Dartmouth College Department of Mathematics
**Math 115 Number Theory:**
**Galois Cohomology and Descent**
Spring 2024

Group Work # 1 (Friday, April 5th and 12th)

**Reading:** [M] Ch. 7, [GS] §4.1, [S] §1.1-1.4, [Sh] Ch. I, IV.1

**Group Work:** To be discussed during the X-hour, with the discussion led by a student selected ahead of time.

**1.** Understand the following facts about subgroups $H$ of a topological group $G$.

(a) The closure $\overline{H}$ of any subgroup $H$ of $G$ is a subgroup.

(b) The closure $\overline{H}$ of any normal subgroup $H$ of $G$ is a normal subgroup.

(c) The coset space $G/H$, with the quotient topology, is a topological group if $H$ is a normal subgroup of $G$.

(d) The trivial subgroup $\{1_G\}$ is closed if and only if $G$ is Hausdorff. Thus $G/\overline{\{1_G\}}$ is a Hausdorff topological group (called the **Kolmogorov quotient**).

(e) The coset space $G/H$, with the quotient topology, is Hausdorff if and only if $H$ is closed in $G$. (This is why one generally sticks to closed subgroups when taking quotients of topological groups.)

(f) The connected component of the identity $G^\circ$ in $G$ is a closed normal subgroup. The quotient $G/G^\circ$ is a totally disconnected Hausdorff topological group.

(g) If $G$ is a connected topological group, then $G$ does not contain any proper open subgroups.

(h) Every open subgroup $H$ of $G$ is closed.

(i) Every finite index closed subgroup $H$ of $G$ is open.

(j) If $G$ is compact then every open subgroup $H$ has finite index in $G$. In particular, a subgroup $H$ of $G$ is open if and only if it is closed and of finite index.

It is a highly nontrivial theorem of Nikolov and Segal, whose proof depends on the classification of finite simple groups, that if $G$ is a topologically finitely generated (i.e., contains a finitely generated dense subgroup) profinite group, then any subgroup of finite index is open. On the other hand, the absolute Galois group $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ has uncountably many nonopen normal finite index subgroups (see [M] Chapter 7 page 103)!

**2.** Let $X$ be a set and $\mathcal{B}$ a set of subsets of $X$. Then $\mathcal{B}$ is called a **base** or **basis** for a topology on $X$ if $\mathcal{B}$ covers $X$ and any intersection of a finite collection of elements of $\mathcal{B}$ is a union of elements of $\mathcal{B}$.

(a) Verify that the set $\mathcal{T}$ of all unions of elements of $\mathcal{B}$ is a topology on $X$, called the topology **generated** by $\mathcal{B}$.

(b) Prove that the set of bounded open intervals in $\mathbb{R}$ is a base for the standard Euclidean topology. Prove that the set of bounded open intervals in $\mathbb{R}$ whose endpoints are rational is also a base for the standard Euclidean topology.

(c) Let $G$ be a abstract group. Prove that the set of all left cosets of all subgroups of finite index is a basis for a topology on $G$. The topology generated is called the **profinite topology** on $G$. Prove that the set of all cosets of normal subgroups of finite index is also a base for the profinite topology on $G$.

(d) Describe the profinite topology on the additive groups $\mathbb{Z}$ and $\mathbb{R}$?

**3.** The **profinite completion** $\widehat{G}$ of an abstract group $G$ is defined to be the inverse limit $\varprojlim_N G/N$ over the inverse system of quotients $G/N$ indexed by the normal subgroups $N$ of finite index in $G$, ordered so that for any inclusion $N \subset N'$ we consider the induced quotient $G/N' \to G/N$.

(a) Prove that there is a canonical homomorphism $G \to \widehat{G}$, which is universal for homomorphisms from $G$ to profinite groups.

(b) Describe the profinite completion of the additive group $\mathbb{R}$?

(c) Prove that $\widehat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$ and is topologically generated by 1.

**4.** Prove that the following statements are equivalent for an abstract group $G$.

(a) The profinite topology on $G$ is Hausdorff.

(b) The intersection $\bigcap U$, taken over all finite index normal subgroups $U$ of $G$, is the trivial subgroup $\{1_G\}$.

(c) The canonical homomorphism $G \to \widehat{G}$ is injective.

A group $G$ satisfying these conditions is called **residually finite**. Any profinite group (hence, any Galois group) is residually finite. Prove that any free group is residually finite.

As a warning, if $G$ is profinite (hence residually finite), then the injection $G \to \widehat{G}$ may fail to be an isomorphism (i.e., a profinite group may not be equal to to profinite completion)! However, by the result of Nikolov and Segal mentioned above, any topologically generated profinite group is isomorphic to its profinite completion.

Residually finite groups are important in geometric group theory, as they contain the class of fundamental groups of compact 3-manifolds.

**5.** Let $G$ be a locally compact (i.e., every point has a compact neighborhood) Hausdorff topological group. Examples include any discrete group, any profinite group, $\mathbb{Q}_p$, and $\mathbb{R}$. 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 $\phi : G \to U$, and equip $\check{G}$ with the compact-open topology.

(a) Prove that $\check{\mathbb{Z}} \cong U$ and that $\check{U} \cong \mathbb{Z}$. This underlies the theory of Fourier coefficients.

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

(c) Prove that if $G$ is a finite abelian group, then $\check{G} \cong G$. This underlies the class of "Fast Fourier Transform" algorithms.

(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.** View $\mathbb{Q}/\mathbb{Z}$ as a direct limit.

Pontryagin duality is the statement that for an topological abelian group, the canonical evaluation map $G \to \check{\check{G}}$ defined by $g \mapsto (\phi \mapsto \phi(g))$ is an isomorphism of topological groups.

**6.** Let $G$ be a topological group and $X$ a set. Then $G$ acts continuously on $X$ if the action map $G \times X \to X$ is continuous.

(a) Assume that $X$ has the discrete topology. Prove that $G$ acts continuously on $X$ if and only if the stabilizer subgroup $G_x \subset G$ is open for every $x \in X$. A discrete set with a continous action of $G$ is called a **discrete $G$-set**.

(b) Prove that if $G$ is compact and $X$ is a discrete $G$-set then all orbits of $G$ in $X$ are finite.

(c) Let $K/F$ be a Galois extension with Galois group $G$. Verify that $K$ is a discrete $G$-set, and more generally, that the $K$-vector space $K^n$ is a discrete $G$-set with the diagonal action $\sigma(\alpha_1, \ldots, \alpha_n) = (\sigma(\alpha_1), \ldots, \sigma(\alpha_n))$. Describe the $G$-orbit of $(\alpha_1, \ldots, \alpha_n) \in K^n$.

**7.** Let $F$ be a field, $\mathsf{Alg}_F$ be the category of commutative unital $F$-algebras, and $\mathsf{Set}$ the category of sets. We introduce **affine $n$-space** $\mathbb{A}^n$ over $F$ as the functor $\mathsf{Alg}_F \to \mathsf{Set}$ defined on objects by $\mathbb{A}^n(R) = R^n$ for all $R \in \mathsf{Alg}_F$ and on morphisms $\varphi : R \to S$ by $\mathbb{A}^n(\varphi) = \varphi^n : R^n \to S^n$.

Given a system of polynomials $f_1, \ldots, f_m \in F[x_1, \ldots, x_n]$, the associated **affine $F$-variety** $V = V(f_1, \ldots, f_n)$ is the subfunctor $V : \mathsf{Alg}_F \to \mathsf{Set}$ of $\mathbb{A}^n$ defined by

$$V(R) = \{(r_1, \ldots, r_n) \in R^n \ : \ f_1(r_1, \ldots, r_n) = \cdots = f_m(r_1, \ldots, r_n) = 0\}.$$

We say that $V$ is a **closed subvariety** of $\mathbb{A}^n$ and often write $V \subset \mathbb{A}^n$. Affine varieties are convenient tools for talking about solutions to systems of polynomial equations. Technically, we are considering the **functor of points** viewpoint of the $F$-variety $V$; later on, you may learn about the scheme theory viewpoint.

(a) Let $V \subset \mathbb{A}^2$ be the affine $\mathbb{Q}$-variety defined by $x^2 + y^2 - 1$. Show that $V(\mathbb{Q})$ can be described in terms of Pythagorean triples, that $V(\mathbb{R})$ is a unit circle, and that $V(\mathbb{C})$ is a punctured 2-sphere.

(b) Prove that the affine $F$-variety $V(xy - 1) \subset \mathbb{A}^2$ is isomorphic (as functors) to the **multiplicative group** functor $\mathbb{G}_m : \mathsf{Alg}_F \to \mathsf{Set}$ defined by $\mathbb{G}_m(R) = R^\times$ for all $R \in \mathsf{Alg}_F$.

(c) Let $g \in F[x_1, \ldots, x_n]$. Prove that the affine $F$-variety $V(g\, x_{n+1} - 1) \subset \mathbb{A}^{n+1}$ is isomorphic (as functors) to the functor $\mathbb{A}^n \smallsetminus V(g) : \mathsf{Alg}_F \to \mathsf{Set}$ defined by

$$(\mathbb{A}^n \smallsetminus V(g))(R) = \{(r_1, \ldots, r_n) \in R^n \ : \ g(r_1, \ldots, r_n) \in R^\times\}$$

In particular, for any field extension $K/F$, we have that

$$(\mathbb{A}^n \smallsetminus V(g))(K) = \mathbb{A}^n(K) \smallsetminus V(g)(K),$$

which justifies the notation. The $F$-varieties $\mathbb{A}^n \smallsetminus V(g) \subset \mathbb{A}^n$ are called **basic open**, **standard open**, or **distinguished open** subsets.

(d) Prove that a finite intersection of affine $F$-varieties in $\mathbb{A}^n$ is an affine $F$-variety.

(e) Let $V \subset \mathbb{A}^n$ be an affine $F$-variety and $K/F$ be a Galois extension with group $G$. Prove that $V(K)$ is a discrete $G$-set with respect the the action of $G$ on $K^n$.

Dartmouth College, Department of Mathematics, Kemeny Hall, Hanover, NH 03755
*E-mail address*: asher.auel@dartmouth.edu