Yale University Department of Mathematics
Math 608 Introduction to Arithmetic Geometry
Fall 2018

Problem Set # 1 (due in class on Monday October 15)

Reading: *Gill–Szamuely* §1.1–1.3, §2.1–2.2, §2.4.

Problems:

1. Let G be a group. A **basis of open neighborhoods of the identity** in G is a collection $\mathcal{U}$ of subgroups with the property that for each $U_1, U_2 \in \mathcal{U}$ there exists $U_3 \in \mathcal{U}$ such that $U_3 \subset U_1 \cap U_2$.

(a) Let $\mathcal{U}$ be a basis of open neighborhoods of the identity in G satisfying that for every $U \in \mathcal{U}$ and for every $g \in G$ there exists $V \in \mathcal{U}$ such that $gVg^{-1} \subset U$. Prove that the collection of all translates by elements of G of all subsets in $\mathcal{U}$ is a base $\mathcal{B}$ for a topological group structure on G.

(b) Prove that there is no basis of open neighborhoods of the identity that generates the usual Euclidean topology on $\mathbb{R}$ or on $\mathbb{R}^\times$. Describe the topology on $\mathbb{R}$ and on $\mathbb{R}^\times$ generated by the basis of open neighborhoods of the identity consisting of all subgroups.

(c) Find a nice basis of open neighborhoods of the identity generating the profinite topology on $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$.

2. Recall that a group G is called **residually finite** if the profinite topology (whose basis of open neighborhoods of the identity are all finite index subgroups) on G is Hausdorff; it is called **profinite** if it is an inverse limit of finite groups.

(a) Prove that G is residually finite if and only if $\bigcap U = \{e\}$, where the intersection is taken over all finite index normal subgroups U of G.

(b) Prove that G is residually finite if and only if the canonical homomorphism $G \to \widehat{G}$ to the profinite completion is injective.

(c) Let K/F be any Galois extension of fields. Prove that the Galois group $G = \mathrm{Gal}(K/F)$ is a profinite group.

(d) Prove that any free group is residually finite.

3. Let G be a locally compact (i.e., every point has a compact neighborhood) Hausdorff topological group. For example, $\mathbb{R}$ or any discrete group is locally compact. Let $U \subset \mathbb{C}^\times$ be the unit circle, which is a locally compact topological group. Define the **Pontryagin dual** $\check{G}$ to be the group of all continuous homomorphisms $\phi : G \to U$ equipped with the compact-open topology.

(a) Prove that $\check{\mathbb{Z}} \cong U$ and that $\check{U} \cong \mathbb{Z}$.

(b) Prove that $\check{\mathbb{R}} \cong \mathbb{R}$ via a map (in the other direction) $x \mapsto (y \mapsto e^{2ixy})$.

(c) Prove that if G is a finite abelian group, then $\check{G} \cong G$.

(d) Prove that if G is a discrete torsion group, then $\check{G}$ is a profinite group.

(e) Prove that $\widecheck{\mathbb{Q}/\mathbb{Z}} \cong \widehat{\mathbb{Z}}$. **Hint.** $\mathbb{Q}/\mathbb{Z}$ is a "direct limit"!

4. Let A be an (associative unital) F-algebra. We say that an F-linear map $^{-} : A \to A$ is an **involution** if $\overline{1} = 1$, $\overline{\overline{a}} = a$ for all $a \in A$, and $\overline{ab} = \overline{b}\overline{a}$ for all $a, b \in A$. An involution is called **standard** if $a\overline{a} \in F$ for all $a \in A$. As usual, we consider $F \subset A$ as the F-subspace spanned by the identity in A.

(a) Prove that if $^{-}$ is a standard involution on an F-algebra A then $a + \overline{a} \in F$ for all $a \in A$. **Hint.** Consider $(1 + a)(\overline{1 + a})$.

(b) If $^{-}$ is a standard involution on an F-algebra A, define the **reduced trace** $\mathrm{trd} : A \to F$ by $a \mapsto a + \overline{a}$ and the **reduced norm** $\mathrm{nrd} : A \to F$ by $a \mapsto a\overline{a}$. Prove that any $a \in A$ satisfies $a^2 - \mathrm{trd}(a)a + \mathrm{nrd}(a) = 0$. This is an analogue of the Cayley–Hamilton theorem and one often calls $x^2 - \mathrm{trd} = (a)x + \mathrm{nrd}(a) \in F[x]$ the reduced characteristic polynomial of $a \in A$.

(c) Prove that if K is an F-algebra of dimension 2, then K is commutative and admits a unique standard involution. What is this in the case that K/F is a separable extension of degree 2? What about $K = F \times F$? What about the "dual numbers" $K = F[x]/(x^2)$?

(d) Prove that if A is a quaternion algebra over F, then A has a unique standard involution. **Hint.** Restrict to a quadratic extension contained in A.

5. About division algebras.

(a) Over an algebraically closed field F, the only finite dimensional division F-algebra if F itself. **Hint.** Use the existence of eigenvalues of linear operators on finite dimensional vector spaces over algebraically closed fields.

(b) Let $A = \mathbb{C}(t)$ the rational function field over the complex numbers. Then A is an infinite dimensional division $\mathbb{C}$-algebra. Where does your previous argument break down for A?

(c) Prove that if A is a (nonsplit) quaternion algebra over a field F (of characteristic not 2) and K/F is a quadratic extension with $K \subset A$ a sub F-algebra, then $A \otimes_F K$ is split.

(d) Read the proof of *Gille–Szamuely* Lemma 2.4.4, really Theorem 2.2.1. This was not as easy as I made it appear in class!

Yale University, Department of Mathematics, 10 Hillhouse Ave, New Haven, CT 06511
E-mail address: `asher.auel@yale.edu`