D-MATH Number Theory II FS 2024
Prof. Richard Pink

Solutions 20

Profinite Groups, Infinite Galois Theory

1. Consider a topological group G.

   (a) Show that if G is hausdorff, then the center of G and the centralizer of any element $g \in G$ are closed subgroups.

   (b) Show that for any continuous action of G on a topological space the stabilizer of any closed point is closed.

   (c) Show that G is hausdorff if and only if G is T_0. (A topological space is called T_0 if for any two distinct points, one of them possesses a neighborhood that does not contain the other.)

   Solution:

   (a) If a topological space is hausdorff, then every point is closed. Since for any $g \in G$ the map $G \to G$, $h \mapsto [g,h] = ghg^{-1}h^{-1}$ is continuous, it follows that the centralizer $\mathrm{Cent}_G(g) := \{h \in H \colon [g,h] = 1\}$ is a closed subset. As an intersection of the closed subsets the center $Z(G) := \bigcap_{g \in G} \mathrm{Cent}_G(g)$ is then also a closed subset.

   (b) By assumption the action $G \times X \to X$ is a continuous map; hence so is the map $G \to X$, $g \mapsto gx$ for any $x \in X$. If x is a closed point, it follows that $\mathrm{Stab}_G(x) := \{g \in G \colon gx = x\}$ is a closed subset.

   (c) Every hausdorff space is T_0. Conversely suppose that G is T_0. Consider two distinct points $g, h \in G$. Suppose that $U \subset G$ is an open subset with $g \notin U \ni h$. Since inversion on G is a homeomorphism, the subset $U^{-1} := \{u^{-1} \mid u \in U\}$ is again open with $g^{-1} \notin U^{-1} \ni h^{-1}$. Since left and right translation by fixed elements of G are homeomorphisms, it follows that $gU^{-1}h$ is again open with $h = gg^{-1}h \notin gU^{-1}h \ni gh^{-1}h = g$. Thus G is T_1.

   This implies that every point in G is closed. Since the map $G \times G \to G$, $(g,h) \mapsto gh^{-1}$ is continuous, it follows that the diagonal $\{(g,h) \in G \times G \mid gh^{-1} = 1\}$ is closed. But this implies that G is hausdorff.

*2. A topological space is called *totally disconnected* if every connected subset contains only one element. Prove that a topological group is profinite if and only if it is compact and totally disconnected.

   Solution: See Proposition 1.1.3 in *Cohomology of Number Fields* by J. Neukirch.

3. Consider a Galois extension L/K with $\Gamma := \mathrm{Gal}(L/K)$ and an intermediate field K' with $\Gamma' := \mathrm{Gal}(L/K')$. Show that K'/K is Galois if and only if $\Gamma' \triangleleft \Gamma$, and that then there is a natural isomorphism of profinite groups $\Gamma/\Gamma' \cong \mathrm{Gal}(K'/K)$.

Solution: First we claim that K'/K is Galois if and only if $\gamma(K') = K'$ for all $\gamma \in \Gamma$. To see this observe that since L/K is separable, so is K'/K. Thus K'/K is Galois if and only if it is normal. Choosing an algebraic closure $\bar{L}$ of L, this is equivalent to saying that for every homomorphism $\sigma\colon K' \to \bar{L}$ over K we have $\sigma(K') \subset K'$. Since L/K is algebraic, any such homomorphism σ can be extended to a homomorphism $\tilde{\sigma}\colon L \to \bar{L}$ over K. Moreover, since L/K is normal, for any such $\tilde{\sigma}$ we have $\tilde{\sigma}(L) \subset L$, and since L/K is algebraic even $\tilde{\sigma}(L) = L$. Thus $\tilde{\sigma}$ induces an element $\gamma \in \mathrm{Gal}(L/K) = \Gamma$. Together this shows that K'/K is Galois if and only if $\gamma(K') \subset K'$ for every $\gamma \in \Gamma$. Since again K'/K is algebraic, for any such γ we then even have $\gamma(K') = K'$. This proves the claim.

Next, for any elements $\gamma, \gamma' \in \Gamma$ we have

$$\gamma' \in \Gamma' \iff \gamma'|K' = \mathrm{id} \iff \gamma\gamma'\gamma^{-1}|\gamma(K') = \mathrm{id} \iff \gamma\gamma'\gamma^{-1} \in \mathrm{Gal}(L/\gamma(K')).$$

Thus for any $\gamma \in \Gamma$ we have $\mathrm{Gal}(L/\gamma(K')) = \gamma\Gamma'\gamma^{-1}$. By the bijective Galois correspondence we therefore have $\gamma(K') = K'$ if and only if $\gamma\Gamma'\gamma^{-1} = \Gamma'$. Varying γ and using the above claim it follows that K'/K is Galois if and only if $\Gamma' \triangleleft \Gamma$.

Now assume that K'/K is Galois. By the claim we then have a natural homomorphism

$$c\colon \Gamma = \mathrm{Gal}(L/K) \longrightarrow \bar{\Gamma} := \mathrm{Gal}(K'/K), \quad \gamma \mapsto \gamma|K'.$$

By construction its kernel is $\mathrm{Gal}(L/K') = \Gamma'$. On the other hand, by the same argument as above any isomorphism $K' \to K'$ over K extends to an isomorphism $L \to L$ over K; so c is surjective. Together it thus induces a group isomorphism $\bar{c}\colon \Gamma/\Gamma' \xrightarrow{\sim} \bar{\Gamma}$.

Next, the subgroups $\mathrm{Gal}(K'/K'')$ for all subfields $K'' \subset K'$ that are finite over K form a fundamental system of open neighborhoods of the identity element in $\bar{\Gamma}$. For all these the subgroups $c^{-1}(\mathrm{Gal}(K'/K'')) = \mathrm{Gal}(L/K'')$ are open neighborhoods of the identity element in Γ. Thus c is continuous at the identity element, and by translation it is therefore continuous everywhere.

Finally, we endow Γ/Γ' with the quotient topology from Γ. Then since c is continuous, so is $\bar{c}\colon \Gamma/\Gamma' \xrightarrow{\sim} \bar{\Gamma}$. Conversely, for any closed subset $X \subset \Gamma/\Gamma'$ its inverse image in Γ is closed and therefore compact; so by the continuity of c its image $\bar{c}(X)$ in $\bar{\Gamma}$ is compact and therefore closed, because $\bar{\Gamma}$ is Hausdorff. Thus $\bar{c}^{-1}$ is continuous, and therefore $\bar{c}$ is a homeomorphism.

4. *(The cyclotomic $\mathbb{Z}_p$-extension)* Set $\mathbb{Q}(\mu_{p^\infty}) := \bigcup_n \mathbb{Q}(\mu_{p^n})$ for a prime number p.

   (a) Show that $\mathbb{Q}(\mu_{p^\infty})$ possesses a unique subfield K_∞ with $\mathrm{Gal}(K_\infty/\mathbb{Q}) \cong \mathbb{Z}_p$.

   *(b) Give explicit generators for K_∞.

   Solution:

   (a) The natural isomorphisms $\mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q}) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times$ yield an isomorphism

$$\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \;\cong\; \varprojlim_n \mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q}) \;\cong\; \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^\times \;\cong\; \mathbb{Z}_p^\times.$$

   Thus by infinite Galois theory it suffices to show that there exists a unique closed subgroup $H < \mathbb{Z}_p^\times$ such that $\mathbb{Z}_p^\times/H \cong \mathbb{Z}_p$. But we already know that

$$\mathbb{Z}_p^\times = \begin{cases} \mu_{p-1} \times (1 + p\mathbb{Z}_p) & \text{if } p > 2, \\ \mu_2 \times (1 + 4\mathbb{Z}_2) & \text{if } p = 2, \end{cases}$$

   where the second factor is isomorphic to $\mathbb{Z}_p$. Since $\mathbb{Z}_p$ is a torsion free abelian group, the subgroup H must contain all torsion elements of $\mathbb{Z}_p^\times$ and hence the first factor. The quotient is then isomorphic to the quotient of $\mathbb{Z}_p$ by a closed subgroup. But the quotient of $\mathbb{Z}_p$ by any non-trivial closed subgroup is finite. Therefore the only possibility for H is the first factor in the above decomposition.

   *(b) For any $n \geqslant 0$ the subgroup $p^n\mathbb{Z}_p < \mathbb{Z}_p \cong \mathrm{Gal}(K_\infty/\mathbb{Q})$ corresponds to a unique subfield $K_n \subset K$ with $\mathrm{Gal}(K_n/K) \cong \mathbb{Z}/p^n\mathbb{Z}$. If p is odd, then

$$\mathrm{Gal}(\mathbb{Q}(\mu_{p^{n+1}})/\mathbb{Q}) \;\cong\; (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times \;\cong\; \mu_{p-1} \times \mathbb{Z}/p^n\mathbb{Z};$$

   hence K_n must be the fixed field of $\mathbb{Q}(\mu_{p^{n+1}})$ under the subgroup μ_{p-1}. By a theorem from Galois theory the trace map $\mathbb{Q}(\mu_{p^{n+1}}) \to K_n$ is surjective. Since the p^{n+1}-st roots of unity ζ generate $\mathbb{Q}(\mu_{p^{n+1}})$ as a $\mathbb{Q}$-vector space, it follows that K_n is generated by the traces of these, namely by the elements $t(\zeta) := \sum_{a \in \mu_{p-1}} \zeta^a$. Varying n we find that K_∞ is generated by the elements $t(\zeta)$ for all p-power roots of unity ζ.

   If $p = 2$, we similarly have

$$\mathrm{Gal}(\mathbb{Q}(\mu_{2^{n+2}})/\mathbb{Q}) \;\cong\; (\mathbb{Z}/2^{n+2}\mathbb{Z})^\times \;\cong\; \mu_2 \times \mathbb{Z}/2^n\mathbb{Z},$$

   where the complex conjugation corresponds to the non-trivial element of μ_2. By the same arguments as above, K_∞ is therefore generated by the elements $\zeta + \bar{\zeta} = \zeta + \zeta^{-1} = 2\,\mathrm{Re}(\zeta)$ for all 2-power roots of unity ζ.

5. Let p be a prime number and $\bar{\mathbb{Q}}$ an algebraic closure of $\mathbb{Q}$.

   (a) Show that $|\ |_p$ extends to some absolute value $|\ |$ on $\bar{\mathbb{Q}}$.

   (b) For any subfield $K \subset \bar{\mathbb{Q}}$ which is finite over $\mathbb{Q}$ let $\hat{K}$ be the completion of K with respect to the restriction of $|\ |$. Show that for any subfields $K \subset L \subset \bar{\mathbb{Q}}$ which are finite over $\mathbb{Q}$ we get a natural inclusion $\hat{K} \hookrightarrow \hat{L}$.

   (c) Show that the union $\bar{\mathbb{Q}}_p$ of all these $\hat{K}$ is an algebraic closure of $\mathbb{Q}_p$.

   (d) Show that there is a natural isomorphism

$$\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \xrightarrow{\sim} \mathrm{Stab}_{\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})}(|\ |).$$

Solution:

   (a) Let $\bar{\mathbb{Q}}_p$ be any algebraic closure of $\mathbb{Q}_p$. Then the p-adic absolute value on $\mathbb{Q}_p$ possesses a unique extension to $\bar{\mathbb{Q}}_p$. Since $\bar{\mathbb{Q}}_p$ is algebraically closed, the embedding $\mathbb{Q} \hookrightarrow \bar{\mathbb{Q}}_p$ extends to some embedding $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_p$. The pullback of the absolute value on $\bar{\mathbb{Q}}_p$ under this embedding yields the desired extension.

   Aliter: For any finite extension $K/\mathbb{Q}$, there exists an extension of $|\ |_p$ to K. Construct the desired extension to $\bar{\mathbb{Q}}$ using Zorn's lemma.

   (b) Any Cauchy sequence in K is also a Cauchy sequence in L, as the absolute value on K is the restriction of the absolute value on L. Hence we obtain an inclusion of metric spaces $\hat{K} \hookrightarrow \hat{L}$. It follows directly from the definition of addition and multiplication for the completion that this inclusion respects the field structure.

   (c) The natural inclusions $\hat{K} \hookrightarrow \hat{L}$ are compatible with each other; hence we can form the union $M := \varinjlim \hat{K}$. Since each $\hat{K}$ is finite over $\mathbb{Q}_p$, this M is algebraic over $\mathbb{Q}_p$. We claim that it is algebraically closed.

   For this consider any finite extension $\tilde{K}/\mathbb{Q}_p$. Then $\tilde{K}$ is a local field, so by exercise 2 of sheet 19 it is the completion of a global field K at an absolute value $|\ |$. Since $\mathbb{Q} \subset \mathbb{Q}_p \subset \tilde{K}$, we also have $\mathbb{Q} \subset K$; so K is finite extension of $\mathbb{Q}$. Also, the restriction of $|\ |$ to $\mathbb{Q}$ is the restriction of the usual absolute value on $\mathbb{Q}_p$ and hence equal to $|\ |_p$.

   (*Aliter:* Consider any irreducible monic polynomial $f \in \mathbb{Q}_p[X]$ with roots $x = x_1, x_2, \ldots, x_n \in \bar{\mathbb{Q}}_p$. As in the solution of exercise 3 of sheet 18, we can choose a monic polynomial $g \in \mathbb{Q}[X]$ of degree n that is coefficientwise close to f and has a root y in M such that $|y - x| < \min\{|x - x_i| : 2 \leqslant i \leqslant n\}$. Krasner's lemma (exercise 2 of sheet 18) then implies that $\mathbb{Q}_p(x) \subset \mathbb{Q}_p(y)$. Thus $\mathbb{Q}_p(x)$ lies in the completion of the number field $K := \mathbb{Q}(y)$ at an absolute value $|\ |$ extending the p-adic absolute value on $\mathbb{Q}$.)

   Let L be a galois closure of K over $\mathbb{Q}$. Then $\mathrm{Gal}(L/\mathbb{Q})$ acts transitively on the set of primes of $\mathcal{O}_L$ above p and hence also on the set of extensions of

$|\ |_p$ to L. Any such extension thus arises from the extension to $\bar{\mathbb{Q}}$ in (a) via some embedding $L \hookrightarrow \bar{\mathbb{Q}}$. After extending our given absolute value $|\ |$ on K to L, this therefore arises from the extension to $\bar{\mathbb{Q}}$ in (a) via some embedding $K \hookrightarrow \bar{\mathbb{Q}}$. For this embedding we then have $\tilde{K} = \hat{K} \subset M$. Varying $\tilde{K}$ this proves that M is algebraically closed. In particular we have a natural equality $M = \bar{\mathbb{Q}}_p$.

(d) First consider any finite extension $K \subset \bar{\mathbb{Q}}$ which is galois over $\mathbb{Q}$ with galois group G. Then by Proposition 9.5.6 of the lecture, the pullback of $|\ |_p$ via $K \hookrightarrow \bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_p$ corresponds to a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ above p, and by Prop 9.5.10 the extension $\hat{K}/\mathbb{Q}_p$ is galois with galois group $G_{\mathfrak{p}} = \mathrm{Stab}_G(\mathfrak{p})$. By the natural bijection between primes above p and extensions of the absolute value this subgroup is equal to $\mathrm{Stab}_G(|\ |_p|_K)$.

For any two finite extensions $K \subset K' \subset \bar{\mathbb{Q}}$ that are galois over $\mathbb{Q}$ we have a natural surjection $\mathrm{Gal}(K'/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(K/\mathbb{Q})$. Moreover, if $\mathfrak{p} \subset \mathcal{O}_K$ and $\mathfrak{p}' \subset \mathcal{O}_{K'}$ are the primes above p associated to the respective pullbacks of $|\ |_p$, then $\mathfrak{p}'$ lies above $\mathfrak{p}$, and by the solution of exercise 2 of sheet 2 we obtain a natural commutative diagram with vertical surjections

$$\begin{array}{ccccccc}
\mathrm{Gal}(\hat{K}'/\mathbb{Q}_p) & \cong & \mathrm{Stab}_{\mathrm{Gal}(K'/\mathbb{Q})}(\mathfrak{p}') & = & \mathrm{Stab}_{\mathrm{Gal}(K'/\mathbb{Q})}(|\ |_p|_{K'}) & \subset & \mathrm{Gal}(K'/\mathbb{Q}) \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
\mathrm{Gal}(\hat{K}/\mathbb{Q}_p) & \cong & \mathrm{Stab}_{\mathrm{Gal}(K/\mathbb{Q})}(\mathfrak{p}) & = & \mathrm{Stab}_{\mathrm{Gal}(K/\mathbb{Q})}(|\ |_p|_K) & \subset & \mathrm{Gal}(K/\mathbb{Q}).
\end{array}$$

As K varies over all finite extensions within $\bar{\mathbb{Q}}$ which are galois over $\mathbb{Q}$, we thus obtain compatible inverse systems. Since the union of the resulting fields $\hat{K}$ is $\bar{\mathbb{Q}}_p$ by part (c), in the limit we obtain an isomorphism

$$\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \cong \mathrm{Stab}_{\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})}(|\ |_p|_{\bar{\mathbb{Q}}}) \subset \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$$