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

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

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

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

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 $r^{\text{ss}} : G \to \mathrm{GL}_n(\mathbb{F})$ such that $\mathrm{cp}_r = \mathrm{cp}_{r^{\text{ss}}}$ (Brauer–Hesbitt), where r^{ss} is unique up to isomorphism.*

(b) We have $\mathrm{cp}_\rho \in \mathcal{O}[X]$ and $\mathrm{cp}_{\overline{\rho}_\Lambda} \in \mathbb{F}[X]$, 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 $v \in \mathrm{Pl}_K^{\text{fin}} \setminus S$, we have*

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

References