vertex n, there is a *surjective path* (see Definition 2.3.1) from some core vertex to n. (Hint: in the proof of Corollary 2.7.2, take c to be a nonzero element of $p^{m-1}H^1_{\mathcal{F}(n)}(\mathbf{Q}, A)$. Show that

$$\mathrm{Res}_\ell : H^1_{\mathcal{F}(n)}(\mathbf{Q}, A) \to H^1_{\mathrm{u}}(\mathbf{Q}_\ell, A)$$

is surjective, and so

$$\mathrm{Res}_\ell : p^{\lambda(n,A^*)}H^1_{\mathcal{F}(n)}(\mathbf{Q}, A) \to p^{\lambda(n,A^*)}H^1_{\mathrm{u}}(\mathbf{Q}_\ell, A)$$

is an isomorphism.)

Theorem 2.8.4. *Suppose $\chi(A) = 1$. Then the natural inclusion $\Gamma(\mathcal{H}') \hookrightarrow \Gamma(\mathcal{H})$ is an isomorphism, i.e., if $\boldsymbol{\kappa} \in \mathbf{KS}(A)$ then $\kappa_n \in \mathcal{H}'(n)$ for every $n \in \mathcal{N}$.*

Sketch of proof. We give the proof in the special case where $m = 1$, so $R = \mathbf{F}_p$. See [**MR1**, Theorem 4.3.4] for the complete proof. (In this special case, it is not necessary to assume that $\chi(A) = 1$.)

Suppose $R = \mathbf{F}_p$ and $\boldsymbol{\kappa} \in \mathbf{KS}(A)$. If n is a core vertex, then $\mathcal{H}'(n) = \mathcal{H}(n)$ and there is nothing to prove. If n is not a core vertex, then $\mathcal{H}'(n) = 0$ and we need to show $\kappa_n = 0$.

Suppose n is not a core vertex, and $\kappa_n \neq 0$. Using Proposition 2.7.1, we can find an $\ell \in \mathcal{P}$ such that $\mathrm{Res}_\ell(\kappa_n) \neq 0$ and $\mathrm{Res}_\ell(H^1_{\mathcal{F}^*}(\mathbf{Q}, A^*)) \neq 0$. In the notation of Proposition 2.6.1, we have $a^* = 1$, so $a = 0$, so $d = 0$. But then $\mathrm{Res}_\ell(\kappa_{n\ell}) = 0$, so $\mathrm{Res}_\ell(\kappa_n) = 0$ by definition of a Kolyvagin system. This is a contradiction. □

Theorem 2.8.5. *Suppose $\chi(A) = 1$. Then the stub sheaf $\mathcal{H}'$ is locally cyclic, and every core vertex is a hub.*

A key part of the proof of Theorem 2.8.5 is the following.

Definition 2.8.6. Suppose $\chi(A) = 1$. Let $\mathcal{X}^0$ be the subgraph of $\mathcal{X}$ whose vertices are the core vertices in $\mathcal{N}$, with an edge joining n and $n\ell$ whenever both maps ψ^e_n and $\psi^e_{n\ell}$ are isomorphisms.

Let $\mathcal{H}^0$ be the restriction of the Selmer sheaf $\mathcal{H}$ to $\mathcal{X}^0$, i.e., $\mathcal{H}^0(n) = \mathcal{H}(n)$ for core vertices n, and $\mathcal{H}^0(e) = \mathcal{H}(e)$. Note that $\mathcal{H}^0$ is also the restriction of $\mathcal{H}'$ to $\mathcal{X}^0$, since $\mathcal{H}'$ and $\mathcal{H}$ agree precisely at the vertices and edges of $\mathcal{X}^0$.

Theorem 2.8.7. *The graph $\mathcal{X}^0$ is connected.*

Proof. The proof is "more of the same". See [**MR1**, Theorem 4.3.12] □

Proof of Theorem 2.8.5. We have already seen (Exercise 2.8.2) that $\mathcal{H}'$ is locally cyclic. Suppose $n \in \mathcal{N}$ and v is a core vertex; we need to show that there is a surjective path from v to n. By Exercise 2.8.3, there is a core vertex w and a surjective path from w to n. By Theorem 2.8.7, there is a path in $\mathcal{X}^0$ from v to w. But every path in $\mathcal{X}^0$ is a surjective path, so the concatenated path from v to w to n is a surjective path from v to n. □

Theorem 2.8.8 (Howard, Appendix B of [**MR1**])**.** *For every $n \in \mathcal{N}$, the map $\Gamma(\mathcal{H}') \to \mathcal{H}'(n)$ is surjective.*

Corollary 2.8.9.
(1) *If $\chi(A) = 0$, then $\mathbf{KS}(A) = 0$.*
(2) *If $\chi(A) = 1$, then $\mathbf{KS}(A)$ is free of rank one over R.*
(3) *If $\chi(A) > 1$, then $\mathbf{KS}(A)$ is infinite.*

Proof. The first assertion is Theorem 2.7.6. If $\chi(A) = 1$ and n is a core vertex (core vertices exist by Corollary 2.7.3), then Theorem 2.8.5 and Proposition 2.3.2 show that the map $\mathbf{KS}(A) \to \mathcal{H}(n)$ is injective, Theorem 2.8.8 shows that it is surjective, and Exercise 2.5.4(2) shows that $\mathcal{H}(n)$ is free of rank one over R.

For (3), see the following exercise. □

Exercise 2.8.10 (Proof of Corollary 2.8.9(3))**.** If $\chi(A, \mathcal{F}) > 0$, and $\ell \in \mathcal{P}$, use Proposition 2.6.1 to show that $\chi(\bar{A}, \mathcal{F}_\ell) = \chi(\bar{A}, \mathcal{F}) - 1$. (Note: the Selmer structure $\mathcal{F}_\ell$ for A may not satisfy condition (H.5) of §2.4, but for $\bar{A}$, (H.5) is vacuous.) Deduce that there are many different n such that $\chi(\bar{A}, \mathcal{F}_n) = 1$, and for each of these we have $\mathbf{KS}(\bar{A},\mathcal{F}_n) \subset \mathbf{KS}(\bar{A},\mathcal{F}) = \mathbf{KS}(A,\mathcal{F})[p]$. Now apply Corollary 2.8.9(2) to each of the $\mathbf{KS}(\bar{A},\mathcal{F}_n)$.

We end this section with one example of how to use the results above to bound the size of a Selmer group.

Corollary 2.8.11. *Suppose $\chi(A) = 1$ and $\boldsymbol{\kappa} \in \mathbf{KS}(A)$. If $\kappa_1 \in H^1_{\mathcal{F}}(\mathbf{Q},A)$ has order p^k, then*

$$\mathrm{length}(H^1_{\mathcal{F}^*}(\mathbf{Q},A^*)) \leq m - k.$$

Proof. By Theorem 2.8.4(1), $\kappa_1 \in p^{\mathrm{length}(H^1_{\mathcal{F}^*}(\mathbf{Q},A^*))}H^1_{\mathcal{F}}(\mathbf{Q},A)$, so κ_1 is killed by $p^{m-\mathrm{length}(H^1_{\mathcal{F}^*}(\mathbf{Q},A^*))}$. □

2.9. Recovering the group structure of the dual Selmer group.

For this section we suppose that A is a $G_{\mathbf{Q}}$-module, free of finite rank over $R = \mathbf{Z}/p^m\mathbf{Z}$, and $\mathcal{F}$ is a Selmer structure for A, satisfying all the hypotheses of §2.4. We assume in addition that $\chi(A) = 1$.

Proposition 2.9.1. *Suppose $\chi(A) = 1$ and $0 \leq k \leq m$. The natural quotient map $A \twoheadrightarrow A/p^kA$ induces a map $\mathbf{KS}(A) \twoheadrightarrow \mathbf{KS}(A/p^kA)$.*

Exercise 2.9.2. Prove Proposition 2.9.1 Hint: this is not as easy as it might seem, because the index set $\mathcal{N}$ in the definition of a Kolyvagin system is larger for A/p^kA than for A. Use Exercise 2.4.7, and show that the map $\mathbf{KS}(A/p^kA) \hookrightarrow \mathbf{KS}(A)[p^k]$ of Exercise 2.4.7 is an isomorphism if $\chi(A) = 1$.

Proposition 2.9.3. *Suppose $\chi(A) = 1$ and $\boldsymbol{\kappa} \in \mathbf{KS}(A)$. Then the following are equivalent.*

(1) *κ_n generates $\mathcal{H}'(n)$ for every $n \in \mathcal{N}$,*
(2) *κ_n generates $\mathcal{H}'(n)$ for some $n \in \mathcal{N}$ with $\mathcal{H}'(n) \neq 0$,*
(3) *$\boldsymbol{\kappa} \notin p\mathbf{KS}(A)$,*
(4) *$p^{m-1}\boldsymbol{\kappa} \neq 0$,*
(5) *$\boldsymbol{\kappa}$ generates $\mathbf{KS}(A)$,*
(6) *the image of $\boldsymbol{\kappa}$ in $\mathbf{KS}(\bar{A})$ (under the map of Proposition 2.9.1) is nonzero,*

Exercise 2.9.4. Prove Proposition 2.9.3, using Theorems 2.8.4 and 2.8.5, and Proposition 2.3.2.

Definition 2.9.5. We say that $\boldsymbol{\kappa} \in \mathbf{KS}(A)$ is *primitive* if it satisfies the equivalent conditions of Proposition 2.9.3

If $\boldsymbol{\kappa}$ is primitive, we have the following sharpening of Corollary 2.8.11.

Corollary 2.9.6. *Suppose $\chi(A) = 1$ and $\boldsymbol{\kappa} \in \mathbf{KS}(A)$ is primitive. If $\kappa_1 \neq 0$ then*

$$\mathrm{length}(H^1_{\mathcal{F}^*}(\mathbf{Q},A^*)) = m - \mathrm{length}(R\kappa_1) = \max\{i : \kappa_1 \in p^iH^1_{\mathcal{F}}(\mathbf{Q},A)\}.$$

If $\kappa_1 = 0$ then $\mathrm{length}(H^1_{\mathcal{F}^*}(\mathbf{Q},A^*)) \geq k$.

Proof. Let $\lambda = \mathrm{length}(H^1_{\mathcal{F}^*}(\mathbf{Q},T^*))$. Since $\boldsymbol{\kappa}$ is primitive, we have

$$R\kappa_1 = \mathcal{H}'(1) = p^\lambda H^1_{\mathcal{F}}(\mathbf{Q},A),$$

and $\mathrm{length}(p^\lambda H^1_{\mathcal{F}}(\mathbf{Q},A)) = \max\{m-\lambda, 0\}$ by Exercise 2.8.2. □

We can formulate a more precise version of Corollary 2.9.6, which in some cases determines the group structure of $H^1_{\mathcal{F}^*}(\mathbf{Q},T^*)$.

Definition 2.9.7. If $\boldsymbol{\kappa} \in \mathbf{KS}(T)$ and $r \geq 0$, define

$$\partial^r(\boldsymbol{\kappa}) = \max\{k : k \leq m \text{ and } \kappa_n \in p^k H^1_{\mathcal{F}(n)}(\mathbf{Q}, A) \otimes G_n \\ \text{for every } n \in \mathcal{N} \text{ with } \omega(n) = r\}.$$

The *elementary divisors* of $\boldsymbol{\kappa}$ are defined by

$$e_i(\boldsymbol{\kappa}) = \partial^{i-1}(\boldsymbol{\kappa}) - \partial^i(\boldsymbol{\kappa}), \quad i \geq 1.$$

Proposition 2.9.8. *Suppose $\chi(A) = 1$, $\boldsymbol{\kappa} \in \mathbf{KS}(A)$, and let j be such that $\boldsymbol{\kappa}$ generates $p^j\mathbf{KS}(A)$. Write $H^1_{\mathcal{F}^*}(\mathbf{Q}, A^*) \cong \oplus_i \mathbf{Z}/p^{d_i}\mathbf{Z}$ with nonnegative integers $d_1 \geq d_2 \geq \cdots$. Then for every $r \geq 0$,*

$$\partial^r(\boldsymbol{\kappa}) = \min\{m, j + \sum_{i>r} d_i\}.$$

Proof. Note that since $\boldsymbol{\kappa}$ generates $p^j\mathbf{KS}(A)$, Proposition 2.3.2 shows that κ_n generates $p^j\mathcal{H}'(n) = p^{j+\lambda(n,A^*)}\mathcal{H}(n)$ for every n. Therefore

$$\partial^r(\boldsymbol{\kappa}) = \min\{m, j + \lambda(n, A^*) : n \in \mathcal{N}, \omega(n) = r\},$$

and to prove the proposition we need to show that

$$\min\{\lambda(n, A^*) : n \in \mathcal{N}, \omega(n) = r\} = \sum_{i>r} d_i. \tag{2.3}$$

This is clear when $r = 0$, since $\lambda(1, A^*) = \sum_i d_i$.

Suppose $n \in \mathcal{N}$ and $\omega(n) = r$. Consider the map

$$H^1_{\mathcal{F}^*}(\mathbf{Q}, A^*) \longrightarrow \bigoplus_{\ell \mid n} H^1_{\mathrm{f}}(\mathbf{Q}_\ell, A^*).$$

The right-hand side is free of rank r over R, so the image is a quotient of $H^1_{\mathcal{F}^*}(\mathbf{Q}, A^*)$ generated by (at most) r elements. Hence the image has length at most $\sum_{i \leq r} d_i$. Therefore the kernel has length at least $\sum_{i>r} d_i$. But by definition this kernel is contained in $H^1_{\mathcal{F}(n)^*}(\mathbf{Q}, A^*)$, so we conclude that $\lambda(n, A^*) \geq \sum_{i>r} d_i$, which is one inequality in (2.3).

We will prove the opposite inequality by induction on r. The case $r = 0$ was proved above.

Since $\chi(A) > 0$, Theorem 2.5.2 shows that $p^{m-1}H^1_{\mathcal{F}}(\mathbf{Q}, A) \neq 0$. Fix a nonzero element $c \in p^{m-1}H^1_{\mathcal{F}}(\mathbf{Q}, A) \subset H^1_{\mathcal{F}}(\mathbf{Q}, A)[p]$. If $d_1 > 0$, then choose a nonzero element $c^* \in p^{d_1-1}H^1_{\mathcal{F}^*}(\mathbf{Q}, A^*) \subset H^1_{\mathcal{F}^*}(\mathbf{Q}, A^*)[p]$. Using Proposition 2.7.1, choose a prime $\ell \in \mathcal{P}$ such that the localization $\mathrm{Res}_\ell(c)$ is nonzero and, if $d_1 > 0$, such that $\mathrm{Res}_\ell(c^*)$ is nonzero as well.

It follows that

- the localization map $H^1_{\mathcal{F}}(\mathbf{Q}, A) \to H^1_{\mathrm{u}}(\mathbf{Q}_\ell, A)$ is surjective, and
- $H^1_{(\mathcal{F}^\ell)^*}(\mathbf{Q}, A^*) \cong \oplus_{i \geq 1}\mathbf{Z}/p^{d_{i+1}}\mathbf{Z}$.

By Theorem 2.6.2(2) we have $H^1_{\mathcal{F}(\ell)^*}(\mathbf{Q}, A^*) = H^1_{(\mathcal{F}^\ell)^*}(\mathbf{Q}, A^*)$. Thus

$$\begin{aligned}\min\{\lambda(n, A^*) : n \in \mathcal{N}, \omega(n) = r\} &\leq \min\{\lambda(n\ell, A^*) : n \in \mathcal{N}, \ell \nmid n, \omega(n) = r-1\} \\ &= \min\{\mathrm{length}_R(H^1_{\mathcal{F}(\ell)(n)^*}(\mathbf{Q}, A^*)) : n \in \mathcal{N}, \ell \nmid n, \omega(n) = r-1\} \\ &= \sum_{i>r-1} d_{i+1}\end{aligned}$$

where the last equality comes from our induction hypothesis applied to $(A, \mathcal{F}(\ell))$. This completes the proof of (2.3). $\square$

Theorem 2.9.9. *Suppose* $\chi(A) = 1$, $\boldsymbol{\kappa} \in \mathbf{KS}(A)$, *and* $\kappa_1 \neq 0$. *Then*

$$\partial^0(\boldsymbol{\kappa}) \geq \partial^1(\boldsymbol{\kappa}) \geq \partial^2(\boldsymbol{\kappa}) \geq \cdots \geq 0,$$
$$e_1(\boldsymbol{\kappa}) \geq e_2(\boldsymbol{\kappa}) \geq e_3(\boldsymbol{\kappa}) \geq \cdots \geq 0,$$

$\partial^r(\boldsymbol{\kappa})$ *stabilizes at a value* $\partial^\infty(\boldsymbol{\kappa})$ *for large* r, $e_r(\boldsymbol{\kappa}) = 0$ *for large* r, *and*

$$H^1_{\mathcal{F}^*}(\mathbf{Q}, A^*) \cong \bigoplus_{i \geq 1} \mathbf{Z}/p^{e_i(\boldsymbol{\kappa})}\mathbf{Z}.$$

In particular $\operatorname{length}(H^1_{\mathcal{F}^*}(\mathbf{Q}, A^*)) = \partial^0(\boldsymbol{\kappa}) - \partial^\infty(\boldsymbol{\kappa})$.

Proof. If $\kappa_1 \neq 0$ then $\partial^0(\boldsymbol{\kappa}) < k$, so in Proposition 2.9.8 we have $\partial^r(\boldsymbol{\kappa}) = j + \sum_{i>r} d_i$ for every r. The theorem follows immediately. $\square$

Remark 2.9.10. Theorem 2.9.9 shows that the elementary divisors of $\boldsymbol{\kappa}$ are independent of $\boldsymbol{\kappa}$ as long as $\kappa_1 \neq 0$. Note that $\boldsymbol{\kappa}$ is primitive if and only if $\partial^\infty(\boldsymbol{\kappa}) = 0$.

LECTURE 3

Kolyvagin systems for p-adic representations.

Suppose for this lecture that $\mathcal{A}$ is a free $\mathbf{Z}_p$-module of finite rank, with a continuous action of $G_{\mathbf{Q}}$. We assume further that $\mathcal{A}$ is ramified at only finitely many primes. Let $\mathcal{A}^* = \mathrm{Hom}(\mathcal{A}, \boldsymbol{\mu}_{p^\infty})$. For every positive integer m we have the finite $G_{\mathbf{Q}}$-modules $A_m := A/p^m A$ and $A_m^* = \mathcal{A}^*[p^m]$. We will study Selmer groups attached to $\mathcal{A}^*$ by applying the results of the previous section to A_m and A_m^*.

Typical examples for $\mathcal{A}$ will be

$$\begin{aligned} \mathbf{Z}_p(1) &:= \varprojlim \boldsymbol{\mu}_{p^m}, & \mathbf{Z}_p(1)^* &= \mathbf{Q}_p/\mathbf{Z}_p, \\ T_p(E) &:= \varprojlim E[p^m], & T_p(E)^* &= E[p^\infty], \end{aligned}$$

for an elliptic curve E defined over $\mathbf{Q}$.

3.1. Cohomology groups for p-adic representations.

Exercise 3.1.1. Show that $\mathcal{A}^*$ is a discrete, torsion $G_{\mathbf{Q}}$-module, and $\mathcal{A}^* = \varinjlim A_m^*$.

Since $\mathcal{A}$ is not a discrete $G_{\mathbf{Q}}$-module, our definitions in Lecture 1 do not apply. We will simply define, for any closed subgroup G of $G_{\mathbf{Q}}$,

$$H^0(G, \mathcal{A}) = \mathcal{A}^G, \qquad H^1(G, \mathcal{A}) := \varprojlim H^1(G, A_m).$$

This is the same group one would get by defining $H^1(G, \mathcal{A})$ using continuous cocycles, but that would not be true in general for $H^i(G, \mathcal{A})$ with $i > 1$. Since $\mathcal{A}^*$ is a discrete $G_{\mathbf{Q}}$-module, no modifications are necessary to define $H^i(G, \mathcal{A}^*)$.

The definitions of $H^1_{\mathrm{u}}(\mathbf{Q}_\ell, \mathcal{A})$, Selmer structures for $\mathcal{A}$, and the corresponding Selmer groups, are exactly the same as Definitions 1.4.12 and 1.5.1. If $\mathcal{F}$ is a Selmer structure for $\mathcal{A}$, then $\mathcal{F}$ induces a Selmer structure (that we also denote by $\mathcal{F}$) for every A_m, by taking $H^1_{\mathcal{F}}(\mathbf{Q}_v, A_m)$ to be the image of $H^1_{\mathcal{F}}(\mathbf{Q}_v, \mathcal{A})$ under the canonical map $H^1(\mathbf{Q}_v, \mathcal{A}) \to H^1(\mathbf{Q}_v, A_m)$. This in turn defines a Selmer structure $\mathcal{F}^*$ on every A_m^*, and we also denote by $\mathcal{F}^*$ the Selmer structure on $\mathcal{A}^*$ defined by $H^1_{\mathcal{F}^*}(\mathbf{Q}_\ell, \mathcal{A}^*) = \varinjlim H^1_{\mathcal{F}^*}(\mathbf{Q}_\ell, A_m^*)$.

Exercise 3.1.2. Show that the construction described above defines a Selmer structure on A_m for every m (i.e., show that if $\mathcal{A}$ is unramified at ℓ and $H^1_{\mathcal{F}}(\mathbf{Q}_\ell, \mathcal{A}) = H^1_{\mathrm{u}}(\mathbf{Q}_\ell, \mathcal{A})$, then $H^1_{\mathcal{F}}(\mathbf{Q}_\ell, A_m) = H^1_{\mathrm{u}}(\mathbf{Q}_\ell, A_m)$). Show that

$$H^1_{\mathcal{F}}(\mathbf{Q}, \mathcal{A}) = \varprojlim H^1_{\mathcal{F}}(\mathbf{Q}, A_m), \qquad H^1_{\mathcal{F}^*}(\mathbf{Q}, \mathcal{A}^*) = \varinjlim H^1_{\mathcal{F}^*}(\mathbf{Q}, A_m^*).$$

We will make the following assumptions on $(\mathcal{A}, \mathcal{F})$, in order to ensure that the $(A_m, \mathcal{F})$ satisfy the hypotheses of §2.4. Let $\bar{A} := \mathcal{A}/p\mathcal{A} = A_1$, so $\bar{A}^* = \mathcal{A}^*[p]$.

(H.1) $\bar{A}$ is an absolutely simple $\mathbf{F}_p[G_{\mathbf{Q}}]$-module, not isomorphic (as a $G_{\mathbf{Q}}$-module) to $\mathbf{F}_p$ or to $\boldsymbol{\mu}_p$.

(H.2) There is a $\tau \in G_{\mathbf{Q}}$ such that $\tau = 1$ on $\boldsymbol{\mu}_{p^\infty}$ and $\mathcal{A}/(\tau-1)\mathcal{A}$ is free of rank one over $\mathbf{Z}_p$.

(H.3) $H^1(\mathbf{Q}(\mathcal{A})/\mathbf{Q}, \bar{A}) = H^1(\mathbf{Q}(\mathcal{A}^*)/\mathbf{Q}, \bar{A}^*) = 0$, where $\mathbf{Q}(\mathcal{A})$ is the fixed field of the kernel of the map $G_{\mathbf{Q}} \to \mathrm{Aut}(\mathcal{A})$, and similarly for $\mathbf{Q}(\mathcal{A}^*)$.

(H.4) Either $\bar{A} \not\cong \bar{A}^*$, or $p \geq 5$.

Let Σ be a finite set of places containing ∞, p, all ℓ such that $\mathcal{A}$ is ramified at ℓ, and all ℓ such that $H^1_{\mathcal{F}}(\mathbf{Q}_\ell, \mathcal{A}) \neq H^1_{\mathrm{u}}(\mathbf{Q}_\ell, \mathcal{A})$. We will also assume that:

(H.5) For every $v \in \Sigma$, $H^1(\mathbf{Q}_v, \mathcal{A})/H^1_{\mathcal{F}}(\mathbf{Q}_v, \mathcal{A})$ is a torsion-free $\mathbf{Z}_p$-module.

Lemma 3.1.3. *If $\mathcal{A}$ and $\mathcal{F}$ satisfy the properties above, then:*

(1) *A_m and $\mathcal{F}$ satisfy the hypotheses of §2.4,*

(2) *the core rank $\chi(A_m)$ is independent of m.*

Proof. It is immediate that property (H.i) for $\mathcal{A}$ implies the corresponding property (H.i) for every A_m, $1 \leq i \leq 4$. That (H.5) for $(\mathcal{A}, \mathcal{F})$ implies (H.5) for $(A_m, \mathcal{F})$ is [**MR1**, Lemma 3.7.1(i)], and we omit the proof.

The second assertion follows from Proposition 2.4.5 and Theorem 2.5.2; the details are left as an exercise. □

Definition 3.1.4. We define the core rank $\chi(\mathcal{A})$ to be the common value $\chi(A_m)$.

Example 3.1.5. We define a canonical Selmer structure $\mathcal{F}_{\mathrm{can}}$ on $\mathcal{A}$ by:

- if $v \in \{\infty, p\}$ then $H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbf{Q}_v, \mathcal{A}) = H^1(\mathbf{Q}_v, \mathcal{A})$,
- if $v \notin \{\infty, p\}$ then $H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbf{Q}_v, \mathcal{A}) = \ker\big[H^1(\mathbf{Q}_\ell, \mathcal{A}) \to H^1(\mathbf{Q}_\ell^{\mathrm{ur}}, \mathcal{A}) \otimes \mathbf{Q}_p\big]$.

Note that if $\mathcal{A}$ is unramified at ℓ, then $H^1(\mathbf{Q}_\ell^{\mathrm{ur}}, \mathcal{A}) = \mathrm{Hom}(I_{\mathbf{Q}_\ell}, \mathcal{A})$ where $I_{\mathbf{Q}_\ell}$ is the inertia group, and $\mathrm{Hom}(I_{\mathbf{Q}_\ell}, \mathcal{A})$ is torsion-free, so $H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbf{Q}_\ell, \mathcal{A}) = H^1_{\mathrm{u}}(\mathbf{Q}_\ell, \mathcal{A})$ in this case.

Exercise 3.1.6. (1) Check that $\mathcal{F}_{\mathrm{can}}$ as defined above is a Selmer structure, and that it satisfies (H.5).

(2) Show that if $\ell \neq p$, $\mathcal{A}$ is unramified at ℓ, and $m > 0$, then $H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbf{Q}_\ell, A_m) = H^1_{\mathrm{u}}(\mathbf{Q}_\ell, A_m)$.

Proposition 3.1.7. *For every v, the limit of the Tate pairings of Theorem 1.8.1 induces a nondegenerate pairing*

$$H^1(\mathbf{Q}_v, \mathcal{A}) \times H^1(\mathbf{Q}_v, \mathcal{A}^*) \longrightarrow \mathbf{Q}_p/\mathbf{Z}_p$$

under which $H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbf{Q}_v, \mathcal{A})$ and $H^1_{\mathcal{F}^*_{\mathrm{can}}}(\mathbf{Q}_v, \mathcal{A}^*)$ are orthogonal complements. In particular:

(1) *if $v \in \{\infty, p\}$ then $H^1_{\mathcal{F}^*_{\mathrm{can}}}(\mathbf{Q}_v, \mathcal{A}^*) = 0$,*

(2) *if $v \notin \{\infty, p\}$ then $H^1_{\mathcal{F}^*_{\mathrm{can}}}(\mathbf{Q}_v, \mathcal{A}^*) = H^1_{\mathrm{u}}(\mathbf{Q}_v, \mathcal{A}^*)_{\mathrm{div}}$, the maximal divisible subgroup of $H^1_{\mathrm{u}}(\mathbf{Q}_v, \mathcal{A}^*)$.*

(3) *If $m > 0$ then $H^1_{\mathcal{F}^*_{\mathrm{can}}}(\mathbf{Q}_v, A^*_m)$ is the inverse image of $H^1_{\mathcal{F}^*_{\mathrm{can}}}(\mathbf{Q}_v, \mathcal{A}^*)$ under the map $H^1(\mathbf{Q}_v, A^*_m) \to H^1(\mathbf{Q}_v, \mathcal{A}^*)$.*

Proof. See [**R2**, §1.3], or work out the details as an exercise. □

Exercise 3.1.8. Suppose that either $v = p$ or $H^1_{\mathrm{u}}(\mathbf{Q}_v, \mathcal{A}^*)$ is finite. Use Proposition 3.1.7 to show that there are natural isomorphisms

$$H^0(\mathbf{Q}_v, \mathcal{A}^*)/p^m H^0(\mathbf{Q}_v, \mathcal{A}^*) \xrightarrow{\sim} H^1_{\mathcal{F}^*_{\mathrm{can}}}(\mathbf{Q}_v, A^*_m).$$

Show that if in addition $H^1(\mathbf{Q}_v, \mathcal{A}^*)$ is divisible then

$$H^1_{\mathcal{F}^*_{\mathrm{can}}}(\mathbf{Q}_v, A^*_m) = 0, \qquad H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbf{Q}_v, A_m) = H^1(\mathbf{Q}_v, A_m).$$

If M is a $\mathbf{Z}_p$-module, we let

$$\mathrm{rank}_{\mathbf{Z}_p}(M) = \dim_{\mathbf{Q}_p} M \otimes \mathbf{Q}_p, \quad \mathrm{corank}_{\mathbf{Z}_p}(M) := \mathrm{rank}_{\mathbf{Z}_p}\mathrm{Hom}(M, \mathbf{Q}_p/\mathbf{Z}_p).$$

Proposition 3.1.9.

$$\chi(\mathcal{A}, \mathcal{F}_{\mathrm{can}}) = \mathrm{rank}_{\mathbf{Z}_p}\mathcal{A}^- + \mathrm{corank}_{\mathbf{Z}_p} H^0(\mathbf{Q}_p, \mathcal{A}^*).$$

where $\mathcal{A}^-$ denotes the minus part of $\mathcal{A}$ for some complex conjugation.

Idea of proof. For the details of the proof, see [**MR1**, Theorem 5.2.15]. The outline is as follows. By Proposition 2.4.5 and Theorem 2.5.2, there is an integer k such that

$$\mathrm{length}(H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbf{Q}, A_m)) - \mathrm{length}(H^1_{\mathcal{F}^*_{\mathrm{can}}}(\mathbf{Q}, A^*_m)) = km \tag{3.1}$$

for every m, and $\chi(\mathcal{A}) = \max\{k, 0\}$. To prove the proposition we need to compute the left-hand side of (3.1) (in fact, computing it up to an error bounded independently of m will suffice). This can be done using [**Wi**, Proposition 1.6]. □

3.2. Kolyvagin systems for $\mathcal{A}$.

Fix a $\mathbf{Z}_p[G_{\mathbf{Q}}]$-module $\mathcal{A}$ as above and a Selmer structure $\mathcal{F}$ for $\mathcal{A}$, satisfying hypotheses (H.1) through (H.5).

If $\ell \notin \Sigma$, let

$$\nu(\ell) = \max\{m : \ell \equiv 1 \pmod{p^m} \\ \text{and } A_m/(\mathrm{Fr}_\ell - 1)A_m \text{ is free of rank 1 over } \mathbf{Z}/p^m\mathbf{Z}\}.$$

Let $\mathcal{N}_{\mathcal{A}}$ be the set of squarefree product of primes $\ell \notin \Sigma$, and if $n \in \mathcal{N}_{\mathcal{A}}$ define $\nu(n) = \min\{\nu(\ell) : \ell \mid n\}$ (by convention we let $\nu(1) = \infty$).

Definition 3.2.1. A Kolyvagin system for $\mathcal{A}$ is a collection

$$\{\kappa_n \in H^1_{\mathcal{F}(n)}(\mathbf{Q}, A_{\nu(n)}) \otimes G_n : n \in \mathcal{N}_{\mathcal{A}}\}$$

such that if $n\ell \in \mathcal{N}$, then $\mathrm{Res}_\ell(\kappa_{n\ell}) = \phi^{\mathrm{ut}}_\ell \circ \mathrm{Res}_\ell(\kappa_n)$ in $H^1_{\mathrm{t}}(\mathbf{Q}_\ell, A_{\nu(n\ell)}) \otimes G_{n\ell}$. (We understand $A_\infty = \mathcal{A}$, so $\kappa_1 \in H^1_{\mathcal{F}}(\mathbf{Q}, \mathcal{A})$.) Let $\mathbf{KS}(\mathcal{A})$ be the $\mathbf{Z}_p$-module of Kolyvagin systems for $\mathcal{A}$.

Exercise 3.2.2. Show that restricting from $\mathcal{N}_{\mathcal{A}}$ to $\{n \in \mathcal{N}_{\mathcal{A}} : \nu(n) \geq m\}$ induces a map $\mathbf{KS}(\mathcal{A}) \to \mathbf{KS}(A_m)$. Show that if $\chi(\mathcal{A}) = 1$, then

$$\mathbf{KS}(\mathcal{A}) = \varprojlim \mathbf{KS}(A_m),$$

inverse limit with respect to the maps of Proposition 2.9.1.

We say that $\boldsymbol{\kappa} \in \mathbf{KS}(\mathcal{A})$ is primitive if its image in $\mathbf{KS}(A_1)$ is nonzero.

Theorem 3.2.3. *Suppose $\chi(\mathcal{A}) = 1$. Then $\mathbf{KS}(\mathcal{A})$ is free of rank one over $\mathbf{Z}_p$, and every generator is primitive.*

Exercise 3.2.4. Prove Theorem 3.2.3.

Definition 3.2.5. Suppose $\boldsymbol{\kappa} \in \mathbf{KS}(\mathcal{A})$, $\boldsymbol{\kappa} \neq 0$. We define the *order of vanishing* of $\boldsymbol{\kappa}$ by

$$\operatorname{ord}(\boldsymbol{\kappa}) := \min\{\omega(n) : \kappa_n \neq 0\}.$$

If $r \geq 0$ we define

$$\partial^r(\boldsymbol{\kappa}) := \max\{j : \kappa_n \in p^j H^1_{\mathcal{F}(n)}(\mathbf{Q}, A_{\nu(n)}) \otimes G_n \text{ for all } n \in \mathcal{N}_{\mathcal{A}} \text{ with } \omega(n) = r\}.$$

In particular $\partial^0(\boldsymbol{\kappa}) = \max\{j : \kappa_1 \in p^j H^1_{\mathcal{F}}(\mathbf{Q}, \mathcal{A})\}$, and $\partial^r(\boldsymbol{\kappa}) = \infty$ if $r < \operatorname{ord}(\boldsymbol{\kappa})$. For $i > \operatorname{ord}(\boldsymbol{\kappa})$ define the sequence of *elementary divisors*

$$e_i(\boldsymbol{\kappa}) = \partial^{i-1}(\boldsymbol{\kappa}) - \partial^i(\boldsymbol{\kappa}).$$

Theorem 3.2.6. *Suppose $\chi(\mathcal{A}) = 1$ and $\boldsymbol{\kappa} \in \mathbf{KS}(\mathcal{A})$ is nonzero. Let $r = \operatorname{ord}(\boldsymbol{\kappa})$. Then $\operatorname{corank}_{\mathbf{Z}_p}(H^1_{\mathcal{F}^*}(\mathbf{Q}, \mathcal{A}^*)) = r$, $\partial^i(\boldsymbol{\kappa}) \neq \infty$ if $i \geq r$, the sequence $e_i(\boldsymbol{\kappa})$ is nonincreasing, nonnegative, equal to zero for large i, and*

$$H^1_{\mathcal{F}^*}(\mathbf{Q}, \mathcal{A}^*) \cong (\mathbf{Q}_p/\mathbf{Z}_p)^r \times \bigoplus_{i>r} \mathbf{Z}/p^{e_i(\boldsymbol{\kappa})}\mathbf{Z}.$$

Exercise 3.2.7. Deduce Theorem 3.2.6 from Propositions 2.9.8 and 2.4.5 and Exercise 3.2.2.

Corollary 3.2.8. *The value of $\operatorname{ord}(\boldsymbol{\kappa})$ and the sequence of $e_i(\boldsymbol{\kappa})$ are independent of (the nonzero) $\boldsymbol{\kappa}$.*

Corollary 3.2.9. *Suppose $\chi(\mathcal{A}) = 1$. Then:*

1. $\operatorname{length}(H^1_{\mathcal{F}^*}(\mathbf{Q}, \mathcal{A}^*)) \leq \partial^0(\boldsymbol{\kappa})$*, with equality if and only if $\boldsymbol{\kappa}$ is primitive.*
2. *If $\kappa_1 \neq 0$, then $H^1_{\mathcal{F}^*}(\mathbf{Q}, \mathcal{A}^*)$ is finite.*
3. *If $\boldsymbol{\kappa} \neq 0$ but $\kappa_1 = 0$, then $H^1_{\mathcal{F}^*}(\mathbf{Q}, \mathcal{A}^*)$ is infinite.*

3.3. Example: units and ideal class groups.

Fix a character $\rho : G_{\mathbf{Q}} \to \mathbf{Z}_p^\times$ of finite order. Assume that $p > 2$, so that the order of ρ is prime to p. Let L be the cyclic extension of $\mathbf{Q}$ which is the fixed field of ρ, and $\Delta = \operatorname{Gal}(L/\mathbf{Q})$. We will also view ρ as a (primitive) Dirichlet character in the usual way, so for every prime ℓ,

$$\rho(\ell) = 0 \iff \rho \text{ is ramified at } \ell \iff L/\mathbf{Q} \text{ is ramified at } \ell,$$
$$\rho(\ell) = 1 \iff \rho(G_{\mathbf{Q}_\ell}) = 1 \iff \ell \text{ splits completely in } L/\mathbf{Q}.$$

If B is a $\mathbf{Z}_p[\Delta]$-module, we define

$$B^\rho = \{b \in B : \delta b = \rho(\delta) b \text{ for every } \delta \in \Delta\}.$$

Let

$$\mathcal{A} := \mathbf{Z}_p(1) \otimes \rho^{-1} = \varinjlim \boldsymbol{\mu}_{p^m} \otimes \rho^{-1},$$

a free, rank-one $\mathbf{Z}_p$-module with $G_{\mathbf{Q}}$ acting via the product of ρ^{-1} and the cyclotomic character. (We write "$\otimes\rho^{-1}$" as an abbreviation for tensoring with a free, rank-one module on which $G_{\mathbf{Q}}$ acts as ρ^{-1}.) The dual representation

$$\mathcal{A}^* = \operatorname{Hom}(\mathcal{A}, \boldsymbol{\mu}_{p^\infty}) \cong \mathbf{Q}_p/\mathbf{Z}_p \otimes \rho,$$

i.e., A^* is isomorphic as a group to $\mathbf{Q}_p/\mathbf{Z}_p$, with $G_{\mathbf{Q}}$ acting via ρ.

For every $m \geq 1$, let $A_m = \mathcal{A}/p^m\mathcal{A} = \boldsymbol{\mu}_{p^m} \otimes \rho^{-1}$, so $A^*_m = \mathcal{A}^*[p^m] = \mathbf{Z}/p^m\mathbf{Z} \otimes \rho$.

Exercise 3.3.1. Describe $H^0(\mathbf{Q}_\ell, \mathcal{A}^*)$ for every prime ℓ, and show in particular that it is a divisible $\mathbf{Z}_p$-module.

Exercise 3.3.2. Suppose $\ell \neq p$ and ρ is ramified at ℓ. Show that $H^1(\mathbf{Q}_\ell, \mathcal{A}) = 0$, $H^1(\mathbf{Q}_\ell, \mathcal{A}^*) = 0$, and for every m, $H^1(\mathbf{Q}_\ell, A_m) = 0$ and $H^1(\mathbf{Q}_\ell, \mathcal{A}^*) = 0$. (Hint: show that $H^1_{\mathrm{u}}(\mathbf{Q}_\ell, A_m) = 0$ and $H^1_{\mathrm{u}}(\mathbf{Q}_\ell, A^*_m) = 0$, and use Proposition 1.9.1.)

We have an inflation-restriction exact sequence

$$0 \to H^1(L/\mathbf{Q}, (A_m)^{G_L}) \to H^1(\mathbf{Q}, A_m) \to H^1(L, A_m)^\Delta \to H^2(L/\mathbf{Q}, (A_m)^{G_L})$$

and similarly with A_m replaced by A^*_m. Since $[L : \mathbf{Q}]$ is prime to p, Exercise 1.4.3 shows that $H^i(L/\mathbf{Q}, A_m) = H^i(L/\mathbf{Q}, A^*_m) = 0$ for $i = 1, 2$, so

$$H^1(\mathbf{Q}, A_m) \cong H^1(L, A_m)^\Delta \cong (H^1(L, \boldsymbol{\mu}_{p^m}) \otimes \rho^{-1})^\Delta,$$
$$H^1(\mathbf{Q}, A^*_m) \cong H^1(L, A^*_m)^\Delta \cong (H^1(L, \mathbf{Z}/p^m\mathbf{Z}) \otimes \rho)^\Delta$$

Since (using Theorem 1.6.3)

$$H^1(L, \boldsymbol{\mu}_{p^m}) = L^\times/(L^\times)^{p^m}, \quad H^1(L, \mathbf{Z}/p^m\mathbf{Z}) = \mathrm{Hom}(G_L, \mathbf{Z}/p^m\mathbf{Z})$$

we conclude that

$$H^1(\mathbf{Q}, A_m) \cong (L^\times/(L^\times)^{p^k})^\rho, \quad H^1(\mathbf{Q}, A^*_m) \cong \mathrm{Hom}(G_L, \mathbf{Z}/p^m\mathbf{Z})^{\rho^{-1}} \tag{3.2}$$

the isomorphisms depending on a choice of generators of the free rank-one $\mathbf{Z}_p$-modules ρ and ρ^{-1}.

Exercise 3.3.3. Show that (3.2) has the following generalization. If F is a number field and $L \cap F = \mathbf{Q}$, then

$$H^1(F, A_m) \cong (FL^\times/(FL^\times)^{p^k})^\rho, \quad H^1(F, A^*_m) \cong \mathrm{Hom}(G_{FL}, \mathbf{Z}/p^m\mathbf{Z})^{\rho^{-1}}$$

For every prime ℓ, let $L_\ell = L \otimes_{\mathbf{Q}} \mathbf{Q}_\ell$, the sum of the completions of L at primes above ℓ, let $\mathcal{O}_{L,\ell} = \mathcal{O}_L \otimes_{\mathbf{Z}} \mathbf{Z}_\ell$, and if λ is a prime of L above ℓ, let $I_{L_\lambda} \subset G_{L_\lambda}$ be the inertia group.

Exercise 3.3.4. Show that for every prime ℓ,

(1) $H^1(\mathbf{Q}_\ell, A_m) \cong (\bigoplus_{\lambda | \ell} (L^\times_\lambda/(L^\times_\lambda))^{p^m})^\rho = (L^\times_\ell/(L^\times_\ell)^{p^m})^\rho$,

(2) $H^1(\mathbf{Q}_\ell, A^*_m) \cong (\bigoplus_{\lambda | \ell} \mathrm{Hom}(G_{L_\lambda}, \mathbf{Z}/p^m\mathbf{Z}))^{\rho^{-1}}$.

Exercise 3.3.5. Show that since $p \neq 2$, $H^1(\mathbf{R}, A_m) = H^1(\mathbf{R}, A^*_m) = 0$ for every m, so we can safely ignore the infinite place in our definition of Selmer group and Selmer structure.

Let $\mathcal{F}$ be the canonical Selmer structure $\mathcal{F}_{\mathrm{can}}$ defined in Example 3.1.5. Let $\mathbb{1}$ denote the trivial character of $G_{\mathbf{Q}}$, and $\epsilon_{\mathrm{cycl}} : G_{\mathbf{Q}} \to \mathrm{Aut}(\boldsymbol{\mu}_p) \cong \mathbf{F}_p^\times \hookrightarrow \mathbf{Z}_p^\times$ the mod-p cyclotomic character.

Exercise 3.3.6. Show that if $\rho \neq \mathbb{1}$ and $\rho \neq \epsilon_{\mathrm{cycl}}$, then $\mathcal{A}$ and $\mathcal{F}$ satisfy assumptions (H.1) through (H.5) of §3.1.

Exercise 3.3.7. Use Proposition 3.1.9 to show that with the canonical Selmer structure (and with $\rho \neq \mathbb{1}, \epsilon_{\mathrm{cycl}}$), $\chi(\mathcal{A})$ is given by the following table:

$$\chi(\mathcal{A}) = \left\{ \begin{array}{r|c|c} & \rho \text{ even} & \rho \text{ odd} \\ \hline \rho(p) \neq 1 & 1 & 0 \\ \hline \rho(p) = 1 & 2 & 1 \end{array} \right.$$

(recall that ρ is even if and only if $\rho(-1) = 1$).

Proposition 3.3.8. *For every $m \geq 1$, with the identifications of Exercise 3.3.4 we have*

1. $H^1_{\mathcal{F}}(\mathbf{Q}_p, A_m) = (L_p^\times/(L_p^\times)^{p^m})^\rho$ *and* $H^1_{\mathcal{F}^*}(\mathbf{Q}_p, A_m^*) = 0$,
2. *If $\ell \neq p$, then*

$$H^1_{\mathcal{F}}(\mathbf{Q}_\ell, A_m) = (\mathcal{O}_{L,\ell}^\times/(\mathcal{O}_{L,\ell}^\times)^{p^m})^\rho,$$
$$H^1_{\mathcal{F}^*}(\mathbf{Q}_\ell, A_m^*) = (\bigoplus_{\lambda|\ell}\mathrm{Hom}(G_{L_\lambda}/I_{L_\lambda}, \mathbf{Z}/p^m\mathbf{Z}))^{\rho^{-1}}$$

Proof. By Exercises 3.1.8 and 3.3.1, $H^1_{\mathcal{F}}(\mathbf{Q}_p, A_m) = H^1(\mathbf{Q}_p, A_m)$, so the first part of (1) follows from Exercise 3.3.4(1).

For (2) we consider three cases.

Case 1: $\ell \neq p$ and $\rho(\ell) = 1$. In this case ℓ splits completely in L/K, and $A_m \cong \boldsymbol{\mu}_{p^m}$ as a $G_{\mathbf{Q}_\ell}$-module, so (using Exercise 1.6.8)

$$H^1_{\mathrm{u}}(\mathbf{Q}_\ell, A_m) = H^1_{\mathrm{u}}(\mathbf{Q}_\ell, \boldsymbol{\mu}_{p^m}) = \mathbf{Z}_\ell^\times/(\mathbf{Z}_\ell^\times)^{p^m} = (\mathcal{O}_{L,\ell}^\times/(\mathcal{O}_{L,\ell}^\times)^{p^m})^\rho.$$

Since ρ is unramified at ℓ, Exercise 3.1.6(2) shows that $H^1_{\mathcal{F}}(\mathbf{Q}_\ell, A_m) = H^1_{\mathrm{u}}(\mathbf{Q}_\ell, A_m)$. This proves the first part of (2) in this case.

Case 2: $\ell \neq p$, $\mathcal{A}$ is unramified at ℓ, and $\rho(\ell) \neq 1$. In this case Exercise 3.1.6(2) shows that $H^1_{\mathcal{F}}(\mathbf{Q}_\ell, A_m) = H^1_{\mathrm{u}}(\mathbf{Q}_\ell, A_m)$. On the other hand, the inflation-restriction exact sequence gives

$$0 \longrightarrow H^1_{\mathrm{u}}(\mathbf{Q}_\ell, A_m) \longrightarrow H^1(\mathbf{Q}_\ell, A_m) \longrightarrow H^1(\mathbf{Q}_\ell^{\mathrm{ur}}, A_m)^{G_{\mathbf{Q}_\ell}}. \tag{3.3}$$

We have

$$H^1(\mathbf{Q}_\ell^{\mathrm{ur}}, A_m) = H^1(\mathbf{Q}_\ell^{\mathrm{ur}}, \boldsymbol{\mu}_{p^m} \otimes \rho^{-1})$$
$$= H^1(\mathbf{Q}_\ell^{\mathrm{ur}}, \boldsymbol{\mu}_{p^m}) \otimes \rho^{-1} = ((\mathbf{Q}_\ell^{\mathrm{ur}})^\times \otimes \mathbf{Z}/p^m\mathbf{Z}) \otimes \rho^{-1}$$

and, writing $\mathbf{Z}_\ell^{\mathrm{ur}}$ for the ring of integers of $\mathbf{Q}_\ell^{\mathrm{ur}}$,

$$0 \longrightarrow (\mathbf{Z}_\ell^{\mathrm{ur}})^\times \longrightarrow (\mathbf{Q}_\ell^{\mathrm{ur}})^\times \xrightarrow{\mathrm{ord}_\ell} \mathbf{Z} \longrightarrow 0.$$

The unit group $(\mathbf{Z}_\ell^{\mathrm{ur}})^\times$ is p-divisible, so $(\mathbf{Q}_\ell^{\mathrm{ur}})^\times \otimes \mathbf{Z}/p^m\mathbf{Z} \cong \mathbf{Z}/p^m\mathbf{Z}$ as $G_{\mathbf{Q}_\ell}$-modules, and so

$$H^1(\mathbf{Q}_\ell^{\mathrm{ur}}, A_m)^{G_{\mathbf{Q}_\ell}} = (\mathbf{Z}/p^m\mathbf{Z} \otimes \rho)^{G_{\mathbf{Q}_\ell}} = (\mathbf{Z}/p^m\mathbf{Z})^{\rho^{-1}} = 0.$$

Thus (3.3) and Exercise 3.3.4 yield

$$H^1_{\mathcal{F}}(\mathbf{Q}_\ell, A_m) = H^1_{\mathrm{u}}(\mathbf{Q}_\ell, A_m) = H^1(\mathbf{Q}_\ell, A_m) = (L_\ell^\times/(L_\ell^\times)^{p^m})^\rho.$$

In the exact sequence

$$0 \longrightarrow \mathcal{O}_{L,\ell}^\times \longrightarrow L_\ell^\times \xrightarrow{\oplus \mathrm{ord}_\lambda} \bigoplus_{\lambda|\ell}\mathbf{Z}\lambda \longrightarrow 0,$$

the decomposition group Δ_ℓ of ℓ in Δ acts trivially on $\oplus_\lambda \mathbf{Z}\lambda$, but $\rho(\Delta_\ell) \neq 1$, so $(\oplus_\lambda(\mathbf{Z}/p^m\mathbf{Z})\lambda)^\rho = 0$. Therefore $(L_\ell^\times/(L_\ell^\times)^{p^m})^\rho = (\mathcal{O}_{L,\ell}^\times/(\mathcal{O}_{L,\ell}^\times)^{p^m})^\rho$, and this proves (2) for A_m in this case.

Case 3: $\ell \neq p$ and $\mathcal{A}$ is ramified at ℓ. Exercise 3.3.2 shows that $H^1_{\mathcal{F}}(\mathbf{Q}_\ell, A_m) = 0$. On the other hand, the kernel of the reduction map

$$\mathcal{O}_{L,\ell}^\times \twoheadrightarrow \bigoplus_{\lambda|\ell}(\mathcal{O}_L/\lambda)^\times$$

is a pro-ℓ-group, so tensoring with $\mathbf{Z}/p^m\mathbf{Z}$ gives an isomorphism

$$\mathcal{O}_{L,\ell}^\times/(\mathcal{O}_{L,\ell}^\times)^{p^m} \xrightarrow{\sim} \bigoplus_{\lambda|\ell}(\mathcal{O}_L/\lambda)^\times/((\mathcal{O}_L/\lambda)^\times)^{p^m}.$$

Since the inertia group I_ℓ acts trivially on the right-hand side, but $\rho(I_\ell) \neq 1$, we conclude that $(\mathcal{O}_{L,\ell}^\times/(\mathcal{O}_{L,\ell}^\times)^{p^m})^\rho = 0$, which proves assertion (2) for A_m.

The proof of the proposition for A_m^* is left as the following exercise. □

Exercise 3.3.9. Prove the assertions in Proposition 3.3.8 about A_m^*.

Let $\mathcal{C}_L$ denote the p-part of the ideal class group of L, and

$$\mathcal{C}'_L = \mathrm{Pic}(\mathcal{O}_L[1/p])[p^\infty],$$

the quotient of $\mathcal{C}_L$ by the classes of primes above p.

Exercise 3.3.10. Suppose $\rho(p) \neq 1$. Show that $H^1_{\mathcal{F}}(\mathbf{Q}_p, A_m) = (\mathcal{O}_{L,p}^\times/(\mathcal{O}_{L,p}^\times)^{p^m})^\rho$, $(\mathcal{O}_L[1/p]^\times/(\mathcal{O}_L[1/p]^\times)^{p^m})^\rho = (\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^{p^m})^\rho$, and $(\mathcal{C}'_L)^\rho = \mathcal{C}_L^\rho$.

Proposition 3.3.11. *For every m there is a natural exact sequence*

$$0 \longrightarrow (\mathcal{O}_L[1/p]^\times/(\mathcal{O}_L[1/p]^\times)^{p^m}))^\rho \longrightarrow H^1_{\mathcal{F}}(\mathbf{Q}, A_m) \longrightarrow \mathcal{C}'_L[p^m]^\rho \longrightarrow 0$$

and an isomorphism

$$H^1_{\mathcal{F}^*}(\mathbf{Q}, \mathcal{A}_m^*) \cong \mathrm{Hom}((\mathcal{C}'_L)^\rho, \mathbf{Z}/p^m\mathbf{Z}).$$

If $\rho(p) \neq 1$ we can replace $\mathcal{O}_L[1/p]^\times/(\mathcal{O}_L[1/p]^\times)^{p^m}$ by $\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^{p^m}$ and $\mathcal{C}'_L$ by $\mathcal{C}_L$.

Proof. Under the identification (3.2), using Proposition 3.3.8 we have

$$H^1_{\mathcal{F}}(\mathbf{Q}, A_m) = \{x \in (L^\times/(L^\times)^{p^m})^\rho : \mathrm{ord}_\lambda(x) \equiv 0 \pmod{p^m} \text{ for every } \lambda \nmid p\}.$$

If $x \in L^\times$ represents a class in $c \in H^1_{\mathcal{F}}(\mathbf{Q}, A_m)$, then the ideal $x\mathcal{O}_L[1/p] = \mathfrak{a}^{p^m}$ for some fractional ideal $\mathfrak{a}$ of $\mathcal{O}_L[1/p]$. The map that sends c to the class of $\mathfrak{a}$ is a well-defined surjection from $H^1_{\mathcal{F}}(\mathbf{Q}, A_m)$ to $\mathcal{C}'_L[p^m]$, and its kernel is $\mathcal{O}_L[1/p]^\times/(\mathcal{O}_L[1/p]^\times)^{p^m}$. This gives the desired exact sequence.

Under the identification (3.2), Proposition 3.3.8 shows that $H^1_{\mathcal{F}^*}(\mathbf{Q}, A_m^*)$ consists of everywhere unramified homomorphisms in $\mathrm{Hom}(G_L, \mathbf{Z}/p^m\mathbf{Z})^{\rho^{-1}}$ that are trivial on the decomposition group at p, i.e.,

$$H^1_{\mathcal{F}^*}(\mathbf{Q}, A_m^*) = \mathrm{Hom}(\mathcal{C}'_L, \mathbf{Z}/p^m\mathbf{Z})^{\rho^{-1}}.$$

The isomorphism of the proposition follows from this. □

Exercise 3.3.12. Use Proposition 3.3.11 to give a direct proof (i.e., without using Proposition 3.1.9 as in Exercise 3.3.7) that if $\rho \neq \mathbb{1}, \epsilon_{\mathrm{cycl}}$, then $\chi(\mathcal{A})$ is given by the table in Exercise 3.3.7.

Corollary 3.3.13. *Suppose ρ is even, $\rho(p) \neq 1$, and $\boldsymbol{\kappa} \in \mathbf{KS}(\mathcal{A})$ is nonzero. Then $\kappa_1 \neq 0$ and*

$$|\mathcal{C}_L^\rho| \leq [(\mathcal{O}_L^\times \otimes \mathbf{Z}_p)^\rho : \mathbf{Z}_p\kappa_1],$$

with equality if and only if $\boldsymbol{\kappa}$ is primitive.

Proof. By Proposition 3.3.11 we have $H^1(\mathbf{Q}, \mathcal{A}) = (\mathcal{O}_L^\times \otimes \mathbf{Z}_p)^\rho$. The proof of the Dirichlet Unit Theorem shows that this is a free $\mathbf{Z}_p$-module of rank one, so

$$\partial^0(\boldsymbol{\kappa}) = [(\mathcal{O}_L^\times \otimes \mathbf{Z}_p)^\rho : \mathbf{Z}_p \kappa_1].$$

Now the corollary follows directly from Corollary 3.2.9(1) and Proposition 3.3.11. □

Proposition 3.3.14. *Suppose $\ell \notin \Sigma$ and $1 \le m \le \nu(\ell)$. Then*

1. *$\rho(\ell) = 1$ and ℓ splits completely in $\mathbf{Q}(\boldsymbol{\mu}_p)/\mathbf{Q}$,*
2. *the isomorphism $H^1(\mathbf{Q}_\ell, A_m) \cong H^1(\mathbf{Q}_\ell, \boldsymbol{\mu}_{p^m}) \cong \mathbf{Q}_\ell^\times/(\mathbf{Q}_\ell^\times)^{p^m}$ identifies $H^1_{\mathrm{u}}(\mathbf{Q}_\ell, A_m)$ with $\mathbf{Z}_\ell^\times/(\mathbf{Z}_\ell^\times)^{p^m}$ and $H^1_{\mathrm{t}}(\mathbf{Q}_\ell, A_m)$ with the subgroup generated by ℓ,*
3. *there is a commutative diagram (recall that $G_\ell := \mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_\ell)/\mathbf{Q})$)*

$$\begin{tikzcd}
H^1_{\mathrm{u}}(\mathbf{Q}_\ell, A_m) \arrow[r, "\phi_\ell^{\mathrm{ut}}"] \arrow[d, "\cong"] & H^1_{\mathrm{t}}(\mathbf{Q}_\ell, A_m) \otimes G_\ell \arrow[d, "\cong"] \\
\mathbf{Z}_\ell^\times/(\mathbf{Z}_\ell^\times)^{p^m} \arrow[r, "\ell \otimes [\,\cdot\,, \mathbf{Q}_\ell(\boldsymbol{\mu}_\ell)/\mathbf{Q}_\ell]"] & \langle \ell \rangle \otimes G_\ell
\end{tikzcd}$$

where the vertical isomorphisms are from (2) and $[\,\cdot\,, \mathbf{Q}_\ell(\boldsymbol{\mu}_\ell)/\mathbf{Q}_\ell]$ is the local Artin map.

Proof. Since $m \le \nu(\ell)$, we have $\ell \equiv 1 \pmod{p^m}$ and $(\mathrm{Fr}_\ell - 1)A_m = 0$, so $\ell\rho^{-1}(\ell) \equiv 1 \pmod{p^m}$. Hence $\rho(\ell) \equiv 1 \pmod{p^m}$, and so $\rho(\ell) = \epsilon_{\mathrm{cycl}}(\ell) = 1$. This proves (1).

Since $\rho(\ell) = 1$ and $\ell \equiv 1 \pmod{p^m}$,

$$H^1(\mathbf{Q}_\ell, A_m) = H^1(\mathbf{Q}_\ell, \boldsymbol{\mu}_{p^m}) = \mathbf{Q}_\ell^\times/(\mathbf{Q}_\ell^\times)^{p^m},$$

and the description of $H^1_{\mathrm{u}}(\mathbf{Q}_\ell, A_m)$ in (2) is similar to Proposition 3.3.8. By definition,

$$\begin{aligned} H^1_{\mathrm{t}}(\mathbf{Q}_\ell, A_m) &= \ker\bigl[H^1(\mathbf{Q}_\ell, A_m) \to H^1(\mathbf{Q}_\ell(\boldsymbol{\mu}_\ell), A_m)\bigr] \\ &= \ker\bigl[\mathbf{Q}_\ell^\times/(\mathbf{Q}_\ell^\times)^{p^m} \to \mathbf{Q}_\ell(\boldsymbol{\mu}_\ell)^\times/(\mathbf{Q}_\ell(\boldsymbol{\mu}_\ell)^\times)^{p^m}\bigr] \end{aligned}$$

Let ζ_ℓ denote a primitive ℓ-th root of unity in $\mathbf{Q}_\ell(\boldsymbol{\mu}_\ell)$. We have

$$\ell = \mathbf{N}_{\mathbf{Q}_\ell(\boldsymbol{\mu}_\ell)/\mathbf{Q}_\ell}(1 - \zeta_\ell) = \prod_{i=1}^{\ell-1}(1 - \zeta_\ell^i) = (1 - \zeta_\ell)^{\ell-1} \prod_{i=1}^{\ell-1} \frac{1 - \zeta_\ell^i}{1 - \zeta_\ell}$$

Since $\prod_{i=1}^{\ell-1} \frac{1-\zeta_\ell^i}{1-\zeta_\ell} \equiv \prod_{i=1}^{\ell-1} i \equiv -1 \pmod{\zeta_\ell - 1}$, we also see that $\prod_{i=1}^{\ell-1} \frac{1-\zeta_\ell^i}{1-\zeta_\ell} \in (\mathbf{Q}_\ell(\boldsymbol{\mu}_\ell)^\times)^{p^m}$. Hence $\ell \in (\mathbf{Q}_\ell(\boldsymbol{\mu}_\ell)^\times)^{p^m}$, so $\ell \in H^1_{\mathrm{t}}(\mathbf{Q}_\ell, A_m)$. On the other hand, since $G_{\mathbf{Q}_\ell}$ acts trivially on A_m,

$$H^1_{\mathrm{t}}(\mathbf{Q}_\ell, A_m) = H^1(\mathbf{Q}_\ell(\boldsymbol{\mu}_\ell)/\mathbf{Q}_\ell, A_m) = \mathrm{Hom}(\mathrm{Gal}(\mathbf{Q}_\ell(\boldsymbol{\mu}_\ell)/\mathbf{Q}_\ell), A_m)$$

is cyclic of order p^m, and (2) follows.

The proof of (3) is left as an exercise. □

3.4. Example: Tate modules of elliptic curves.

Now suppose that E is an elliptic curve defined over $\mathbf{Q}$, and

$$\mathcal{A} = T_p(E) := \varprojlim E[p^m]$$

is the p-adic Tate module of E. Then the Weil pairing shows that $\mathcal{A}^* = E[p^\infty]$, and for every m, $A_m = A_m^* = E[p^m]$. We will also assume that

(3.4)
- $p \geq 5$,
- the p-adic representation $G_{\mathbf{Q}} \to \mathrm{Aut}(E[p^\infty]) \cong \mathrm{GL}_2(\mathbf{Z}_p)$ is surjective

and we let $\mathcal{F}$ be the Selmer structure $\mathcal{F}_{\mathrm{can}}$ on $T_p(E)$.

Exercise 3.4.1. Show that under the assumptions of (3.4), $T_p(E)$ and $\mathcal{F}$ satisfy hypotheses (H.1) through (H.5) of §3.1.

Exercise 3.4.2. Show using Proposition 3.1.9 that $\chi(T_p(E)) = 1$.

Proposition 3.4.3. (1) *If $\ell \neq p$, then $H^1(\mathbf{Q}_\ell, T_p(E))$ and $H^1(\mathbf{Q}_\ell, E[p^\infty])$ are finite.*
(2) *For every ℓ, $H^1_{\mathcal{F}}(\mathbf{Q}_\ell, T_p(E)) = H^1(\mathbf{Q}_\ell, T_p(E))$ and $H^1_{\mathcal{F}^*}(\mathbf{Q}_\ell, E[p^\infty]) = 0$.*

Proof. Suppose first that $\ell \neq p$, and $m > 0$. Writing I_ℓ for the inertia group in $G_{\mathbf{Q}_\ell}$, we have (see (1.2) and Proposition 1.4.13(1))

$$H^1_{\mathrm{u}}(\mathbf{Q}_\ell, E[p^m]) = H^1(\mathbf{Q}_\ell^{\mathrm{ur}}/\mathbf{Q}_\ell, E[p^m]^{I_\ell}) \cong E[p^m]^{I_\ell}/(\mathrm{Fr}_\ell - 1)(E[p^m]^{I_\ell}).$$

It follows from the exact sequence

$$0 \to E(\mathbf{Q}_\ell)[p^m] \to E[p^m]^{I_\ell} \xrightarrow{\mathrm{Fr}_\ell - 1} E[p^m]^{I_\ell} \to E[p^m]^{I_\ell}/(\mathrm{Fr}_\ell - 1)(E[p^m]^{I_\ell}) \to 0$$

that $E[p^m]^{I_\ell}/(\mathrm{Fr}_\ell - 1)(E[p^m]^{I_\ell})$ and $E(\mathbf{Q}_\ell)[p^m]$ have the same order, so

$$|H^1_{\mathrm{u}}(\mathbf{Q}_\ell, E[p^m])| = |E(\mathbf{Q}_\ell)[p^m]|.$$

Since $E[p^m]^* = E[p^m]$, Proposition 1.9.1 shows that $H^1_{\mathrm{u}}(\mathbf{Q}_\ell, E[p^m])$ is its own orthogonal complement in $H^1(\mathbf{Q}_\ell, E[p^m]$, so $|H^1(\mathbf{Q}_\ell, E[p^m])| = |E(\mathbf{Q}_\ell)[p^m]|^2$. Since $|E(\mathbf{Q}_\ell)[p^m]|$ is bounded independently of m, we conclude that both $H^1(\mathbf{Q}_\ell, T_p(E))$ and $H^1(\mathbf{Q}_\ell, E[p^\infty])$ are finite. This proves (1), and (2) follows from the definition of $\mathcal{F}_{\mathrm{can}}$ (for $H^1_{\mathcal{F}}(\mathbf{Q}_\ell, T_p(E))$) and Proposition 3.1.7(2) (for $H^1_{\mathcal{F}^*}(\mathbf{Q}_\ell, E[p^\infty])$).

If $\ell = p$, then (2) is the definition of $\mathcal{F}_{\mathrm{can}}$ (for $H^1_{\mathcal{F}}(\mathbf{Q}_\ell, T_p(E))$) and Proposition 3.1.7(1) (for $H^1_{\mathcal{F}^*}(\mathbf{Q}_\ell, E[p^\infty])$). □

Exercise 3.4.4. Show that if $E(\mathbf{Q}_\ell)[p] = 0$, then $H^1_{\mathcal{F}}(\mathbf{Q}_\ell, E[p^m]) = H^1(\mathbf{Q}_\ell, E[p^m])$ and $H^1_{\mathcal{F}^*}(\mathbf{Q}_\ell, E[p^m]) = 0$. (Hint: use Theorem 1.8.1 with $i = 2$.)

Recall (Definition 1.6.13) that for every ℓ and m, $H^1_{\mathrm{f}}(\mathbf{Q}_\ell, E[p^m])$ is the image of the Kummer map $E(\mathbf{Q}_\ell)/p^m E(\mathbf{Q}_\ell) \hookrightarrow H^1(\mathbf{Q}_\ell, E[p^m])$, and $\mathrm{Sel}_{p^m}(E/\mathbf{Q})$ is the corresponding Selmer group.

Proposition 3.4.5. *Suppose $\ell \neq p$ and $m > 0$. Then*

$$H^1_{\mathcal{F}}(\mathbf{Q}_\ell, E[p^m]) = H^1_{\mathcal{F}^*}(\mathbf{Q}_\ell, E[p^m]) = H^1_{\mathrm{f}}(\mathbf{Q}_\ell, E[p^m]).$$

Proof. By Exercise 3.1.8 and Proposition 3.4.3, there is a natural isomorphism

$$E(\mathbf{Q}_\ell)[p^\infty]/p^m E(\mathbf{Q}_\ell)[p^\infty] \xrightarrow{\sim} H^1_{\mathcal{F}^*}(\mathbf{Q}_\ell, E[p^m]). \tag{3.5}$$

By [**Si**, Theorem IV.6.4 and Proposition VII.2.2], there is a (noncanonical) decomposition

$$E(\mathbf{Q}_\ell) \cong \mathbf{Z}_\ell \times E(\mathbf{Q}_\ell)_{\mathrm{tors}}$$

so there is a canonical isomorphism

$$E(\mathbf{Q}_\ell)/p^m E(\mathbf{Q}_\ell) \xrightarrow{\sim} E(\mathbf{Q}_\ell)_{\mathrm{tors}}/p^m E(\mathbf{Q}_\ell)_{\mathrm{tors}} = E(\mathbf{Q}_\ell)[p^\infty]/p^m E(\mathbf{Q}_\ell)[p^\infty].$$

Combined with (3.5) (and checking that the obvious diagram commutes) this proves that $H^1_{\mathcal{F}^*}(\mathbf{Q}_\ell, E[p^m]) = H^1_{\mathrm{f}}(\mathbf{Q}_\ell, E[p^m])$. By Example 1.8.4, $H^1_{\mathrm{f}}(\mathbf{Q}_\ell, E[p^m])$ is its own orthogonal complement in $H^1(\mathbf{Q}_\ell, E[p^m])$ under the Tate pairing, so we have $H^1_{\mathcal{F}}(\mathbf{Q}_\ell, E[p^m]) = H^1_{\mathrm{f}}(\mathbf{Q}_\ell, E[p^m])$ as well. □

Corollary 3.4.6. *There are exact sequences*

$$0 \longrightarrow \mathrm{Sel}_{p^m}(E/\mathbf{Q}) \longrightarrow H^1_{\mathcal{F}}(\mathbf{Q}, E[p^m]) \longrightarrow H^1_{\mathcal{F}}(\mathbf{Q}_p, E[p^m])/H^1_{\mathrm{f}}(\mathbf{Q}_p, E[p^m])$$

$$0 \longrightarrow H^1_{\mathcal{F}^*}(\mathbf{Q}, E[p^m]) \longrightarrow \mathrm{Sel}_{p^m}(E/\mathbf{Q}) \longrightarrow H^1_{\mathrm{f}}(\mathbf{Q}_p, E[p^m])/H^1_{\mathcal{F}^*}(\mathbf{Q}_p, E[p^m]).$$

Exercise 3.4.7. Show directly from the definition that $\chi(T_p(E)) = 1$. Hint: use Corollary 3.4.6, Theorem 1.10.2, Exercise 3.1.8, and the fact that $E(\mathbf{Q}_p) \cong E(\mathbf{Q}_p)_{\mathrm{tors}} \oplus \mathbf{Z}_p$.

LECTURE 4

Euler systems

The preceding lectures have shown that Kolyvagin systems are useful for describing the structure of Selmer groups, and even that Kolyvagin systems exist for certain p-adic representations. It still remains to construct Kolyvagin systems and to relate them to special values of L-functions (something that has been done only in very special cases). In this lecture we describe general machinery for constructing Kolyvagin systems.

4.1. Definition of an Euler system.

Fix a rational prime p and a p-adic representation $\mathcal{A}$ (a free $\mathbf{Z}_p$-module of finite rank with a continuous action of $G_{\mathbf{Q}}$) as in the previous lecture. Fix a finite set Σ of places containing ∞, p, and all primes ℓ where $\mathcal{A}$ is ramified.

If $\ell \notin \Sigma$, define

$$P_\ell(x) = \det(1 - \mathrm{Fr}_\ell x | \mathcal{A}) \in \mathbf{Z}_p[x].$$

Let

$$\mathcal{N} = \{np^k : n \text{ is a squarefree product of primes } \ell \notin \Sigma,\ k \geq 0\},$$

An *Euler system* for $\mathcal{A}$ is a collection

$$\boldsymbol{\xi} = \{\xi_n \in H^1(\mathbf{Q}(\boldsymbol{\mu}_n), \mathcal{A}) : n \in \mathcal{N}\}$$

such that for $n\ell \in \mathcal{N}$,

$$\mathrm{Cor}_{\mathbf{Q}(\boldsymbol{\mu}_{n\ell})/\mathbf{Q}(\boldsymbol{\mu}_n)} \xi_{n\ell} = \begin{cases} P_\ell(\mathrm{Fr}_\ell^{-1})\xi_n & \text{if } \ell \neq p, \\ \xi_n & \text{if } \ell = p. \end{cases} \tag{4.1}$$

Let $\mathbf{ES}(\mathcal{A})$ denote the $\mathbf{Z}_p[G_{\mathbf{Q}}]$-module of Euler systems for $\mathcal{A}$.

4.2. Example: the cyclotomic unit Euler system

Fix a nontrivial character $\rho : G_{\mathbf{Q}} \twoheadrightarrow \mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_p)/\mathbf{Q}) \to \mathbf{Z}_p^\times$, and let $\mathcal{A} = \mathbf{Z}_p(1) \otimes \rho^{-1}$ as in §3.3. Then for every $\ell \neq p$, Fr_ℓ acts on $\mathcal{A}$ as $\ell\rho^{-1}(\ell)$, so

$$P_\ell(x) = 1 - \ell\rho^{-1}(\ell)x.$$

Let $\Sigma = \{\infty, p\}$.

If $p \mid n$ then $\rho(G_{\mathbf{Q}(\boldsymbol{\mu}_n)}) = 1$, so there are isomorphisms

$$H^1(\mathbf{Q}(\boldsymbol{\mu}_n), \mathcal{A}) \cong H^1(\mathbf{Q}(\boldsymbol{\mu}_n), \mathbf{Z}_p(1)) \otimes \rho^{-1} \cong (\mathbf{Q}(\boldsymbol{\mu}_n)^\times \otimes \mathbf{Z}_p) \otimes \rho^{-1} \tag{4.2}$$

and commutative diagrams for every ℓ

$$\begin{tikzcd}
(\mathbf{Q}(\boldsymbol{\mu}_{n\ell})^\times \otimes \mathbf{Z}_p) \otimes \rho^{-1} \arrow[r, "\sim"] \arrow[d, "\mathbf{N}_{\mathbf{Q}(\boldsymbol{\mu}_{n\ell})/\mathbf{Q}(\boldsymbol{\mu}_n)} \otimes 1"'] & H^1(\mathbf{Q}(\boldsymbol{\mu}_{n\ell}), \mathcal{A}) \arrow[d, "\mathrm{Cor}_{\mathbf{Q}(\boldsymbol{\mu}_{n\ell})/\mathbf{Q}(\boldsymbol{\mu}_n)}"] \\
(\mathbf{Q}(\boldsymbol{\mu}_n)^\times \otimes \mathbf{Z}_p) \otimes \rho^{-1} \arrow[r, "\sim"] & H^1(\mathbf{Q}(\boldsymbol{\mu}_n), \mathcal{A}).
\end{tikzcd} \tag{4.3}$$

If $p \nmid n$, then Exercise 3.3.3 gives a commutative diagram

$$\begin{tikzcd}
(\mathbf{Q}(\boldsymbol{\mu}_{np})^\times \otimes \mathbf{Z}_p) \otimes \rho^{-1} \arrow[r, "\sim"] \arrow[d, "\sum_{\delta\in\Delta}\rho^{-1}(\delta)\delta\otimes 1="'] & H^1(\mathbf{Q}(\boldsymbol{\mu}_{np}), \mathcal{A}) \arrow[d, "\mathrm{Cor}_{\mathbf{Q}(\boldsymbol{\mu}_{np})/\mathbf{Q}(\boldsymbol{\mu}_n)}"] \\
((\mathbf{Q}(\boldsymbol{\mu}_{np})^\times \otimes \mathbf{Z}_p) \otimes \rho^{-1})^\Delta \arrow[r, "\sim"] & H^1(\mathbf{Q}(\boldsymbol{\mu}_n), \mathcal{A}).
\end{tikzcd} \tag{4.4}$$

For every $n \geq 1$ fix a primitive n-th root of unity ζ_n such that for every m, $\zeta_{mn}^m = \zeta_n$. If $n \in \mathcal{N}$ and $p \mid n$, we identify $\Delta := \mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_p)/\mathbf{Q})$ with a subgroup of $\mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_n)/\mathbf{Q})$ as follows. Write $n = p^k n'$ with $k \geq 1$ and $p \nmid n'$, and identify Δ with the (unique) subgroup of order $p-1$ in $\mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_n)/\mathbf{Q}(\boldsymbol{\mu}_{n'})) \cong \mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_{p^k})/\mathbf{Q}) \cong (\mathbf{Z}/p^k\mathbf{Z})^\times$.

If $n \in \mathcal{N}$, define

$$\alpha_n = \begin{cases} \prod_{\delta\in\Delta} (\zeta_n^\delta - 1)^{\rho^{-1}(\delta)/(p-1)} \in (\mathbf{Q}(\boldsymbol{\mu}_n)^\times \otimes \mathbf{Z}_p)^\rho & \text{if } p \mid n, \\ \prod_{\delta\in\Delta} (\zeta_{np}^\delta - 1)^{\rho^{-1}(\delta)} \in (\mathbf{Q}(\boldsymbol{\mu}_{np})^\times \otimes \mathbf{Z}_p)^\rho & \text{if } p \nmid n, \end{cases}$$

$$\beta_n = \prod_{d\mid n, p\nmid d} \alpha_{n/d}^{\prod_{\ell\mid d}(-\mathrm{Fr}_\ell^{-1})}.$$

Note that $\alpha_n^\delta = \alpha_n^{\rho(\delta)}$ and $\beta_n^\delta = \beta_n^{\rho(\delta)}$ for every $\delta \in \Delta$.

Lemma 4.2.1. *Suppose $n\ell \in \mathcal{N}$. Then*

$$\mathbf{N}_{\mathbf{Q}(\boldsymbol{\mu}_{n\ell})/\mathbf{Q}(\boldsymbol{\mu}_n)}\beta_{n\ell} = \begin{cases} \beta_n^{1-\ell\mathrm{Fr}_\ell^{-1}} & \text{if } \ell \neq p, \\ \beta_n & \text{if } \ell = p \text{ and } p \mid n. \end{cases}$$

If $p \nmid n$, then $\prod_{\delta\in\Delta} \beta_{np}^{\rho^{-1}(\delta)\delta} = \beta_n$.

Sketch of proof. First suppose $\ell \neq p$, and note that $\eta_0 := \zeta_n^{\mathrm{Fr}_\ell^{-1}}/\zeta_{n\ell} \in \boldsymbol{\mu}_\ell$ (see this by raising both sides to the ℓ-th power). Then

$$\mathbf{N}_{\mathbf{Q}(\boldsymbol{\mu}_{n\ell})/\mathbf{Q}(\boldsymbol{\mu}_n)}(\zeta_{n\ell} - 1) = \prod_{\eta\in\boldsymbol{\mu}_\ell, \eta\neq\eta_0} (\eta\zeta_{n\ell} - 1) = \frac{\zeta_n - 1}{\zeta_n^{\mathrm{Fr}_\ell^{-1}} - 1} = (\zeta_n - 1)^{1-\mathrm{Fr}_\ell^{-1}}$$

$$\implies \quad \mathbf{N}_{\mathbf{Q}(\boldsymbol{\mu}_{n\ell})/\mathbf{Q}(\boldsymbol{\mu}_n)}\alpha_{n\ell} = \alpha_n^{1-\mathrm{Fr}_\ell^{-1}}$$

$$\implies \quad \mathbf{N}_{\mathbf{Q}(\boldsymbol{\mu}_{n\ell})/\mathbf{Q}(\boldsymbol{\mu}_n)}\beta_{n\ell} = \beta_n^{1-\ell\mathrm{Fr}_\ell^{-1}}.$$

If $\ell = p$ and $p \mid n$, a similar argument shows that $\mathbf{N}_{\mathbf{Q}(\boldsymbol{\mu}_{np})/\mathbf{Q}(\boldsymbol{\mu}_n)}(\zeta_{np} - 1) = \zeta_n - 1$. If $\ell = p$ and $p \nmid n$, the desired equality follows easily from the definition of α_n. □

Definition 4.2.2. Fix a generator u_ρ of the free, rank-one $\mathbf{Z}_p$-module "ρ^{-1}". For every $n \in \mathcal{N}'$ define $\xi_n^{\mathrm{cycl}} \in H^1(\mathbf{Q}(\boldsymbol{\mu}_n), \mathcal{A})$ to be the image of $\beta_n \otimes u_\rho$ under the isomorphism (4.2). Let

$$\boldsymbol{\xi}^{\mathrm{cycl}} = \{\xi_n^{\mathrm{cycl}} : n \in \mathcal{N}\}.$$

Proposition 4.2.3. *The collection $\boldsymbol{\xi}^{\mathrm{cycl}}$ is an Euler system for $\mathcal{A}$.*

Proof. This follows from Lemma 4.2.1 and the commutative diagram (4.3). □

Exercise 4.2.4. If $\boldsymbol{\xi}^{\mathrm{cycl}}$ is the cyclotomic unit Euler system defined above, show that

$$\xi_1^{\mathrm{cycl}} = \beta_1 = \alpha_1 = \prod_{\delta \in \Delta} (\zeta_p^{\delta} - 1)^{\rho^{-1}(\delta)} \in (\mathbf{Q}(\boldsymbol{\mu}_p)^{\times} \otimes \mathbf{Z}_p)^{\rho}.$$

What can you say about ξ_1^{cycl} when ρ is trivial? When ρ is odd? When ρ is even?

Exercise 4.2.5. Define an Euler system $\boldsymbol{\xi}^{\mathrm{cycl}}$ for $\mathbf{Z}_p(1) \otimes \rho^{-1}$ for more general characters ρ than the ones in §4.2.

4.3. Euler systems and Kolyvagin systems.

Theorem 4.3.1. *Suppose*

(1) *for every $\ell \notin \Sigma$, $P_\ell(x)$ has no roots in $\boldsymbol{\mu}_{p^\infty}$,*

(2) *$H^0(\mathbf{Q}_p, \mathcal{A}^*)$ is a divisible $\mathbf{Z}_p$-module.*

Then there is a canonical map $\mathbf{ES}(\mathcal{A}) \to \mathbf{KS}(\mathcal{A}, \mathcal{F}_{\mathrm{can}})$ such that if $\boldsymbol{\xi}$ maps to $\boldsymbol{\kappa}$, then $\kappa_1 = \xi_1 \in H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbf{Q}, \mathcal{A})$, where $\mathcal{F}_{\mathrm{can}}$ is the canonical Selmer structure of Example 3.1.5.

For the proof of Theorem 4.3.1, see [**MR1**, Theorem 3.2.4] and [**R2**, Chapter 4]. Here we will describe the construction of the map of Theorem 4.3.1, and give some details for the cyclotomic unit Euler system of §4.2 where the construction is particularly explicit.

Let $\mathcal{N}' = \{n \in \mathcal{N} : p \nmid n\}$. For every $n \in \mathcal{N}$, let $\Gamma_n = \mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_n)/\mathbf{Q})$. If $n = n_1 n_2$, then there is a canonical isomorphism $\Gamma_n \cong \Gamma_{n_1} \times \Gamma_{n_2}$, so we can view Γ_{n_1} as either a subgroup or a quotient of Γ_n. With this identification we have

$$\Gamma_n = \prod_{\ell \mid n} \Gamma_\ell.$$

For every $\ell \notin \Sigma$, fix a generator σ_ℓ of Γ_ℓ. Define Kolyvagin's derivative operators

$$D_\ell := \sum_{i=1}^{\ell-2} i \sigma_\ell^i \in \mathbf{Z}[\Gamma_\ell]$$

and for $n \in \mathcal{N}$,

$$D_n := \prod_{\ell \mid n} D_\ell \in \mathbf{Z}[\Gamma_n]$$

where we view $\mathbf{Z}[\Gamma_\ell] \subset \mathbf{Z}[\Gamma_n]$ as above. Also define the norm elements

$$N_n := \sum_{\gamma \in \Gamma_n} \gamma \in \mathbf{Z}[\Gamma_n]$$

for $n \in \mathcal{N}$.

Lemma 4.3.2. *For every $\ell \notin \Sigma$, we have $(\sigma_\ell - 1) D_\ell = (\ell - 1) - N_\ell$.*

Proof. Exercise. □

As in §3.2, if $\ell \notin \Sigma$, let

$$\begin{aligned} \nu(\ell) := \max\{m : \ell \equiv 1 \pmod{p^m} \\ \text{and } A_m/(\mathrm{Fr}_\ell - 1)A_m \text{ is free of rank 1 over } \mathbf{Z}/p^m\mathbf{Z}\}. \end{aligned}$$

and if $n \in \mathcal{N}_{\mathcal{A}}$ define $\nu(n) := \min\{\nu(\ell) : \ell \mid n\}$. By convention we let $\nu(1) = \infty$, and $A_\infty := \mathcal{A}$.

Exercise 4.3.3. Show that $p^{\nu(\ell)}$ divides $P_\ell(1)$ for every $\ell \notin \Sigma$. Deduce that the reduction of $P_\ell(x)$ modulo $p^{\nu(\ell)}$ lies in $(x-1)(\mathbf{Z}/p^{\nu(\ell)}\mathbf{Z})[x]$.

Let $\mathcal{N}' = \{n \in \mathcal{N} : p \nmid n\}$.

Proposition 4.3.4. *If $\boldsymbol{\xi} \in \mathbf{ES}(\mathcal{A})$ and $n \in \mathcal{N}'$, then the image of $D_n\xi_n$ under the map $H^1(\mathbf{Q}(\boldsymbol{\mu}_n), \mathcal{A}) \to H^1(\mathbf{Q}(\boldsymbol{\mu}_n), A_{\nu(n)})$ lies in $H^1(\mathbf{Q}(\boldsymbol{\mu}_n), A_{\nu(n)})^{\Gamma_n}$.*

Proof. We need to show that $(\gamma-1)D_n\xi_n$ maps to zero in $H^1(\mathbf{Q}(\boldsymbol{\mu}_n), A_{\nu(n)})$ for every $\gamma \in \Gamma_n$. Since Γ_n is generated by $\{\sigma_\ell : \ell \mid n\}$, it is enough to check this for $\gamma = \sigma_\ell$. We will show, by induction on the number of primes dividing n, that $(\sigma_\ell - 1)D_n\xi_n \in p^{\nu(n)}H^1(\mathbf{Q}(\boldsymbol{\mu}_n), \mathcal{A})$. This will prove the lemma.

Using Lemma 4.3.2 we have

$$(\sigma_\ell - 1)D_n\xi_n = ((\ell-1) - N_\ell)D_{n/\ell}\xi_n = (\ell-1)D_{n/\ell}\xi_n - D_{n/\ell}N_\ell\xi_n.$$

The composition

$$H^1(\mathbf{Q}(\boldsymbol{\mu}_n), \mathcal{A}) \xrightarrow{\mathrm{Cor}_{\mathbf{Q}(\boldsymbol{\mu}_n)/\mathbf{Q}(\boldsymbol{\mu}_{n/\ell})}} H^1(\mathbf{Q}(\boldsymbol{\mu}_{n/\ell}), \mathcal{A}) \xrightarrow{\mathrm{Res}} H^1(\mathbf{Q}(\boldsymbol{\mu}_n), \mathcal{A})$$

is multiplication by N_ℓ, so by definition of an Euler system we conclude

$$(\sigma_\ell - 1)D_n\xi_n = (\ell-1)D_n\xi_n - \mathrm{Res}(D_nP_\ell(\mathrm{Fr}_\ell^{-1})\xi_{n/\ell}).$$

We have $p^{\nu(\ell)} \mid \ell - 1$, so $p^{\nu(n)} \mid \ell - 1$. By Exercise 4.3.3, we have

$$P_\ell(x) = (x-1)g(x) + p^{\nu(\ell)}h(x)$$

with $h(x), g(x) \in \mathbf{Z}[x]$, so we conclude by induction that

$$P_\ell(\mathrm{Fr}_\ell^{-1})\xi_{n/\ell} \in (p^{\nu(n/\ell)}, p^{\nu(\ell)})H^1(\mathbf{Q}(\boldsymbol{\mu}_{n/\ell}), \mathcal{A}) = p^{\nu(n)}H^1(\mathbf{Q}(\boldsymbol{\mu}_{n/\ell}), \mathcal{A}).$$

This completes the proof. □

Proposition 4.3.5. *Suppose $\boldsymbol{\xi} \in \mathbf{ES}(\mathcal{A})$ and $n \in \mathcal{N}'$. The image of $D_n\xi_n$ in $H^1(\mathbf{Q}(\boldsymbol{\mu}_n), A_{\nu(n)})$ has a canonical inverse image in $H^1(\mathbf{Q}, A_{\nu(n)})$ under the restriction map*

$$H^1(\mathbf{Q}, A_{\nu(n)}) \longrightarrow H^1(\mathbf{Q}(\boldsymbol{\mu}_n), A_{\nu(n)})^{\Gamma_n}.$$

Sketch of proof. The inflation-restriction exact sequence of Theorem 1.4.5 shows that the kernel and cokernel of the restriction map of the proposition are $H^1(\mathbf{Q}(\boldsymbol{\mu}_n)/\mathbf{Q}, A_{\nu(n)}^{G_{\mathbf{Q}(\boldsymbol{\mu}_n)}})$ and $H^2(\mathbf{Q}(\boldsymbol{\mu}_n)/\mathbf{Q}, A_{\nu(n)}^{G_{\mathbf{Q}(\boldsymbol{\mu}_n)}})$, respectively. If $A_{\nu(n)}^{G_{\mathbf{Q}(\boldsymbol{\mu}_n)}} = 0$, then it follows that the the restriction map is an isomorphism, and the proposition follows directly from Proposition 4.3.4.

For the proof in the general case, see [**R2**, §4.4] □

Exercise 4.3.6. Show that if $\mathcal{A} = \mathbf{Z}_p(1) \otimes \rho^{-1}$ as in §4.2, and ρ is not the mod-p cyclotomic character, then $A_m^{G_{\mathbf{Q}(\boldsymbol{\mu}_n)}} = 0$ for every $n \in \mathcal{N}'$ and every m.

Example 4.3.7. Let $\boldsymbol{\xi}^{\mathrm{cycl}}$ be the cyclotomic unit Euler system of §4.2. We will describe the construction of Proposition 4.3.5 explicitly in this case.

Keep the notation of §4.2; in particular for every $n \in \mathcal{N}'$ we identify

$$\xi_n^{\mathrm{cycl}} = \beta_n \in (\mathbf{Q}(\boldsymbol{\mu}_{np})^\times \otimes \mathbf{Z}_p)^\rho.$$

Fix $n \in \mathcal{N}'$ and let $m = \nu(n)$. The proof of Proposition 4.3.4 shows that for every $\sigma \in \Gamma_n$,

$$\beta_n^{(\sigma-1)D_n} \in (\mathbf{Q}(\boldsymbol{\mu}_{np})^\times \otimes \mathbf{Z}_p)^{p^m}$$

but even more, that argument gives a *canonical* p^m-th root

$$c_n(\sigma) \in (\mathbf{Q}(\boldsymbol{\mu}_{np})^\times \otimes \mathbf{Z}_p)^\rho$$

of $\beta_n^{(\sigma-1)D_n}$. The map $\sigma \mapsto c_n(\sigma)$ is a 1-cocycle in $Z^1(\Gamma_n, (\mathbf{Q}(\boldsymbol{\mu}_{np})^\times \otimes \mathbf{Z}_p)^\rho)$. Since $H^1(\Gamma_n, (\mathbf{Q}(\boldsymbol{\mu}_{np})^\times \otimes \mathbf{Z}_p)^\rho) = 0$ (see Proposition 1.6.1) it follows that there is a $\gamma_n \in (\mathbf{Q}(\boldsymbol{\mu}_{np})^\times \otimes \mathbf{Z}_p)^\rho$ and $x_n \in (\mathbf{Q}(\boldsymbol{\mu}_p)^\times \otimes \mathbf{Z}_p)^\rho$ such that

$$\beta_n^{D_n} = \gamma_n^{p^m} x_n.$$

Then γ_n is well-defined modulo $(\mathbf{Q}(\boldsymbol{\mu}_p)^\times \otimes \mathbf{Z}_p)^\rho$, so x_n is well-defined element of $(\mathbf{Q}(\boldsymbol{\mu}_p)^\times/(\mathbf{Q}(\boldsymbol{\mu}_p)^\times)^{p^m})^\rho = H^1(\mathbf{Q}, A_m)$ that restricts to $D_n\xi_n^{\mathrm{cycl}} \in H^1(\mathbf{Q}(\boldsymbol{\mu}_n), A_m)$.

Recall (Definition 2.1.3) that if $n \in \mathcal{N}'$, then $G_n = \otimes_{\ell \mid n}\Gamma_\ell$.

Fix an Euler system $\boldsymbol{\xi} \in \mathbf{ES}(\mathcal{A})$. For every $n \in \mathcal{N}'$, let $x_n \in H^1(\mathbf{Q}, A_{\nu(n)})$ be the canonical inverse image of $D_n\xi_n \in H^1(\mathbf{Q}(\boldsymbol{\mu}_n), A_{\nu(n)})$ given by Proposition 4.3.5, and define

$$\xi'_n := x_n \otimes (\otimes_{\ell \mid n}\sigma_\ell) \in H^1(\mathbf{Q}(\boldsymbol{\mu}_n), A_{\nu(n)}) \otimes G_n.$$

Exercise 4.3.8. Show that, although $D_n\xi_n$ depends on the choice of the generators σ_ℓ of Γ_ℓ, ξ'_n does not.

Definition 4.3.9. Suppose $n \in \mathcal{N}'$ and $\ell \mid n$. By Proposition 1.9.5(3) we have a decomposition

$$H^1(\mathbf{Q}_\ell, A_{\nu(n)}) \cong H^1_{\mathrm{u}}(\mathbf{Q}_\ell, A_{\nu(n)}) \oplus H^1_{\mathrm{t}}(\mathbf{Q}_\ell, A_{\nu(n)})$$

and if $x \in H^1(\mathbf{Q}, A_{\nu(n)})$ we let $x_{\ell,\mathrm{u}}$ and $x_{\ell,\mathrm{t}}$ denote the projections of $\mathrm{Res}_\ell(x) \in H^1(\mathbf{Q}_\ell, A_{\nu(n)})$ into $H^1_{\mathrm{u}}(\mathbf{Q}_\ell, A_{\nu(n)}) \otimes G_n$ and $H^1_{\mathrm{t}}(\mathbf{Q}_\ell, A_{\nu(n)}) \otimes G_n$, respectively.

Ideally, we would like to show that the collection

$$\boldsymbol{\xi}' = \{\xi'_n : n \in \mathcal{N}'\}$$

is a Kolyvagin system for $\mathcal{A}$ as defined in §3.2. (In fact it isn't in general, but a slight modification of it will be.) To do this we would need to verify that for every $n \in \mathcal{N}'$:

- $\mathrm{Res}_\ell(\xi'_n) \in H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbf{Q}_\ell, A_{\nu(n)}) \otimes G_n$ if $\ell \nmid n$,
- $\mathrm{Res}_\ell(\xi'_n) \in H^1_{\mathrm{t}}(\mathbf{Q}_\ell, A_{\nu(n)}) \otimes G_n$ if $\ell \mid n$,
- $\phi_\ell^{\mathrm{ut}} \circ \mathrm{Res}_\ell(\xi'_{n/\ell}) = (\xi'_n)_{\ell,\mathrm{t}} \in H^1_{\mathrm{t}}(\mathbf{Q}_\ell, A_{\nu(n)}) \otimes G_n$ if $\ell \mid n$.

The following theorem deals with the first and third of these conditions, and Theorem 4.3.12 below investigates the second.

Theorem 4.3.10. *Suppose $\boldsymbol{\xi} \in \mathbf{ES}(\mathcal{A})$ and $H^0(\mathbf{Q}_p, \mathcal{A}^*)$ is a divisible $\mathbf{Z}_p$-module, and $n \in \mathcal{N}'$.*

(1) *If $\ell \nmid n$, then $\mathrm{Res}_\ell(\xi'_n) \in H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbf{Q}_\ell, A_{\nu(n)}) \otimes G_n$.*
(2) *If $\ell \mid n$, then $\phi_\ell^{\mathrm{ut}} \circ \mathrm{Res}_\ell(\xi'_{n/\ell}) = (\xi'_n)_{\ell,\mathrm{t}}$ in $H^1_{\mathrm{t}}(\mathbf{Q}_\ell, A_{\nu(n)}) \otimes G_n$.*

Proof. For the proof of Proposition 4.3.10, see [**R2**, Theorem 4.5.1] for (1) when $\ell \neq p$, and [**R2**, Theorem 4.5.4] for (2). Note that since $H^0(\mathbf{Q}_p, \mathcal{A}^*)$ is divisible, Exercise 3.1.8 shows that $H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbf{Q}_p, A_{\nu(n)}) = H^1(\mathbf{Q}_p, A_{\nu(n)})$, so (1) is trivially satisfied when $\ell = p$.

See also [**R1**, Proposition 2.4] for the proof in the case of the cyclotomic unit Euler system. □

Note that if $\ell \mid n$ and $x \in H^1(\mathbf{Q}, A_{\nu(n)})$, then

$$\mathrm{Res}_\ell(x) \in H^1_{\mathrm{t}}(\mathbf{Q}_\ell, A_{\nu(n)}) \Longleftrightarrow x_{\ell,\mathrm{u}} = 0.$$

The $(\xi'_n)_{\ell,\mathrm{u}}$ are not zero in general, but they are described by Theorem 4.3.12 below.

Definition 4.3.11. If $\ell \notin \Sigma$, let I_ℓ be the augmentation ideal of $(\mathbf{Z}/p^{\nu(\ell)}\mathbf{Z})[G_\ell]$. Then there is a canonical isomorphism

$$\rho_\ell : I_\ell/I_\ell^2 \longrightarrow G_\ell \otimes (\mathbf{Z}/p^{\nu(\ell)}\mathbf{Z})$$

that sends $g-1$ to g for every $g \in G_\ell$.

If $n \in \mathcal{N}'$ let $\mathfrak{S}(n)$ denote the set of permutations of the primes dividing n, and if $\ell \mid n$ let $\mathfrak{S}^1_\ell(n) \subset \mathfrak{S}(n)$ be the subset

$$\{\pi \in \mathfrak{S}(n) : \text{the } \ell \text{ not fixed by } \pi \text{ form a single } \pi\text{-orbit, and } \pi(\ell) \neq \ell\}.$$

If $\pi \in \mathfrak{S}(n)$ let $d_\pi = \prod_{\pi(q)=q} q$.

Recall that $\omega(d)$ is the number of prime factors of a positive integer d.

Theorem 4.3.12. *Suppose $\boldsymbol{\xi} \in \mathbf{ES}(\mathcal{A})$ and for every $\ell \notin \Sigma$, $P_\ell(x)$ has no roots in $\boldsymbol{\mu}_{p^\infty}$. If $n \in \mathcal{N}'$ and $\ell \mid n$ then*

$$(\xi'_n)_{\ell,\mathrm{u}} = \sum_{\pi \in \mathfrak{S}^1_\ell(n)} (-1)^{\omega(n/d_\pi)} \mathrm{Res}_\ell(\xi'_{d_\pi}) \bigotimes_{q \mid (n/d_\pi)} \rho_q(P_q(\mathrm{Fr}^{-1}_{\pi(q)}|_{\mathbf{Q}(\boldsymbol{\mu}_q)})).$$

Proof. For the proof, see [**MR1**, Theorem A.4]. For a proof in the special case of the cyclotomic unit Euler system, see [**MR2**, Appendix A]. □

Corollary 4.3.13. *Suppose $\boldsymbol{\xi} \in \mathbf{KS}(\mathcal{A})$ and*

1. *for every $\ell \notin \Sigma$, $P_\ell(x)$ has no roots in $\boldsymbol{\mu}_{p^\infty}$,*
2. *$H^0(\mathbf{Q}_p, \mathcal{A}^*)$ is a divisible $\mathbf{Z}_p$-module.*

For $n \in \mathcal{N}'$ define

$$\kappa_n = \sum_{\pi \in \mathfrak{S}(n)} \mathrm{sign}(\pi) \xi'_{d_\pi} \bigotimes_{\ell \mid (n/d_\pi)} \rho_\ell(P_\ell(\mathrm{Fr}^{-1}_{\pi(\ell)}|_{\mathbf{Q}(\boldsymbol{\mu}_\ell)})) \in H^1(\mathbf{Q}, A_{\nu(n)}) \otimes G_n.$$

Then the collection $\boldsymbol{\kappa} := \{\kappa_n : n \in \mathcal{N}'\}$ is a Kolyvagin system for $(\mathcal{A}, \mathcal{F}_{\mathrm{can}})$, and $\kappa_1 = \xi_1$.

Proof. By Theorem 4.3.10, it is enough to prove that $(\kappa_n)_{\ell,\mathrm{u}} = 0$ whenever $n \in \mathcal{N}'$ and $\ell \mid n$. This follows from Theorem 4.3.12; for the details see the proof of Theorem 3.2.4 on pages 80–81 of [**MR1**]. □

The map $\mathbf{ES}(\mathcal{A}) \to \mathbf{KS}(\mathcal{A}, \mathcal{F}_{\mathrm{can}})$ of Theorem 4.3.1 is given by $\boldsymbol{\xi} \mapsto \boldsymbol{\kappa}$ as described above.

LECTURE 5

Applications

5.1. Cyclotomic units and ideal class groups.

Fix a rational prime $p > 2$, and let $F = \mathbf{Q}(\boldsymbol{\mu}_p)^+$, the real subfield of $\mathbf{Q}(\boldsymbol{\mu}_p)$. Let $\mathcal{C}_F$ denote the p-part of the ideal class group of F. Let $\mathcal{E}_F \subset \mathcal{O}_F^\times$ denote the group of cyclotomic units of F, the intersection of $\mathcal{O}_F^\times$ with the group generated by

$$\{\zeta, \zeta - 1 : \zeta \in \boldsymbol{\mu}_p, \zeta \neq 1\}.$$

The following theorem was first proved (by a different method) by Mazur and Wiles [**MW**].

Theorem 5.1.1. *Let* $\rho : \mathrm{Gal}(F/\mathbf{Q}) \to \mathbf{Z}_p^\times$ *be a nontrivial (even) character. Then*

$$|\mathcal{C}_F^\rho| = |((\mathcal{O}_F^\times/\mathcal{E}_F) \otimes \mathbf{Z}_p)^\rho|.$$

Proof. As in §4.2, let $\boldsymbol{\xi}^{\mathrm{cycl}} \in \mathbf{ES}(\mathbf{Z}_p(1) \otimes \rho^{-1})$ be the Euler system constructed there. Let $\boldsymbol{\kappa}^{\mathrm{cycl}} \in \mathbf{KS}(\mathbf{Z}_p(1) \otimes \rho^{-1})$ be the Kolyvagin system constructed from $\boldsymbol{\xi}^{\mathrm{cycl}}$ in Theorem 4.3.1. Then we have

$$\kappa_1^{\mathrm{cycl}} = \xi_1^{\mathrm{cycl}} = \prod_{\delta \in \mathrm{Gal}(\mathbf{Q}(F)/\mathbf{Q})} (\zeta_p^\delta - 1)^{\rho^{-1}(\delta)} \in (\mathcal{E}_F \otimes \mathbf{Z}_p)^\rho$$
$$\subset (\mathcal{O}_F^\times \otimes \mathbf{Z}_p)^\rho = H^1(\mathbf{Q}, \mathbf{Z}_p(1) \otimes \rho^{-1}).$$

In fact, κ_1^{cycl} is a $\mathbf{Z}_p$-generator of $(\mathcal{E}_F \otimes \mathbf{Z}_p)^\rho$, so by Corollary 3.3.13,

$$|\mathcal{C}_F^\rho| \leq [(\mathcal{O}_F^\times \otimes \mathbf{Z}_p)^\rho : \mathbf{Z}_p\kappa_1] = |((\mathcal{O}_F^\times/\mathcal{E}_F) \otimes \mathbf{Z}_p)^\rho|. \tag{5.1}$$

Note that (5.1) also holds when $\rho = 1$, since in that case both sides are equal to 1. Taking the product over all ρ, we have

$$|\mathcal{C}_{\mathbf{Q}(F}| = \prod_\rho |\mathcal{C}_F^\rho| \leq \prod_\rho |((\mathcal{O}_F^\times/\mathcal{E}_F) \otimes \mathbf{Z}_p)^\rho| = |(\mathcal{O}_F^\times/\mathcal{E}_F) \otimes \mathbf{Z}_p|.$$

The analytic class number formula (see for example [**L**, Theorem 5.1 of Chapter 3]) says that $|\mathcal{C}_{\mathbf{Q}(F}| = |(\mathcal{O}_F^\times/\mathcal{E}_F) \otimes \mathbf{Z}_p|$, so we must have equality in (5.1) for every ρ. □

Remark 5.1.2. Note that using Corollary 3.3.13, the proof of Theorem 5.1.1 also shows that the cyclotomic unit Kolyvagin system $\boldsymbol{\kappa}^{\mathrm{cycl}}$ is primitive.

5.2. Elliptic curves.

Return now to the example of §3.4. Namely, E is an elliptic curve defined over $\mathbf{Q}$, $p \geq 5$ is a rational prime, and the p-adic representation $G_Q \to \mathrm{Aut}(E[p^\infty]) \cong \mathrm{GL}_2(\mathbf{Z}_p)$ is surjective.

In this setting, an Euler system for $T_p(E)$ was constructed by Kato in [**K**]. We will not touch on his construction here, but we will discuss briefly the essential properties of Kato's Euler system, and some of its consequences. For more details, see [**K**], [**R2**, §3.5], and [**Sc**].

For simplicity, we also assume from now on that

$$E \text{ has good reduction at } p \text{ and } p \nmid |E(\mathbf{F}_p)|. \tag{5.2}$$

Recall that for every $m > 0$, $H^1_{\mathrm{f}}(\mathbf{Q}_p, E[p^m])$ is the image of $E(\mathbf{Q}_p)/p^m E(\mathbf{Q}_p)$ in $H^1(\mathbf{Q}_p, E[p^m])$ under the (injective) Kummer map as in Definition 1.6.13. We define

$$H^1_{\mathrm{f}}(\mathbf{Q}_p, T_p(E)) = \varprojlim H^1_{\mathrm{f}}(\mathbf{Q}_p, E[p^m]) \subset H^1(\mathbf{Q}_p, T_p(E))$$

so $H^1_{\mathrm{f}}(\mathbf{Q}_p, T_p(E)) \cong E(\mathbf{Q}_p) \otimes \mathbf{Z}_p$. It follows from (5.2) that $E(\mathbf{Q}_p)$ has no p-torsion, so $H^1_{\mathrm{f}}(\mathbf{Q}_p, T_p(E))$ is a free, rank-one $\mathbf{Z}_p$-module.

Fix a minimal Weierstrass model of E. Let ω_E and Ω_E be the corresponding holomorphic differential on E, and real period. Corresponding to ω_E there is a *dual exponential map* $\exp_{\omega_E}$ and an exact sequence

$$0 \longrightarrow H^1_{\mathrm{f}}(\mathbf{Q}_p, T_p(E)) \longrightarrow H^1(\mathbf{Q}_p, T_p(E)) \xrightarrow{\exp_{\omega_E}} p^{-1}\mathbf{Z}_p \longrightarrow 0. \tag{5.3}$$

Let $L(E, s)$ denote the Hasse-Weil L-function of E, and

$$L_p(E, s) = (1 - a_p p^{-s} + p^{1-2s}) L(E, s),$$

the L-function with the Euler factor at p removed (here $a_p := p + 1 - |E(\mathbf{F}_p)|$).

We make no attempt here to prove the following theorem of Kato.

Theorem 5.2.1 (Kato [**K**])**.** *There is a nonzero Euler system* $\boldsymbol{\xi}^{\mathrm{Kato}} \in \mathbf{ES}(T_p(E))$ *such that*

$$\exp_{\omega_E}(\mathrm{Res}_p(\xi_1^{\mathrm{Kato}})) = \frac{L_p(E, 1)}{\Omega_E}.$$

Theorem 5.2.2 (Kato [**K**])**.** *With assumptions as above, we have:*

(1) *If* $L(E, 1) \neq 0$ *then* $E(\mathbf{Q})$ *is finite and* $|\text{Ш}(E/\mathbf{Q})[p^\infty]|$ *divides* $L(E, 1)/\Omega_E$*.*
(2) *If* $L(E, 1) = 0$ *and* $\xi_1^{\mathrm{Kato}} \neq 0$*, then either* $E(\mathbf{Q})$ *or* $\text{Ш}(E/\mathbf{Q})[p^\infty]$ *is infinite.*

Proof. Let $\mathcal{F}$ denote the canonical Selmer structure on $T_p(E)$, and let $\boldsymbol{\kappa}^{\mathrm{Kato}} \in \mathbf{KS}(T_p(E), \mathcal{F})$ be the Kolyvagin system attached to $\boldsymbol{\xi}^{\mathrm{Kato}}$ by Theorem 4.3.1. (Note that the hypotheses of Theorem 4.3.1 hold, thanks to (5.2).)

Suppose first that $L(E, 1) \neq 0$. Define integers $-1 \leq b \leq c$ by

$$\begin{array}{ccc} p^b\mathbf{Z}_p & = & \exp_{\omega_E}(\mathrm{Res}_p(H^1_{\mathcal{F}}(\mathbf{Q}, T_p(E)))) \\ \cup & & \cup \\ p^c\mathbf{Z}_p & = & \exp_{\omega_E}(\mathbf{Z}_p \mathrm{Res}_p(\xi_1^{\mathrm{Kato}})) \end{array}$$

so $c = \mathrm{ord}_p(L_p(E, 1)/\Omega_E)$. Then (see Definition 3.2.5) $\partial^0(\boldsymbol{\kappa}^{\mathrm{Kato}}) \leq c - b$, so by Corollary 3.2.9(1)

$$|H^1_{\mathcal{F}^*}(\mathbf{Q}, E[p^\infty])| \text{ divides } p^{c-b}. \tag{5.4}$$

We need to compare $H^1_{\mathcal{F}^*}(\mathbf{Q}, E[p^\infty])$ with the classical Selmer group

$$\mathrm{Sel}_{p^\infty}(E/\mathbf{Q}) := H^1_{\mathrm{f}}(\mathbf{Q}, E[p^\infty])$$

defined using the Selmer structure of local cohomology groups $H^1_{\mathrm{f}}(\mathbf{Q}_\ell, E[p^\infty])$ (see Definition 1.6.13). By Proposition 3.4.5, $H^1_{\mathcal{F}}((\mathbf{Q}_\ell, E[p^\infty]) = H^1_{\mathrm{f}}(\mathbf{Q}_\ell, E[p^\infty])$ for every $\ell \neq p$. Passing to the limit in Corollary 3.4.6 gives

$$0 \longrightarrow H^1_{\mathrm{f}}(\mathbf{Q}, T_p(E)) \longrightarrow H^1_{\mathcal{F}}(\mathbf{Q}, T_p(E)) \longrightarrow H^1(\mathbf{Q}_p, T_p(E))/H^1_{\mathrm{f}}(\mathbf{Q}_p, T_p(E))$$

$$0 \longrightarrow H^1_{\mathcal{F}^*}(\mathbf{Q}, E[p^\infty]) \longrightarrow \mathrm{Sel}_{p^\infty}(E/\mathbf{Q}) \xrightarrow{\qquad\qquad} H^1_{\mathrm{f}}(\mathbf{Q}_p, E[p^\infty]).$$

By global duality (Theorem 1.10.2), together with the fact that $H^1_{\mathrm{f}}(\mathbf{Q}_\ell, E[p^m])$ is its own orthogonal complement under the Tate pairing for every ℓ (Example 1.8.4), the images of the two right-hand maps are orthogonal complements under the limit of the local Tate pairings. By definition of b and (5.3), the cokernel of the upper right-hand map has order p^{b+1}. Hence we conclude from the bottom sequence that

$$[\mathrm{Sel}_{p^\infty}(E/\mathbf{Q}) : H^1_{\mathcal{F}^*}(\mathbf{Q}, E[p^\infty])] = p^{b+1},$$

and combining this with (5.4) we see that

$$|\mathrm{Sel}_{p^\infty}(E/\mathbf{Q})| \text{ divides } p^{c-b} \cdot p^{b+1} = p^{c+1}.$$

Further

$$\begin{aligned} c + 1 = \mathrm{ord}_p(pL_p(E,1)/\Omega_E) &= \mathrm{ord}_p((p + a_p - 1)L(E,1)/\Omega_E) \\ &= \mathrm{ord}_p(|E(\mathbf{F}_p)|L(E,1)/\Omega_E) = \mathrm{ord}_p(L(E,1)/\Omega_E) \end{aligned}$$

since we assumed that $p \nmid |E(\mathbf{F}_p)|$. Now (1) follows from the exact sequence

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

the direct limit of the exact sequences (1.3).

Suppose now that $L(E,1) = 0$ and $\xi_1^{\mathrm{Kato}} \neq 0$. By (5.3) we have $\mathrm{Res}_p(\xi_1^{\mathrm{Kato}}) \in H^1_{\mathrm{f}}(\mathbf{Q}_p, T_p(E))$, so

$$\xi_1^{\mathrm{Kato}} \in H^1_{\mathrm{f}}(\mathbf{Q}, T_p(E))$$

and in particular $H^1_{\mathrm{f}}(\mathbf{Q}, T_p(E)) \neq 0$. But the inverse limit of the exact sequences (1.3) give

$$0 \longrightarrow E(\mathbf{Q}) \otimes \mathbf{Z}_p \longrightarrow H^1_{\mathrm{f}}(\mathbf{Q}, T_p(E)) \longrightarrow \varprojlim Ш(E/\mathbf{Q})[p^m] \longrightarrow 0.$$

The inverse limit on the right is with respect to the maps "multiplication by p", so this inverse limit is either zero or infinite. Similarly, since we assumed that the p-adic representation $G_{\mathbf{Q}} \to \mathrm{Aut}(E[p^\infty])$ is surjective, $E(\mathbf{Q})$ has no p-torsion so $E(\mathbf{Q}) \otimes \mathbf{Z}_p$ is either zero or infinite. Hence if $\xi_1^{\mathrm{Kato}} \neq 0$ then one of those two groups is infinite, and this completes the proof of (2). □

Exercise 5.2.3. Using Corollary 3.2.9(1) and the proof of Theorem 5.2.2, show that if $L(E,1) \neq 0$ then

$$\mathrm{length}(Ш(E/\mathbf{Q})[p^\infty]) = \mathrm{ord}_p(L(E,1)/\Omega_E) \iff \boldsymbol{\kappa}^{\mathrm{Kato}} \text{ is primitive.}$$

Note that according to the Birch and Swinnerton-Dyer conjecture, it is *not* always the case that $\mathrm{length}(Ш(E/\mathbf{Q})[p^\infty]) = \mathrm{ord}_p(L(E,1)/\Omega_E)$, and therefore it is *not* always the case that $\boldsymbol{\kappa}^{\mathrm{Kato}}$ is primitive.

5.3. General speculation.

In this section we sketch a general framework for the example of the previous section.

Suppose $\mathcal{A}$ is a p-adic representation of $G_{\mathbf{Q}}$ as in Lecture 3: a free $\mathbf{Z}_p$-module of finite rank with a continuous action of $G_{\mathbf{Q}}$, ramified at only finitely many primes. Let $\mathcal{F}$ denote the canonical Selmer structure on $\mathcal{A}$, and suppose $\mathcal{G}$ is another Selmer structure on $\mathcal{A}$, with the property that $H^1_{\mathcal{G}}(\mathbf{Q}_\ell, \mathcal{A}) = H^1_{\mathcal{F}}(\mathbf{Q}_\ell, \mathcal{A})$ for all ℓ different from p. Then $H^1_{\mathcal{G}}(\mathbf{Q}, \mathcal{A}) \subset H^1_{\mathcal{F}}(\mathbf{Q}, \mathcal{A})$, and we have a diagram

$$\begin{tikzcd}
0 \arrow[r] & H^1_{\mathcal{G}}(\mathbf{Q}, \mathcal{A}) \arrow[r] & H^1_{\mathcal{F}}(\mathbf{Q}, \mathcal{A}) \arrow[r, "\mathrm{Res}_p"] & H^1(\mathbf{Q}_p, \mathcal{A})/H^1_{\mathcal{G}}(\mathbf{Q}_p, \mathcal{A}) \\
0 \arrow[r] & H^1_{\mathcal{F}^*}(\mathbf{Q}, \mathcal{A}^*) \arrow[r] & H^1_{\mathcal{G}^*}(\mathbf{Q}, \mathcal{A}^*) \arrow[r, "\mathrm{Res}_p"] & H^1_{\mathcal{G}^*}(\mathbf{Q}_p, \mathcal{A}^*).
\end{tikzcd}$$

Passing to the limit in Theorem 1.10.2, we see that

$$[H^1_{\mathcal{G}^*}(\mathbf{Q}, \mathcal{A}^*) : H^1_{\mathcal{F}^*}(\mathbf{Q}, \mathcal{A}^*)] = [H^1(\mathbf{Q}_p, \mathcal{A}) : H^1_{\mathcal{G}}(\mathbf{Q}_p, \mathcal{A}) + \mathrm{Res}_p(H^1_{\mathcal{F}}(\mathbf{Q}, \mathcal{A}))].$$

Suppose in addition there is an isomorphism

$$\mathfrak{L} : H^1(\mathbf{Q}_p, \mathcal{A})/H^1_{\mathcal{G}}(\mathbf{Q}_p, \mathcal{A}) \xrightarrow{\sim} \mathbf{Z}_p.$$

Then we conclude that

$$[H^1_{\mathcal{G}^*}(\mathbf{Q}, \mathcal{A}^*) : H^1_{\mathcal{F}^*}(\mathbf{Q}, \mathcal{A}^*)] = [\mathbf{Z}_p : \mathfrak{L}(\mathrm{Res}_p(H^1_{\mathcal{F}}(\mathbf{Q}, \mathcal{A})))]. \tag{5.5}$$

Theorem 5.3.1. *Suppose that $\mathcal{A}$, $\mathcal{G}$, and $\mathfrak{L}$ are as above, that $\mathcal{A}$ satisfies hypotheses (H.1-4) of §3.1 and the hypotheses of Theorem 4.3.1, and that the core rank $\chi(\mathcal{A}) = 1$. If $\boldsymbol{\xi} \in \mathbf{ES}(\mathcal{A})$ is an Euler system for $\mathcal{A}$, then*

$$\mathrm{length}_{\mathbf{Z}_p}(H^1_{\mathcal{G}^*}(\mathbf{Q}, \mathcal{A}^*)) \leq \mathrm{ord}_p(\mathfrak{L}(\mathrm{Res}_p(\xi_1))).$$

Proof. Let $\boldsymbol{\kappa} \in \mathbf{KS}(\mathcal{A}, \mathcal{F})$ be the Kolyvagin system corresponding to $\boldsymbol{\xi}$ under Theorem 4.3.1. By Corollary 3.2.9, using that $\kappa_1 = \xi_1$,

$$|H^1_{\mathcal{F}^*}(\mathbf{Q}, \mathcal{A}^*)| \leq p^{\partial^0(\boldsymbol{\kappa})} \leq [\mathfrak{L}(\mathrm{Res}_p(H^1_{\mathcal{F}}(\mathbf{Q}, \mathcal{A}))) : \mathfrak{L}(\mathrm{Res}_p(\xi_1))\mathbf{Z}_p].$$

Combining this with (5.5), we see that

$$|H^1_{\mathcal{G}^*}(\mathbf{Q}, \mathcal{A}^*)| \leq [\mathbf{Z}_p : \mathfrak{L}(\mathrm{Res}_p(\xi_1))\mathbf{Z}_p],$$

which proves the theorem. □

Example 5.3.2. Suppose E is an elliptic curve as in §5.2. Let $\mathcal{A} = T_p(E)$, let $H^1_{\mathcal{G}}(\mathbf{Q}_\ell, T_p(E)) = H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T_p(E)$ for every ℓ, let $\mathfrak{L} = p\exp_{\omega_E}$, and let $\boldsymbol{\xi} = \boldsymbol{\xi}^{\mathrm{Kato}}$. Then $H^1_{\mathcal{G}}(\mathbf{Q}, \mathcal{A}^*) = \mathrm{Sel}_{p^\infty}(E/\mathbf{Q})$, $\mathfrak{L}(\mathrm{Res}_p(\xi_1)) = |E(\mathbf{F}_p)|L(E,1)/\Omega_E$, and Theorem 5.3.1 is part of Theorem 5.2.2(1).

Example 5.3.3. Suppose ρ is a nontrivial character of $\mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_p)^+/\mathbf{Q})$, $\mathcal{A} = \mathbf{Z}_p(1) \otimes \rho^{-1}$, and $\boldsymbol{\xi}^{\mathrm{cycl}} \in \mathbf{ES}(\mathbf{Z}_p(1) \otimes \rho^{-1})$ is the cyclotomic unit Euler system of §4.2. Let $\mathcal{F}$ be the canonical Selmer structure on $\mathbf{Z}_p(1) \otimes \rho^{-1}$, and let $\mathcal{G}$ be the Selmer structure defined by

$$H^1_{\mathcal{G}}(\mathbf{Q}_\ell, \mathbf{Z}_p(1) \otimes \rho^{-1}) = \begin{cases} H^1_{\mathcal{F}}(\mathbf{Q}_\ell, \mathbf{Z}_p(1) \otimes \rho^{-1}) & \text{if } \ell \neq p, \\ 0 & \text{if } \ell = p. \end{cases}$$

Let M is the maximal abelian p-extension of $\mathbf{Q}(\boldsymbol{\mu}_p)^+$ unramified outside of p (with no local restriction at p), and $\mathcal{X} := \mathrm{Gal}(M/\mathbf{Q}(\boldsymbol{\mu}_p)^+)$. Then $H^1_{\mathcal{G}^*}(\mathbf{Q}_p, \mathbf{Q}_p/\mathbf{Z}_p \otimes \rho) = H^1(\mathbf{Q}_p, \mathbf{Q}_p/\mathbf{Z}_p \otimes \rho)$, so as in Proposition 3.3.11 we have

$$H^1_{\mathcal{G}^*}(\mathbf{Q}, \mathbf{Q}_p/\mathbf{Z}_p \otimes \rho) = \mathrm{Hom}(\mathcal{X}^\rho, \mathbf{Q}_p/\mathbf{Z}_p).$$

Let $F := \mathbf{Q}(\boldsymbol{\mu}_p)^+$. By Exercise 3.3.10, $H^1_{\mathcal{F}}(\mathbf{Q}_p, \mathbf{Z}_p(1) \otimes \rho^{-1}) \cong (\mathcal{O}_{F,p}^\times \otimes \mathbf{Z}_p)^\rho$. Let $\log_p : \mathcal{O}_{F,p}^\times \to F_p$ denote the p-adic logarithm map, let $\tau(\rho^{-1}) : \sum_{a=1}^{p-1} \rho^{-1}(a)\zeta_p^a \in F_p$ be the Gauss sum, and define

$$\mathfrak{L} = \tfrac{1}{\tau(\rho^{-1})} \log_p : H^1_{\mathcal{F}}(\mathbf{Q}_p, \mathbf{Z}_p(1) \otimes \rho^{-1}) \xrightarrow{\sim} (\mathcal{O}_{F,p}^\times \otimes \mathbf{Z}_p)^\rho \longrightarrow F_p.$$

Exercise 5.3.4. Show that $\mathfrak{L}$ is an isomorphism from $H^1_{\mathcal{F}}(\mathbf{Q}_p, \mathbf{Z}_p(1) \otimes \rho^{-1})$ onto $\mathbf{Z}_p$.

By Exercise 4.2.4 we have

$$\mathfrak{L}(\mathrm{Res}_p(\xi_1^{\mathrm{cycl}})) = -L_p(1, \rho)$$

where $L_p(s, \rho)$ is the Kubota-Leopoldt p-adic L-function attached to ρ (see for example [**L**, Theorem 4.3.6]). Therefore we can apply Theorem 5.3.1 to conclude that

$$\mathrm{length}(\mathcal{X}^\rho) \le \mathrm{ord}_p(L_p(1, \rho)). \tag{5.6}$$

Exercise 5.3.5. Use the fact that $\boldsymbol{\kappa}^{\mathrm{cycl}}$ is primitive (Remark 5.1.2) to show that equality holds in (5.6).

Remark 5.3.6. Returning to the case of a more general p-adic representation $\mathcal{A}$, it is clear what we would like to do in general: find an Euler system $\boldsymbol{\xi} \in \mathbf{ES}(\mathcal{A})$, and a map

$$\mathfrak{L} : H^1(\mathbf{Q}_p, \mathcal{A}) \twoheadrightarrow \mathbf{Z}_p$$

such that $\mathfrak{L}(\mathrm{Res}_p(\xi_1))$ is (related to) a special value of a (p-adic) L-function attached to $\mathcal{A}$. Then (under suitable assumptions) Theorem 5.3.1 will bound the length of the Selmer group $H^1_{\mathcal{G}^*}(\mathbf{Q}, \mathcal{A}^*)$ in terms of that L-value, where the Selmer structure $\mathcal{G}$ is defined by $H^1_{\mathcal{G}}(\mathbf{Q}_p, \mathcal{A}) := \ker(\mathfrak{L})$.

Although very little general progress has been made in this direction, one can formulate a more precise conjecture. See for example [**PR**], or [**R2**, Chapter 8].

Bibliography

[AT] M. Artin, J. Tate, Class field theory. New York: Benjamin (1967).

[AW] M. Atiyah, C.T.C. Wall, Cohomology of groups. In: Algebraic Number Theory, J. W. S. Cassels and A. Fröhlich, eds., London: Academic Press (1967) 94–115.

[Ca] J.W.S. Cassels, Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer. *J. Reine Angew. Math.* **217** (1965) 180–199.

[Gr] K. Gruenberg, Profinite groups. In: Algebraic Number Theory, J. W. S. Cassels and A. Fröhlich, eds., London: Academic Press (1967) 116–127.

[K] K. Kato, p-adic Hodge theory and values of zeta functions of modular forms. *Astérisque* **295** (2004) 117–290.

[L] S. Lang, Cyclotomic fields I and II. *Graduate Texts in Math.* **121**, New York: Springer-Verlag (1990).

[MR1] B. Mazur and K. Rubin, Kolyvagin systems. *Memoirs of the Amer. Math. Soc.* **799** (2004).

[MR2] B. Mazur and K. Rubin, Introduction to Kolyvagin systems. In: Starks Conjectures: Recent Work and New Directions, *Contemp. Math.* **358**, Providence: Amer. Math. Soc. (2004) 207-221.

[MW] Mazur, B., Wiles, A.: Class fields of abelian extensions of **Q**, *Invent. math.* **76** (1984) 179–330.

[Mi] J.S. Milne, Arithmetic duality theorems, *Perspectives in Math.* **1**, Orlando: Academic Press (1986).

[PR] B. Perrin-Riou, Fonctions L p-adiques des représentations p-adiques. *Astérisque* **229** (1995).

[R1] K. Rubin, The main conjecture. Appendix to: Cyclotomic fields I and II, S. Lang, *Graduate Texts in Math.* **121**, New York: Springer-Verlag (1990) 397–419.

[R2] K. Rubin, Euler systems. *Annals of Math. Studies* **147**, Princeton: Princeton University Press (2000).

[Sc] Scholl, A.: An introduction to Kato's Euler systems. In: Galois representations in arithmetic algebraic geometry, A. J. Scholl and R. L. Taylor, eds., *London Math. Soc. Lect. Notes* **254** Cambridge: Cambridge Univ. Press (1998) 379–460.

[Se1] J-P. Serre, Cohomologie Galoisienne, Fifth edition. *Lecture Notes in Math.* **5**, Berlin: Springer-Verlag (1994).

[Se2] J-P. Serre, Corps Locaux, 2nd edition. Paris: Hermann (1968).

[Si] J.H. Silverman, The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics **106**, New York: Springer-Verlag (1986).

[Ta1] J. Tate, WC-groups over $\mathfrak{p}$-adic fields. *Séminaire Bourbaki* **4**, Exp. 156, Paris: Soc. Math. France (1995) 265–277.

[Ta2] Tate, J.: Duality theorems in Galois cohomology over number fields. In: *Proc. Intern. Cong. Math.*, Stockholm (1962) 234–241.

[Ta3] J. Tate, Galois cohomology. In: Arithmetic algebraic geometry (Park City, UT, 1999), *IAS/Park City Math. Ser.* **9**, Providence: Amer. Math. Soc. (2001) 465–479.

[Wi] A. Wiles, Modular elliptic curves and Fermat's Last Theorem. *Annals of Math.* **141** (1995) 443–551.