

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

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

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:

- (1) 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 $v \mid p$.

- (2) 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:

Example 3. (d) Let ζ_t be a primitive t th root of 1. For k a finite field, we have $G_k \cong \hat{\mathbb{Z}} = \langle \overline{\text{Fr}_k} \rangle$, where $\text{Fr}_k : \alpha \mapsto \alpha^{|k|}$.

- (e) Let $E \supseteq \mathbb{Q}_p$ (finite extension). Then G_E (???–Wingberg for $p \geq 2$). Local class field theory: the Artin map $E^\times \rightarrow G_E^{ab}$ 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

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

is finite.

++++

REFERENCES