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

Group Work # 3 (Friday, May 10, 17, 24)

Reading: *Gill–Szamuely* §2.3, 3.2, 3.4, 4.1, *Serre* §1.1-1.4, *Shatz* 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. *Extension class.* Learn how group extensions $1 \to A \to E \to G \to 1$ of G by A are classified by $H^2(G, A)$, see [GS] Example 3.2.6. Learn about the Baer sum of extensions, and how this gives an explicit way of representing the abelian group structure on $H^2(G, A)$.

2. Let G be a finite cyclic group of order n and fix a generator σ. Let A be a G-module. Consider the maps $N : A \to A$ and $\sigma - 1 : A \to A$ defined by

$$N(x) = \sum_{i=0}^{n-1} \sigma^i(x) \qquad \text{and} \qquad (\sigma - 1)(x) = \sigma(x) - x.$$

(a) Verify that the $\mathbb{Z}[G]$-module $\mathbb{Z}$ has a free resolution

$$\cdots \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{\sigma-1} \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{\sigma-1} \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \to 0$$

where $\epsilon : \mathbb{Z}[G] \to \mathbb{Z}$ is the usual **augmentation** map sending every group element to 1. **Hint.** Finally learn about homotopy retractions.

(b) Show that this resolution gives the following periodicity on the level of cohomology

$$H^0(G, A) = A^G \qquad \text{and} \qquad H^i(G, A) = \begin{cases} {}_NA/(\sigma - 1)A & \text{if } i \text{ is odd} \\ A^G/NA & \text{if } i \text{ is even} \end{cases}$$

for $i > 0$, where ${}_NA = \ker(N : A \to A)$.

(c) Give formulas for $H^i(G, A)$ when G acts trivially on A. For example, for G acting trivially on $\mathbb{Z}$ and on $\mathbb{Z}/n\mathbb{Z}$, compute $H^2(G, \mathbb{Z})$ and $H^2(G, \mathbb{Z}/n\mathbb{Z})$. What is the interpretation in terms of group extensions?

(d) Now, do the above three parts when G is infinite cyclic (e.g., $G = \mathbb{Z}$). **Hint.** The free resolution, as above, is quite short, hence the cohomology is no longer periodic, but vanishes in high degree!

3. Let L/K be a finite Galois extension with cyclic Galois group G. Recall that the usual field-theoretic norm map $N_{L/K} : L \to K$ is given by $N_{L/K}(x) = \prod_{\sigma \in G} \sigma(x)$.

(a) Use the cohomology of cyclic groups to show that the cohomological form of Hilbert's Theorem 90, namely $H^1(G, L^\times) = 1$, is equivalent to the classical form: that $x \in L^\times$ satisfies $N_{L/K}(x) = 1$ if and only if $x = \sigma(y)/y$ for some $y \in L^\times$.

(b) Use the cohomology of cyclic groups to prove that $H^2(G, L^\times) \cong K^\times / N_{L/K}(L^\times)$.

(c) Conclude that $H^2(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), \mathbb{C}^\times) \cong \{\pm 1\}$ and that $H^2(\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p), \mathbb{F}_{p^2}^\times)$ is trivial.

4. Let K be a field of characteristic 0 with algebraic (also separable) closure $\overline{K}$. Assume that the absolute Galois group $G_K = \mathrm{Gal}(\overline{K}/K)$ is cyclic of prime order p.

(a) Prove that $H^2(K, \overline{K}^\times) \cong K^\times / K^{\times p}$. **Hint.** Use the long exact sequence in Galois cohomology associated to the Kummer sequence, along with Hilbert's Theorem 90, and the periodicity of the cohomology of cyclic groups.

(b) Conclude that $N_{\overline{K}/K}(\overline{K}^\times) = K^{\times p}$ and hence that the only possibility is $p = 2$ and $\overline{K} = K(\sqrt{-1})$. **Hint.** Show that K contains a primitive pth root of unity (if not try adjoining it), hence that the cyclic extension $\overline{K}/K$ is a Kummer extension, i.e., $\overline{K} = K(\alpha)$ where $\alpha^p = y$ for some $y \in K^\times \smallsetminus K^{\times p}$, then try computing $N_{\overline{K}/K}(\alpha)$.

(c) Show that declaring the squares in $K^\times$ to be positive will equip K with the structure of an ordered field.

(d) (Artin–Schreier) Prove that if K is a field of characteristic 0 whose absolute Galois group is a nontrivial finite group, then $\overline{K} = K(\sqrt{-1})$ and K is an ordered field where the squares are positive. **Hint.** Take a p-Sylow subgroup of the Galois group and use the fact that p-groups are solvable, then iteratively apply the previous results.

Remark. Such fields are called **real closed**. In fact, Artin and Schreier proved that in positive characteristic, the absolute Galois group is either trivial or infinite.

5. *Artin–Schreier theory.* [GS] 4.4. Let F be a field of characteristic $p > 0$ and F^s a separable closure.

(a) Let K/F be a finite Galois extension of fields with group G. Show that the normal basis theorem implies that $K \cong \mathbb{F}[G]$ as G-modules.

(b) Prove that $H^i(F, F^s) = 0$ for all $i > 0$. Hint. Use the above, together with the adjunct property

$$H^i(G, F[G]) = \mathrm{Ext}^i_{\mathbb{Z}[G]}(\mathbb{Z}, F[G]) = \mathrm{Ext}^i_{F[G]}(F, F[G])$$

together with the fact that $\mathbb{F}[G]$ is a free $\mathbb{F}[G]$-module, to prove that $H^i(G, K) = 0$ if K/F is a Galois extension with group G, then take a limit.

(c) Prove that the map $\wp : F^s \to F^s$ defined by $\wp(x) = x^p - x$ is a surjective homomorphism of G_F-modules whose kernel is the group $\mathbb{Z}/p\mathbb{Z}$ with trivial action. Hence there is, in the language of group schemes above, an exact sequence

$$0 \to \mathbb{Z}/p\mathbb{Z} \to \mathbb{G}_a \xrightarrow{\wp} \mathbb{G}_a \to 0$$

(d) Use the long exact sequence to prove that the map

$$F/\wp(F) \to H^1(F, \mathbb{Z}/p\mathbb{Z})$$

defined by $a \mapsto (\sigma \mapsto \sigma(\alpha) - \alpha)$ where α is a root of $x^p - x - a$, is an isomorphism of abelian groups.

(e) Conclude that every $\mathbb{Z}/p\mathbb{Z}$-Galois extension K/F is of the form $K = F(\alpha)$ where α is a root of $x^p - x - a$ for some $a \in F$. In this case, determine an explicit generator for the Galois group. What happens when $a = 0$?

6. *Group schemes.* Let F be a field, Alg_F the category of commutative unital F-algebras, and Grp the category of groups. An **F-group functor** is a functor $G : \mathsf{Alg}_F \to \mathsf{Grp}$. For example, take the functor $\mathrm{GL}_n : \mathsf{Alg}_F \to \mathsf{Grp}$ where $\mathrm{GL}_n(R)$ is the set of invertible $n \times n$ matrices over R. Here GL_n can be replaced with SL_n or PGL_n or your favorite linear algebraic group, but it could also be given be the functor of points of an elliptic curve or abelian variety. We write $\mathbb{G}_m = \mathrm{GL}_1$ for the functor $\mathbb{G}_m(R) = R^\times$, called the **multiplicative group**, and $\mathbb{G}_a$ for the functor $\mathbb{G}_a(R) = (R, +)$, called the **additive group**.

An F-group functor G is an **affine F-group scheme** if there exists $A \in \mathsf{Alg}_F$ and an isomorphism of functors $G \cong \mathrm{Hom}_{\mathsf{Alg}_F}(A, -)$, where we consider $G : \mathsf{Alg}_F \to \mathsf{Set}$ as a functor to the category of sets via the forgetful functor $\mathsf{Grp} \to \mathsf{Set}$. Such an F-algebra A is said to **represent** G, and G is called a **representable functor**.

(a) Show that $\mathbb{G}_a$ is represented by $F[x]$ and that $\mathbb{G}_m$ is represented by $F[x, x^{-1}]$. Think about why the group functors determined by all of your favorite linear algebraic groups defined over F, e.g., GL_n, SL_n, PGL_n, O_n, μ_n, are representable by finitely generated F-algebras.

(b) Let G be an F-group functor. Show that if K/F is a Galois extension then $\mathrm{Gal}(K/F)$ acts on $G(K)$. Show that if G is represented by an F-algebra A, then the isomorphism $G(K) \cong \mathrm{Hom}_{\mathsf{Alg}_F}(A, K)$ is $\mathrm{Gal}(K/F)$-equivariant, with the action on the Hom group being given by postcomposition as usual.

(c) Show that if G is represented by a finitely generated F-algebra A, then the action of $\mathrm{Gal}(K/F)$ on $G(K)$ is continuous. In this case, we write $H^i(F, G) := H^i(F, G(F^s))$, where only $i = 0, 1$ is possible when G is nonabelian, so that, for exampe, Hilbert 90 reads $H^1(F, \mathrm{GL}_n) = 0$. **Hint.** Use the fact that a profinite group acts on a discrete set continuously if and only if all stabilizers are open subgroups.

(d) For a separable quadratic extension K/F, define

$$\mathbb{G}_m^K(R) = \ker(N : (R \otimes_F K)^\times \to R^\times)$$

where $N(r \otimes \alpha) = r^2 N_{K/F}(\alpha)$. Prove that if $F = \mathbb{R}$ then $\mathbb{G}_m^{\mathbb{C}} = \mathbb{S}^1$ is the "unit circle" $\mathbb{S}^1(R) = \{(x, y) \in R^2 : x^2 + y^2 = 1\}$. Prove that if $K = F \times F$, then $\mathbb{G}_m^K \cong \mathbb{G}_m$, and hence that the base change of $\mathbb{G}_m^K$ to the separable closure of F is isomorphic to $\mathbb{G}_m$. Thus $\mathbb{G}_m^K$ is a twisted form of $\mathbb{G}_m$. Use Galois descent and twisting, and the fact that $\mathrm{Aut}(\mathbb{G}_m) = \mathbb{Z}/2\mathbb{Z}$, to show that every twisted form of $\mathbb{G}_m$ is isomorphic to $\mathbb{G}_m^K$ for some separable quadrtic K/F. These are called the rank 1 tori over F.

7. *Induced modules.* Let G be a profinite group, $H \subset G$ a closed subgroup, and B an H-module. Consider the abelian group

$$\mathrm{Ind}_H^G(B) = \{f : G \to B \mid f \text{ continuous and } f(\tau\sigma) = \tau f(\sigma) \text{ for all } \tau \in H,\ \sigma \in G\}$$

(a) Prove that $\mathrm{Ind}_H^G(B)$ is a G-module via $(\rho \cdot f)(\sigma) = f(\sigma\rho)$ for $\rho \in G$. **Hint.** The hard part is to show that G acts continuously. Use the fact that a profinite group acts on a discrete set continuously if and only if all stabilizers are open subgroups. For this, note that since each f is continuous from a compact space to a discrete space, it has only finitely many values, so that f is a finite sum of characteristic functions of open sets. Reduce to f being a single characteristic function of an open set and handle this case by itself.

(b) Recall that if A is a G-module, we have the restriction $\mathrm{Res}^G_H(A)$, which is just A considered as an H-module with the restricted action. Prove that Ind^G_H and Res^G_H are adjoint functors between the categories of H-modules and G-modules, i.e., that for any G-module A and any H-module B the map

$$\mathrm{Hom}_G(A, \mathrm{Ind}^G_H(B)) \to \mathrm{Hom}_H(\mathrm{Res}^G_H(A), B)$$

defined by $\varphi \mapsto (a \mapsto \varphi(a)(1))$, is an isomorphism. **Hint.** Besides proving that this map makes sense, you need to prove it is an isomorphism. For this, prove that $\psi \mapsto (a \mapsto (\sigma \mapsto \psi(\sigma a)))$, whatever that means, is an inverse.

(c) Prove Shapiro's Lemma, that for any G-module A and any H-module B, the map

$$H^i(G, \mathrm{Ind}^G_H(B)) \to H^i(H, B)$$

induced from the compatibility of the map $\mathrm{Ind}^G_H(B) \to B$, defined by $f \mapsto f(1)$, with the natural inclusion $H \hookrightarrow G$, is an isomorphism of cohomology groups. **Hint.** For G finite, use the fact that the standard resolution of $\mathbb{Z}$ by $\mathbb{Z}[G]$-modules is also a resolution by $\mathbb{Z}[H]$-modules since $\mathbb{Z}[G]$ is a free $\mathbb{Z}[H]$-module. Then apply the above adjoint property for $A = \mathbb{Z}$ to get Shapiro's Lemma for finite groups G, using the fact that cohomology is an Ext group, then take limits.

(d) Assume that $H \subset G$ is an open subgroup, so in particular, has finite index. For any G-module A consider the map $\mathrm{Ind}^G_H(\mathrm{Res}^G_H(A)) \to A$ defined by $f \mapsto \sum_\rho \rho(f(\rho^{-1}))$ where the sum ranges over coset representatives ρ for H in G. Show that this map is independent of the choice of coset representatives and is a homomorphism of G-modules. The corestriction map is then defined to be the composition

$$\mathrm{cor} : H^i(H, \mathrm{Res}^G_H(A)) \cong H^i(G, \mathrm{Ind}^G_H(\mathrm{Res}^G_H(A))) \to H^i(G, A)$$

of the isomorphism in Shapiro's Lemma and the map on cohomology induced from the above map.

(e) Prove that the composition

$$H^i(G, A) \xrightarrow{\mathrm{res}} H^i(H, \mathrm{Res}^G_H(A)) \xrightarrow{\mathrm{cor}} H^i(G, A)$$

of restriction and corestriction is multiplication by the index $[G : H]$. Conclude, as in class, that any cohomology group $H^i(G, A)$ is a torsion group for $i > 0$.

8. *Cup products.* [GS] 3.4, [Sh] II.3. Let G be a profinite group and A, B, and C be G-modules. A pairing $\theta : A \times B \to C$ is called G-bilinear if it is a $\mathbb{Z}$-bilinear map such that $\theta(\sigma(a), \sigma(b)) = \sigma(\theta(a, b))$ for all $\sigma \in G$, $a \in A$, and $b \in B$.

(a) Review the construction of the associated cup product map

$$H^i(G, A) \times H^j(G, B) \to H^{i+j}(G, C).$$

(b) Let Γ be a profinite group. Prove that if $1 \to A \to B \to C \to 1$ is a short exact sequence of discrete Γ-groups, with A mapping into the center of B, then the longish exact sequence can be extended by a coboundary map $\delta^2 : H^1(F, C) \to H^2(F, A)$.

(c) Let F be a field of characteristic $\neq 2$. Consider the short exact sequence of affine F-group schemes

$$1 \to \mu_2 \to \mathrm{SL}_2 \to \mathrm{PGL}_2 \to 1$$

using the group scheme language from the sixth problem. Recall that $H^1(F, \mathrm{PGL}_2)$ is in bijection with the set of quaternion algebras over F up to isomorphism. Prove that the coboundary map $\delta^2 : H^1(F, \mathrm{PGL}_2) \to H^2(F, \mu_2)$ from the previous part is injective.

(d) For $a \in F^\times$ denote by $(a) \in F^\times/F^{\times 2} \cong H^1(F, \mu_2)$ the associated class. Prove that, under the cup product $H^1(F, \mu_2) \times H^1(F, \mu_2) \to H^2(F, \mu_2)$ associated to the multiplication pairing $\mu_2 \times \mu_2 \to \mu_2$, we have

$$(a) \cup (b) = \delta^2(a, b)$$

where (a, b) is the usual quaternion algebra and δ^2 is the coboundary map from the previous part. **Hint.** See the heavy homological algebra and cohomology computations in GS Propositions 3.4.9 and 4.7.3 for inspiration. Can you prove this in an elementary way purely on the level of cocycles?

9. *Fourier transforms.* Cf. Ramakrishnan and Valenza, *Fourier analysis on number fields*, §1.2, 3.1–3.4. Recall, from GW1, the notion of the Pontryagin dual group $\check{G}$, the group of continuous homomorphisms $\chi : G \to U$ where $U \subset \mathbb{C}^\times$ is the unit circle, of a locally compact topological group G.

(a) Make sure you understand the following facts: $\check{G}$ is an abelian locally compact topological group; if G is a profinite group then $\check{G}$ is a discrete torsion group and vice versa; $\widehat{\mathbb{Q}/\mathbb{Z}} \cong \widehat{\mathbb{Z}}$ and $\check{\widehat{\mathbb{Z}}} \cong \mathbb{Q}/\mathbb{Z}$. **Hint.** For a profinite group G, convince yourself that any continuous homomorphism from G to the unit circle has finite image.

(b) Understand the canonical evaluation homomorphism $G \to \check{\check{G}}$. The Pontryagin duality theorem states that the evaluation homomorphism induces an isomorphism $G^{\mathrm{ab}} \to \check{\check{G}}$ from the abelianization. Note that the Pontryagin dual of G and G^{ab} are the same.

(c) Understand the existence and uniqueness of a (left-invariant) Haar measure μ on any locally compact topological group G. Let $L^1(G)$ be the space of μ-integrable complex-valued functions $f : G \to \mathbb{C}$. Define the **Fourier transform** $\check{f} : \check{G} \to \mathbb{C}$ by

$$\check{f}(\chi) = \int_G f(x)\overline{\chi}(x)\, dx$$

for $\chi \in \check{G}$. Understand the existence of the dual Haar measure $\check{\mu}$ on $\check{G}$ and the Fourier inversion formula.

(d) Recall that if $F = \mathbb{F}_p$ and $G = G_F$, then $G \cong \widehat{\mathbb{Z}}$ with the Frobenius automorphism $\phi \in G_F$ defined by $\phi(x) = x^p$ corresponding to $1 \in \widehat{\mathbb{Z}}$. Letting $K = \mathbb{F}_{p^n}$, then the extension K/F is Galois with group $\mathbb{Z}/n\mathbb{Z}$ generated by Frobenius, and the associated quotient $\psi : \widehat{\mathbb{Z}} = G \to \mathrm{Gal}(K/F) = \mathbb{Z}/n\mathbb{Z}$ defined by restricting an automorphism to K coincides with the quotient appearing in the inverse limit.

Define a function $f : G \to \mathbb{C}$ by $f(x) = e^{2\pi i \psi(x)/n}$. Prove that $\int_G f(x)\, dx = 0$. Compute the Fourier transform as a function $\check{F} : \mathbb{Q}/\mathbb{Z} = \check{G} \to \mathbb{C}$.

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