AN INTRODUCTORY LECTURE ON EULER SYSTEMS

BARRY MAZUR, HARVARD UNIVERSITY

Notes by Jung-Jo Lee, Ariel Pacetti, and John Voight

The purpose of these notes is to describe the notion of an *Euler system*, a collection of compatible cohomology classes arising from a tower of fields that can be used to bound the size of Selmer groups. There are applications to the study of the ideal class group, Iwasawa's main conjecture, Mordell-Weil group of an elliptic curve, Ш (the Safarevich-Tate group), Birch-Swinnerton-Dyer conjecture, and a study of the p-adic main conjecture for elliptic curves. For a reference, consult [R 1], the bibliography there, and also [R 2].

Our group will be giving four hour lectures, as the schedule indicates, as follows:

1. Introduction to Euler Systems and Kolyvagin Systems. (B.M.)

2. L-functions and applications of Euler systems to ideal class groups (ascending cyclotomic towers over $\mathbf{Q}$). (T.W.)

3. Student presentation: The "Heegner point" Euler System and applications to the Selmer groups of elliptic curves (ascending anti-cyclotomic towers over quadratic imaginary fields).

4. Student presentation: "Kato's Euler System" and applications to the Selmer groups of elliptic curves (ascending cyclotomic towers over $\mathbf{Q}$).

1. Anchor Problem

Fix E an elliptic curve over $\mathbf{Q}$. So, modular. Let K be a number field. We wish to study the "basic arithmetic" of E over K. That is, we want to understand the structure of these objects:

- The *Mordell-Weil group* $E(K)$ of K-rational points on E.
- The *Shafarevich-Tate group* $Ш(K,E)$. Via multiplication by n on the elliptic curve, we have an exact sequence
$$0 \to E(\overline{K})[n] \to E(\overline{K}) \xrightarrow{n} E(\overline{K}) \to 0$$
which after taking Galois invariants we obtain
$$0 \to E(K)/nE(K) \to H^1(G_K, E(\overline{K})[n]) \to H^1(G_K, E)[n] \to 0$$
and hence by global-to-local maps we may look at
$$Ш(K,E) = \ker(H^1(G_K,E) \to \textstyle\prod_v H^1(G_{K_v},E)).$$
The elements of this group are isomorphism classes of locally trivial E-*curves*, i.e. pairs (C,i) where C is a proper smooth curve defined over K and i is an $\overline{K}$-isomorphism between the Jacobian of C and E [S, §10.4] (called homogeneous spaces).

Now experience has led us to realize

1. *(that cohomological methods apply:)* We can use cohomological methods if we study both $E(K)$ and $Ш(K, E)$ at the same time. That is, for each positive integer n we have *the Classical Selmer group* $S(K, E; \mathbf{Z}/n\mathbf{Z})$ which fits into an exact sequence

$$0 \to E(K)/n \cdot E(K) \to S(K, E; \mathbf{Z}/n\mathbf{Z}) \to Ш(K, E)[n] \to 0,$$

and the Selmer group is directly expressible in terms of one-dimensional Galois cohomology over K. Euler systems can be used to investigate $E(K)$ and $Ш(K, E)$ suimultaneously, by bounding the size of the Selmer group. We will be defining a more general kind of Selmer group in a moment.

2. *(that varying the ground field sometimes helps:)* There is an advantage to studying Mordell-Weil groups, Shafarevich-Tate groups, and Selmer groups for a large class $\mathcal{L}$ of number fields which are abelian Galois extensions of a "base" number field K (" all at once") rather than for just a single number field K. Here are some standard choices of $\mathcal{L}$:

• (*p-cyclotomic extensions of the rational number field.*) When $K = \mathbf{Q}$ we may take $\mathcal{L}$ to be the class of all abelian extensions of $\mathbf{Q}$; or we may fix a prime number p and take the class of *all* p-abelian extensions of $\mathbf{Q}$, restricting to the p-primary components of the Selmer groups; or (as in classical Iwasawa theory) we might take $\mathcal{L}$ to be the class of all p-abelian extensions of $\mathbf{Q}$ unramified outside p. Much work has been done in studying the asymptotics of Mordell-Weil groups, Shafarevich-Tate groups, and Selmer groups ascending this tower . [See **Appendix** below for the case $\ell \neq p$].

• (*anti-cyclotomic extensions of the quadratic imaginary fields.*) When K is a quadratic imaginary field and take $\mathcal{L}$ to be the class of (all, or just those with ramification restricted to the primes dividing p) abelian extensions of K which are Galois extensions of $\mathbf{Q}$ and such that the conjugation action of the nontrivial element of $\mathrm{Gal}(K/\mathbf{Q})$ on their Galois group is via multiplication by -1.

3. *(the principle that you can't get something for nothing:)* There is a powerful method of bounding (from above) the "size" of the Selmer group attached to a given representation over K. This method requires *constructing* certain (*"Euler"*) systems of elements in the Selmer groups attached to the dual representation over each of the number fields in the given "large" class $\mathcal{L}$. The "Heegner point Euler system" in the anti-cyclotomic context, and the "Kato's Euler system" in the cyclotomic context.

Here is an amusing instance of this principle: given what has been proved to date, one knows that any smooth proper curve defined over $\mathbf{Q}$ of genus one and conductor 37 has a rational point over $\mathbf{Q}$. Here we can allow our curve to be given to us as a curve in any dimensional projective space, and as cut out by any number of equations; or perhaps, it may be given abstractly. We then can ask: does the proof that it *has* a $\mathbf{Q}$-rational point actually find one such point on the curve for us? The answer is yes, but only if we have either explicitly or implicitly previously found some nontrivial point on its jacobian (if its jacobian is the elliptic curve over $\mathbf{Q}$ with positive Mordell-Weil rank).

4. *(that L-functions "control" Euler systems which "control" Selmer groups:)* Here is where the real power lies. Cohomological methods are pretty good at ferreting out information modulo a single number n, or equivalently modulo powers of prime numbers p but only for finitely many prime numbers p "at a time". But a *single* special value of an L-function can, at times, by its connection to an Euler System, bound from above the size of the relevant p-Selmer groups for *all* (or at least for all but a finite number of) prime numbers p.

The following flow-chart summarizes the construction that follows:

$$\begin{tikzcd}
 & \boxed{\text{Arithmetic geometry}} \arrow[d] & \\
 & \boxed{\text{Euler systems}} \arrow[dl] \arrow[dr, "\text{descent}"] & \\
\boxed{L\text{-functions}} \arrow[dr] & & \boxed{\text{Kolyvagin systems}} \arrow[dl] \\
 & \boxed{\text{Selmer group}} &
\end{tikzcd}$$

We begin with some amount of data arising from algebraic geometry, for example, cyclotomic units, Heegner points, or Kato-Beilinson elements arising from K-theory. From these, we construct the Euler system, compatible collections of cohomology classes. From the Euler system we obtain information about L-functions and Kolyvagin systems which give us bounds on the Selmer group.

2. Selmer groups. How playing off local duality against global duality gives a mechanism for bounding Selmer groups.

If K is a field, $\bar{K}/K$ denotes a choice of separable algebraic closure and $G_K :=$ Gal$(\bar{K}/K)$ its Galois group. Let T be a finite abelian group with continuous G_K action, and $H^*(K,T) := H^*(G_K,T)$ cohomology computed with continuous cochains. Let $T^* := \mathrm{Hom}(T, \mathrm{G}_m) = \mathrm{Hom}(T, \mu)$ be the Cartier dual of T, and

$$T \times T^* \to \mu$$

the duality pairing. This pairing induces a bilinear pairing (via cup-product)

$$H^1(K,T) \times H^1(K,T^*) \to H^2(K,\mu)$$

which looks quite different when we take K to be a global field, or a local field. The mechanism we are about to describe will play one against the other (the global against the local).

Suppose, then, that K is a number field, and K_v is some completion of K (non-archimedean or archimedean). We have the global-to-local restriction mappings

$$H^1(K,T) \longrightarrow \prod_v H^1(K_v,T),$$

(denoting by $\prod_v h_v$ the image of the global cohomology class h) and

$$H^1(K,T^*) \longrightarrow \prod_v H^1(K_v,T^*).$$

Let us consider how duality enters the story, beginning with the local situation. Let v be a place of K. We have that the cup pairing

$$H^1(K_v,T) \times H^1(K_v,T^*) \to H^2(K_v,\mu) \subset \mathbf{Q}/\mathbf{Z}$$

is a perfect pairing. Hence the cohomology class h_v may be identified with the functional "cupping with h_v", $h_v : H^1(K_v,T^*) \to H^2(K,\mu)$.

In contrast, Global Class Field Theory tells us that if we compose the global (cup-product) pairing

$$H^1(K,T) \times H^1(K,T^*) \to H^2(K,\mu)$$

with the homomorphism $H^2(K,\mu) \to \mathbf{Q}/\mathbf{Z}$ which is given by summing local invariants, we get a beautiful bilinear pairing

$$H^1(K,T) \times H^1(K,T^*) \to \mathbf{Q}/\mathbf{Z}$$

which has the virtue of vanishing identically.

How can we make this disparity work for us?

We wish to impose *local conditions* on the restrictions of global cohomology classes to K_v for places v. To prepare for this let us simply call a **local condition** $\mathcal{F}$ **at** v (for T) any choice of subgroup, which we denote

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

By the **singular cohomology** for such a local condition $\mathcal{F}$, which we will just denote $H^1_{\mathcal{S}}(K_v,T)$, we mean the quotient group

$$H^1_{\mathcal{S}}(K_v,T) := H^1(K_v,T)/H^1_{\mathcal{F}}(K_v,T).$$

We get then an exact sequence,

$$0 \longrightarrow H^1_{\mathcal{F}}(K_v,T) \longrightarrow H^1(K_v,T) \longrightarrow H^1_{\mathcal{S}}(K_v,T) \longrightarrow 0. \tag{1}$$

Given such a local condition at v, Tate Duality allows us to stipulate a "dual" local condition at v (for T^*), namely, $H^1_{\mathcal{F}^*}(K_v,T^*) \subset H^1(K_v,T^*)$ is defined to be the annihilator subgroup of $H^1_{\mathcal{F}}(K_v,T)$ under the Tate pairing, and the dualization of the above exact sequence yields

$$0 \longrightarrow H^1_{\mathcal{F}^*}(K_v,T^*) \longrightarrow H^1(K_v,T^*) \longrightarrow H^1_{\mathcal{S}*}(K_v,T^*) \longrightarrow 0. \tag{2}$$

The natural choice. If K_v is nonarchimedean let $\mathcal{O}_v$ be the ring of integers in K_v, $\mathbf{F}_v$ its residue field, and $K_v^{unr} \subset \bar{K}_v$ the maximal unramified subfield of $\bar{K}_v$. Let $\mathcal{I}_v$ denote the inertia group $\mathrm{Gal}(\bar{K}_v/K_v^{unr})$, and $G_{\mathbf{F}_v} := \mathrm{Gal}(K_v^{unr}/K_v)$. These groups fit into the exact sequence

$$\{1\} \longrightarrow \mathcal{I}_v \longrightarrow G_{K_v} \longrightarrow G_{\mathbf{F}_v} \longrightarrow \{1\}. \tag{3}$$

Note that if $\bar{\mathbf{F}}_v$ is an algebraic closure of $\mathbf{F}_v$, then $G_{\mathbf{F}_v} \cong \mathrm{Gal}(\bar{\mathbf{F}}_v/\mathbf{F}_v) \cong \hat{\mathbf{Z}}$ (the latter isomorphism sending the Frobenius automorphism in $\mathrm{Gal}(\bar{\mathbf{F}}_v/\mathbf{F}_v)$, $x \mapsto x^{|\mathbf{F}_v|}$, to $1 \in \hat{\mathbf{Z}}$).

The vanishing of $H^2(G_{\mathbf{F}_v}, T^{\mathcal{I}_v})$ yields the canonical exact sequence

$$0 \longrightarrow H^1(G_{\mathbf{F}_v}, T^{\mathcal{I}_v}) \longrightarrow H^1(K_v, T) \longrightarrow H^1(\mathcal{I}_v, T)^{G_{\mathbf{F}_v}} \longrightarrow 0. \tag{4}$$

Now the above exact sequence presents a "natural" choice of local condition for any nonarchimedean v; namely we *could* take $H^1_{\mathcal{F}}(K_v, T)$ to be equal to $H^1(\mathbf{F}_v, T^{I_v}) \subset H^1(K_v, T)$. In this case, $H^1_{\mathcal{S}}(K_v, T) = H^1(\mathcal{I}_v, T)^{G_{\mathbf{F}_v}}$ and If T is unramified for at v the"natural choices" for T and for T^* are dual under Poitou-Tate duality. In particular, we may identify elements of $H^1_{\mathcal{S}}(K_v, T)$ with linear functionals on $H^1_{\mathcal{F}^*}(K_v, T^*)$.

Let us return to the global situation and say that a **Selmer structure** $\mathcal{F}$ on a (finite) G_K-module T is a local condition $\mathcal{F}_v$ at all v which is the "natural choice" for almost all v. The dual of Selmer structure for T is a Selmer structure for T^*. Note that if we are given a Selmer structure for T the global-to-local mapping $H^1(K, T) \to H^1_{\mathcal{S}_v}(K_v, T)$ vanishes for almost all v, and therefore we have a well-defined global-to-local homomorphism

$$H^1(K, T) \to \bigoplus_v H^1_{\mathcal{S}}(K_v, T).$$

By the **Selmer group** $\mathrm{Sel}_{\mathcal{F}}(K, T)$ associated to $(T, \mathcal{F})$ let us mean the kernel of the above homomorphism. So we have an exact sequence:

$$0 \longrightarrow \mathrm{Sel}_{\mathcal{F}}(K, T) \longrightarrow H^1(K, T) \longrightarrow \bigoplus_v H^1_{\mathcal{S}}(K_v, T). \tag{5}$$

Dually,

$$0 \longrightarrow \mathrm{Sel}_{\mathcal{F}^*}(K, T^*) \longrightarrow H^1(K, T^*) \longrightarrow \bigoplus_v H^1_{\mathcal{S}^*}(K_v, T^*). \tag{6}$$

We can now say what the basic mechanism is which allows global cohomology to bound Selmer groups: given any global cohomology class $h \in H^1(K, T)$ consider its image,

$$\bigoplus_v h_{\mathcal{S}_v} \in \bigoplus_v H^1_{\mathcal{S}_v}(K_v, T),$$

and note that since the global duality mapping as displayed above is zero, we get a "semi-local" relation satisfied by any class $\sigma \in \mathrm{Sel}_{\mathcal{F}}(K, T)$. namely,

$$\sum_v h_{\mathcal{S}_v}(\sigma_v) = 0.$$

Given enough of these relations, we can completely describe $\mathrm{Sel}_{\mathcal{F}}(K, T)$ in *good cases.*

3. Passing from Selmer structure to Selmer structure; Global Duality

The Global Duality Theorem allows us to understand quite precisely how changes in the "stringency" of a Selmer structure effects change in cohomology. ("Adjusting" Selmer structures is one of the *arts* in Kolyvagin's theory.) Suppose, then, that T is a finite G_K-module endowed with *two* Selmer structures $\mathcal{F}_1$, and $\mathcal{F}_2$. Suppose further that $\mathcal{F}_1 \leq \mathcal{F}_2$ in the evident sense that the local conditions for $\mathcal{F}_1$ are more "stringent" than those for $\mathcal{F}_2$.

We have exact sequences

$$0 \longrightarrow H^1_{\mathcal{F}_1}(\mathbf{Q},T) \longrightarrow H^1_{\mathcal{F}_2}(\mathbf{Q},T) \longrightarrow \oplus_\ell H^1_{\mathcal{F}_2}(\mathbf{Q}_\ell,T)/H^1_{\mathcal{F}_1}(\mathbf{Q}_\ell,T),$$

$$0 \longrightarrow H^1_{\mathcal{F}_2^*}(\mathbf{Q},T^*) \longrightarrow H^1_{\mathcal{F}_1^*}(\mathbf{Q},T^*) \longrightarrow \oplus_\ell H^1_{\mathcal{F}_1^*}(\mathbf{Q}_\ell,T^*)/H^1_{\mathcal{F}_2^*}(\mathbf{Q}_\ell,T^*)$$

where the sums are over primes ℓ such that $H^1_{\mathcal{F}_2}(\mathbf{Q}_\ell,T) \neq H^1_{\mathcal{F}_1}(\mathbf{Q}_\ell,T)$, and (reading from left to right) the last mappings of each sequence are the natural localization maps and their images are orthogonal complements of each other with respect to the sum of the local Tate pairings. This latter statement is (Poitou-Tate) global duality; see for example [T] Theorem 3.1 or [Mi] Theorem I.4.10 (see also [R 1] Theorem 1.7.3).

4. Euler Systems

We recall here the notion of Euler systems [R 1] (with some minor modifications). See also the forthcoming article[M-R]. Let R be a complete noetherian local ring with finite residue field of characteristic p. Let K be a number field, $\bar{K}/K$ an algebraic closure, and K' be an "intermediate field"; i.e., a field K' such that $K \subset K' \subset \bar{K}$, so $G_{K'} \subset G_K$ is the subgroup which fixes the elements of K'; if K'/K is Galois, let $G(K'/K) \cong G_K/G_{K'}$ be its Galois group. If M is a compact R-module equipped with continuous G_K-action let $H(K',M) := H^1_{\mathcal{F}'}(G_{K'},M)$, i.e., $H(K',M)$ is the R-module of one-dimensional Galois cohomology of M over K', computed with continuous cochains, and with some chosen Selmer structure $\mathcal{F}$. From now on our Selmer structure will be the natural one outside p and no condition for primes dividing p. If K'/K is Galois, then $H(K',M)$ is naturally an $R[[G(K'/K)]]$-module. Note that besides the covariant functoriality of $H(K',M)$ in the pair (K',M) we have a contravariant functoriality given by the corestriction, or norm, mappings $\nu_{K''/K'} : H(K'',M) \to H(K',M)$ for finite (intermediate) field extensions K''/K'. More generally, we might think of allowing $H(K',M)$ in the discussion below to stand for any "decent" functor from pairs (K',M) to the category of R-modules which admits "norms" (i.e., corestrictions).

Let T be a *free* R-module of finite rank equipped with a continuous R-linear G_K-action and which is unramified outside a finite set of primes of K. Let $T^* := Hom_{cont}(T,\mathbf{Z}_p(1))$ denote the dual G_K-module. For each prime q of K fix $\phi_q^{-1} \in G_K$, a choice of Frobenius-inverse element at q. If q is a prime of K unramified in the action of G_K on T^*, form:

$$P_q(X) := det(1 - X\phi_q^{-1}|T^*) \in R[X],$$

the characteristic polynomial of ϕ_q^{-1} acting on the dual module, T^* defined above. This is well-defined since q is unramified in the action of G_K on T^*.

Fix $\mathcal{N}$, a set of primes containing all ramified primes of T and the primes of K lying above p.

If K''/K' is an intermediate Galois extension, let $\Sigma(K''/K';\mathcal{N})$ denote the (finite) set of primes of K not in $\mathcal{N}$ which are unramified in the extension K'/K and ramified in the extension K''/K. Define:

$$P(K''/K';\mathcal{N}) := \prod_{q\in\Sigma(K''/K';\mathcal{N})} P_q(\phi_q^{-1}) \in R[G_K],$$

noting that this element in the group ring depends upon the choices of Frobenius elements, and on a choice of ordering of the factors in this product. However, since the action of $R[G_K]$ on $H(K',T)$ factors through the quotient ring $R[[G(K'/K)]]$, and the primes q contributing to the above product are all unramified in K'/K, we see that the natural action of $P(K''/K';\mathcal{N})$ on $H(K',T)$ provides us with a unique R-endomorphism

$$P(K''/K';\mathcal{N}) : H(K',T) \to H(K',T)$$

independent of choice of Frobenius elements if K'/K is an abelian Galois extension. Now let L/K be any "intermediate" abelian Galois extension.

Definition 4.1. By the $\mathcal{N}$-**Euler (projective) limit** of the system

$$\{H(K',T)\}_{K\subset K'\subset L}$$

is an $R[[G(L/K)]]$-module of systems of elements $\{c'_K \in H(K',T)\}_{K\subset K'\subset L}$, with the following compatibility relation for finite intermediate extensions $K' \subset K''$:

$$\nu_{K''/K'} \cdot c_{K''} = P(K''/K';\mathcal{N}) \cdot c'_K.$$

Provisional notation for this $R[[G(L/K)]]$-module could be

$$\text{E.S.}(L/K,T) := \text{EulerLim}_{K'\to L} H(K',T)$$

when the choice of $\mathcal{N}$ is understood. We will refer to this as the $R[[G(L/K)]]$-module of **Euler systems for** $(L/K,T;\mathcal{N})$ noting, however, that the term *Euler systems* is reserved in [R 1] (Defn. 2.1.1) for the more restricted situation where L contains all the ray class fields over K relative to primes not dividing $\mathcal{N}$ and it contains a $\mathbf{Z}_p$-extension in which no (finite) prime of K splits completely.

Comments. If L/K is unramified outside $\mathcal{N}$, then the "Euler limit" is just the standard inverse limit compiled via norms. In particular, this is the case if L/K is a $\mathbf{Z}_p$ extension. A nontrivial element in E.S.$(L/K,T)$ corresponds to a large number of cohomology classes all compatible in this Euler limit way, something of a *hyper*-universal norm! We will restrict attention, below, to p-abelian extensions L/K.

In our present case, let Γ denote the quotient of the compact p-abelian group $G(L/K)$ by its torsion subgroup. Let K_∞/K be the fixed subextension of L/K under the torsion subgroup of $G(L/K)$. Then we have a natural surjection $G(L/K) \to G(K_\infty/K)$. Putting $\Gamma := G(K_\infty/K)$ we have $G(K_\infty/K) \cong \mathbf{Z}_\nu^d$ for some non-negative integer ν (which we can call the $\mathbf{Z}_p$-rank of L/K). Put $\Lambda := R[[\Gamma]]$.

Let us denote:

$$H_\infty(K',T) := \text{proj.lim.}_{K'\to K_\infty} H(K',T).$$

We have the natural homomorphism of Λ-modules,

$$\text{E.S.}(L/K,T) \otimes_{R[[G(L/K)]]} \Lambda \xrightarrow{\gamma} \text{E.S.}(K_\infty/K,T) = H_\infty(K',T).$$

Example. Let R, T be as above with $K = \mathbf{Q}$ and take L/K to be the maximal p-abelian extension of $\mathbf{Q}$. Let $\mathcal{N}$ denote the set containing the ramified primes for

T and the prime number p. Let $\mathbf{Q}(\infty)/\mathbf{Q}$ be the (cyclotomic) $\mathbf{Z}_p$-extension and $\mathbf{Q}(n) \subset \mathbf{Q}(\infty)$ the subfield of degree p^n over $\mathbf{Q}$. It follows from the "weak Leopoldt Conjecture" that

$$\mathrm{rank}_\Lambda H_\infty(\mathbf{Q}, T) = d^-,$$

where d^- is the dimension of the minus eigenspace of the complex conjugation involution acting on T. Also very reasonable hypotheses guarantee that $H_\infty(\mathbf{Q}, T)$ has no Λ-torsion.

Thus we are led to the following questions:

- Is the kernel $\ker \gamma$ a Λ-torsion module?
- What is the Λ-rank (the vector space dimension after tensoring with the field of fractions $\mathbf{Z_p}((\mathrm{Gal}(\mathbf{L}/\mathbf{K}))))$ of $S_F(\mathbf{Q}_\infty/\mathbf{Q}, \mathbf{T})$? Is it equal to the minus eigenspace of the complex conjugation acting on T? (This conjecture is tied to the weak Leopoldt conjecture.)
- Is it true that cokernel $\mathrm{coker}\gamma$ and the dual Selmer group $S_{F^*}(\mathbf{Q}_\infty/\mathbf{Q}, \mathbf{T}^*)$ are both Λ-torsion and their semisimplifications as Λ-modules isomorphic up to finite modules?
- What are the connections with p-adic L-functions? Is there a possible modification of the p-adic L-function at p such that quotient of Λ by that L-function has a similar statement with kernels and cokernels?

For discussion of this, see [M-R], currently in preparation. Kato has given several examples where the second statement is true, and we know at least that the Selmer of the dual is bounded by the cokernel of γ, due to the role of the p-adic L-function (which bounds both). Even more recent results begin to produce a similar theory using Heegner points over quadratic imaginary fields where instead of cyclotomic tower one uses an anticyclotomic tower.

5. General Bounds.

Here are two "hypotheses" and it would be very good to establish them quite generally.

Hypothesis A. The kernel of

$$\mathrm{E.S.}(L/\mathbf{Q}, T) \otimes_{R[[G(L/K)]]} \Lambda \to H_\infty(\mathbf{Q}, T)$$

is a Λ-torsion module.

Hypothesis B. If $d^- = 1$ the characteristic ideal of the cokernel of

$$\mathrm{E.S.}(L/\mathbf{Q}, T) \otimes_{R[[G(L/K)]]} \Lambda \to H_\infty(\mathbf{Q}, T)$$

is equal to the characteristic ideal of the Selmer group of the (Cartier) dual Galois representation T^* with dual Selmer structure $\mathcal{K}'^*$.

As for **B.** one has that under very general hypotheses the characteristic ideal of the Selmer group of the (Cartier) dual Galois representation T^* with dual Selmer structure $\mathcal{K}'^*$ *divides* the characteristic ideal of the cokernel of

$$\mathrm{E.S.}(L/\mathbf{Q}, T) \otimes_{R[[G(L/K)]]} \Lambda \to H_\infty(\mathbf{Q}, T).$$

But we can establish the full strength of **B** at present only in very few instances. (For example, when $T = \mathbf{Z}_p(1) \otimes \chi$ where χ an even nontrivial character of finite order. **Query:** Can one show hypothesis **A** in this case?)

6. Bounds governed by L-functions

The example for which we have the most complete information, and which might serve as a template for what we might try to get in other cases is given by taking $K = \mathbf{Q}$ and $T = \mathbf{Z}_p(1) \otimes \chi$ where χ an even nontrivial character of finite order. Modify the Selmer structure on T by putting the *natural* local condition at p; and form

$$H_{\infty,\mathcal{S}}(\mathbf{Q}_p, T) := \text{proj.Lim}_{n\to\infty} H_{\mathcal{S}}(\mathbf{Q}_p(n), T).$$

Either of the two standard proofs of the classical *main conjecture* establishes the fact that the Λ module $\text{E.S.}(L/\mathbf{Q}, T) \otimes_{R[[G(L/K)]]} \Lambda$ is generated by the *cyclotomic Euler system* and the characteristic ideal of the cokernel

$$\text{E.S.}(L/\mathbf{Q}, T) \otimes_{R[[G(L/K)]]} \Lambda \longrightarrow H_{\infty,\mathcal{S}}(\mathbf{Q}, T),$$

is generated by the Leopoldt-Kubota L-function $L_p(\chi, s)$ viewed as element of Λ, which is the characteristic ideal of the Iwasawa module constructed from of p-primary components of ideal class groups of layers of the p-cyclotomic tower.

In the case of elliptic curves E defined over $\mathbf{Q}$, working with the Heegner Euler System over an anti-cyclotomic tower over a quadratic imaginary field, or using Kato's Euler System over the cyclotomic tower over $\mathbf{Q}$ one presently has *divisibility results* (i.e., the characteristic ideal of the appropriate Selmer group *divides* the ideal generated by corresponding p-adic L function (cf. Chapter 3 of [R 1]), and this alone is enough to establish striking information about Mordell-Weil and Ш, as the later lectures will explain, but in both cases we still await a general "main conjecture."

Appendix. The ℓ-asymptotics of Ш as one ascends a p-cyclotomic tower. The p-adic "main conjecture" for elliptic curves packages much that one might want to understand about p-asymptotics of Ш as one ascends a p-cyclotomic tower, but I have never heard, or read, any mention of the perfectly natural companion question alluded to in the title of this section, when $\ell \neq p$. The natural guess here, is to follow the lead of Larry Washington's 1978 Inventiones article where he proves that if $\ell \neq p$, k is any abelian number field, k_n/k the n-th layer of the p-cyclotomic $\mathbf{Z_p}$-extension of k, $(n = 1, 2, \dots)$, and ℓ^{e_n} the exact power of ℓ dividing the class number of k_n. then e_n is constant for n sufficiently large. If we allow ourselves to be influenced by that, and by the "standard analogy" between ideal class groups and Ш, a first guess might be that if $\ell \neq p$, and E is an elliptic curve over k such that the G_k-representation on $E[\ell]$ is absolutely irreducible, then the order of the ℓ-primary component of $Ш(E/k_n)$ is constant for n sufficiently large. It would be even more interesting if there were counter-examples to this first guess. Using modular symbols, how hard would it be to get data on this? I also wonder whether people have considered the analogous questions for arithmetic K-groups.

References

[K] V. A. Kolyvagin, *Euler Systems*, Prog. Math. **87**, Birkhäuser, Boston (1990), 435–483.

[M-R] B. Mazur, K.Rubin: Kolyvagin Systems *(article in preparation)*.

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

[R 1] Karl Rubin, *Euler systems*, Annals of mathematics studies, vol. 147, Princeton: Princeton University Press, 2000.

[R 2] Karl Rubin: Euler systems and modular elliptic curves, pp. 351-367 in *Galois Representations in Arithmetic Algebraic Geometry*, eds: A.J. Scholl & R.L. Taylor, London Mathematical Society, Lecture Note Series 254, Cambridge : Cambridge University Press, 1998.

[S] J.H. Silverman, *The arithmetic of elliptic curves*, Graduate texts in mathematics, vol. 106, Berlin: Springer, 1994.

[T] Tate, J.: Duality theorems in Galois cohomology over number fields, in: *Proc. Intern. Cong. Math.*, Stockholm (1962) 234–241.