1. Gebhard Boeckle's lectures

1.1. **Galois representations and congruences.** We first discuss profinite groups. Let G be a topological group.

Theorem 1. *The following are equivalent:*

(a) G is compact, Hausdorff, and totally disconnected.
(b) G is compact, and admits a neighborhood basis of the identity by open normal subgroups.
(c) There is a directed poset I and an inverse system (G_i) of finite (discrete) groups such that $G = \varprojlim_I G_i$.

We say that G is *profinite* if the above conditions hold. The topology on $\varprojlim G_i$ is that obtained by regarding it as a closed subgroup of the product $\prod G_i$.

Constructions:

(a) If G is discrete, then we equip it with the profinite topology $G^{\mathrm{pf}} := \varprojlim G/N$, where N runs over the finite index subgroups.
(b) If $G = \varprojlim G_i$ is profinite, then
  (i) The abelianization is given by
$$G^{\mathrm{ab}} = G/\overline{[G,G]} = \varprojlim G_i^{\mathrm{ab}},$$
  and in particular, is profinite.
  (ii) For H finite, write H_p for its maximal p-group quotient. Then
$$G_p = \varprojlim (G_i)_p$$
  is a pro-p-group (and in particular, profinite).
  (iii) If $N \leq G$ is closed and normal, then G/N is profinite.

Example 2. (a) Let F be a field. Set $G_F := \mathrm{Aut}_F(F^{\mathrm{sep}}) = \mathrm{Gal}(F^{\mathrm{sep}}/F)$ profinite. Define the poset
$$\mathcal{I}_F := \{L \subseteq F^{\mathrm{sep}} : L \supseteq F \text{ finite Galois}, \subseteq\}.$$
Then
$$G_F \xrightarrow{\cong} \varprojlim_{L \in \mathcal{I}_F} \mathrm{Gal}(L/F).$$

(b) Let $F' \subseteq F^{\mathrm{sep}}$ be a normal extension of F. Then $G_{F'} \leq G_F$ is closed and normal. We may thus write
$$\mathrm{Gal}(F'/F) \cong G_F/G_{F'} = \varprojlim_{\substack{L \in \mathcal{I}_F, \\ L \subseteq F'}} \mathrm{Gal}(L/F).$$

(c) Let $\mathbb{N}$ denote the natural numbers, ordered by divisibility. Then
$$\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n = \prod_p \mathbb{Z}_p,$$
where the last step is the Chinese remainder theorem. We sometimes need a slight modification:
$$\hat{\mathbb{Z}}^{(p)} = \varprojlim_{p \nmid n} \mathbb{Z}/n = \prod_{\ell \text{ prime}, \ell \neq p} \mathbb{Z}_\ell.$$

Let's fix some notation:

(a) Let K be a number field, $\mathcal{O}_K$ its ring of integers. Let $\mathrm{Pl}_K = \mathrm{Pl}_K^\infty \sqcup \mathrm{Pl}_K^{\mathrm{fin}}$ denote the set of places v of K. Let v be a finite place. We may then attach to it a maximal ideal $\mathfrak{q}_v$ of $\mathcal{O}_K$, giving a bijection

$$\mathrm{Pl}_K^{\mathrm{fin}} \leftrightarrow \mathrm{Max}(\mathcal{O}_K).$$

We may form the residue field $k_v := \mathcal{O}_K/\mathfrak{q}_v$. We denote q_v for the cardinality of k_v. We write $\mathrm{char}(v)$ for the characteristic of k_v. We denote by $\mathcal{O}_v = \varprojlim \mathcal{O}/\mathfrak{q}_v^n$, with fraction field K_v. Also, we have a short exact sequence

$$1 \to I_v \to G_v := \mathrm{Gal}_{K_v} \to \mathrm{Gal}_{k_v} \to 1.$$

A topological generator for Gal_{k_v} is given by

$$\mathrm{Fr}_v : \alpha \mapsto \alpha^{q_v}.$$

We denote by $\mathrm{Frob}_v \in G_v$ some lift of Fr_v.
We write $S_\infty := \mathrm{Pl}_K^\infty$ for the set of archimedean places, so that $K \otimes_{\mathbb{Q}} \mathbb{R} \cong \prod_{v \in S_\infty} K_v$. For a rational prime p, we write S_p for the set of places v of K such that $v \mid p$.

(b) We also need some local analogues for $E \supseteq \mathbb{Q}_p$ a p-adic field. Let $\mathcal{O} = \mathcal{O}_E$ denote the ring of integers, $\pi = \pi_E$ a uniformizer, and $\mathbb{F} = \mathcal{O}_E/\pi$ the residue field, with $q = \#\mathbb{F}$. Then $E \supseteq \mathbb{Q}_q = \mathbb{Q}_p[\zeta_{q-1}] \supseteq \mathbb{Q}_p$. We have $W(\mathbb{F}) = \mathbb{Z}_q = \mathbb{Z}_p[\zeta_{q-1}]$.

Contiuing the examples, which may serve as exercises:

(d) Let ζ_t be a primitive tth root of 1. For k a finite field, we have $G_k \cong \hat{\mathbb{Z}} = \overline{\langle \mathrm{Fr}_k \rangle}$, where $\mathrm{Fr}_k : \alpha \mapsto \alpha^{|k|}$.

(e) Let $E \supseteq \mathbb{Q}_p$ (finite extension). Then G_E (Jannsen–Wingberg for $p \geq 2$). Local class field theory: the Artin map $E^\times \to G_E^{\mathrm{ab}}$ is a continuous inclusion with dense image. Writing $E^\times = \pi_E^{\mathbb{Z}} \times \mathcal{O}_E^\times = \pi_E^{\mathbb{Z}} \times \mathbb{F}^\times \times \mathcal{U}_E^1$. Since the units are known to be a finitely generated $\mathbb{Z}_p$-module, we get as a corollary that

$$\mathrm{Hom}_{\mathrm{cts}}(G_E, \mathbb{F}_p) = H^1_{\mathrm{cts}}(G_E, \mathbb{F}_p)$$

is finite.

(f) We turn to the case of a number field K. We fix an embedding $K^{\mathrm{sep}} \subseteq K_v^{\mathrm{sep}}$ for each place v, which gives an embedding of Galois groups $G_v \to G_K$. For $S \subseteq \mathrm{Pl}_K$ finite, we write

$$K_S := \{\alpha \in K^{\mathrm{sep}} : K(\alpha) \text{ is unramified outside } S\},$$

which is a normal (typically infinite) extension of K. We write

$$G_{K,S} := \mathrm{Gal}(K_S/K) = G_K/G_{K_S}$$

for its Galois group. We remark that if we take $v \notin S$, then since v does not ramify in K_S, we know that the map $G_v \to G_{K,S}$ factors via the quotient $G_v/I_v \cong G_{k_v}$, so that $\mathrm{Frob}_v \in G_{K,S}$ is independent of the choice of lift. On the other hand, if $v \in S$, then we might ask whether the map $G_v \hookrightarrow G_{K,S}$ (see the work of Cheniever–Clozel). The structure of $G_{K,S}$ is unknown, but global class field theory describes $G_{K,S}^{\mathrm{ab}}$. A corollary is that

$$H^1_{\mathrm{cts}}(G_{K,S}, \mathbb{F}_p) = \mathrm{Hom}_{\mathrm{cts}}(G_{K,S}, \mathbb{F}_p)$$

is finite whenever S is finite. (One can appeal to Hermite–Minkowski, or class field theory.)

(g) Consider the tame quotient of G_E, for $E \supseteq \mathbb{Q}_p$. Given $E \supseteq \mathbb{Q}_p$, we form the tower of extensions $E^{\mathrm{tame}}/E^{\mathrm{unr}}/E$, where

$$E^{\mathrm{unr}} = \cup \{E(\zeta_n) : p \nmid n\},$$

$$E^{\mathrm{tame}} = \cup \{E^{\mathrm{unr}}(\sqrt[n]{\pi_E}) : p \nmid n\}.$$

It's a fact that G_E^{tame} may be expressed as the profinite completion of $\langle st : sts^{-1} = t^q \rangle$.

We finally come to **Galois representations**. They will typically be called $\rho : G \to \mathrm{GL}_n(A)$, where G is a topological group, A is a topological ring, and ρ is a continuous map. The topology on $\mathrm{GL}_n(A)$ is the subspace topology coming from embedding inside $M_n(A) \times A$ via $g \mapsto (g, \det(g)^{-1})$, for instance. We call ρ a Galois representation if $G = G_F$ for some field F. The main examples of interest for A will be $\mathbb{C}$, finite fields, and p-adic fields, to interpolate $\mathrm{CNL}_{\mathcal{O}}$ (complete Noetherian local $\mathcal{O}$-algebras).

Exercise 1. Let G be profinite, and ρ as above.

(a) If $A = \mathbb{C}$, then $\rho(G)$ is finite.
(b) If $A = \overline{\mathcal{O}_p}$, then there is a finite extension $E \supseteq \mathbb{Q}_p$ such that $\rho(G) \subseteq \mathrm{GL}_n(E)$ up to conjugation.
(c) If $A = E \supseteq \mathbb{Q}_p$ (finite extension), then after conjugation, we can assume that $\rho(G) \subseteq \mathrm{GL}_n(\mathcal{O})$.

In case (c), we have a G-stable lattice $\Lambda \cong \mathcal{O}^n \subseteq E^n$. We can apply reduction $\mathcal{O} \to \mathbb{F}$. This gives a reduction

$$\overline{\rho}_\Lambda : G \to \mathrm{GL}_n(\mathbb{F}).$$

Let's use the notation cp_α for the characteristic polynomial of $\alpha \in M_n(A)$.

Theorem 3. *(a) Given a representation $r : G \to \mathrm{GL}_n(\mathbb{F})$. Then there exists a semisimple representation $r^{\mathrm{ss}} : G \to \mathrm{GL}_n(\mathbb{F})$ such that $\mathrm{cp}_r = \mathrm{cp}_{r^{\mathrm{ss}}}$ (Brauer–Hesbitt), where r^{ss} is unique up to isomorphism.*
(b) We have $\mathrm{cp}_\rho \in \mathcal{O}[X]$ and $\mathrm{cp}_{\bar{\rho}_\Lambda} \in \mathbb{F}[X]$, independent of Λ.

Theorem 4. *For $\rho, \rho' : G_{K,S} \to \mathrm{GL}_n(E)$ semisimple, we have that $\rho \sim \rho'$ (conjugate) if and only if for all $v \in \mathrm{Pl}_K^{\mathrm{fin}} \setminus S$, we have*

$$\mathrm{cp}_{\rho(\mathrm{Frob}_v)} = \mathrm{cp}_{\rho'(\mathrm{Frob}_v)}.$$

Example 5. (1) p-adic cyclotomic character $\chi_p^{\mathrm{cyc}} : G_{\mathbb{Q}} \to \mathbb{Z}_p^\times$. We have

$$G_{\mathbb{Q}} \circlearrowright \mu_{p^n} = \langle \zeta_{p^n} \rangle \cong \mathbb{Z}/p^n,$$

$(\mathbb{Z}/p^n)^\times = \mathrm{Aut}_{\mathbb{Z}}(\mathbb{Z}/p^n)$. **Facts**:
- $\chi_p^{\mathrm{cyc}} \mid_{G_K}$: unramified outside $S_p \cup S_\infty$.
- $\chi_p^{\mathrm{cyc}}(\mathrm{Frob}_v) = q_v \in \mathbb{Z}_p^\times$.

(2) The Tate module of an elliptic curve $\mathcal{E}_{/K}$. We again have $G_K \circlearrowright \mathcal{E}[p^n](\bar{K}) \cong (\mathbb{Z}/p^n)^{\oplus 2}$, which gives rise to $G_K \to \mathrm{GL}_2(\mathbb{Z}/p^n)$. In the limit, we get

$$\rho_{\mathcal{E},p} : G_K \to \mathrm{GL}_2(\mathbb{Z}_p) \hookrightarrow \mathrm{GL}_2(\mathbb{Q}_p).$$

Facts:
- $\rho_{\mathcal{E},p}$ is unramified outside $S_\infty \cup S_p \cup \mathrm{Bad}$.

- For v outside those places, we have
$$\mathrm{cp}_{\rho_{\mathcal{E},p}}(\mathrm{Frob}_v) = X^2 - a_v(\mathcal{E})X + q_v,$$
where
$$a_v := \#\mathcal{E}(k_v).$$
This shows the geometric meaning of Frobenius.

(3) Let $f = q + \sum_{n\geq 2} a_n q^n$ be the q-expansion of a cuspidal Hecke eigenform $f \in S_k(N,\varepsilon)$, $k \geq 1$, $\varepsilon : (\mathbb{Z}/N)^\times \to \mathbb{C}^\times$.

Theorem 6. *(a) $E_f = \mathbb{Q}(a_n : n \geq 1)$ is a number field, with $a_n \in \mathcal{O}_{E_f}$ for all n.*

(b) (Eichler–Shimura, Deligne, Deligne–Serre) For all finite places λ of E_f (with E_λ the completion of λ and p the characteristic of k_λ) there exists an absolutely irreducible representation
$$\rho_{f,\lambda} : G_{\mathbb{Q},N\cup\{p,\infty\}} \to \mathrm{GL}_2(\bar{E}_\lambda)$$
and for all primes $\ell \nmid Np$, we have the relation that we just saw in Chris's talk:
$$\mathrm{cp}_{\rho_{f,\lambda}}(\mathrm{Frob}_\ell) = X^2 - a_\ell X + \varepsilon(\ell)\ell^{k-1}.$$

This characterizes the representation and maybe gives the main link to Galois representation.

Now, we want to study congruences. To do this, we first go from

- cusp forms that start life over the complex numbers on the upper half plane, to
- Fourier coefficients, that live over the integers.

(For simplicity, assume that nebentypus is trivial: $\varepsilon = 1$.) Let $S_k(N,\mathbb{Z})$ denote the set of all $f = \sum_{n\geq 1} a_n q^n$ such that $a_n \in \mathbb{Z}$ for all n.

Fact 7. *$S_k(N,\mathbb{Z})$ is a $\mathbb{Z}$-module of rank equal to $\dim_{\mathbb{C}} S_k(N)$.*

For any ring A, we have
$$\underline{S}_A = S_k(N,\mathbb{Z}) \otimes_{\mathbb{Z}} A \circlearrowright \mathbb{T}_A = \mathbb{T}(N,A).$$

Definition 8. For Hecke eigenforms $f = \sum a_n q^n$ and $g = b_n q^n \in S_k(N,\bar{\mathbb{Z}}_p)$, we say that $f \equiv g \pmod{p}$ if the following equivalent conditions hold:

- for all primes $\ell \nmid Np$, we have $a_\ell \equiv b_\ell \pmod{\mathfrak{m}_{\overline{\mathbb{Z}_p}}}$.
- $\rho_f \equiv \rho_g \pmod{\mathfrak{m}\bar{\mathbb{Z}}_p}$ as maps $G_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{F}}_p)$.

We pass to the same Hecke algebra. Let $\mathbb{T}'_A$ denote the subalgebra of $\mathbb{T}_A$ generated by T_ℓ for all $\ell \nmid N$. This is acted on by $\underline{S}_A$.

Fact 9. *We have bijections between the following:*

- *$\mathbb{T}'$-Hecke eigensystems of forms in $S_k(N)$.*
- $\mathrm{Hom}_{\mathbb{C}}(\mathbb{T}'_{\mathbb{C}},\mathbb{C})$.
- $\mathrm{Hom}_{\mathcal{O}}(\mathbb{T}'_{\mathcal{O}},\mathcal{O})$*, where we choose E large enough with $\mathbb{C} \supseteq \bar{\mathbb{Q}} \subseteq \bar{\mathbb{Q}}_p \supseteq E \supseteq \mathcal{O}$, where $\mathcal{O}$ always denotes the ring of integers of E.*

We also have a bijection between

- $\mathrm{Hom}_{\mathcal{O}}(\mathbb{T}_{\mathcal{O}},\mathbb{F})$*, and*

- *The set of $\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F})$ that are semisimple reductions from some ρ_f, with $f \in S_k(N)$.*

$\mathbb{T}'$ is a finite free $\mathcal{O}$-algebra. For any $\bar{\rho}$, we get a maximal ideal $\mathfrak{m}_{\bar{\rho}} \subseteq \mathbb{T}'_{\mathcal{O}}$. For a given $\bar{\rho}$, if we take

$$(\mathbb{T}'_{\mathcal{O}})_{\mathfrak{m}_{\bar{\rho}}},$$

then this is the relevant Hecke algebra for understanding the forms congruent to $\bar{\rho}$.

Theorem 10 (Carayol, Serre)**.** *Assume that $\bar{\rho}$ is absolutely irreducible. Then there exists a continuous representation*

$$\rho_{\bar{\rho}}^{\mathrm{mod}} : G_{\mathbb{Q},N\cup\{p,\infty\}} \to \mathrm{GL}_2\left((\mathbb{T}'_0)_{\mathfrak{m}_{\bar{\rho}}}\right) \tag{1}$$

"built" from the ρ_f, for $f \in S_k(N, \bar{\mathbb{Z}}_p)$, with $\rho_f \equiv \bar{\rho}$ modulo $\mathfrak{m}_{\bar{\mathbb{Z}}_p}$.

(One can write down a characteristic polynomial, similar to the above.) Maybe one should also say that

$$(\mathbb{T}'_{\mathcal{O}})_{\mathfrak{m}_{\bar{\rho}}} \subseteq \prod_{f,\rho_f\equiv\bar{\rho}} \mathcal{O}, \tag{2}$$

where the left hand side is generated by all the

$$\{\mathrm{trace}\,\rho_f(\mathrm{Frob}_\ell) : \rho_f \equiv \bar{\rho}, \ell \nmid Np\}.$$

Now, is the inclusion (2) strict? If you take twice the same form, then you get twice the same value.

Vision of Mazur? Can $\rho_{\bar{\rho}}^{\mathrm{mod}}$ be characterized purely in terms of "Galois" theory, maybe at least once $\bar{\rho}$ is given? You need to start somewhere. Start with the mod p representation. Then there's a sort of p-adic representation (1) that you get here, which sees all forms congruent to $\bar{\rho}$. Can you see this sort of thing from a purely Galois-theoretic perspective? This might have been the starting point for the study of deformations of Galois representations. Mazur maybe had one example in mind: Hida had just written down his Hida families, which are much bigger than things of fixed weight and level.

Let's now turn to *deformation functors*. In many ways, what we're doing now at the beginning is very formal, and maybe in the next lecture it gets a bit more Galois-theoretic. Let G be a profinite group – think of some global Galois group. Let $E \supseteq \mathcal{O} \to \mathbb{F}$ be a local field, with uniformizer π and residue field cardinality q. In what natural category do these $\mathcal{O}$-algebras $\mathbb{T}'_{\mathcal{O}}$ live?

Definition 11. $\mathrm{CNL}_{\mathcal{O}}$ is the category of complete noetherian $\mathcal{O}$-algebras $(A, \mathfrak{m}_A)$ with residue field $\mathbb{F}$ and with local homomorphisms.

Typical rings: $\mathcal{O}[\![X_1, \ldots, X_r]\!]/I$. Some structure theorem tells you that this is all you can get. There is a finite subcategory

$$\mathrm{Ar}_{\mathcal{O}} \subseteq \mathrm{CNL}_{\mathcal{O}}$$

consisting of Artin objects.

Question 12. For $\bar{\rho} : G \to \mathrm{GL}_n(\mathbb{F})$, when is the functor

$$D_{\bar{\rho}} : \mathrm{CNL}_{\mathcal{O}} \to \mathrm{Set}$$
$$(A, \mathfrak{m}_A) \mapsto \{\rho_A : G \to \mathrm{GL}_n(A) \mid \rho \mod \mathfrak{m}_A \equiv \bar{\rho}\} / \sim$$

representable by $R_{\bar{\rho}} \in \mathrm{CNL}_{\mathcal{O}}$?

To fill in some terminology:

Definition 13. (a) For $A \in \mathrm{CNL}_{\mathcal{O}}$, set

$$F_A := \mathrm{Hom}_{\mathrm{CNL}_{\mathcal{O}}}(A, \bullet) : \mathrm{CNL}_{\mathcal{O}} \to \mathrm{Set}.$$

(b) Say that a functor $F : \mathrm{CNL}_{\mathcal{O}} \to \mathrm{Set}$ is
  (i) *representable* if there exists $A \in \mathrm{CNL}_{\mathcal{O}}$ such that $F \cong F_A$, and
  (ii) *continuous* if for all $(A, \mathfrak{m}_A) \in \mathrm{CNL}_{\mathcal{O}}$, the map $F(A) \to \lim_n F(A/\mathfrak{m}_A^n)$ is an isomorphism.

Exercise 2. (a) The fiber product of the diagram Δ given by

$$\begin{array}{ccc} & & B \\ & & \downarrow{\scriptstyle \psi} \\ A & \xrightarrow{\varphi} & C \end{array}$$

inside $\mathrm{Ar}_{\mathcal{O}}$ is

$$\{(a, b) \in A \times B \mid \varphi(a) \equiv \psi(b)\}.$$

(b) $\mathrm{CNL}_{\mathcal{O}}$ "has no fiber products".

Exercise 3. Suppose $F = F_A$ for $A \in \mathrm{CNL}_{\mathcal{O}}$. Then

(a) $F(\mathbb{F}) = \{*\}$, and F is continuous.
(b) The Mayer–Vietoris property (MV) holds for F, i.e., for all diagrams Δ, the induced map $(*)_\Delta$ is bijective, where

$$(*)_\Delta : F(A \times_C B) \to F(A) \times_{F(C)} F(B),$$

where on the right hand side, we take the fiber product in Set.

Notation 14.
- $\mathbb{F}[\varepsilon] := \mathbb{F}[X]/(X^2)$.
- Call $\varphi : A \twoheadrightarrow A'$ in $\mathrm{CNL}_{\mathcal{O}}$ *small* if $\mathfrak{m}_{A'} \cdot (\ker(\varphi)) = 0$. (e.g., $\mathbb{F}[\varepsilon] \to \mathbb{F}$)
- For $F : \mathrm{CNL}_{\mathcal{O}} \to \mathrm{Set}$, define the $T_F := F(\mathbb{F}[\varepsilon])$, the *tangent space* of F.

You can translate this back into rings. Here are some more exercises:

Exercise 4. If the functor F satisfies

- $F(\mathbb{F}) = \{*\}$, and
- $(*)_{T_F} : F(\mathbb{F}[\varepsilon] \times_{\mathbb{F}} \mathbb{F}[\varepsilon]) \to T_F \times T_F$ is bijective,

then T_F is an $\mathbb{F}$-vector space.

Example 15. For $F = F_A$, we have

$$T_F = \mathrm{Hom}_{\mathrm{CNL}_{\mathcal{O}}}(A, \mathbb{F}[\varepsilon]) = \mathrm{Hom}_{\mathbb{F}}\left(\mathfrak{m}_A/(\mathfrak{m}_A^2, \pi), \mathbb{F}\right) =: T_A.$$

Exercise 5. For $\varphi : A \to B$ in $\mathrm{CNL}_{\mathcal{O}}$, the map φ is surjective if and only if $T_\varphi : T_B \to T_A$ is injective.

Theorem 16 (Grothendieck)**.** *Suppose $F : \mathrm{CNL}_{\mathcal{O}} \to \mathrm{Set}$ is continuous, satisfies $F(\mathbb{F}) = \{*\}$, the MV-property holds, and $\dim_{\mathbb{F}} T_F < \infty$. Then F is representable.*

Remark 17. For this last theorem, there are simplifications by Schlessinger, *Functors of Artin rings*. Schlessinger realized that these axioms of Grothendieck may be hard to verify in concrete situations, so he gave a simple (but somewhat long) list of axioms to verify. See Mazur '87, and Gouvêa's survey.

Let's now turn to *Galois deformations functors*. We have our usual

$$\bar{\rho} : G \to \mathrm{GL}_n(\mathbb{F}).$$

We can do something about the conjugation.

$$\Gamma_n(A) := \ker\left(\mathrm{GL}_n(A) \to \mathrm{GL}_n(\mathbb{F})\right).$$

We define

$$D^{\square}_{\bar{\rho}},\ D_{\bar{\rho}} : \mathrm{CNL}_{\mathcal{O}} \to \mathrm{Set},$$

$$(A, \mathfrak{m}_A) \mapsto \{\rho_A : G \to \mathrm{GL}_n(A) \mid \rho_A \equiv \bar{\rho} \mod \mathfrak{m}_A\}$$

("lifting functor" or "framed deformation functor"), and where for $D_{\bar{\rho}}$, we take things modulo $\Gamma_n(A)$-conjugacy.

Theorem 18. *Suppose Φ_ρ holds, i.e., $\#\operatorname{Hom}(G, \mathbb{F}_p) < \infty$. Then:*

(a) $D_{\bar{\rho}}$ always has a "hull".
(b) If $\operatorname{End}_G(\bar{\rho}) = \mathbb{F}$, then $D_{\bar{\rho}}$ is representable (uses Schlessinger). This gives rise to $R_{\bar{\rho}}$.
(c) (Always) $D^{\square}_{\bar{\rho}}$ is representable (Kisin, Magid–Lubokliy). Gives rise to $R^{\square}_{\bar{\rho}}$.

Here (c) is an exercise you can do.

Part 1. Chris Skinner's lectures

Integral representations, Euler systems, and multiplicity one.

My choice of these topics is motivated by my interest in special values of L-functions, and in particular problems like the BSD conjecture. We'll focus on some representation theory, that plays a role in both the analytic and the algebraic sides of these problems. You can possibly view this as a bridge between the talks at the start and at the end of the week.

Let's start by talking about *integral representations*. It's helpful to think

$$L\text{-function} = \int_{\text{symmetric space } X} (\text{automorphic form}),$$

where perhaps the automorphic form starts on some larger symmetric space $Y \supseteq X$. This is useful because it's our main tool for studying L-functions.

The next part of my title is *Euler systems*. This is going to seem like something different. What are Euler systems? One starts off with a continuous action

$$G_k = \mathrm{Gal}(\bar{k}/k) \circlearrowright V,$$

where V is a $\mathbb{Q}_p$-space of finite dimension (with $\mathbb{Q}_p$ acting linearly and continuously). At least conjecturally, there's a fairly general framework for producing such V from automorphic forms or representations. This Galois representation captures something about the automorphic form that can be expressed in terms of the L-function. All of these things are thus related to one another, even if they are frequently encountered separately. Here V often stabilizes in a $\mathbb{Z}_p$-submodule (lattice), which might yield a good exercise for later. An Euler system is a collection of classes in Galois cohomology $c_F \in H^1(F, T)$, where F/k are certain abelian extensions of k satisfying certain compatibilities: for $F' \supseteq F$,

$$\mathrm{cores}_{F'/F}(c_{F'}) =? c_F,$$

where ? often seems the local Euler factors of V (or some L-function attached to V, depending upon the setting).

Both of these settings have been useful for exploring special values of L-functions (Kolyvagin, Gross–Zagier, ...). What we'll focus on in these lectures is the role that multiplicity one plays in seeing these L-functions and in producing these Euler systems. We'll see that they essentially play the same role, which is further evidence for what people say, to the effect that Euler systems are some sort of algebraic incarnation of L-functions.

What do we mean by "multiplicity one"? One frequently encounters this term in the theory of automorphic forms, in various guises:

(1) Uniqueness of a representation in some space of functions, e.g.:
   (a) A cuspidal automorphic representation of GL_2 shows up with multiplicity one $L^2(\mathrm{GL}_2(k)\backslash\mathrm{GL}_2(\mathbb{A}_k))$.
   (b) Uniqueness of (local) Whittaker models for GL_2.

(2) Uniqueness of some (invariant) linear functional: for $H \leq G$ and π a representation of G,
$$\dim \mathrm{Hom}_H(\pi, \mathbb{C}) \leq 1.$$
   Or, for σ a representation of H, as the assertion that $\dim \mathrm{Hom}_H(\pi, \sigma) \leq 1$.

The first examples can be understood in terms of the latter. The latter will be a useful framework for us.

Let's now turn to integral representations and give some examples. The first integral representation we see is that of the Riemann zeta function. Let
$$\psi(t) = \sum_{n=1}^{\infty} e^{-\pi n^2 t}. \tag{3}$$
Then for $\Re s$ sufficiently large,
$$\int_0^{\infty} \psi(t) t^{\frac{1}{2}s-1}\, dt = \pi^{-s/2}\Gamma(\tfrac{s}{2})\zeta(s). \tag{4}$$
We see this by bringing the summation outside the integral. This gives a Mellin transform.

What's the automorphic side of this? If we look at, for $\tau = x + iy$,
$$\theta(\tau) = \sum_{n\in\mathbb{Z}} e^{-2\pi i n^2 \tau}.$$
This is an automorphic form, and we have
$$(\tfrac{1}{2}(\theta(iy) - 1)) = \psi(2y),$$
so (4) is an integral representation for the Riemann zeta function coming from the symmetric space for a torus embedded inside GL_2. One has similar integral representations for the Dirichlet L-functions. (No multiplicity one that we can see thus far.)

This gets souped up in the work of Hecke and Iwasawa–Tate, which inspired how automorphic L-functions have been studied subsequently. Let's recall how that goes. Let k be a number field. We have the adeles $\mathbb{A}_k$ and the ideles $\mathbb{A}_k^\times$. We have a Hecke character
$$\chi : k^\times\backslash\mathbb{A}_k^\times \to \mathbb{C}^\times,$$
which factors as a product $\chi = \prod \chi_v$ of characters $\chi_v : k_v^\times \to \mathbb{C}^\times$ indexed by the places v of k. (This is of course very useful, but is specific for GL_1, and so obscures

some of the more general features.) Let $\phi \in \mathcal{S}(\mathbb{A})$ be a Schwartz function, which could also be a product $\phi = \prod \phi_v$ of local Schwartz functions $\phi_v \in \mathcal{S}(k_v)$. We recall that this means that

- when v is finite, ϕ_v is smooth and compactly-supported, and
- when v is archimedean, all derivatives decay faster than any polynomial, e.g., $e^{-\pi t^2}$.

Furthermore, $\phi_v = 1_{\mathcal{O}_{k_v}}$ for almost all finite v. We then form

$$\theta(x) = \sum_{\alpha \in k} \phi(\alpha x).$$

(It's a good exercise to see how to specialize this to obtain something like (3).) We then form the integral

$$\int_{k^\times \backslash \mathbb{A}_k^\times} \chi(x)|x|^s \theta(x)\, d^\times x.$$

These integrals converge absolutely for $\Re s$ sufficiently large and unfold in the usual way, giving (at least for χ not a power of the absolute value, so that we don't need to worry about the contribution of $\alpha = 0$)

$$\int_{\mathbb{A}_k^\times} \chi(x)|x|^s \phi(x)\, dx.$$

If $\phi = \prod \phi_v$, then these factor further as

$$\prod \int_{k_v^\times} \chi_v(x)|x|_v^s \phi_v(x)\, dx. \tag{5}$$

One can show that the local integrals at non-archimedean places are rational functions, form the greatest common divisor of their denominators, and this turns out to be the way you can define the local L-function. This is Tate's thesis. We haven't yet really made any reference to multiplicity one. This shows up when you try to generalize to other settings.

We may think of $\mathbb{A}_k^\times$ as $\mathrm{GL}_1(\mathbb{A}_k)$. Let's now consider $\mathrm{GL}_n(\mathbb{A}_k)$. We discuss Godement–Jacquet theory, which is a generalization of what Tate did to GL_n. Let π be a cuspidal automorphic representation (by convention, irreducible). Abstractly, this is isomorphic to a restricted tensor product $\otimes \pi_v$ of irreducible local representations π_v of $\mathrm{GL}_n(k_v)$. We can thus identify an element $\varphi \in \pi$ with a sum of tensor products of vectors (although, unlike in the case of characters, it will not pointwise be a product of local functions). Now, mimicking what was done before, we take a Schwartz function $\phi \in \mathcal{S}(M_n(\mathbb{A}_k))$, and form a theta function

$$\theta(x) = \sum_{\alpha \in M_n(k)} \phi(\alpha x).$$

We then form

$$\int_{\mathrm{GL}_n(k)\backslash \mathrm{GL}_n(\mathbb{A}_k)} \varphi(x)|\det(x)|\theta(x)\, d^\times x.$$

This unfolds to

$$\int_{\mathrm{GL}_n(\mathbb{A})} \varphi(x)|\det x|^s \phi(x)\, d^\times x.$$

But does it factor? Not obviously.

Let's now form

$$\theta(h,g) = \sum_{\alpha \in M_n(k)} \phi(h^{-1}xg)$$

and consider

$$\int_{[\mathrm{GL}_n]} \varphi(g)|\det g|^s \theta(h,g)\, dg.$$

This is now automorphic as a function of h, so we can decompose it with respect to the automorphic spectrum. To compute the coefficients in that decomposition, we consider, for $\tilde{\varphi}$ in the contragredient (or dual) $\tilde{\pi}$ of π, the iterated integral

$$\int_{[\mathrm{GL}_n^1]} \left(\int_{[\mathrm{GL}_n]} \varphi(g)|\det g|^s \theta(h,g)\, dg \right) \tilde{\varphi}(h)\, dh,$$

where GL_n^1 means either that we mod out by the center or that we restrict to $|\det| = 1$. Then, reordering terms and unfolding, we obtain

$$\int_{\mathrm{GL}_n(\mathbb{A})} \phi(g)|\det g|^s \left(\int_{[\mathrm{GL}_n^1]} \tilde{\varphi}(h)\varphi(hg)\, dh \right) dg.$$

We can understand the parenthetical inner integral as

$$\langle \tilde{\varphi}, \pi(g)\varphi \rangle,$$

where

$$\langle \varphi_1, \varphi_2 \rangle = \int_{[\mathrm{GL}_n^1]} \varphi_1(h)\varphi_2(h)\, dh.$$

This pairing defines a G-invariant functional $\langle , \rangle : \tilde{\pi} \times \pi \to \mathbb{C}$, which is locally unique, hence factors as a product of local invariant functionals $\langle , \rangle_v : \tilde{\pi}_v \times \pi_v \to \mathbb{C}$, thus

$$\langle , \rangle = (*) \prod_v \langle , \rangle_v.$$

The leading constant $(*)$ will depend upon our normalizations of the local and global integrals, and our normalization of the comparison between π and $\otimes \pi_v$.

This is the first example where multiplicity one shows up in what we've discussed. In the afternoon talk, we'll very quickly describe a few other automorphic L-function settings where we see multiplicity one, and then start to move to the Euler system side of things.

Afternoon talk.

Factoring the integral is only one step towards understanding the L-functions. The next thing one needs to do is to compute these local integrals. This of course seems more tractable than working globally, which is the point. For instance, in the Iwasawa–Tate setting, when all of the data is unramified (meaning χ_v is an unramified character and ϕ_v is the characteristic function of the ring of integers), then the local factor in (5) is easy to compute, and gives a local zeta function. This is more complicated in the Godement–Jacquet setting, but still doable. Then in the ramified situations, there is the question of how to choose good vectors so that one gets the L-function on the nose. This is useful for many of the applications that the speaker makes of these kinds of functions. In some settings it's still much of an art and there are lots of interesting questions.

Let's turn to Rankin–Selberg convolutions. We'll begin classically, say with holomorphic modular eigenforms f and g of weights $k_f \geq k_g$, say of level 1, i.e., on $\mathrm{SL}_2(\mathbb{Z})$. Write

$$f = \sum a_n q^n, \qquad g = \sum b_n q^n.$$

We'll consider the Dirichlet series

$$\sum_n \overline{a_n} b_n n^{-s}. \tag{6}$$

The integral representation is

$$\int_{\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}} \overline{f(\tau)} g(\tau) E_k(\tau, s) y^{k_f} \, d\,\mathrm{vol}(\tau), \tag{7}$$

where $k := k_f - k_g$ and

$$E_k(\tau, s) := \sum_{\gamma \in \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \backslash \mathrm{SL}_2(\mathbb{Z})} j(\gamma, \tau)^{-k} |y(\gamma(\tau))|^k. \tag{8}$$

The way you get from (7) to (6) is to unfold the sum in (8) with the integral in (7), which yields an integral over $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \backslash \mathbb{H}$. This is a nice exercise if you haven't done it.

What does this have to do with multiplicity one? Maybe we try to set this up a bit more automorphically. Let π_1 and π_2 be cuspidal automorphic representations of $\mathrm{GL}_2(\mathbb{A}_k)$. Let χ_1, χ_2 be Hecke characters $\chi_i : k^\times \backslash \mathbb{A}_k^\times \to \mathbb{C}$ such that $\chi_1\chi_2 = (\chi_{\pi_1}\chi_{\pi_2})^{-1}$. Let $I_s(\chi_1, \chi_2)$ denote the space of functions $f : \mathrm{GL}_2(\mathbb{A}) \to \mathbb{C}$ that are smooth (meaning the usual thing at archimedean places and "fixed by an open subgroup" at finite places) and "K-finite" and satisfying

$$f_s\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} g\right) = \chi_1(a)\chi_2(d) \left|\frac{a}{d}\right|^{s+\frac{1}{2}} f_s(g).$$

We then define an Eisenstein series by averaging:

$$E(f_s, g) := \sum_{\gamma \in B(\mathbb{Q})\backslash \mathrm{GL}_2(\mathbb{Q})} f_s(\gamma g).$$

The Rankin–Selberg integral is now just the integral

$$\int_{[\mathrm{GL}_2]} \varphi_1(g)\varphi_2(g) E(f_s, g) \, dg.$$

We can unfold this to obtain

$$\int_{Z(\mathbb{A})B(\mathbb{Q})\backslash \mathrm{GL}_2(\mathbb{A})} \varphi_1(g)\varphi_2(g) f_s(g) \, dg.$$

Let's replace φ_i by its Whittaker expansion

$$\varphi_1(g) = \sum_{a \in k^\times} W_\psi\left(\begin{pmatrix} a & \\ & 1 \end{pmatrix} g\right).$$

Then, unfolding a bit further, we arrive at

$$\int_{Z(\mathbb{A})N(\mathbb{A})\backslash \mathrm{GL}_2(\mathbb{A})} W_\psi(g)\varphi_2(g) f_s(g) \, dg = \int_{Z(\mathbb{A})N(\mathbb{A})\backslash \mathrm{GL}_2(\mathbb{A})} W_\psi(g) W'_{\bar{\psi}}(g) f_s(g) \, dg,$$

where W'_ψ is the Whittaker function for φ_2 with respect to the conjugate character. This last integrand is a product of local functions, so the integral factors, assuming that all vectors in our representations are pure tensors.

Where's the multiplicity one? It's hidden, because, just like in the case of GL_1 characters, we have taken for one of our automorphic forms something particularly special, namely an Eisenstein series. The picture that might be better is, to give something slightly more complicated, there's something called the **triple product integral**. Now we'll take $\varphi_i \in \pi_i$ for $i = 1, 2, 3$, where it'll be slightly simpler to assume that at least one is cuspidal. Look at the function

$$\int_{[Z\backslash \mathrm{GL}_2]} \varphi_1(g)\varphi_2(g)\varphi_3(g)\, dg.$$

This integral defines a trilinear form on the product of the three representations that is invariant by the diagonal action of $\mathrm{GL}_2(\mathbb{A})$, or equivalently, a $\mathrm{GL}_2(\mathbb{A})$-invariant functional Λ on the tensor product $\pi_1 \otimes \pi_2 \otimes \pi_3$, i.e, an element

$$\Lambda \in \mathrm{Hom}_{\mathrm{GL}_2(\mathbb{A})}(\pi_1 \otimes \pi_2 \otimes \pi_3, \mathbb{C}).$$

This space is one-dimensional, as are its local avatars:

$$\dim \mathrm{Hom}_{\mathrm{GL}_2(k_v)}(\pi_{1,v} \otimes \pi_{2,v} \otimes \pi_{3,v}) \leq 1.$$

We can thus factor $\Lambda = \prod \Lambda_v$, where each $\Lambda_v \in \mathrm{Hom}_{\mathrm{GL}_2(k_v)}(\pi_{1,v} \otimes \pi_{2,v} \otimes \pi_{3,v})$. Suppose v is a place for which $\pi_{i,v}$ is unramified for each i. Then we can take

$$\Lambda_v = \int_{ZN(k_v)\backslash \mathrm{GL}_2(k_v)} W_{\psi_v} W_{\overline{\psi_v}}(g) f_v(g)\, dg.$$

Here, locally, we're realizing the unramified representation $\pi_{3,v}$ as an induced representation $\pi_{3,v} = \pi_v(\chi_{1,v}, \chi_{2,v})$. We didn't unfold to this computation; this was all local.

There's one more example we'd like to emphasize: *toric integrals*. Let K/k be a quadratic extension. We can then think of K as a two-dimensional k-space, which gives a way to identify

$$\mathrm{GL}_2/k \cong \mathrm{Aut}_k(K) \hookleftarrow K^\times.$$

We might for simplicity that π is a cuspidal automorphic representation of $\mathrm{GL}_2(\mathbb{A}_k)$, and let $\varphi \in \pi$ be a cusp form. Let $\chi : K^\times \backslash \mathbb{A}_K^\times \to \mathbb{C}^\times$ be a Hecke character for our extension. Let's assume that $\chi\,|_{\mathbb{A}_k^\times} = \chi_\pi^{-1}$, i.e., the restriction is the inverse of the central character. We are then going to think of the integral

$$\int_{\mathbb{A}_k^\times K^\times \backslash \mathbb{A}_K^\times} \varphi(t)\chi(t)\, d^\times t$$

as defining an element of the space $\mathrm{Hom}_{\mathbb{A}_k^\times}(\pi, \mathbb{C}(\chi^{-1}))$, which has dimensional ≤ 1. Such integrals will thus factor as prodcuts of local linear functionals.

Some of these can be computed quickly in terms of integrals we already know. Suppose π_v is unramified and v splits in K/k. Then

$$K_v^\times = k_v^\times \times k_v^\times \cong \left\{ \begin{pmatrix} a & \\ & b \end{pmatrix} \right\} \subseteq \mathrm{GL}_2(k).$$

We may thus identify χ_v with a pair of characters $(\chi_{1,v}, \chi_{2,v})$. We can define the local functional

$$\int_{k_v^\times} W_\psi \begin{pmatrix} t & \\ & 1 \end{pmatrix} \chi_{1,v}(t)\, d^\times t,$$

which defines an element of $\mathrm{Hom}_{K_v^\times}(\pi_v, \mathbb{C}(\chi_v^{-1}))$. For unramified data, this evaluates to $L(\pi_v, \chi_{1,v})$. It turns out that (Waldspurger's formula)

$$\left| \int \varphi(t)\chi(t)\, d^\times y \right|^2 \sim L(\mathrm{BC}_{K/k}(\pi) \otimes \chi, \tfrac{1}{2}).$$

There's a similar relation in the triple product case, which we can guess using the Rankin–Selberg unfolding that we saw earlier.

Remark 19. This doesn't make sense for general arguments other than $s = \frac{1}{2}$, except in some form when φ is an Eisenstein series ("formula of Damerell"). One needs to be able to vary φ (or χ) in a family, preserving the central character compatibility condition.

¡++¿

All of these examples are special cases of the Gan–Gross–Prasad conjectures, which we'll hear more about later in the week.

We'll now begin by giving one example of an Euler system. Tomorrow, we'll explore this in greater generality and more detail. The simplest case is that of cyclotomic units. Let F be a number field or a local field. Kummer theory gives an isomorphism

$$F^\times / F^{\times N} \to H^1(F, \mu_N),$$

as follows. Let $\alpha \in F^\times$. Choose an nth root $\alpha^{1/N}$. The ambiguity in this choice is an element of μ_N, i.e., an nth root of unity. For any $\sigma \in G_F$, we can look at $\sigma(\alpha^{1/N})/\alpha^{1/N}$. Since the numerator and denominator are both Nth roots of 1, the ratio must lie in μ_N. This gives us a way of constructing elements of H^1 very concretely. The classes we obtain are unramified away from $N\alpha$.

Let's now restrict ourselves to the field $\mathbb{Q}[\mu_N]$. Restrict the above map to the unit group of that field:

$$\mathcal{O}^\times_{\mathbb{Q}[\mu_N]} \to H^1(\mathbb{Q}(\mu_N), \mu_{p^n}).$$

Taking inverse limits, we obtain, with $\mathbb{Z}_p(1) = \varprojlim \mu_{p^n}$ (where the Galois group acts via the cyclotomic character), a map

$$\mathcal{O}^\times_{\mathbb{Q}[\mu_N]} \otimes \mathbb{Z}_p \to H^1(\mathbb{Q}(\mu_N), \mathbb{Z}_p(1)).$$

Thus, for any $(a, N) = 1$, we get , say with $\zeta_N = e^{2\pi i/N}$,

$$\frac{\zeta_N^a - 1}{\zeta_N - 1} \mapsto z_N,$$

say. If we look at the corestriction

$$\mathrm{cores}_{\mathbb{Q}[\mu_{N\ell}]/\mathbb{Q}[\mu_N]}(z_{N\ell}) = \begin{cases} z_N & \text{if } \ell \mid N \\ (1 - \mathrm{Fr}_\ell^{-1}) z_N & \text{if } \ell \nmid N. \end{cases}$$

We look at

$$\det\left(1 - \mathrm{Fr}_\ell^{-1} X \mid \mathbb{Z}_p(1)^*\right) \mid X = \mathrm{Fr}_\ell^{-1}.$$

Some idea for checking this: $(\mathbb{Z}/\ell\mathbb{Z})^\times \subset (\mathbb{Z}/\ell N\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\mu_{N\ell})/\mathbb{Q})$, where the last map sends $a \mapsto \sigma_\alpha(\zeta_{N\ell}) = \zeta_{N\ell}^a$.

Remark 20. Given f a holomorphic modular form, say of weight 2, we have $\omega_f = f(\tau)\, d\tau \in H^0(X, \Omega^1_X) \subseteq H^1(X, \mathbb{C})$. Then $\|f\|^2 = \int_X \omega_f \wedge \overline{\omega_f}$.

Similarly, for $X \hookrightarrow X \times X \times X$, we get some particular values of the Rankin–Selberg convolution by looking at $\int_X \overline{\omega_f} \wedge \omega_g \wedge \omega_{E_k}$. Then from the rational structure on cohomology, one can get something like rational structure on the L-values.

Remark 21. Let's talk about the corestriction map in this setting. Abstractly, it's a map

$$H^1(\mathbb{Q}[\mu_{N\ell}], \mathbb{Z}_p(1)) \to H^1(\mathbb{Q}[\mu_N], \mathbb{Z}_p(1)).$$

How are we going to understand this? We could of course write it down at the level of cocycles, or something. But what's it's really doing is that if we restrict back, i.e., compose with the restriction map

$$H^1(\mathbb{Q}[\mu_N], \mathbb{Z}_p(1)) \to H^1(\mathbb{Q}[\mu_{N\ell}], \mathbb{Z}_p(1)), \tag{9}$$

then the composition is just the trace map, given by

$$\sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}[\mu_{N\ell}]/\mathbb{Q}[\mu_N])} \sigma.$$

The restriction map (9) is actually an injection because there are no Galois invariants of $\mathbb{Z}_p(1)$.

Also, we have the Kummer map

$$\mathbb{Q}[\mu_{N\ell}]^\times \xrightarrow{\text{Kummer}} H^1(\mathbb{Q}[\mu_{N\ell}], \mathbb{Z}_p(1)).$$

And this construction is Galois-invariant. We have the trace map $\alpha \mapsto \prod_\sigma \sigma(\alpha)$ from $\mathbb{Q}[\mu_{N\ell}]^\times \to \mathbb{Q}[\mu_N]^\times$. We claim that this induces the corestriction map via the Kummer map. This remains the case when we tensor with $\mathbb{Z}_p$.

So when we're dealing with corestriction, what we really want to understand is what is the norm of the particular α that we're working with.

All of this is fairly formal applied to a specific setting. The Kummer map is also a connecting map in a long exact sequence of Galois cohomology, associated to

$$0 \to \mu_{p^n} \to \bar{F}^\times \xrightarrow{\alpha \mapsto \alpha^{p^n}} \bar{F}^\times \to 0.$$

From the formal stuff, we have an arithmetic question. We take

$$\alpha = \frac{\zeta_{N\ell}^a - 1}{\zeta_{N\ell} - 1},$$

and we want to know, what is the norm of this element? Look at

$$\mathrm{norm}_{\mathbb{Q}(\mu_{N\ell})/\mathbb{Q}(\mu_N)}(\alpha).$$

We have

$$\mathrm{Gal}(\mathbb{Q}(\mu_{N\ell})/\mathbb{Q}(\mu_N)) \subseteq \mathrm{Gal}(\mathbb{Q}(\mu_{N\ell})/\mathbb{Q}) \cong (\mathbb{Z}/N\ell)^\times,$$

The subgroup here will be identified with congruence classes b satisfying $b \equiv 1 \pmod N$. The last isomorphism is given by $\sigma_c \mapsto c$, where $\sigma_c(\zeta_{N\ell}) = \zeta_{N\ell}^c$. Now, suppose for instance that $\ell \nmid N$. Then $\zeta_{N\ell}^{b\ell} = \zeta_N^b = \zeta_N$. As $b \in (\mathbb{Z}/N\ell)^\times$ runs over $\ell - 1$ residue classes modulo $\equiv 1 \pmod N$, then $\zeta_{N\ell}^b$ runs over ℓth roots of ζ_N, but excluding $\zeta_N^{\ell^{-1}}$. A short calculation then gives the claim corestriction formula. In the other case where $\ell \mid N$, b runs over ℓ classes, and we get the other answer.

We're going to continue our discussion of Euler systems. We turn to the example given by Heegner points. Let $K/\mathbb{Q}$ be an imaginary quadratic field, with ring of integers $\mathcal{O}_K$. Let N be a positive integer such that all primes $\ell \mid N$ split in $K/\mathbb{Q}$. We take

$$X_0(N) = \Gamma_0(N)\backslash[\mathfrak{h} \sqcup \mathbb{P}^1(\mathbb{Q})],$$

and write $\tau \in \mathfrak{h}$. This classifies elliptic curves together with an isogeny of order N, e.g.,

$$E := \mathbb{C}/\mathbb{Z} \oplus \mathbb{Z}\tau \to E' := \mathbb{C}/\tfrac{1}{N}(\mathbb{Z} + N\tau\mathbb{Z}) \cong \mathbb{C}/\mathbb{Z} + N\tau\mathbb{Z},$$

whose kernel is $\frac{1}{N}\mathbb{Z}/\mathbb{Z}$.

We're going to produce some points on $X_0(N)$. Let c be positive integer. We can have an order

$$\mathcal{O}_c := \mathbb{Z} + c\mathcal{O}_K \subseteq \mathcal{O}_K.$$

This gives us a lattice inside the complex numbers (having chosen a complex embedding of K). We can then form the quotient $\mathbb{C}/\mathcal{O}_c$. To produce a lattice that is slightly larger, we will use that each $\ell \mid N$ splits to *choose* an ideal $\mathfrak{n} \subseteq \mathcal{O}_K$ such that $\mathcal{O}_K/\mathfrak{n} \cong \mathbb{Z}/N\mathbb{Z}$. We then obtain an isogeny of elliptic curves

$$\left[\mathbb{C}/\mathcal{O}_c \to \mathbb{C}/\mathfrak{n}^{-1}\mathcal{O}_c\right] \in X_0(N)(K[c]),$$

where $K[c]$ denotes the *ring class field* of K of conductor c. To explain what this means, we introduce some notation. For a module M, write $\hat{M} := M \otimes \hat{\mathbb{Z}}$, where $\hat{\mathbb{Z}} = \prod_\ell \mathbb{Z}_\ell$. (For instance, if M is a $\mathbb{Q}$-module, then we may also write $\hat{M}$ as $M \otimes_{\mathbb{Q}} \mathbb{A}_f$.) Class field theory tells us that

$$\mathrm{Pic}(\mathcal{O}_c) = K^\times\backslash\hat{K}^\times/\hat{\mathcal{O}}_c^\times \xrightarrow{\mathrm{rec}} \mathrm{Gal}(K[c]/K),$$
$$[\mathfrak{b}] \mapsto \sigma_{\mathfrak{b}}.$$

More generally, for any fractional ideal $\mathfrak{a}$ of $\mathcal{O}_c$, we get a point

$$x_c(\mathfrak{a}) := \left[\mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{n}^{-1}\mathfrak{a}\right] \in X_0(N)(K[c]).$$

The action of $\mathrm{Gal}(K[c]/K)$ on $X_0(N)(K[c])$ on these points is described by the relation

$$\sigma_{\mathfrak{b}} x_c(\mathfrak{a}) = x_c(\mathfrak{b}^{-1}\mathfrak{a}). \tag{10}$$

This is the content of CM theory.

Now we're going to look at the divisors

$$y_c(\mathfrak{a}) := x_c(\mathfrak{a}) - \infty$$

obtained by subtracting off the cusp at infinity, which is defined over $\mathbb{Q}$. This difference defines an element of the Jacobian $J_0(N) := \mathrm{Jac}(X_0(N))$, defined over $K[c]$. The Jacobian is an abelian variety. For abelian varieties, there is a construction very similar to Kummer theory that gives us an analogue of the Kummer map defined yesterday,

$$J_0(N)(K[c]) \to H^1(K[c], J_0(N)[p^m]),$$

where $J_0(N)[p^m]$ is the p^m-torsion subgroup of the Jacobian. The map is defined as follows. Given $y \in J_0(N)(K[c])$, let us choose y' so that $p^m y' = y$. We send this to the class of the cocycle $\sigma \mapsto \sigma(y') - y'$. Applying this map to $y_c(\mathfrak{a})$ gives us a cohomology class

$$z_c(\mathfrak{a}) \in H^1(K[c], J_0(N)[p^m]).$$

In the special case where $\mathfrak{a} = \mathcal{O}_c$, we drop it from the notation and write simply z_c.

Suppose now that $\ell \nmid cD_K N$. Then we're going to look at what happens when we take the point $z_{c\ell}$ (attached as above to the order $\mathcal{O}_{c\ell}$) and form the norm

$$\sum_{\sigma \in \mathrm{Gal}(K[c\ell]/K[c])} \sigma z_{c\ell}.$$

We can write this as the sum

$$\sum_{\mathfrak{b} \in \ker(\mathrm{Pic}\,\mathcal{O}_{c\ell} \to \mathrm{Pic}\,\mathcal{O}_c)} \sigma_{\mathfrak{b}} z_{c\ell}.$$

We can in turn rewrite $\sigma_{\mathfrak{b}} z_{c\ell}$ as $\sum_{\mathfrak{b}} y_{c\ell}(\mathfrak{b}^{-1}) - \infty$, summing over the same $\mathfrak{b}$ as before. Now, how many $\mathfrak{b}$'s are there, and what is this sum?

Suppose that ℓ is inert in K. Comparing what happens with c and $c\ell$, we get

$$\frac{(\mathcal{O}_K \otimes \mathbb{Z}_\ell)^\times}{((\mathbb{Z} + \ell\mathcal{O}_K) \otimes \mathbb{Z}_\ell)^\times},$$

which is cyclic of order $\ell + 1$. Now, $\mathfrak{b}$ lying in the kernel of the above map means that $\mathfrak{b}\mathcal{O}_c$ is a principal ideal, say $\beta\mathcal{O}_c$ with $\beta \in K^\times$. If we look at $\beta\mathfrak{b}^{-1}\mathcal{O}_c$, then we see that inside $\mathcal{O}_c$, it has index ℓ. As $\mathfrak{b}$ varies, this exhausts all lattices of index ℓ. By definition of the Hecke operator T_ℓ, we see that

$$\sum_{\mathfrak{b}} \big(y_{c\ell}(\mathfrak{b}^{-1}) - \infty\big) = T_\ell(y_c - \infty).$$

Under the Kummer map, this tells us that

$$\mathrm{cor}_{K[c\ell]/K[c]}\, z_{c\ell} = T_\ell z_c.$$

Kolyvagin used these relations as follows.

$$y_K = \mathrm{trace}_{K[1]/K}\, y_1 \in J_0(N)(K) \xrightarrow{\phi_E} E(K),$$

where E is an elliptic curve of conductor N with a modular parametrization $\phi_N : X_0(N) \to E$ sending ∞ to 0. Using relations, Kolyvagin could show that if the point is not torsion, then the rank of the elliptic curve is 1. Around the same time, Gross–Zagier showed that the Néron–Tate height of this point is nonzero if and only if L-function for E/K vanishes exactly to order one. This gave some of the first theoretical evidence for the Birch and Swinnerton-Dyer conjecture. This was a spectacular application by Kolyvagin that got people interested in Euler systems.

You can also run Kolyvagin's argument in another way. You can look at the primes ℓ that are *split* in K, say $\ell = \lambda\bar{\lambda}$. Then

$$\frac{(\mathcal{O}_K \otimes \mathbb{Z}_\ell)^\times}{((\mathbb{Z} + \ell\mathcal{O}_K) \otimes \mathbb{Z}_\ell)^\times} = \frac{\mathcal{O}_\lambda^\times \times \mathcal{O}_{\bar{\lambda}}^\times}{\{(a,b) : a \equiv b(\ell)\}},$$

where the numerator is really $\mathbb{Z}_\ell^\times \times \mathbb{Z}_\ell^\times$. Arguing as above, we're no longer summing over all the lattices, but instead we miss two of them: $\lambda\mathcal{O}_c$ and $\bar{\lambda}\mathcal{O}_c$. One obtains

$$\sum_{\mathfrak{b}} (y_{c\ell}(\mathfrak{b}^{-1}) - \infty) = T_\ell(y_c - \infty) - (\mathrm{Fr}_\lambda^{-1} + \mathrm{Fr}_{\bar{\lambda}}^{-1})(y_c - \infty).$$

(The inverses come from (10).)

Work of the speaker and Jetchev and Wan used the split primes to do something like what Kolyvagin did.

Let $\mathfrak{c} = \lambda_1 \cdots \lambda_r$ be a squarefree product of ideals $\lambda_i \nmid ND_K$ of degree 1 in K, with $\lambda_i = \overline{\lambda_i}$. Let c be the integer such that $(c) = \mathfrak{c} \cap \mathbb{Z}$. Let $z(\mathfrak{c})$ be basically the class that we were just analyzing, but let's modify it slightly:

$$z(\mathfrak{c}) := \prod_{i=1}^{r} (-\mathrm{Fr}_{\lambda_i})\, z_c \in H^1(K[c], T_p J_0(N)), \tag{11}$$

where $T_p J_0(N) = \varprojlim J_0(N)[p^m]$. We obtain now, for $\lambda \mid \ell$,

$$\mathrm{cores}_{K[c\ell]/K[c]}\, z(\mathfrak{c}\lambda) = \left(\mathrm{Fr}_\lambda^{-2} - T_\ell \mathrm{Fr}_\lambda^{-1} + 1\right) z(\mathfrak{c}). \tag{12}$$

Let's think about this last expression in terms of the Hecke polynomial $X^2 - T_\ell X + \ell$. You can see that if we evaluate this at λ^{-1}, we almost get the quantity appearing on the right hand side of (12):

$$(X^2 - T_\ell X + \ell)\,|_{X = \mathrm{Fr}_\lambda^{-1}}\ .$$

They are congruent modulo $\ell - 1$, which is $N(\lambda) - 1$. When working with Euler systems, it's acceptable to work with congruences modulo $\ell - 1$. There's a general way to massage those classes so that they give the relations on the nose, but there's no need to do so. Later, we'll pose a question that will suggest that this comparison is a feature of some integral representation theory, once we see where these norm relations come from in those terms. In any event, once you have these relations, you can take these objects and run Kolyvagin's argument and reprove Kolyvagin's theorem.

We next want to explain how to set up the construction of the Kolyvagin system in such a way that some representation theory naturally shows up, with this Galois relation (12) showing up as something like a Hecke module, which in turn is closely related to representation theory. The argument we're going to give generalizes quite significantly, for instance, it produces an Euler system in the sense of these split primes for the diagonal cycles coming from the arithmetic Gan–Gross–Prasad settings, and one can generalize Kolyvagin's statement to a rank one statement about Selmer groups for certain Rankin–Selberg convolutions of $\mathrm{GL}_n \times \mathrm{GL}_{n+1}$. With Euler systems, we're trying to bound the orders of Selmer groups of elliptic curves, something like $H^1_f(\mathbb{Q}, E[p^N])$, where the subscript f denotes some sort of Block–Kato condition coming from the geometry of the elliptic curve. One way to bound a Selmer group like this is to use global duality to give classes in the arithmetic dual, i.e., $H^1_f(\mathbb{Q}, E[p^N]^*)$, where

$$E[p^N]^* = \mathrm{Hom}(E[p^N], \mathbb{Q}_p/\mathbb{Z}_p(1)). \tag{13}$$

Here one wants to allow ramification at good primes ℓ, chosen to capture the orders of classes that we want to control. One can then reduce to looking at

$$H^1_{\mathrm{ur}}(\mathbb{Q}_\ell, E[p^N]). \tag{14}$$

The local duality relates this to $H^1(I_\ell, E[p^N]^*)^{G_{\mathbb{Q}_\ell}}$. So if we can produce a class in the latter that is highly ramified (of large order), then we can force the class in (14) to have small order. That, in a nutshell, is how Selmer groups are bounded. The whole trick is to produce ramified classes in (13) that you can measure the size of in some way. Now, producing things that are provably ramified is a hard problem. There are few cases where we can do this. It's much easier to check that something is unramified (think of the criterion of Néron–Ogg–Shafarevich or

something like that). What Kolyvagin's argument does is, he says well, let's start off with classes (11) that are over ramified extensions. If they are truly over that ramified extension and not, say, defined over some extension with less ramification, then Kolyvagin can use that to produce ramified classes, and it is exactly these relations (12) that allow him to understand how ramified these classes actually are. These norm relations are thus crucial for producing ramified classes with controlled or measurable ramification. That's sort of the algebra background for why one is interested in Euler systems.

Tomorrow, we'll describe a more representation-theoretic picture that produces these Kolyvagin classes.

References