Aalto University

Galois Representations

Solved exercises - Part 1

The following problems are from Lecture 1 of Fernando Gouvêa's notes "Deformations of Galois Representations". These are the problems which were covered in the exercises sessions (some details are left for you). We also include some theoretical observations concerning absolute Galois groups and extension of valuations, Chebotarev's theorem and representations over profinite rings.

Problem 1.1.

Check the details in this construction. Specifically, show that many non-constant sequences $\{a_n\}$ exist and that the conditions defining ψ are indeed compatible.

Solution.

The construction mentioned in the statement is the one carried out in the example right above the problem, in Gouvêa's notes.

The goal is to show there exist many non-constant sequences of integers $\{a_n\}$ satisfying

$$a_n \equiv a_m \pmod{m} \tag{1}$$

whenever $m|n$.

We will show that any sequence in $\mathbb{Z}_p = \varprojlim_k \mathbb{Z}/p^k\mathbb{Z}$, the p-adic integers, can be used to construct a sequence $\{a_n\}$ satisfying (1). Since there are uncountably many p-adic integers (see Problem 1.2.), we get uncountably many sequences $\{a_n\}$.

Let p be a rational prime, $a_0 = 0$, $a_p \in \mathbb{Z}/p\mathbb{Z}$ and consider for every $k \geq 2$, $a_{p^k} \in \mathbb{Z}/p^k\mathbb{Z}$ such that

$$a_{p^{k+1}} \equiv a_{p^k} \pmod{p^k}. \tag{2}$$

In practice, due to the compatibility condition (2), we are considering the p-adic integer given by the sequence $\{a_{p^k}\}$. Note that the sequence $\{a_{p^k}\}$ is not enough for our purpose, since it only includes indices corresponding to p-powers. To "complete" the sequence, set $a_n = 0$ if $0 < n \leq p-1$, $a_n = a_p$ if $p \leq n \leq p^2 - 1$, $a_n = a_{p^2}$ if $p^2 \leq n \leq p^3 - 1$, and so on. In sum, let

$$a_n = \begin{cases} 0 & \text{if } 0 \leq n \leq p-1 \\ a_{p^k} & \text{if } p^k \leq n \leq p^{k+1} - 1 \, \forall k \geq 1. \end{cases}$$

The completed sequence looks like

$$(0, \ldots, 0, a_p, \ldots, a_p, a_{p^2}, \ldots, a_{p^2}, a_{p^3}, \ldots).$$

Let us check that this sequence satisfies condition (1). Consider non-negative integers m, n such that $m|n$. We consider four separate cases:

(i) Suppose both m and n are p-powers. Since $m|n$, $m = p^{k_1}$ and $n = p^{k_2}$ for some $k_1, k_2 \geq 1$ with $k_1 \leq k_2$. By construction of $\{a_n\}$ and condition (2), $a_n = a_{p^{k_2}} \equiv a_{p^{k_1}} \equiv a_m \pmod{m}$.

(ii) If n is a p-power but m is not, then m does not divide n, so we discard this case.

(iii) Suppose n is not a p-power but m is. Then $m = p^k$ for some $k \geq 1$ and $n = p^k v$ for some integer v which is not a p-power. In this case, $a_n = a_{p^k} = a_m$ and so $a_n \equiv a_m \pmod{m}$.

(iv) The case where n and m are not p-powers can be reduced to case (i). Check it.

It remains to verify that the conditions defining ψ are compatible with such a sequence $\{a_n\}$. Recall ψ is defined as the automorphism of $\mathbb{F} = \overline{\mathbb{F}_p}$ satisfying $\psi|_{\mathbb{F}_{p^n}} = \phi^{a_n}$ for every $n \geq 1$, where ϕ denotes the Frobenius automorphism. Note that $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ implies that $m|n$, which in turn implies that $a_n \equiv a_m \pmod{m}$ (by construction of $\{a_n\}$). Hence, $a_n = a_m + mt$ for some integer t. In that case, for every $x \in \mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$,

$$\begin{aligned}\phi^{a_n}(x) &= x^{p^{a_n}} = x^{p^{a_m+mt}} = x^{p^{a_m}p^{mt}} \\ &= (x^{p^{a_m}})^{p^{mt}} = x^{p^{a_m}} \\ &= \phi^{a_m}(x),\end{aligned}$$

which shows ψ is well-defined.

Problem 1.2.

How big is $G_{\mathbb{F}_p}$? For example, is it a countable set?

Solution.

We start by showing that $\mathbb{Z}_p$ is uncountable. Consider the map

$$\begin{aligned}\mathbb{Z}_p &\to [0,1] \\ \sum_{k\geq 0} a_k p^k &\mapsto \sum_{k\geq 1} a_k p^{-k}.\end{aligned}$$

This is well-defined since every element in $\mathbb{Z}_p$ has a unique p-adic expansion of the form $\sum_{k\geq 0} a_k p^k$ with $0 \leq a_k \leq p-1$. It is a surjective map, since for every $\alpha \in [0,1]$ with $\alpha = \sum_{k\geq 1} a_k p^{-k}$ (basis p expansion of α), $0 + \sum_{k\geq 1} a_k p^k$ is a p-adic integer mapping to α. Hence, since $[0,1]$ is uncountable, $\mathbb{Z}_p$ is also uncountable.

Now consider the map

$$\begin{aligned}\mathbb{Z}_p = \varprojlim_k \mathbb{Z}/p^k\mathbb{Z} &\to G_{\mathbb{F}_p} \\ \{a_{p^k}\} &\mapsto \psi,\end{aligned}$$

where ψ is given as in Problem 1.1. This map is injective (check it) and so since $\mathbb{Z}_p$ uncountable, $G_{\mathbb{F}_p}$ is also uncountable.

Problem 1.3.

Let F/K be an infinite Galois extension, and let G be the group of automorphisms of F which induce the identity on K. For each *finite* Galois subextension K'/K let $G(F/K')$ denote the normal subgroup of G consisting of all automorphisms which induce the identity on K'. Define a topology on G by defining a basis of neighborhoods of each $\sigma \in G$ to be the set of all cosets $\sigma G(F/K')$, where K' runs through all finite Galois extensions of K. Show that this yields the same group and the same topology as in the definition above.

Solution.

The "definition above" refers to Definition 1.1. Let us recall it. For each finite Galois subextension K'/K of an infinite Galois extension F/K, we consider the Galois group $G(K'/K)$ and, given two finite subextensions $K' \subseteq K''$, we consider the restriction homomorphism

$$\mathrm{Res}_{K',K''} : G(K''/K) \to G(K'/K). \tag{3}$$

This defines an inverse system of groups and we define the Galois group of F over K as

$$G(F/K) := \varprojlim_{K'/K} G(K'/K) \tag{4}$$

with the natural profinite topology.

The group G introduced in the problem statement is given by

$$G := \{\sigma \in \mathrm{Aut}(F) \mid \sigma|_K = \mathrm{id}\}, \tag{5}$$

with the topology given by the described basis of neighborhoods.

The purpose of the problem is to show that (i) $G \cong G(F/K)$ and (ii) the profinite topology over $G(F/K)$ coincides with the topology given by the basis of neighborhoods described in the statement.

(i) We have an explicit construction for the inverse limit (4) as a subset of the cartesian product containing the "coherent" sequences (see Problem 1.36.):

$$G(F/K) = \{(\sigma_{K'})_{K' \in I} \mid \mathrm{Res}_{K',K''}(\sigma_{K''}) = \sigma_{K'} \text{ whenever } K' \subseteq K''\},$$

where the index set I is the set of all finite Galois subextensions K' over K. Consider the map

$$\begin{aligned} \psi : G &\to G(F/K) \\ \sigma &\mapsto (\sigma|_{K'})_{K' \in I}. \end{aligned}$$

We will show that this is an isomorphism of groups, and hence $G \cong G(F/K)$.

First, note that for every $\sigma \in G$ and every finite Galois (and hence normal) subextension K'/K, $\sigma|_{K'}$ is an automorphism of K' which induces the identity on K. Moreover, normality of K'/K ensures that $\mathrm{Res}_{K',K''}(\sigma_{K''}) = \sigma_{K'}$ whenever $K' \subseteq K''$. So ψ has indeed values in $G(F/K)$. It is also clear that ψ is a well-defined group homomorphism. We check injectivity and surjectivity of ψ.

- Injectivity. Let $\sigma_1, \sigma_2 \in G$ such that $\psi(\sigma_1) = \psi(\sigma_2)$, that is, $\sigma_1|_{K'} = \sigma_2|_{K'}$ for every finite Galois subextension K'/K. For every $\alpha \in F$, there exists some finite Galois subextension K'/K such that $\alpha \in K'$. In that case,

  $$\sigma_1(\alpha) = \sigma_1|_{K'}(\alpha) = \sigma_2|_{K'}(\alpha) = \sigma_2(\alpha).$$

  This shows that $\sigma_1(\alpha) = \sigma_2(\alpha)$ for all $\alpha \in F$ and so $\sigma_1 = \sigma_2$.
- Surjectivity. Let $\overline{\sigma} = (\sigma_{K'})_{K' \in I}$ such that $\sigma_{K'} \in G(K'/K)$ and $\mathrm{Res}_{K',K''}(\sigma_{K''}) = \sigma_{K'}$ whenever $K' \subseteq K''$. For every $\alpha \in F$, there exists some finite Galois subextension K'/K such that $\alpha \in K'$. So define $\sigma : F \to F$ by putting $\sigma(\alpha) = \sigma_{K'}(\alpha)$. The restriction compatibility conditions make σ a well-defined map and it is clear that it is an automorphism of F inducing the identity on K. Hence $\sigma \in G$ and $\psi(\sigma) = \overline{\sigma}$.

(ii) Denote the basis of neighborhoods for G by $\mathcal{B}_1$. We show that the topologies of G and $G(F/K)$ coincide. To do that, we will provide a subbasis $\mathcal{B}_2$ for the topology of $G(F/K)$ and show that $\psi(\mathcal{B}_1) = \mathcal{B}_2$.

$G(F/K)$ has the product topology on $\prod_{K' \in I} G(K'/K)$ restricted to the set where

$$\mathrm{Res}_{K',K''}(\sigma_{K''}) = \sigma_{K'}$$

whenever $K' \subseteq K''$. The product topology has as a subbasis consisting of elements

$$\{(\sigma_{K'})_{K' \in I} \mid \sigma_{K^*} = \sigma^0_{K^*}\}$$

where $K^* \in I$ and $\sigma^0_{K^*} \in G(K^*/K)$. Thus the topology on $G(F/K)$ has a subbasis $\mathcal{B}_2$ consisting of elements

$$\{(\sigma_{K'})_{K' \in I} \mid \sigma_{K^*} = \sigma^0_{K^*}\} \cap G(F/K) \tag{6}$$

(by definition of subspace topology). Open sets in $G(F/K)$ are then unions of finite intersections of sets of this type.

Now, given $g \in G$ and a neighborhood $gG(F/K^*) \in \mathcal{B}_1$ of g (the extension K^*/K is fixed and is such that $g \in G(K^*/K)$), we have that

$$\begin{aligned} \psi(gG(F/K^*)) &= \{\psi(g\sigma) \mid \sigma \in G(F/K^*)\} \\ &= \{(g\sigma|_{K'})_{K' \in I} \mid \sigma \in G(F/K^*)\}. \end{aligned} \tag{7}$$

We verify that (7) is a set of the form (6). It is obvious that $(g\sigma|_{K'})_{K' \in I} \in G(F/K)$ simply because ψ takes values in $G(F/K)$. Moreover, every $\sigma \in G(F/K^*)$ satisfies $\sigma|_{K^*} = \mathrm{id}$ and consequently $g\sigma|_{K^*} = g \in G(K^*/K)$. So if we take $\sigma^0_{K^*} = g$, we can realize (7) in the form of (6). This shows that $\psi(\mathcal{B}_1) \subseteq \mathcal{B}_2$.

To show the reverse inclusion, consider the basis element $U = \{(\sigma_{K'})_{K' \in I} \mid \sigma_{K^*} = \sigma^0_{K^*}\} \cap G(F/K) \in \mathcal{B}_2$. We show that for every sequence $(\sigma_{K'})_{K' \in I}$ in U, there exists a unique $\tau \in G(F/K^*)$ such that $\psi(\sigma^0_{K^*}\tau) = (\sigma_{K'})_{K' \in I}$, concluding that $U \in \psi(\mathcal{B}_1)$ and hence

$$\mathcal{B}_2 \subseteq \psi(\mathcal{B}_1).$$

Note that restricting $\{(\sigma_{K'})_{K' \in I} \mid \sigma_{K^*} = \sigma^0_{K^*}\}$ to $G(F/K)$ is the same as imposing that

$$\mathrm{Res}_{K',K''}(\sigma_{K''}) = \sigma_{K'}$$

whenever $K' \subseteq K''$. Then, if we define $\tau \in G(F/K^*)$ by $\tau|_{K'} = (\sigma^0_{K^*})^{-1} \circ \sigma_{K'}$, we get a well-defined map satisfying

$$\psi(\sigma^0_{K^*}\tau) = ((\sigma_{K'})_{K' \in I})$$

(check the details). This shows the pretended result.

Problem 1.4.

Show that $G(F/K)$ is Hausdorff, compact, and totally disconnected.

Solution.

Let us recall the topological concepts mentioned in the statement. A topological space X is *Hausdorff* (or T2) if for all $x, y \in X$ such that $x \neq y$ there exist neighborhoods U_x of x and U_y of y such that $U_x \cap U_y = \emptyset$. The space X is *compact* if all open coverings of X admit a finite subcovering. X *totally disconnected* if its only connected components are the singletons.

We show these three properties are satisfied by $G(F/K)$. Recall $G(F/K)$ is endowed with a subspace topology of the product topology on $P = \prod_{K' \in I} G(K'/K)$ (see part (ii) of the previous problem for more details). Here, each $G(K'/K)$ has the discrete topology.

- $G(F/K)$ is Hausdorff and totally disconnected. This follows from some results in general topology. Indeed, discrete spaces such as $G(K'/K)$ are both Hausdorff and totally disconnected. The product of Hausdorff spaces is Hausdorff and the product of totally disconnected spaces is also totally disconnected. Hence P is Hausdorff and totally disconnected. Finally, the Hausdorff and totally disconnected properties are also inherited by subspaces, so $G(F/K)$ is Hausdorff and totally disconnected.

- $G(F/K)$ is compact. The fact that the groups $G(K'/K)$ are discrete and finite implies that they are compact. Moreover, the product of compact spaces is compact, so P is compact. We want to conclude that the subspace $G(F/K)$ is also compact. But compactness is only inherited by closed subspaces, so let us show that $G(F/K)$ is closed in P. The projection maps

$$\pi_{K'} : P \to G(K'/K) \tag{8}$$

  are continuous. Hence $\pi_{K'}^{-1}(G(K'/K))$ is closed for all $K' \in I$ since $G(K'/K)$ is closed. But

$$G(F/K) = \bigcap_{K' \in I} \pi_{K'}^{-1}(G(K'/K))$$

  (check this). Since intersections of closed sets are closed, we get that $G(F/K)$ is closed. We conclude that $G(F/K)$ is a closed subspace of the compact P and thus compact as well.

Problem 1.5.

Let G be a topological group. Show that all open subgroups of G are also closed. If G is compact, show that all open subgroups are of finite index in G. Conversely, show that a closed subgroup of finite index in a topological group G is open.

Solution.

Let us divide this problem in three parts.

a) All open subgroups of G are also closed. Let $H \leqslant G$ be open. To show H is closed, we show that $G \setminus H$ is open. Now,

$$G \setminus H = \bigcup_{g \in G \setminus H} gH,$$

   where the cosets gH are open (check this). Since unions of open sets are open, we conclude that $G \setminus H$ is open.

b) If G is compact, then all open subgroups are of finite index in G. Assume G is compact and let $H \leqslant G$ be open. We can write G as

$$G = \bigcup_{g \in G} gH,$$

where the gH are open, since H is open. By compactness, there exist finitely many $g_1, \ldots, g_n$ such that

$$G = \bigcup_{i=1}^{n} g_i H.$$

But this implies that $G/H = \{g_1 H, \ldots, g_n H\}$ and so $[G : H] \leq n < \infty$.

c) A closed subgroup of finite index is open. Let $H \leqslant G$ be a closed subgroup of finite index. We show that $G \setminus H$ is closed. Suppose $G/H = \{g_1 H, \ldots, g_n H\}$ and without loss of generality, assume g_1 is the identity of G. Then,

$$G \setminus H = \bigcup_{i=2}^{n} g_i H.$$

Since H is closed, $g_i H$ is closed for all $i = 2, \ldots, n$. Finite unions of closed sets are closed and hence $G \setminus H$ is closed.

Remark. A profinite topological group, as $G(F/K)$ in Definition 1.1., is compact. Then $H \leqslant G$ is open if and only if H is closed and of finite index. This is an important characterization of open subgroups of profinite groups.

Problem 1.6.

Prove the theorem.

Solution.

The problem statement refers to Theorem 1.1., which gives a generalization of the Galois correspondence for infinite Galois extensions F/K. Let us state the theorem first:

Let F/K be a (finite or infinite) Galois extension. The map

$$K' \mapsto G(F/K')$$

defines a bijective inclusion-reversing correspondence between subextensions K'/K and closed subgroups of $G(F/K)$. The inverse correspondence is given by

$$H \mapsto F^H,$$

where, as usual, F^H denotes the subfield of F consisting of those elements which are fixed by every element of H.

In particular, open subgroups $G(F/K')$ correspond to finite subextensions of F/K. Indeed, $G(F/K')$ is open in $G(F/K)$ if and only if it is also closed and has finite index (since $G(F/K)$ is a profinite group). In this case, and only in this case, $G(K'/K)$ is finite, since by the finite Galois correspondence

$$|G(K'/K)| = [G(F/K) : G(F/K')].$$

Hence $G(F/K')$ is open if and only if K'/K is finite.

Let us prove the theorem. Let F/K be a Galois extension. We starting by checking that the map

$$K' \mapsto G(F/K') \tag{9}$$

is well-defined in the sense that for every subextension K'/K (not necessarily finite), $G(F/K')$ is a closed subgroup of $G(F/K)$. Consider a finite subset $S \subseteq K'$ and the stabilizer

$$\begin{aligned} G(F/K)_S &= \{\sigma \in G(F/K) \mid \sigma(s) = s \text{ for all } s \in S\} \\ &= \bigcap_{s \in S} \{\sigma \in G(F/K) \mid \sigma(s) = s\} \\ &= \bigcap_{s \in S} G(F/K(s)). \end{aligned}$$

Note that every set $G(F/K(s))$ is a basis element for $G(F/K)$ in the sense of Problem 1.3., since the extension $K(s)/K$ is finite and Galois. Hence $G(F/K(s))$ is open. Since S is finite, we have $G(F/K)_S$ realized as a finite intersection of open sets, making it an open set. By Problem 1.5., $G(F/K)_S$ is closed as well. We now show that

$$G(F/K') = \bigcap_{S \subseteq K' \text{ finite}} G(F/K)_S. \tag{10}$$

Given $\sigma \in G(F/K')$ and $S \subseteq K'$, $\sigma(x) = x$ for all $x \in K'$ so in particular for all $s \in S$. This shows that the LHS is contained in the RHS. If σ is in the RHS, then $\sigma(\alpha) = \alpha$ for all $\alpha \in S$, for all finite $S \subseteq K'$. Given $\alpha \in K'$, there exists a finite subset $S \subseteq K'$ such that $\alpha \in S$. Hence $\sigma(\alpha) = \alpha$. So σ fixes all elements of K', that is, $\sigma \in G(F/K')$. This shows (10). Therefore, we have $G(F/K')$ realized as an intersection of closed sets, which implies that $G(F/K')$ is closed.

The next step is to show that the map in (9) really induces a bijection between subextensions K'/K and closed subgroups of $G(F/K)$ and has inverse given by

$$H \mapsto F^H.$$

In practice, we ought to show that

$$G(F/F^H) = H \tag{11}$$

for all closed subgroups H of $G(F/K)$ and

$$F^{G(F/K')} = K' \tag{12}$$

for all subextensions K'/K.

Consider a subgroup $H \leqslant G(F/K)$ (not necessarily closed). We show that $G(F, F^H) = \overline{H}$, where $\overline{H}$ denotes the topological closure of H. Since $G(F/F^H)$ is closed (as shown right above), $\overline{H} \subseteq G(F/F^H)$. The other inclusion requires more work. Let $\sigma \in G(F/K) \setminus \overline{H}$. By definition of closure and since $\{\sigma G(F/E) \mid E/K \text{ is finite}\}$ forms a system of neighborhoods of σ (we are again using the topology described in Problem 1.3.), there exists some finite extension E/K such that $\sigma G(F/E) \cap H = \emptyset$. In particular, if we consider the restriction

$$\begin{aligned} \phi : G(F/K) &\to G(E/K) \\ \tau &\mapsto \tau|_E, \end{aligned}$$

then $\sigma|_E \notin \phi(H)$ (check it). Hence, there exists some

$$\gamma \in E^{\phi(H)} = \{x \in E \mid \tau(x) = x \text{ for all } \tau \in \phi(H)\}$$

which is not fixed by σ. Note that $E^{\phi(H)} \subseteq F^H$ (check it) and so σ does not fix the element γ of F^H. Therefore $\sigma \notin G(F/F^H)$ or in other words, $\sigma \in G(F/K) \setminus G(F/F^H)$. Recall we started with the assumption that $\sigma \in G(F/K) \setminus \overline{H}$ and so we get $G(F/F^H) \subseteq \overline{H}$.

Having proven that $G(F/F^H) = \overline{H}$, we can directly conclude that if H is closed (i.e., $\overline{H} = H$), then

$$G(F/F^H) = H.$$

This proves (11).

To prove (12), consider a subextension K'/K. Since F/K is a Galois extension, F/K' is also Galois. Thus, we get directly that $F^{G(F/K')} = K'$.

Check that the bijection is inclusion-reversing.

Problem 1.8.

Let G_1 and G_2 be profinite groups. Show that a continuous injective homomorphism $G_1 \to G_2$ is an isomorphism from G_1 onto a closed subgroup of G_2.

Solution.

Since f is continuous and G_1 is compact, $f(G_2)$ is compact. Now, G_2 is Hausdorff since it is profinite and hence $f(G_1)$, being a compact subspace of the Hausdorff space G_2, is closed. Finally, since f is injective, its kernel is trivial, and so by the first isomorphism theorem, f induces an isomorphism of G_1 onto $f(G_1)$.

Problem 1.10.

Show that the natural map $\widehat{\mathbb{Z}} \to \prod_p \mathbb{Z}_p$ is an isomorphism.

Sketch of solution.

Recall

$$\widehat{Z} = \varprojlim_n \mathbb{Z}/n\mathbb{Z},$$

where the limit is obtained from the reduction homomorphisms $\mathrm{Red}_{m,n} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, defined whenever $m|n$. Let $m, n \geq 1$ such that $m|n$. Then the prime factorizations of m and n are of the form

$$n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$$
$$m = p_{i_1}^{\beta_{i_1}} \dots p_{i_s}^{\beta_{i_s}}$$

where $p_1, \dots, p_r$ and $p_{i_1}, \dots, p_{i_s}$ are rational primes such that $\{p_{i_1}, \dots, p_{i_s}\}$ is a subset of $\{p_1, \dots, p_r\}$ and $\beta_{i_j} \leq \alpha_{i_j}$ for all $j = 1, \dots, s$.

In more generality, we can define the directed set

$$I = \{((p_1, \dots, p_r), (\alpha_1, \dots, \alpha_r)) \mid p_i \text{ is prime}, \alpha_i \geq 1\},$$

where $((p_{i_1}, \dots, p_{i_s}), (\beta_{i_1}, \dots, \beta_{i_s})) \leq ((p_1, \dots, p_r), (\alpha_1, \dots, \alpha_r))$ if $\{p_{i_1}, \dots, p_{i_s}\}$ is a subset of $\{p_1, \dots, p_r\}$ and $\beta_{i_j} \leq \alpha_{i_j}$ for all $j = 1, \dots, s$. This allows us to define an inverse system given by the groups

$$\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_r^{\alpha_r}\mathbb{Z}$$

and the natural homomorphisms

$$\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_r^{\alpha_r}\mathbb{Z} \to \mathbb{Z}/p_{i_1}^{\beta_{i_1}}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_{i_s}^{\beta_{i_s}}\mathbb{Z}$$

given by reduction.

Consider the factorizations of n and m above, by the Chinese Remainder Theorem, we have that

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_r^{\alpha_r}\mathbb{Z}$$

and

$$\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/p_{i_1}^{\beta_{i_1}}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_{i_s}^{\beta_{i_s}}\mathbb{Z}.$$

Hence we obtain the following commutative diagram

$$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \xrightarrow{\cong} & \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_r^{\alpha_r}\mathbb{Z} \\ \downarrow & & \downarrow \\ \mathbb{Z}/m\mathbb{Z} & \xrightarrow[\cong]{} & \mathbb{Z}/p_{i_1}^{\beta_{i_1}}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_{i_s}^{\beta_{i_s}}\mathbb{Z} \end{array}$$

where the vertical arrows correspond to the restriction homomorphisms. This induces an isomorphism

$$\widehat{Z} = \varprojlim_{n} \mathbb{Z}/n\mathbb{Z} \cong \varprojlim_{((p_1,\ldots,p_r),(\alpha_1,\ldots,\alpha_r))} \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_r^{\alpha_r}\mathbb{Z}.$$

In turn, one get check that

$$\begin{aligned} \varprojlim_{((p_1,\ldots,p_r),(\alpha_1,\ldots,\alpha_r))} \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_r^{\alpha_r}\mathbb{Z} &\cong \varprojlim_{i\geq 1} \varprojlim_{n_i} \mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \mathbb{Z}/p_2^{n_2}\mathbb{Z} \times \ldots \\ &\cong \prod_p \mathbb{Z}/p\mathbb{Z}. \end{aligned}$$

We conclude that

$$\widehat{Z} \cong \prod_p \mathbb{Z}/p\mathbb{Z}.$$

Problem 1.12.

Suppose G is profinite and M has the discrete topology. For each subgroup $H \subseteq G$, write M^H for the set of elements of M which are fixed by every element of H. Show that the map $G \times M \to M$ is continuous if and only if we have

$$M = \bigcup_H M^H,$$

where H runs through all the *open* subgroups of G.

Solution.

"$\Rightarrow$"

Suppose the map $\varphi : G \times M \to M$ is continuous (we denote the map by φ but we sometimes write σm instead of $\varphi(\sigma, m)$). Clearly $\bigcup_H M^H \subseteq M$. Now, given $m \in M$, the stabilizer at m,

$$G_m = \{\sigma \in G \mid \sigma m = m\}$$

is open. Let us see why. Note that the set $\{(\sigma, n) \in G \times M \mid \sigma n = m\} = \varphi^{-1}(\{m\})$ is open with respect to the product topology, since $\{m\}$ is open in M and φ is continuous. Hence, there exist open subgroups of $H_i \subseteq G$ and $n_j \in M$ such that

$$\{(\sigma, n) \in G \times M \mid \sigma n = m\} = \bigcup_{i,j} H_i \times \{n_j\}.$$

In that case, for all $\sigma \in H_i$, $\sigma n_j = m$. Note that the identity map $\sigma = \mathrm{id}$ satisfies $\sigma m = m$ and so the pair $(\mathrm{id}, m) \in H_{i_1} \times \{n_{j_1}\}$ for some i_1, j_1. But this implies $n_{j_1} = m$ and so

$$H_{i_1} \times \{n_{j_1}\} = H_{i_1} \times \{m\} = \{(\sigma, m) \in G \times \{m\} \mid \sigma m = m\}.$$

This implies $H_{i_1} = G_m$ and so G_m is open. Finally, we note that $m \in M^H$ for $H = G_m$ since $\sigma m = m$ for all $\sigma \in G_m$. Hence $m \in \bigcup_H M^H$ where H through the open subgroups of G.

"$\Leftarrow$"

Suppose

$$M = \bigcup_H M^H,$$

where H runs through all the *open* subgroups of G. We have to check that for every $m \in M$, $\varphi^{-1}(\{m\})$ is open in the product topology on $G \times M$. Let $m \in M$. Then,

$$\begin{aligned} \varphi^{-1}(\{m\}) &= \{(\sigma, n) \in G \times M \mid \sigma n = m\} \\ &= \bigcup_{\substack{n \in M \\ \exists \sigma \in G \\ \sigma(n) = m}} \bigcup_{\substack{\sigma \in G \\ \sigma(n) = m}} \{(\sigma, n)\}. \end{aligned}$$

Now, since

$$M = \bigcup_H M^H,$$

there exists an open subgroup $H \subseteq G$ such that $m \in M^H$, that is, $\tau(m) = m$ for all $\tau \in H_n$. In that case, for all $\sigma \in G$ such that $\sigma(n) = m$, we have that $\sigma(n) = \tau(m) \implies (\tau^{-1}\sigma)(n) = m$. Thus,

$$\begin{aligned} \varphi^{-1}(\{m\}) &= \bigcup_{\substack{n \in M \\ \exists \sigma \in G \\ \sigma(n) = m}} \bigcup_{\substack{\sigma \in G \\ \sigma(n) = m}} \{(\sigma, n)\} \\ &= \bigcup_{\substack{n \in M \\ \exists \sigma \in G \\ \sigma(n) = m}} \bigcup_{\substack{\sigma \in G \\ \sigma(n) = m}} H\sigma \times \{n\}. \end{aligned}$$

Note that each $H\sigma$ is open and each $\{n\}$ is open. Hence $\varphi^{-1}(\{m\})$ is open.

Extending valuations from $\mathbb{Q}$ to $\overline{\mathbb{Q}}$

Given a prime p and $n \in \mathbb{Q}$, we can always write $n = p^r u$ for some $r \geq 0$ and some rational number u not divisible by p. Then, we define a valuation v_p on $\mathbb{Q}$ by $v_p(n) = r$.

We want to see how we can extend v_p to an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. In order to do this, for all number fields $L \subseteq \overline{\mathbb{Q}}$, choose a prime ideal $\mathfrak{P}_L$ over p (that is, $\mathfrak{P}_L | (p)\mathcal{O}_L$) such that if $F \subseteq L$ then $\mathfrak{P}_L \cap F = \mathfrak{P}_F$ (we are using the axiom of choice). Fix this sequence $\{\mathfrak{P}_L\}_L$ where L runs through all number fields $L \subseteq \overline{\mathbb{Q}}$.

Now, given $\alpha \in \overline{\mathbb{Q}}$ and a number field $L \subseteq \overline{\mathbb{Q}}$ containing α (for instance, $L = \mathbb{Q}(\alpha)$), we have that

$$(\alpha)\mathcal{O}_L = \mathfrak{P}_L^{a_L} J,$$

where $a_L \geq 0$ and J corresponds to the rest of the factorization of (α) by prime ideals in $\mathbb{Q}(\alpha)$. In this case, we define the valuation $\overline{v_p} : \overline{Q} \to \mathbb{Z}$ as

$$\overline{v_p}(\alpha) = \frac{a_L}{e(\mathfrak{P}_L, p)},$$

where $e(\mathfrak{P}_L, p)$ denotes the ramification index of $\mathfrak{P}_L$ over p (that is, $e(\mathfrak{P}_L, p)$ is the power associated to the prime $\mathfrak{P}_F$ in the factorization of $(p)\mathcal{O}_L$).

We need to show that $\overline{v_p}$ is (i) well-defined, (ii) a valuation in $\overline{\mathbb{Q}}$ and (iii) an extension of v_p.

(i) Showing that $\overline{v_p}$ is well-defined sums up to verifying that it does not depend on the chosen field L. Indeed, given two number fields $L, F \subseteq \overline{\mathbb{Q}}$ containing $\alpha \in \overline{\mathbb{Q}}$, it holds that the number field $L \cap F \subseteq \overline{\mathbb{Q}}$ also contains α. Since $L \cap F \subseteq L, F$, by construction of the sequence $\{\mathfrak{P}_L\}_L$, we get that

$$\mathfrak{P}_L \cap (L \cap F) = \mathfrak{P}_{L \cap F} = \mathfrak{P}_F \cap (L \cap F).$$

This implies that $\mathfrak{P}_L = \mathfrak{P}_F$ and by uniqueness of prime factorization at the level of ideals, we get that $a_L = a_F$ and so $\overline{v_p}$ is well-defined.

(ii) We will show that $\overline{v_p}(\alpha\beta) = \overline{v_p}(\alpha) + \overline{v_p}(\beta)$. We leave the second property of valuations to you ($\overline{v_p}(\alpha + \beta) \geq \min\{\overline{v_p}(\alpha), \overline{v_p}(\beta)\}$, with equality if $\overline{v_p}(\alpha) \neq \overline{v_p}(\beta)$).

Let $\alpha, \beta \in \overline{\mathbb{Q}}$. Then, $\alpha, \beta, \alpha\beta \in L = \mathbb{Q}(\alpha, \beta)$, so if

$$\begin{aligned}(\alpha)\mathcal{O}_L &= \mathfrak{P}_L^{a_\alpha} \dots, \\ (\beta)\mathcal{O}_L &= \mathfrak{P}_L^{a_\beta} \dots \\ \text{and } (\alpha\beta)\mathcal{O}_L &= \mathfrak{P}_L^{a_{\alpha\beta}} \dots\end{aligned}$$

we need to show that

$$a_\alpha + a_\beta = a_{\alpha\beta}.$$

This is follows directly from

$$(\alpha\beta)\mathcal{O}_L = (\alpha)\mathcal{O}_L(\beta)\mathcal{O}_L = \mathfrak{P}_L^{a_\alpha}\mathfrak{P}_L^{a_\beta} \dots = \mathfrak{P}_L^{a_\alpha + a_\beta} \dots$$

and the fact that factorization is unique at the level of ideals.

(iii) Let $n \in \mathbb{Q}$ such that $n = p^r u$ as described in the beginning. We want to check if $v_p(n) = \overline{v_p}(n)$, that is, if $r = a_L/e(\mathfrak{P}_L, p)$. Suppose

$$(p)\mathcal{O}_L = \mathfrak{P}_L^{e(\mathfrak{P}_L,p)} J$$

for some ideal J not divisible by $\mathfrak{P}_L$. Then,

$$\begin{aligned}(n)\mathcal{O}_L &= (p)^r \mathcal{O}_L(u) \\ &= \mathfrak{P}_L^{re(\mathfrak{P}_L,p)} J^r(u)\end{aligned}$$

where $J^r(u)$ is not divisible by p. Hence,

$$\overline{v_p}(n) = \frac{re(\mathfrak{P}_L, p)}{e(\mathfrak{P}_L, p)} = r = v_p(n).$$

How to embed $G_{\mathbb{Q}_p}$ in $G_{\mathbb{Q}}$?

Recall $G_{\mathbb{Q}_p} = \mathrm{Gal}(\overline{Q_p}/\mathbb{Q}_p)$ and $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ for some fixed algebraic closures $\overline{\mathbb{Q}_p}$ and $\overline{\mathbb{Q}}$. We start by noting that the fact that v_p extends to $\overline{\mathbb{Q}}$ implies that the p-adic norm $|\cdot|_p$ also extends to $\overline{\mathbb{Q}}$. Furthermore, $\overline{\mathbb{Q}}$ is (topologically) dense in $\overline{\mathbb{Q}_p}$ under $|\cdot|_p$.

Taking this into account, we can embed $G_{\mathbb{Q}_p}$ in $G_{\mathbb{Q}}$ under the restriction map

$$\begin{aligned}\iota : G_{\mathbb{Q}_p} &\hookrightarrow G_{\mathbb{Q}} \\ \sigma &\mapsto \sigma|_{\overline{\mathbb{Q}}}.\end{aligned}$$

We should note the map above does not depend on the chosen algebraic closures. Indeed, given two algebraic closures of $\mathbb{Q}$, say $\overline{\mathbb{Q}}^1$ and $\overline{\mathbb{Q}}^2$, there exists $\tau \in G_{\mathbb{Q}}$ such that for any number fields $F_1 \subseteq \overline{\mathbb{Q}}^1$ and $F_2 \subseteq \overline{\mathbb{Q}}^1$, $\tau(\mathfrak{P}_{F_1}) = \mathfrak{P}_{F_2}$. In that case, the valuations v_p^1 and v_p^2 associated to $\overline{\mathbb{Q}}^1$ and $\overline{\mathbb{Q}}^2$, respectively, are related by

$$v_p^1 \circ \tau = v_p^2,$$

which implies

$$\overline{G_{\mathbb{Q}_p}}^1 \cong \tau^{-1} \overline{G_{\mathbb{Q}_p}}^2 \tau.$$

So if we consider a Galois group $G^*_{\mathbb{Q}_p} = G(\overline{\mathbb{Q}_p}^*/\mathbb{Q}_p)$ where $\overline{\mathbb{Q}_p}^*$ is a different algebraic closure than the one fixed at the beginning, we can simply map $\sigma \in G^*_{\mathbb{Q}_p}$ first to $\tau^{-1}\sigma\tau \in G_{\mathbb{Q}_p}$, and only after apply ι, obtaining still an embedding $G^*_{\mathbb{Q}_p} \hookrightarrow G_{\mathbb{Q}}$.

Chebotarev's Theorem

Chebotarev's theorem, Theorem 1.8., states the following:

Let $K/\mathbb{Q}$ be a Galois extension that is unramified outside a finite set S of primes. Let T be a finite set of primes containing S. For each prime $p \notin T$, there is a well-defined Frobenius conjugacy class $[\phi_p] \subseteq G(K/\mathbb{Q})$. The union of all these Frobenius conjugacy classes is dense in $G(K/\mathbb{Q})$.

Let us make some general observations. First, the union of all the Frobenius conjugacy classes being dense in $G(K/\mathbb{Q})$ means that $G(K/\mathbb{Q})$ is the closure (under the profinite topology) of

$$\bigcup_{p \notin T} [\phi_p].$$

Hence, by definition of closure, this means that for all $\sigma \in G(K/\mathbb{Q})$ and for every open neighborhood σN of σ ($N = G(K/K')$ for some finite subextension K'/K), we have

$$\sigma N \cap \bigcup_{p \notin T} [\phi_p] \neq \emptyset,$$

that is, there exists $p \notin T$ such that

$$\sigma N \cap [\phi_p] \neq \emptyset.$$

This implies there exists some $\eta \in N$ such that

$$\sigma\eta \in [\phi_p] = \phi_p G(K/\mathbb{Q})\phi_p^{-1}. \tag{13}$$

Problem 1.29.

What does this say when K is a finite extension of $\mathbb{Q}$?

Sketch of solution.

The problem refers to Chebotarev's theorem. Let K be a finite Galois extension of $\mathbb{Q}$ and consider $\sigma \in G = G(K/\mathbb{Q})$ and its conjugacy class $[\sigma] = \sigma G \sigma^{-1}$. Denote

$$P_{K/\mathbb{Q}}(\sigma) = \{\mathfrak{p} \subseteq \mathcal{O}_K \mid [\phi_\mathfrak{p}] = [\sigma]\},$$

and consider the density of $P_{K/\mathbb{Q}}(\sigma)$ in G,

$$d(P_{K/\mathbb{Q}}(\sigma)) := \frac{|P_{K/\mathbb{Q}}(\sigma)|}{|G|}.$$

Then,

$$d(P_{K/\mathbb{Q}}(\sigma)) = \frac{|[\sigma]|}{|G|}, \tag{14}$$

that is, the Frobenius elements are uniformly distributed over conjugacy classes. Use Chebotarev's theorem, namely (13), to show (14).

Representations as continuous modules over the group ring

We discuss the construction carried out in the end of Lecture 1 of F. Gouvêa's notes (starting in Definition 1.3.).

Given a topological ring A, a finite set of primes S and a positive integer n, a Galois *representation* (defined over A, unramified outside S) is a continuous homomorphism

$$\rho : G_{\mathbb{Q},S} \to \mathrm{GL}_n(A).$$

Two Galois representations are said to be *equivalent* if they differ only up to conjugation by a matrix in $\mathrm{GL}_n(A)$.

Given a representation ρ, we can consider the free A-module M of rank n and endow it the continuous action

$$\begin{aligned} G_{\mathbb{Q},S} \times M &\to M \\ (g, m) &\mapsto \rho(g)m. \end{aligned}$$

Conversely, given a free A-module M of rank n with such a continuous action of $G_{\mathbb{Q},S}$, we can obtain a representation ρ by choosing a basis for $M \cong A^n$. In this case, changing the basis of M changes ρ to an equivalent representation.

MORAL: Giving (up to equivalence) a representation of $G_{\mathbb{Q},S}$ over A of dimension n is the same as giving a free A-module of rank n with a continuous action of $G_{\mathbb{Q},S}$

Now suppose we have a free A-module M of rank n with a continuous action of a profinite group G and additionally

$$M = \varprojlim_H M^H, \tag{15}$$

where H runs through all open normal subgroups of G.

The completed group ring $A[[G]]$ is defined as

$$A[[G]] := \varprojlim_H A[G/H],$$

where H runs through all open normal subgroups of G and $A[G/H]$ is the usual group ring of the finite group G/H over A (recall that H open in the profinite topology implies that H has finite index). If you are not familiar with the group ring, you can think of it as the group consisting of formal linear combinations of elements of G/H with coefficients in A:

$$A[G/H] = \Big\{ \sum_{g \in G} a_g gH \Big\}.$$

The inverse system defining $A[[G]]$ is given by the induced homomorphisms $A[G/H_1] \to A[G/H_2]$ whenever H_1, H_2 are open normal subgroups of G with $H_1 \hookrightarrow H_2$.

The fact that G acts continuously on M and both $\{M^H\}_H$ and $\{A[G/H]\}_H$ are inverse systems implies that $A[G/H]$ acts continuously on M^H for every open normal subgroup H of G (check this). Hence, by compatibility of the inverse systems, we get that $A[[G]]$ acts continuously on M, that is, M is a continuous $A[[G]]$-module. In conclusion, given a free A-module M of rank n given by the inverse limit (15), with a continuous action of G, M can be seen as a continuous $A[[G]]$-module. In fact, if A is not only a topological ring but a profinite ring, then we automatically have (15), see Problem 1.14.

MORAL: If A is a profinite ring, giving (up to equivalence) a representation of G over A is the same as giving a continuous $A[[G]]$-module M which is finite and free as an A-module

Furthermore, given a representation

$$\rho : G \to \mathrm{GL}_n(A)$$

defined over a profinite ring A, we can extend it by linearity to $A[[G]]$ and get a continuous homomorphism of A-algebras

$$A[[G]] \to \mathrm{M}_n(A).$$

Conversely, given such an homomorphism, we can restrict it to G to obtain a representation as above.