

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 $G^{\text{pf}} := \varprojlim G/N$, where N runs over the finite index subgroups.
- (b) If $G = \varprojlim G_i$ is profinite, then
 - (i) The abelianization is given by

$$G^{\text{ab}} = G/[G, G] = \varprojlim G_i^{\text{ab}},$$

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 $G_F := \text{Aut}_F(F^{\text{sep}}) = \text{Gal}(F^{\text{sep}}/F)$ profinite. Define the poset

$$\mathcal{I}_F := \{L \subseteq F^{\text{sep}} : L \supseteq F \text{ finite Galois}, \subseteq\}.$$

Then

$$G_F \xrightarrow{\cong} \varprojlim_{L \in \mathcal{I}_F} \text{Gal}(L/F).$$

- (b) Let $F' \subseteq F^{\text{sep}}$ be a normal extension of F . Then $G_{F'} \leq G_F$ is closed and normal. We may thus write

$$\text{Gal}(F'/F) \cong G_F/G_{F'} = \varprojlim_{\substack{L \in \mathcal{I}_F, \\ L \subseteq F'}} \text{Gal}(L/F).$$

- (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 $\text{Pl}_K = \text{Pl}_K^\infty \sqcup \text{Pl}_K^{\text{fin}}$ 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

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

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 $\text{char}(v)$ 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

$$1 \rightarrow I_v \rightarrow G_v := \text{Gal}_{K_v} \rightarrow \text{Gal}_{k_v} \rightarrow 1.$$

A topological generator for Gal_{k_v} is given by

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

We denote by $\text{Frob}_v \in G_v$ some lift of Fr_v .

We write $S_\infty := \text{Pl}_K^\infty$ 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 $W(\mathbb{F}) = \mathbb{Z}_q = \mathbb{Z}_p[\zeta_{q-1}]$.

Continuing the examples, which may serve as exercises:

- (d) Let ζ_t be a primitive t th root of 1. For k a finite field, we have $G_k \cong \hat{\mathbb{Z}} = \overline{\langle \text{Fr}_k \rangle}$, where $\text{Fr}_k : \alpha \mapsto \alpha^{|k|}$.
- (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 $E^\times \rightarrow G_E^{\text{ab}}$ is a continuous inclusion with dense image. Writing $E^\times = \pi_E^{\mathbb{Z}} \times \mathcal{O}_E^\times = \pi_E^{\mathbb{Z}} \times \mathbb{F}^\times \times \mathcal{U}_E$. Since the units are known to be a finitely generated \mathbb{Z}_p -module, we get as a corollary that

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

is finite.

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

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

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

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

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 $G_v \rightarrow G_{K,S}$ factors via the quotient $G_v/I_v \cong G_{k_v}$, so that $\text{Frob}_v \in G_{K,S}$ 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 Chenievr–Clozel). The structure of $G_{K,S}$ is unknown, but global class field theory describes $G_{K,S}^{\text{ab}}$. A corollary is that

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

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 $E^{\text{tame}}/E^{\text{unr}}/E$, where

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

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

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 $\rho : G \rightarrow \text{GL}_n(A)$, where G is a topological group, A is a topological ring, and ρ is a continuous map. The topology on $\text{GL}_n(A)$ 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 $\text{CNL}_{\mathcal{O}}$ (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 $\rho(G) \subseteq \text{GL}_n(E)$ up to conjugation.
- (c) If $A = E \supseteq \mathbb{Q}_p$ (finite extension), then after conjugation, we can assume that $\rho(G) \subseteq \text{GL}_n(\mathcal{O})$.

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

$$\bar{\rho}_{\Lambda} : G \rightarrow \text{GL}_n(\mathbb{F}).$$

Let's use the notation cp_{α} for the characteristic polynomial of $\alpha \in M_n(A)$.

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

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

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

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

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

$(\mathbb{Z}/p^n)^{\times} = \text{Aut}_{\mathbb{Z}}(\mathbb{Z}/p^n)$. **Facts:**

- $\chi_p^{\text{cyc}}|_{G_K}$: unramified outside $S_p \cup S_{\infty}$.
- $\chi_p^{\text{cyc}}(\text{Frob}_v) = q_v \in \mathbb{Z}_p^{\times}$.

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

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

Facts:

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

- 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.

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

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

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 ,

$$\dim \operatorname{Hom}_H(\pi, \mathbb{C}) \leq 1.$$

Or, for σ a representation of H , as the assertion that $\dim \operatorname{Hom}_H(\pi, \sigma) \leq 1$. 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

$$\psi(t) = \sum_{n=1}^{\infty} e^{-\pi n^2 t}. \quad (1)$$

Then for $\Re s$ sufficiently large,

$$\int_0^{\infty} \psi(t) t^{\frac{1}{2}s-1} dt = \pi^{-s/2} \Gamma\left(\frac{s}{2}\right) \zeta(s). \quad (2)$$

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

$$\left(\frac{1}{2}(\theta(iy) - 1)\right) = \psi(2y),$$

so (2) 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

$$\chi : k^\times \backslash \mathbb{A}_k^\times \rightarrow \mathbb{C}^\times,$$

which factors as a product $\chi = \prod \chi_v$ of characters $\chi_v : k_v^\times \rightarrow \mathbb{C}^\times$ 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 (1).) 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

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

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

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

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 $\langle, \rangle : \tilde{\pi} \times \pi \rightarrow \mathbb{C}$, which is locally unique, hence factors as a product of local invariant functionals $\langle, \rangle_v : \tilde{\pi}_v \times \pi_v \rightarrow \mathbb{C}$, 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.

REFERENCES