Euler systems (Iwasawa 2017 notes)

David Loeffler

Lecture 1. Galois representations

References for this lecture: for §1 and §2, Bellaiche's CMI notes on the Bloch–Kato conjecture; for §3, Diamond–Shurman, Darmon–Diamond–Taylor.

1. Galois representations

1.1. Definitions. Let K be a number field, $\overline{K}$ its algebraic closure, $G_K = \mathrm{Gal}(\overline{K}/K)$; and let p be a prime. We're interested in representations of G_K on finite-dimensional $\mathbf{Q}_p$-vector spaces V.

We always assume that

(1) $\rho : G_K \to \mathrm{Aut}(V) \cong \mathrm{GL}_d(\mathbf{Q}_p)$ is continuous (where $d = \dim(V)$), with respect to profinite topology of G_K and the p-adic topology on $\mathrm{GL}_d(\mathbf{Q}_p)$.
(2) V is "unramified almost everywhere": for all but finitely many prime ideals v of K, we have $\rho(I_v) = \{1\}$, where I_v is an[1] inertia group at v.

1.2. Examples.

The representation $\mathbf{Z}_p(1)$. Let $\mu_{p^n} = \{x \in \overline{K}^\times : x^{p^n} = 1\}$. Then μ_{p^n} is finite cyclic of order p^n and G_K acts on it.

P-power map sends $\mu_{p^{n+1}} \to \mu_{p^n}$ and we define

$$\mathbf{Z}_p(1) \coloneqq \varprojlim_n \mu_{p^n}, \quad \mathbf{Q}_p(1) \coloneqq \mathbf{Z}_p(1) \otimes \mathbf{Q}_p.$$

This is a 1-dimensional continuous representation, unramified outside the primes dividing p; G_K acts by "cyclotomic character" $\chi_{\mathrm{cyc}} : G_K \to \mathbf{Z}_p^\times$.

(Notation: for any V, $n \in \mathbf{Z}$, we set $V(n) = V \otimes \mathbf{Q}_p(1)^{\otimes n}$.)

Tate modules of elliptic curves. E/K elliptic curve $\Rightarrow E(\overline{K})$ abelian group with G_K-action. Let $E(\overline{K})[p^n]$ subgroup of p^n-torsion points.

Define

$$T_p(E) \coloneqq \varprojlim_n E(\overline{K})[p^n] \text{ (w.r.t. multiplication-by-}p\text{ maps)}, \qquad V_p(E) \coloneqq T_p(E) \otimes \mathbf{Q}_p.$$

2-dimensional cts rep, unramified outside $\{v : v \mid p\} \cup \{v : E \text{ has bad reduction at } v\}$.

[1] I_v depends on a choice of prime of $\overline{K}$ above v, but only up to conjugation in G_K, so whether or not V is unramified at v is well-defined.

Etale cohomology. Let X/K be a smooth algebraic variety. We can define vector spaces

$$H^i_{\text{ét}}(X_{\overline{K}}, \mathbf{Q}_p) \quad \text{for } 0 \le i \le 2\dim X,$$

which are finite-dimensional p-adic Galois representations, unramified outside p and primes of bad reduction[2] of X.

1.3. Representations coming from geometry.

My second example is a special case of the third: for an elliptic curve, it turns out that we have $V_p(E) \cong H^1_{\text{ét}}(E_{\overline{K}}, \mathbf{Q}_p)(1)$.

Definition. *We say a Galois rep V* comes from geometry *if it is a subquotient of $H^i_{\text{ét}}(X_{\overline{K}}, \mathbf{Q}_p)(j)$ for some variety X/K and some integers i, j.*

So all my examples come from geometry. In these lectures we're only ever going to be interested in representations coming from geometry.

Remark. Conjecturally the representations coming from geometry should be exactly those which are continuous, unramified almost everywhere, and *potentially semistable* at the primes above p (a technical condition from p-adic Hodge theory). This is called the Fontaine–Mazur conjecture.

2. L-functions

2.1. Local Euler factors.

Let V as above, v unramified prime. Then $\rho(\mathrm{Frob}_v)$ well-defined up to conjugacy, where Frob_v arithmetic Frobenius.

Definition. *Local Euler factor of V at v*

$$P_v(V, t) := \det(1 - t\rho(\mathrm{Frob}_v^{-1})) \in \mathbf{Q}_p[t]$$

Examples:

V	$P_v(V,t)$
$\mathbf{Q}_p$	$1-t$
$\mathbf{Q}_p(n)$	$1 - \frac{t}{q_v^n}, \quad q_v = \mathrm{Norm}(v)$
$H^1(E_{\overline{K}}, \mathbf{Q}_p)$	$1 - a_v(E)t + q_v t^2$

2.2. Global L-functions (sketch).

Assume V comes from geometry, and V is semisimple (direct sum of irreducibles). Then $P_v(V,t)$ has coefficients in $\overline{\mathbf{Q}}$ (Deligne); and there is a way of defining $P_v(V,t)$ for bad primes v (case $v \mid p$ is hardest).

Fix an embedding $\iota : \overline{\mathbf{Q}} \hookrightarrow \mathbf{C}$. Then we consider the product

$$L(V, s) := \prod_{v \text{ prime}} P_v(V, q_v^{-s})^{-1}.$$

Miraculously, this converges for $\Re(s) \gg 0$.

E.g. for $K = \mathbf{Q}$, $V = \mathbf{Q}_p(n)$ this is $\zeta(s+n)$; for $V = H^1(E_{\overline{K}}, \mathbf{Q}_p)$ it is $L(E/K, s)$ (Hasse–Weil L-function of E).

Conjecture. *For V coming from geometry, $L(V,s)$ has meromorphic continuation to $s \in \mathbf{C}$ with finitely many poles, and satisfies a functional equation relating $L(V,s)$ and $L(V^*, 1-s)$.*

Note that if V is geometric and semisimple, so is its dual V^*. This conjecture is of course super-super-hard – the only cases where it is known is where we can relate V to something *automorphic*, e.g. a modular form.

[2] This is a little delicate to define properly if we don't assume X to be proper over K. Formally, we say X has "good reduction" at v if it's isomorphic to the complement of a relative normal crossing divisor in a smooth proper $O_{K,v}$-scheme.

3. Modular forms

We're particularly interested in the Galois representations coming from modular forms, which come from geometry via modular curves. For simplicity, in these lectures we'll only treat weight 2 modular forms.

3.1. Modular curves. For $N \ge 1$ let

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) : c = 0, a = d = 1 \bmod N \right\}.$$

This acts on the upper half-plane $\mathcal{H}$ via $\tau \mapsto \frac{a\tau+b}{c\tau+d}$. It turns out that the quotient is naturally an algebraic variety:

THEOREM. *For $N \ge 4$ there is an algebraic variety $Y_1(N)$ over $\mathbf{Q}$ with the following properties:*

- *$Y_1(N)$ is a smooth geometrically connected affine curve.*
- *For any field extension[3] $F/\mathbf{Q}$, the F-points of $Y_1(N)$ biject with isomorphism classes of pairs (E, P), where E/F is an elliptic curve and P is a point of order N on E.*
- *$Y_1(N)(\mathbf{C}) \cong \Gamma_1(N)\backslash\mathcal{H}$, via the map sending $\tau \in \mathcal{H}$ to (E_τ, P_τ) where $E_\tau = \mathbf{C}/(\mathbf{Z} + \mathbf{Z}\tau)$ and $P_\tau = 1/N \bmod \mathbf{Z} + \mathbf{Z}\tau$.*

(Much stronger theorems are known – for instance, $Y_1(N)$ has a canonical model over $\mathbf{Z}$ with good reduction away from the primes dividing N – but we won't need this just now.)

We'll also use the modular curve of level $\Gamma(N)$, the kernel of $\mathrm{SL}_2(\mathbf{Z}) \to \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$. The quotient $\Gamma(N)\backslash\mathcal{H}$ is also canonically the $\mathbf{C}$-points of a curve over $\mathbf{Q}$, which we'll denote by $Y(N)$. There's a natural map $Y(N) \to Y_1(N)$ defined over $\mathbf{Q}$.

Because $\Gamma(N)$ is normal in $\mathrm{SL}_2(\mathbf{Z})$, the quotient $\mathrm{SL}_2(\mathbf{Z})/\Gamma(N) \cong \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$ acts on the $\mathbf{C}$-points of $Y(N)$. This action **does not** descend to $\mathbf{Q}$; however, we have the following rather elegant picture:

THEOREM (Shimura). *The base-extension $Y(N)_{\mathbf{Q}(\mu_m)}$ has a left action of $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ such that*

- *the action of the subgroup $\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$ is the expected one on $\mathbf{C}$-points,*
- *the action of $\mathrm{Gal}(\mathbf{Q}(\mu_m)/\mathbf{Q}) \cong (\mathbf{Z}/N\mathbf{Z})^\times$ is given by matrices of the form $\begin{pmatrix} u & 0 \\ 0 & 1 \end{pmatrix}$.*

This is a little confusing, so let me make it slightly more concrete. We can write $Y(N) = \mathrm{Spec}(R)$ for some $\mathbf{Q}$-algebra R. Shimura's theorem tells us that there is a (right) action of $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ on $R \otimes \mathbf{Q}(\mu_N)$ for which R is the invariants under $\begin{pmatrix} * & 0 \\ 0 & 1 \end{pmatrix}$. However, we don't get an action of $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ on $Y(N)(\mathbf{C})$, because not all GL_2 elements act by $\mathbf{Q}(\mu_N)$-algebra automorphisms; only elements of SL_2 do, so it is only $\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$ which acts on the set of $\mathbf{C}$-points of $Y(N)$ (and the action is the one we expect).

REMARK. There lots of choices of conventions for $\mathbf{Q}$-models for $Y_1(N)$ and $Y(N)$ in the literature. Everyone agrees what $Y_1(N)$ means over $\mathbf{C}$, but there are two different ways to descend it to $\mathbf{Q}$. Our conventions agree with Diamond–Shurman, for instance.

For $Y(N)$ the situation is even worse, since many authors (including Kato, and some papers of my own) use the notation $Y(N)$ for a non-connected curve over $\mathbf{Q}$ whose $\mathbf{C}$-points are the disjoint union of $\varphi(N)$ copies of $\Gamma(N)\backslash\mathcal{H}$; this is more natural from an adèlic viewpoint.

3.2. Modular Galois representations. Let $f = \sum a_n q^n$ be a cuspidal modular eigenform, of weight 2, new of level N, normalised so that $a_1 = 1$.

Then there is a number field L such that all $a_n \in L$. I'm going to suppose[4] that L embeds into $\mathbf{Q}_p$, and pick such an embedding.

[3] Any $\mathbf{Q}$-algebra, in fact; this is important if you want to make precise the idea that $Y_1(N)$ represents a functor.

[4] This is only because I didn't set up the theory of p-adic Galois representations with coefficients in a finite extension of $\mathbf{Q}_p$. The general case is no harder, it's just a little more notation to keep track of.

Definition. *We let* $V_p(f)$ *be the largest subspace of* $H^1_{\text{ét}}(Y_1(N)_{\overline{\mathbf{Q}}}, \mathbf{Q}_p)$ *on which the Hecke operators* $T(\ell)$*, for* $\ell \nmid N$*, act as multiplication by* $a_\ell(f)$*.*

By construction, $V_p(f)$ is a Galois representation coming from geometry. However, one can also show that

- $V_p(f)$ is 2-dimensional and irreducible.
- $V_p(f)$ is a direct summand of $H^1_{\text{ét}}$ (not just a subspace).
- For $\ell \nmid pN$, $V_p(f)$ is unramified at ℓ and the trace of Frob_ℓ^{-1} on $V_p(f)$ is $a_\ell(f)$. More precisely, the local Euler factor $P_\ell(V_p(f), t)$ is $1 - a_\ell(f)t + \ell\chi(\ell)t^2$, where χ is the character of f. Thus the global L-series $L(V_p(f), s)$ is just the L-series of f,
$$L(f, s) = \sum a_n(f) n^{-s}.$$
In particular if $L = \mathbf{Q}$, so that f corresponds to an elliptic curve E, then $V_p(f) \cong H^1_{\text{ét}}\left(E_{\overline{\mathbf{Q}}}, \mathbf{Q}_p\right)$.
- $V_p(f)^* = V_p(f \otimes \chi^{-1})(1)$.

(Warning: in Diamond–Shurman chapter 9, the representation they denote by $\rho_{f,p}$ is the *dual* of our $V_p(f)$, which is cancelled out by the fact that they use Frob_p rather than Frob_p^{-1} to define the Euler factor.)

3.3. Products of modular forms. If you take two newforms f, g, and concentrate on the Galois representation $V = V_p(f) \otimes V_p(g)$, then using the Kunneth formula for étale cohomology you can show that V is a direct summand of $H^2_{\text{ét}}\left((Y \times Y)_{\overline{\mathbf{Q}}}, \mathbf{Q}_p\right)$ for $Y = Y_1(N)$ (any N divisible by N_f and N_g). The same works, of course, for three (or more) modular forms.

Lecture 2. Galois cohomology and Selmer groups

References for this lecture: Bellaiche's notes are fantastic for §4. For §5, the best source is probably chapter 3 of Rubin's orange book "Euler Systems".

4. Galois cohomology

4.1. Setup. There is a cohomology theory for Galois representations[5]: for V a G_K-rep, we get $\mathbf{Q}_p$-vector spaces $H^i(K,V)$, zero unless $i = 0,1,2$. Mostly we care about H^0 and H^1, which are given as follows

$$\begin{aligned} H^0(K,V) &= V^{G_K} \\ H^1(K,V) &= \frac{\{\text{cts fcns } s : G_K \to V \text{ such that } s(gh) = s(g) + gs(h)\}}{\{\text{fcns of the form } s(g) = gv - v \text{ for some } v \in V\}}. \end{aligned}$$

These are well-behaved: short exact sequences of V's give long exact sequences of cohomology, for instance. Unfortunately they're *not* finite-dimensional in general.

4.2. The Kummer map. For $V = \mathbf{Q}_p(1)$ the Galois cohomology is related to the multiplicative group K^*. To see this, we have to first think a bit about cohomology with *finite* coefficients.

For any n, we have a short exact sequence

$$0 \longrightarrow \mu_{p^n} \longrightarrow \overline{K}^\times \xrightarrow{[p^n]} \overline{K}^\times \longrightarrow 0$$

which leads to a long exact sequence

$$0 \longrightarrow \mu_{p^n}^{G_K} \longrightarrow K^\times \xrightarrow{[p^n]} K^\times \longrightarrow H^1(K, \mu_{p^n})$$

and thus an injection[6]

$$K^\times \otimes \mathbf{Z}/p^n\mathbf{Z} \hookrightarrow H^1(K, \mu_{p^n}).$$

Passing to the inverse limit we get a map (**Kummer map**)

$$\kappa_p : K^\times \otimes \mathbf{Z}_p \hookrightarrow H^1(K, \mathbf{Z}_p(1)) \quad \text{or} \quad K^\times \otimes \mathbf{Q}_p \hookrightarrow H^1(K, \mathbf{Q}_p(1)).$$

Remark. This already shows that $H^1(K, \mathbf{Q}_p(1))$ can't be finite-dimensional, because $K^\times$ has countably infinite rank.

The same argument works for elliptic curves: we get an embedding

$$E(K) \otimes \mathbf{Q}_p \hookrightarrow H^1(K, V_p(E)).$$

4.3. Selmer groups. Useful to "cut down to size" by imposing extra conditions on our H^1 elements. Note that we have maps

$$H^i(K,V) \to H^i(K_v, V) \text{ for all primes } v$$

Definition. *A* local condition *on V at prime v is a submodule $\mathcal{F}_v \subseteq H^1(K_v, V)$.*

Examples:

- *strict local condition* $\mathcal{F}_{v,\mathrm{strict}} = \{0\}$
- *relaxed local condition* $\mathcal{F}_{v,\mathrm{relaxed}} =$ everything
- *unramified local condition*
$$\mathcal{F}_{v,\mathrm{ur}} = \text{image}\left(H^1(G_{K_v}/I_v, V^{I_v}) \to H^1(K_v, V)\right)$$
- *Bloch–Kato "finite" condition* $\mathcal{F}_{v,BK}$ – defined using p-adic Hodge theory, for $v \mid p$ and V coming from geometry

[5] Technical point: our representations are all continuous, so it makes sense to work with cohomology defined by continuous cochains.

[6] In fact this is an isomorphism, because $H^1(K, \overline{K}^\times)$ is zero ("Hilbert's theorem 90")

DEFINITION. *A* Selmer structure *is a collection* $\mathcal{F} = (\mathcal{F}_v)_{v \text{ prime of } K}$*, satisfying the following condition: for almost all* v *we have* $\mathcal{F}_v = \mathcal{F}_{v,ur}$*. If* $\mathcal{F}$ *is a Selmer structure we define the corresponding Selmer group by*

$$\mathrm{Sel}_{\mathcal{F}}(K, V) = \{x \in H^1(K, V) : \mathrm{loc}_v(x) \in \mathcal{F}_v \ \forall v\}.$$

Fact: The space $\mathrm{Sel}_{\mathcal{F}}(K, V)$ is finite-dimensional over $\mathbf{Q}_p$.

We're mostly interested in three specific choices of Selmer structure, differing only in the choices of the $\mathcal{F}_v$ at primes $v \mid p$: we define the *strict Selmer group* $\mathrm{Sel}_{\mathrm{strict}}(K, V)$ by taking $\mathcal{F}_v = \mathcal{F}_{v,\mathrm{ur}}$ for $v \nmid p$, and $\mathcal{F}_v = \mathcal{F}_{v,\mathrm{strict}}$ for $v \mid p$; and similarly the *relaxed Selmer group* and *Bloch–Kato Selmer group*.

Hence the strict, relaxed, and Bloch–Kato Selmer groups satisfy

$$\mathrm{Sel}_{\mathrm{strict}}(K, V) \subseteq \mathrm{Sel}_{\mathrm{BK}}(K, V) \subseteq \mathrm{Sel}_{\mathrm{relaxed}}(K, V).$$

REMARK. As will soon become clear, it is $\mathrm{Sel}_{\mathrm{BK}}(K, V)$ which is the most important; but $\mathrm{Sel}_{\mathrm{strict}}(K, V)$ and $\mathrm{Sel}_{\mathrm{relaxed}}(K, V)$ are easier to study, and will give us a stepping-stone towards $\mathrm{Sel}_{\mathrm{BK}}(K, V)$.

REMARK. Recall that for $V = \mathbf{Q}_p(1)$ we had the Kummer map $K^\times \otimes \mathbf{Q}_p \xrightarrow{\cong} H^1(K, \mathbf{Q}_p(1))$. One can check that the elements of $K^\times$ whose image under κ_p lands in Sel_{BK} are exactly the global units $O_K^\times$. The relaxed Selmer group allows elements which are units except possibly at the primes above p. (The strict Selmer group, on the other hand, should be zero; this is exactly Leopoldt's conjecture for K.)

4.4. The Bloch–Kato conjecture.

Let V be a representation coming from geometry.

CONJECTURE. *We have*

$$\dim \mathrm{Sel}_{\mathrm{BK}}(K, V) - \dim H^0(K, V) = \mathrm{ord}_{s=0} L(V^*(1), s).$$

There are refined versions using $\mathbf{Z}_p$-modules in place of $\mathbf{Q}_p$-vector spaces, which predict the leading term of the L-function up to a unit; but we won't go into that here.

E.g. if V is $V_p(E)$ for an elliptic curve E, then:

- the H^0 term is zero;
- the Kummer map lands inside the Selmer group, and gives an embedding

$$E(K) \otimes \mathbf{Q}_p \hookrightarrow \mathrm{Sel}_{\mathrm{BK}}(K, V),$$

  so that $\dim \mathrm{Sel}_{\mathrm{BK}} \geq \mathrm{rank}(E/K)$, with equality iff the p-part of Sha is finite;
- $\mathrm{ord}_{s=0} L(V^*(1), s) = \mathrm{ord}_{s=1} L(E/K, s)$.

So this special case of Bloch–Kato is closely related to (but not quite the same as) the Birch–Swinnerton-Dyer conjecture.

5. Euler systems

We'll now introduce the key subject of these lectures: Euler systems, which are tools for studying and controlling Selmer groups.

5.1. The definition.

Let:

- V a $G_{\mathbf{Q}}$-representation (for simplicity)
- $T \subset V$ a $G_{\mathbf{Q}}$-stable $\mathbf{Z}_p$-lattice
- Σ a finite set of primes containing p and all ramified primes for V

Since V is a $G_{\mathbf{Q}}$-rep, we can consider it as a G_K-rep for any number field K and form $H^i(K, V)$, and there are **corestriction** or **norm** maps

$$\mathrm{norm}_K^L : H^i(L, V) \to H^i(K, V) \quad \text{if } L \supset K.$$

If K is Galois, $H^i(K, V)$ is a module over $\mathbf{Q}_p[\mathrm{Gal}(K/\mathbf{Q})]$. Similarly for cohomology of lattices $H^i(K, T)$.

Definition. *An* Euler system for (T, Σ) *is a collection* $\mathbf{c} = (c_m)_{m \ge 1}$*, where* $c_m \in H^1(\mathbf{Q}(\mu_m), T)$*, satisfying the following compatibility for any* $m \ge 1$ *and* ℓ *prime:*

$$\mathrm{norm}_{\mathbf{Q}(\mu_m)}^{\mathbf{Q}(\mu_{m\ell})}(c_{m\ell}) = \begin{cases} c_m & \text{if } \ell \in \Sigma \text{ or } \ell \mid m \\ P_\ell(V^*(1), \sigma_\ell^{-1}) \cdot c_m & \text{otherwise} \end{cases}$$

where σ_ℓ *is the image of* Frob_ℓ *in* $\mathrm{Gal}(\mathbf{Q}(\mu_m)/\mathbf{Q})$*.*

An Euler system for V *is an Euler system for* (T, Σ)*, for some* $T \subset V$ *and some* Σ*.*

Intuitively, the c_m has "something to do with" the L-function $L(V^*(1), s)$ with its Euler factors at primes dividing $m\Sigma$ missing[7]; so when we compare elements for different m, the Euler factors appear.

This definition is bizarre, I admit! Fear not: we'll see an example before too long. The main reason to care about these objects is the following theorem, which is due to Karl Rubin, building on earlier work of Kolyvagin:

Theorem. *Suppose* $\mathbf{c}$ *is an Euler system for* (T, Σ) *with* c_1 *non-zero, and suppose* V *satisfies various technical conditions. Then* $\mathrm{Sel}_{\mathrm{strict}}(\mathbf{Q}, V^*(1))$ *is zero.*

Remark. More generally, one can also define Euler systems for G_K-representations, for K a number field; in place of cyclotomic fields, one has to have classes over every ray class field of K. However, we'll only work with $K = \mathbf{Q}$ here.

5.2. Cyclotomic units. We're going to build an Euler system for $V = \mathbf{Q}_p(1)$. Recall that we have Kummer maps $K^\times \hookrightarrow H^1(K, \mathbf{Z}_p(1))$. Also, for L/K finite, we have a commutative square

$$\begin{tikzcd} L^\times \arrow[r, "\kappa_p"] \arrow[d, "\mathrm{norm}_K^L"'] & H^1(L, \mathbf{Z}_p(1)) \arrow[d, "\mathrm{norm}_K^L"] \\ K^\times \arrow[r, "\kappa_p"] & H^1(K, \mathbf{Z}_p(1)) \end{tikzcd}$$

where the left-hand norm map is the usual field norm, and the right-hand one is the Galois corestriction. So we have to find good elements of the multiplicative groups of cyclotomic fields, satisfying compatibilities under the norm maps.

Fix an embedding $\overline{\mathbf{Q}} \hookrightarrow \mathbf{C}^\times$ and let $\zeta_m = \iota^{-1}(e^{2\pi i/m}) \in \mu_m$.

Definition. *For* $m > 1$*, set* $u_m = 1 - \zeta_m \in \mathbf{Q}(\zeta_m)^\times$*.*

A pleasant computation (exercise!) shows that

$$\mathrm{norm}_{\mathbf{Q}(\mu_m)}^{\mathbf{Q}(\mu_{m\ell})} u_m = \begin{cases} u_m & \text{if } \ell \mid m \\ (1 - \sigma_\ell^{-1}) \cdot u_m & \text{if } \ell \nmid m \text{ and } m > 1 \\ \ell & \text{if } m = 1 \end{cases}$$

This is almost what we need for an Euler system, but there are two problems: firstly, there is no sensible way to define u_1; secondly, we are seeing Euler factors at *all* primes, whereas we only want to see them for primes outside Σ (and Σ can't be empty because it has to contain p). We can get around both of these problems by setting

$$v_m = \begin{cases} u_m & \text{if } p \mid m, \\ \mathrm{norm}_{\mathbf{Q}(\mu_m)}^{\mathbf{Q}(\mu_{pm})}(u_{pm}) & \text{if } p \nmid m \text{ (including } m = 1). \end{cases}$$

Theorem. *The classes* $c_m = \kappa_p(v_m)$ *are an Euler system for* $(\mathbf{Z}_p(1), \{p\})$*.* □

[7] This becomes more precise if you work with the *equivariant* L-function $L(V^*(1), \mathbf{Q}(\mu_m)/\mathbf{Q}, s)$ which is a Dirichlet series taking values in the group ring $\mathbf{C}((\mathbf{Z}/m\mathbf{Z})^\times)$ rather than just in $\mathbf{C}$. The definition of this only makes sense if you drop the Euler factors at primes dividing m.

5.3. Soulé twists. Rubin's theorem applied directly to the cyclotomic unit Euler system isn't actually very interesting (it follows easily from class field theory that $\mathrm{Sel}_{\mathrm{strict}}(\mathbf{Q}, \mathbf{Q}_p) = 0$). However, there is a notion of *twisting* for Euler systems.

THEOREM. *Let $\chi : G_{\mathbf{Q}} \to \mathbf{Z}_p^\times$ be a continuous character unramified outside Σ (e.g. any power of the cyclotomic character). Then there is a canonical bijection $\mathbf{c} \mapsto \mathbf{c}^\chi$ between Euler systems for T and for the twist $T(\chi)$.*

Note that the "bottom class" c_1^χ is *not* uniquely determined by c_1, so even if $c_1 \neq 0$ we might have $c_1^\chi = 0$; thus we have to check carefully that the twisted Euler system satisfies the conditions for Rubin's theorem.

The twists of the cyclotomic unit Euler system are very useful in Iwasawa theory; see §3.2 of Rubin's book.

Lecture 3. Euler systems from geometry

References for this lecture: not as many as there should be! For §6, Jannsen's "Continuous étale cohomology" has the details, but it is not an easy read. For §7, chapters 1 and 2 of Kato's article in Asterisque 295 are the definitive source; Lang's "Elliptic Functions" is also useful.

6. Euler systems from geometry

6.1. Etale cohomology over K. We saw before that, for a variety X/K, the étale cohomology of its base-extension $X_{\overline{K}}$ was an interesting source of Galois representations.

But this isn't the only thing we can do with étale cohomology. Rather than base-extending to $\overline{K}$, we can also take étale cohomology over K directly[8]; there are groups $H^i_{\text{ét}}(X, \mathbf{Q}_p(m))$ for all i and m. These are *not* themselves Galois representations, but it turns out that these are related to the Galois cohomology of the étale cohomology over $\overline{K}$:

Theorem (Jannsen). *For any variety X/K, and any m, there is a convergent "Hochschild–Serre" spectral sequence*

$$E_2^{ij} = H^i\left(K, H^j_{\text{ét}}(X_{\overline{K}}, \mathbf{Q}_p)(m)\right) \Rightarrow H^{i+j}_{\text{ét}}(X, \mathbf{Q}_p(m)).$$

In particular, we get edge maps $H^i(X, \mathbf{Q}_p(m)) \to H^i(X_{\overline{K}}, \mathbf{Q}_p(m))^{G_K}$, and if F^1H^i denotes the kernel of this map, there is a map

$$F^1H^i(X, \mathbf{Q}_p(m)) \to H^1\big(K, H^{i-1}(X_{\overline{K}}, \mathbf{Q}_p(m))\big).$$

So, if V is the Galois representation $H^{i-1}(X_{\overline{K}})$ (or a direct summand of it), we can try to construct an Euler system for V by building lots of classes in $F^1H^i(X)$.

How will we do this? We'll use geometry! To be precise, we'll rely on the following rather simple tricks:

- **Cup products**: étale cohomology has cup-product pairings
$$H^i(X, \mathbf{Q}_p(m)) \times H^j(X, \mathbf{Q}_p(n)) \to H^{i+j}(X, \mathbf{Q}_p(m+n)).$$
- **Kummer maps**: if $f \in \mathcal{O}(X)^\times$ is a unit in the ring of rational functions on X, then there is a class $\kappa_p(f) \in H^1(X, \mathbf{Q}_p(1))$.
- **Pushforward maps**: if $Z \subset X$ is a closed subvariety of codimension d (and X and Z are both smooth), then there are pushforward maps
$$H^i(Z, \mathbf{Q}_p(n)) \to H^{i+2d}(X, \mathbf{Q}_p(n+d)).$$
In particular, the pushforward of the identity class $1_Z \in H^0(Z, \mathbf{Q}_p(0))$ is a class in $H^{2d}(X, \mathbf{Q}_p(d))$, the *cycle class* of Z.

So if we have a good supply of units on X, or of subvarieties of X (or of subvarieties of X with units on them, etc) then we have some objects to play with; and we can try to write down classes landing in the "right" cohomological degree to map into H^1 of our target Galois representation.

If you have a random variety, it's not clear how to find lots of subvarieties, or lots of units, on it; but we're going to home in on the case where X is a *Shimura variety* – a variety coming from automorphic theory, such as a modular curve. Then we can try and write down units and subvarieties using automorphic ideas.

6.2. Numerology. For instance, let's suppose we want to build an Euler system for $V_p(f)$, where f is a modular form. Since we can twist Euler systems, we can choose to work with $V_p(f)(m)$ for any integer m.

Because $Y = Y_1(N)_{\mathbf{Q}}$ is affine, we have $H^2_{\text{ét}}(Y_{\overline{\mathbf{Q}}}, \mathbf{Q}_p) = 0$. So the HS spectral sequence gives us a map

$$H^2_{\text{ét}}(Y_{\mathbf{Q}}, \mathbf{Q}_p(m)) \to H^1(\mathbf{Q}, H^1_{\text{ét}}(Y_{\overline{\mathbf{Q}}}, \mathbf{Q}_p)(m)) \to H^1(\mathbf{Q}, V_p(f)(m)).$$

for any integer m. How can we get at the groups $H^2_{\text{ét}}(Y_{\mathbf{Q}}, \mathbf{Q}_p(m))$ using our geometric toolkit?

[8]Technical point: what we actually want here is "continuous étale cohomology" in the sense of Jannsen.

- For $m \le 0$ this is hopeless, because our toolkit will only ever give classes in $H^i(X, \mathbf{Q}_p(m))$ for $m \ge \frac{i}{2}$.
- For $m = 1$, you can use cycle classes of codimension 1 subvarieties of Y – i.e., points. This is Kolyvagin's original approach: to build an Euler system using cycle classes of Heegner points.
- For $m = 2$, you can use cup-products of units: the Kummer map gives you classes in $H^1_{\text{ét}}(Y, \mathbf{Q}_p(1))$, and the cup-product of two such classes lands in $H^2_{\text{ét}}(Y, \mathbf{Q}_p(2))$. This is Kato's approach.
- $m \ge 3$ can also be made to work similarly (but gives no more information than for $m = 2$).

We can also ask the same question for $V_p(f) \otimes V_p(g)$, using the geometry of $Y \times Y$. Again, different twists m give very different geometric setups; and taking m too small is hopeless – you want $m \ge 2$ at least. The sensible choices are:

- $m = 3$: we can get classes here as cup-products $\kappa_p(f_1) \cup \kappa_p(f_2) \cup \kappa_p(f_3)$, where f_1, f_2, f_3 are units on $Y \times Y$.
- $m = 2$: we can get classes by taking a curve $Z \subset Y \times Y$ and a unit $f \in \mathcal{O}(Z)^\times$, and pushing forward $\kappa_p(f) \in H^1_{\text{ét}}(Z, \mathbf{Q}_p(1))$ along the embedding $Z \hookrightarrow Y \times Y$.

The $m = 3$ approach has, I believe, never been successfully carried out (although people have tried). The $m = 2$ case is where the Euler system of Beilinson–Flach elements lives. I'll talk about this later in these lectures.

7. Siegel units

As we saw above, we can get potentially useful cohomology classes if we have a source of units in the coordinate rings of our varieties. Fortunately, for modular curves, we have lots of nice units at our disposal.

7.1. Modular units. Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbf{Z})$ (e.g. $\Gamma_1(N)$ for any N, or the principal congruence subgroup $\Gamma(N)$).

Definition. *A **modular unit** of level Γ is a nowhere-vanishing, Γ-invariant holomorphic function $\mathcal{H} \to \mathbf{C}$, with poles of finite order at the cusps.*

In more algebraic language, the quotient $\Gamma \backslash \mathcal{H}$ is the complex points of an algebraic curve $Y(\Gamma)_{\mathbf{C}}$ over $\mathbf{C}$, and a modular unit is an element of $\mathcal{O}(Y(\Gamma)_{\mathbf{C}})^\times$.

We're going to construct some "special" modular units, using nothing but classical 19-th century elliptic function theory. These functions are called **Siegel units** and they are really amazingly powerful gadgets. In fact, you can recover virtually every known example of an Euler system by starting from Siegel units!

Definition. *Let $\alpha, \beta \in \mathbf{Q}/\mathbf{Z}$, not both zero. Define the function $g_{\alpha,\beta} : \mathcal{H} \to \mathbf{C}$ as follows: write $(\alpha, \beta) = (a/N, b/N)$ for some $N \ge 1$ and $a, b \in \mathbf{Z}$, with $0 \le a < N$ without loss of generality. Then*

$$g_{\alpha,\beta}(\tau) = q^w \prod_{n \ge 0} \left(1 - q^{n+a/N} \zeta_N^b\right) \prod_{n \ge 1} \left(1 - q^{n-a/N} \zeta_N^{-b}\right),$$

where $q = e^{2\pi i \tau}$ and $w = \frac{1}{12} - \frac{a}{N} + \frac{a^2}{2N^2}$.

This is well-defined (independent of the choice of common denominator N). We'd like to say it's modular of level N, but this doesn't quite work: acting on it by an element of $\Gamma(N)$ multiplies it by a root of unity, so it defines an element of $\mathcal{O}(Y(N)) \otimes \mathbf{Q}$. The denominator can be killed by a very simple modification:

Definition (Siegel units). *For $c > 1$ coprime to 6 and to the order of α, β in $\mathbf{Q}/\mathbf{Z}$, let*

$${}_c g_{\alpha,\beta} = \frac{(g_{\alpha,\beta})^{c^2}}{g_{c\alpha,c\beta}}.$$

Then ${}_c g_{\alpha,\beta}$ is $\Gamma(N)$-invariant, for any N such that $N\alpha = N\beta = 0$, so it is in $\mathcal{O}(Y(N)_{\mathbf{C}})^\times$. However, we can do better than this: it descends to a number field.

Proposition. *The units ${}_c g_{\alpha,\beta}$, for $(\alpha,\beta) \in (\tfrac{1}{N}\mathbf{Z}/\mathbf{Z})^{\oplus 2} - \{(0,0)\}$, are all defined over $\mathbf{Q}(\mu_N)$. The action of $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ on $Y(N)_{\mathbf{Q}(\mu_N)}$ transforms these units via the rule*

$${}_c g_{\alpha,\beta} \mid \sigma = {}_c g_{\alpha',\beta'}, \quad \text{where} \quad (\alpha',\beta') = (\alpha,\beta)\sigma. \quad \square$$

In particular, because $(0, \frac{1}{N})$ is preserved by right-multiplication by matrices of the form $\begin{pmatrix} 1 & y \\ & 1 \end{pmatrix}$ (giving the action of $\Gamma_1(N)/\Gamma(N)$) and matrices of the form $\begin{pmatrix} x & \\ & 1 \end{pmatrix}$ (giving the action of the Galois group), we see that:

Proposition. *The units ${}_c g_{0,1/N}$ have level $\Gamma_1(N)$, and are defined over $\mathbf{Q}$, with respect to the $\mathbf{Q}$-model of $Y_1(N)$ we chose above.* $\square$

7.2. Logarithmic derivatives and Eisenstein series. For any curve Y there is a canonical map

$$\mathrm{dlog} : \mathcal{O}(Y)^\times \to \Omega^1(Y),$$

where $\Omega^1(Y)$ denotes the holomorphic differential forms on Y, defined by

$$\mathrm{dlog}\, u = \frac{\mathrm{d}u}{u}.$$

This map $Y = Y_1(N)_{\mathbf{C}}$, this map target is the space of holomorphic $\Gamma_1(N)$-invariant differentials on $\mathcal{H}$ with (at worst) simple poles at the cusps; this is exactly the space of weight 2 modular forms $M_2(\Gamma_1(N))$, with the modular form f corresponding to the differential $f(q)\frac{\mathrm{d}q}{q} = 2\pi i f(\tau)\,\mathrm{d}\tau$.

Theorem. *We have*

$$\mathrm{dlog}(g_{\alpha,\beta}) = F^{(2)}_{\alpha,\beta}(q)\,\frac{\mathrm{d}q}{q},$$

where $F^{(2)}_{\alpha,\beta}$ is an explicit weight 2 Eisenstein series; for example

$$F^{(2)}_{0,\beta} = \tfrac{1}{12} - \sum_{n \ge 1} q^n \left(\sum_{d \mid n} \tfrac{n}{d} \left(e^{2\pi i \beta d} + e^{-2\pi i \beta d}\right) \right).$$

So the Siegel units are a "lifting" of the weight 2 Eisenstein series to $\mathcal{O}(Y)^\times$. This gives rise to their other, scarier name: "motivic Eisenstein classes".

Remark. There is another, deeper relation between Siegel units and Eisenstein classes: Kronecker's limit formula, which relates $\log|g_{b/N}|$ to a non-holomorphic Eisenstein series of weight 0.

7.3. Changing the level: the basic norm relation.

Theorem. *Let $\alpha, \beta \in \mathbf{Q}/\mathbf{Z}$, not both zero, and let $A \ge 1$. Then we have the three relations*

(1) $$\prod_{\alpha' : A\alpha' = \alpha} {}_c g_{\alpha',\beta}(\tau) = {}_c g_{\alpha,\beta}(A^{-1}\tau),$$

(2) $$\prod_{\beta' : A\beta' = \beta} {}_c g_{\alpha,\beta'}(\tau) = {}_c g_{\alpha,\beta}(A\tau),$$

(3) $$\prod_{\substack{\alpha',\beta' \\ A(\alpha',\beta') = (\alpha,\beta)}} {}_c g_{\alpha',\beta'}(\tau) = {}_c g_{\alpha,\beta}(\tau).$$

Note that (1) and (2) imply (3), and (2) follows from (1) via the action of $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$; so it suffices to prove (1). This can be bashed out directly from the infinite product formula, but there is a much slicker argument in Kato's book, involving a 2-variable theta function ${}_c\theta(\tau, z)$ such that ${}_c\theta(\tau, \alpha\tau + \beta) = {}_c g_{\alpha\beta}$.

This is hugely important, because it's the underlying input for all of the Euler systems we will build out of Siegel units.

Remark. One can check that for ℓ prime

$$\prod_{\substack{\alpha',\beta' \\ \ell(\alpha',\beta')=(0,0) \\ (\alpha',\beta')\neq(0,0)}} {}_c g_{\alpha',\beta'} = \ell^{(c^2-1)}.$$

It follows that there is no way to define a modular unit ${}_c g_{0,0}$ in such a way that the (3) continues to hold.

Lecture 4. The Kato and Beilinson–Flach Euler systems

In this lecture we're going to write down the classes, and prove the norm relations, for two important examples of Euler systems.

References for this lecture: here there is really no alternative to the original papers. For §8, see Kato's Asterisque 295 article, or the alternative account in Colmez's Bourbaki seminar on Kato's work ("La conjecture de Birch–Swinnerton-Dyer p-adique"). For §9, see my 2014 paper with Lei and Zerbes.

8. Kato's Euler system

Let's now concentrate on Kato's Euler system. We want to build an Euler system for $V_p(f)(2)$, where f is some newform of level N; and we're going to do this by cupping together the Kummer-map images of modular units on $Y_1(N)$.

Choose two integers $c, d > 1$ coprime to $6Np$, where N is the level of the modular form f we want to study. We'll assume without further comment that all modular curves we consider have levels coprime to c and d. (This will mean we only get classes over $\mathbf{Q}(\mu_m)$ for $(cd, m) = 1$; but in fact it's OK to throw away a finite set of primes like this.)

We know some modular units on $Y_1(N)$ already – the units ${}_cg_{0,b/N}$ – but these aren't enough: because they're all defined over $\mathbf{Q}$, we will end up with classes on $H^1(\mathbf{Q}, V_p(f)(2))$, while we want also to have classes over cyclotomic fields with interesting Galois actions. So we need some modular units defined over bigger fields.

8.1. The units u and v.

Definition. *Let $N \geq 2$ be an integer coprime to c, and define modular units u_N, v_N by*

$$u_N(\tau) = {}_cg_{1/N,0}(N\tau), \qquad v_N(\tau) = {}_dg_{0,1/N}(\tau).$$

One checks easily that u_N and v_N both have level $\Gamma_1(N)$. We saw above that v_N is defined over $\mathbf{Q}$; but v_N is not – in fact it is defined over $\mathbf{Q}(\mu_N)$, and we have the following key compatibility:

Proposition. *If $A \geq 1$ such that N and AN have the same prime factors, and π denotes the natural map $Y_1(AN) \to Y_1(N)$, then*

$$\operatorname{norm}_{\mathbf{Q}(\mu_N)}^{\mathbf{Q}(\mu_{AN})}(u_{AN}) = \pi^*(u_N), \tag{1}$$

$$\pi_*(v_{AN}) = v_N. \tag{2}$$

Proof. (sketch) Both the pushforward π_*, and the Galois norm map, can be described by sending a unit to the product of its translates by coset representatives for subgroups of GL_2. We know how GL_2 acts on the Siegel units, and in both cases the products turn out to be exactly the ones coming up in our Siegel-unit norm relations. □

8.2. Kato's classes.

Definition. *For integers m, N, with $m \geq 2$ and $m \mid N$, we define*

$$z_{N,m} = \kappa_p(u_m) \cup \kappa_p(v_N) \in H^2_{\text{ét}}\left(Y_1(N)_{\mathbf{Q}(\mu_m)}, \mathbf{Z}_p(2)\right).$$

This is defined over $\mathbf{Q}(\mu_m)$, since both modular units are definable over this field. The restriction to $m \mid N$ is annoying, and we'll get rid of it by using a norm-compatibility in the *level* direction instead!

Proposition. *If $m \mid N \mid N'$, and N and N' have the same prime factors, then*

$$(\pi_{N'/N})_*(z_{N',m}) = z_{N,m},$$

where $\pi_{N'/N}$ is the natural map $Y_1(N') \to Y_1(N)$.

Proof. This relies on a crucial “adjunction formula” for étale cohomology: if $f : X \to Y$ is a (sufficiently nice) map, then the pushforward, pullback, and cup-product maps in étale cohomology are related by

$$f_* \left(f^*(\alpha) \cup \beta \right) = \alpha \cup f_*(\beta).$$

In our case, where f is the natural map from $Y_1(N')$ to $Y_1(N)$, one factor in our cup-product is $\kappa(u_m)$, which already lives at level m. So we can factor it out and write

$$\pi_* \left(z_{N',m} \right) = \kappa(u_m) \cup \pi_* \left(\kappa(v_{N'}) \right).$$

We know that $\pi_*(v_{N'})$ is v_N, and κ is well-behaved with respect to norm maps, so we get $\kappa(u_m) \cup \kappa(v_N) = z_{N,m}$. ☐

It follows that we can define $z_{N,m}$ without assuming that $m \mid N$, by choosing any $L \geq 1$ divisible by m and N and with the same prime factors as mN, and setting

$$z_{N,m} = (\pi_{L/N})_* \left(z_{L,m} \right).$$

The proposition shows that this is independent of the choice of L, so it's a reasonable definition.

8.3. The norm relation.

Theorem (Kato, Proposition 8.10). *If ℓ is prime with $\ell \mid m$, then*

$$\mathrm{norm}_{\mathbf{Q}(\mu_m)}^{\mathbf{Q}(\mu_{m\ell})} \left(z_{N,m\ell} \right) = z_{N,m}.$$

If $\ell \nmid mN$ then

$$\mathrm{norm}_{\mathbf{Q}(\mu_m)}^{\mathbf{Q}(\mu_{m\ell})} \left(z_{N,m\ell} \right) = \left(1 - \langle \ell \rangle^{-1} T(\ell) \sigma_\ell^{-1} + \ell \langle \ell \rangle^{-1} \sigma_\ell^{-2} \right) z_{N,m},$$

where $\langle \ell \rangle$ and $T(\ell)$ are the usual Hecke operators.

Proof. (sketch) For the first statement (the $\ell \mid m$ case), we can assume without loss of generality that $m\ell \mid N$. Then we can use the same adjunction trick (the Galois-cohomology norm map is a special case of étale-cohomology pushforward) to reduce to a statement about the units $u_{m\ell}$ and u_m, which is exactly the proposition we proved above.

The $\ell \nmid mN$ case is more elaborate (Kato's proof, which is §2.11–2.13 of his Asterisque article, takes a little over three pages to write out), but still uses the same essential idea of reducing to a statement about the individual factors of the cup product and then using the norm-compatibility relations of Siegel units. ☐

When we project to the quotient $H^1(\mathbf{Q}(\mu_m), V_p(f)(2))$ of $H^2_{\text{ét}}(Y_1(N)_{\mathbf{Q}(\mu_m)}, \mathbf{Q}_p(2))$, the Hecke operators $T(\ell)$ and $\langle \ell \rangle$ will be acting as $a_\ell(f)$ and $\chi(\ell)$ respectively. So the Euler factor appearing above is $(1 - \chi(\ell)^{-1} a_\ell(f) X + \ell \chi(\ell)^{-1} X^2)$ evaluated at $X = \sigma_\ell^{-1}$.

On the other hand, if $V = V_p(f)(2)$, then $V^*(1) = V_p(f)^*(-1) = V_p(f \otimes \chi^{-1})$. So the Euler factor is exactly $P_\ell(V^*(1), X)$ evaluated at σ_ℓ^{-1}, as it should be; these are the “correct” relations for an Euler system for $V_p(f)(2)$.

Remark. As with the cyclotomic units, we have Euler factors in our norm relations for all primes, including p. We can kill these by replacing $z_{N,m}$ with $z_{N,m}^{(p)} = \mathrm{norm}_m^{mp}(z_{N,mp})$. This class $z_{N,m}^{(p)}$ is a special case of the cohomology classes appearing in (8.1.2) of Kato; he defines a class ${}_{c,d}z_{1,N,m}^{(p)}(k, r, r', a(A), S)$, which reduces to the one considered here if one takes $k = 2$, $r = 0$, $r' = 1$, $a(A) = 0(1)$, and S the set of primes dividing pm.

(Observe that Kato's cohomology class depends on eleven separate parameters $\{c, d, p, N, m, k, r, r', a, A, S\}$. Uncontrollable proliferation of indices is an occupational hazard in Euler system theory!)

9. Beilinson–Flach elements

Now let's turn our attention to Rankin–Selberg convolutions $V_p(f) \otimes V_p(g)$. We saw above that one natural line of attack is to find curves $C \subset Y \times Y$, where $Y = Y_1(N)$, and units on C. This approach goes back to Beilinson in 1984 (and was further refined by Flach in 1992, hence the name).

9.1. Strategy. An obvious first guess is to take C to be the diagonally-embedded copy of Y in $Y \times Y$, and this is exactly what we'll do for $m = 1$. However, how will we get classes over $\mathbf{Q}(\mu_m)$ for $m > 1$?

In Kato's world, one of our modular units (u_m) gave us norm-compatibility in m for $m \mid N$; the other one (v_N) gave us norm-compatibility in N; and putting those together, via the adjunction formula, gives norm-compatibility in m for all m. This trick won't work here; we only have one unit to play with, and we can't find families of units that are simultaneously norm-compatible in the "field" and "level" directions (at least, I don't know how to do this).

So we have to make the curve C vary too, and get some contribution to our norm-compatibility this way instead. In fact, we're going to rig things so that

- the compatibility in the "level" direction comes from the unit,
- the compatibility in the "field" direction comes from the choice of C.

9.2. Mixed-level modular curves. For integers $M \mid N$, let

$$\Gamma(M,N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a = d = 1, c = 0 \bmod N; b = 0 \bmod M \right\}.$$

Notice that $\Gamma(N,N) = \Gamma(N)$, and $\Gamma(1,N) = \Gamma_1(N)$.

Moreover, any matrix in $\mathrm{SL}_2(\mathbf{Z}/N)$ which is upper-triangular modulo N/M normalises $\Gamma(M,N)$ (easy check). One finds that the curve $Y(M,N)$ has a $\mathbf{Q}$-model, but the group action is only defined over $\mathbf{Q}(\mu_M)$.

Definition. *For $j \in \mathbf{Z}/M\mathbf{Z}$, let $C_{M,N} \subseteq Y(M,N)^2$ be the curve defined by*

$$\left\{ (P,Q) \in Y(M,N)^2 : Q = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot P \right\}.$$

This is defined over $\mathbf{Q}(\mu_M)$, and we have the following key compatibility. Suppose $A \geq 1$ with $AM \mid N$, and let $\phi_M^{AM} : Y(AM,N) \to Y(M,N)$ be the natural quotient map.

Proposition. *If M and AM have the same prime factors, then*

$$(\phi_M^{AM} \times \phi_M^{AM})^* \left(C_{M,N}\right) = \bigsqcup_{\gamma \in \mathrm{Gal}(\mathbf{Q}(\mu_{AM})/\mathbf{Q}(\mu_M))} (C_{AM,N})^\sigma.$$

Proof. This just reduces to the group-theoretic fact that the same set of matrices

$$\left\{ \begin{pmatrix} 1 & 1 + xM \\ 0 & 1 \end{pmatrix} : 0 \leq x < A \right\} \subset \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$$

is the orbit of $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ under either of two group actions:

- translation by representatives for $\Gamma(M,N)/\Gamma(MA,N)$;
- conjugation by matrices $\begin{pmatrix} u & \\ & 1 \end{pmatrix}$ with $u = 1 \bmod M$, which give the Galois action. □

(Note the formal similarity to Kato's units u_M: the Galois norm of an object defined over $\mathbf{Q}(\mu_M)$ equals the pullback of something from a smaller level.)

9.3. Beilinson–Flach elements. One more piece of the jigsaw: as well as the natural map $\phi_1^M : Y(M,N) \to Y(1,N) = Y_1(N)$, there is a "twisted" map $\hat{\phi}_1^M : Y(M,N) \to Y_1(N)$, corresponding to $z \mapsto z/M$ on $\mathcal{H}$.

Definition. *For $M \mid N$, and $c > 1$ coprime to $6N$, we define*

$$\xi_{M,N} = \left[(\hat{\phi}_1^M \times \hat{\phi}_1^M)_* \circ (\iota_{M,N})_* \circ \kappa_p\right] \left({}_c g_{0,1/N}\right) \in H^3_{\text{ét}}\left(Y_1(N)^2_{\mathbf{Q}(\mu_M)}, \mathbf{Z}_p(2)\right).$$

where $\iota_{M,N}$ is the inclusion $C_{M,N} \hookrightarrow Y(M,N)^2$.

As in Kato's construction, these elements turn out to satisfy norm-compatibility in N (with respect to the usual degeneracy maps), and we can use this to extend the definition of ${}_c\xi_{M,N}$ to all M by norming down from some ${}_c\xi_{M,L}$, where L is divisible by both M and N.

Theorem. *If ℓ is prime with $\ell \mid M$ and $\ell \mid N$, we have*

$$\operatorname{norm}^{\mathbf{Q}(\mu_{M\ell})}_{\mathbf{Q}(\mu_M)} \left({}_c\xi_{M\ell,N}\right) = [U(\ell)' \times U(\ell)'] \cdot {}_c\xi_{M,N}.$$

Here $U(\ell)'$ is the transpose Hecke operator (defined by the double coset of $\begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix}$, while the usual $U(\ell)$ is $\begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix}$).

Proof. After some unravelling this follows directly from the Proposition about the $C_{M,N,j}$: comparing the two sides, we end up with the term $(\hat{\phi}_1^\ell \times \hat{\phi}_1^\ell)_* (\phi_1^\ell \times \phi_1^\ell)^*$ coming out, and this is exactly the definition of the Hecke operator $U(\ell)' \times U(\ell)'$. ∎

If we don't have $\ell \mid M$ and $\ell \mid N$ then (after a lot of rather intricate calculations of double cosets) one obtains an analogous proposition involving an Euler factor.

Remark. The appearance of the $U(\ell)'$ factors has interesting consequences. Consider the case where $M = p^r$ is a power of p. When we project to the (f,g)-eigenspace this tells us that the classes $(\alpha_f \alpha_g)^{-r} {}_c\xi_{p^r,N}$ are norm-compatible, where α_f is the U_p-eigenvalue of the conjugate form f^*. This is fine if f^* and g^* are ordinary (so $\alpha_f \alpha_g$ is a p-adic unit) but makes life more difficult, and more interesting, in the supersingular case: we have potentially introduced some "denominators" into our classes.

10. Further directions

10.1. P-adic regulators. We've constructed a bunch of Euler systems (c_m) for some interesting representations V, but do they have $c_1 \neq 0$? This is very much non-obvious from our constructions. One approach to this problem goes via Besser's *rigid syntomic cohomology*. This is a cohomology theory for varieties over p-adic fields with a (somewhat) explicit description in terms of p-adic differential forms.

On one hand, there are comparison maps between étale and syntomic cohomology (due to Nizioł). For étale cohomology classes coming from geometric data, as in our examples, the images of the global étale classes under localisation at p agree with their syntomic versions via these comparison maps.

On the other hand, as Darmon and his co-authors have shown, rigid syntomic cohomology is sufficiently computable that one can relate the syntomic versions of the Euler system classes to p-adic L-functions (cf. Shin-ichi Kobayashi's lectures at this conference for the Heegner point case). Combining these two results allows one to prove that the localisations at p of Euler systems are related to p-adic L-functions.

10.2. More Euler systems. Our toolkit for constructing Euler systems seems to work in quite a lot of Shimura variety setups, e.g. Hilbert and Siegel modular varieties: roughly, whenever you have a Shimura variety for a group which contains GL_2, or a product of copies of GL_2, with the "right" codimension then you are in good shape.