Dartmouth College Department of Mathematics
Math 125 Current Problems in Number Theory:
Galois Cohomology and Descent
Winter 2022

Group Work # 3 (Thursday, February 10)

Reading: *Gill–Szamuely* §2.3, 4.1, *Serre* §1.1-1.4, *Shatz* Ch. I, IV.1

Group Work: To be discussed during the second half of class on Thursday, with the discussion led by a student selected ahead of time.

Notation: Let G be a profinite group and A a G-group. Write $Z^1(G,A)$ for the set of crossed homomorphisms $a : G \to A$ and $H^1(G,A)$ for the first cohomology set of G with coefficients in A. Recall that if A is an abelian group then $Z^1(G,A)$ and $H^1(G,A)$ are abelian groups.

1. Let G be a group and A an abelian G-group. The fact that G acts on A via automorphisms can be expressed via a homomorphism $G \to \mathrm{Aut}(A)$. Thus we can form the semidirect product $F = A \rtimes G$ with respect to this action, with its projection homomorphism $f : F \to G$. Thus F is the set $A \times G$ with operation $(a,g)\cdot(a',g') = (a\,g(a'), gg')$. A **section** of F is a set map $s : G \to F$ such that $f \circ s = \mathrm{id}_G$. A **splitting** of F is section that is a homomorphism.

(a) For a section $s : G \to F$ write $s(g) = (\alpha(g), g)$ for a set map $\alpha : G \to A$. Prove that s is a splitting if and only if α is a crossed homomorphism.

(b) We define two splittings $s, s' : G \to F$ to be equivalent if there exists $a \in A \subset F$ such that $s'(g) = as'(g)a^{-1}$ for all $g \in G$. Prove that the set of equivalence classes of splittings of F is in bijection with $H^1(G,A)$.

(c) More generally, consider any extension

$$1 \to A \to F \xrightarrow{f} G \to 1$$

of G by A that is compatible with the action of G on A, i.e., $g(a) = \tilde{g}a\tilde{g}^{-1}$ for any lift $\tilde{g} \in F$ of g (convince yourself that this condition does not depend on the choice of lift). An automorphism of the extension is an automorphism $\phi : F \to F$ such that $\phi|_A : A \to A$ restricts to an automorphism. This defines a subgroup $\mathrm{Aut}(f) \subset \mathrm{Aut}(F)$. Any $a \in A$ determines an inner automorphism ad_a of the extension by conjugation by a. This defines a subgroup $\mathrm{Inn}(f) \subset \mathrm{Aut}(f)$. Consider the left right coset space $\mathrm{Out}(f) = \mathrm{Inn}(f)\backslash\mathrm{Aut}(f)$, equivlently, the set of equivalence classes for where automorphisms of the extension ϕ and ϕ' are equivalent if $\phi' = \mathrm{ad}_a \circ \phi$ for some $a \in A$.

For a crossed homomorphism $\alpha : G \to A$ and an automorphism ϕ of the extension, define $\alpha.\phi$ by $(\alpha.\phi)(x) = \alpha(f(x))\,f(x)$ for $x \in F$. Prove that $\alpha.\phi$ is an automorphism of the extension and that this descends to a well-defined action of $H^1(G,A)$ on $\mathrm{Out}(f)$, and that this action is simply transitive (in particular, $H^1(G,A)$ and $\mathrm{Out}(f)$ have the same cardinality).

2. Let S_n denote the symmetric group on $n \geqslant 2$ letters.

(a) Let A be an abelian group considered with trivial S_n-action. Prove that $H^1(S_n, A) = A[2]$, where $A[2]$ denotes the 2-torsion subgroup of A. Hint: Recall that the abelianization of S_n is given by the sign homomorphism.

(b) Consider the usual action of S_n on $\mathbb{F}_2^n$ permutations and V_n the quotient of $\mathbb{F}_2^n$ by the S_n-invariant subspace spanned by $(1, \ldots, 1)$. The V_n is an abelian S_n-group, usually called the **standard representation**. Prove that $H^1(S_n, V_n) = 0$.

3. Let S_3 denote the symmetric group on 3 letters, A_3 its alternating subgroup, C_2 the cyclic group of order 2, and

$$1 \to A_3 \to S_3 \to C_2 \to 1$$

the short exact sequence of groups induced by the sign homomorphism. Let F be a field of characteristic not 2.

(a) Recall the discriminant of a separable field extension K/F of degree n: Let L/F be the Galois closure of K/F and $G = \mathrm{Gal}(L/F)$, where $G \subset \S_n$ is a transitive subgroup, then $\Delta(K) = L^H$ where $H = A_n \cap G$ is the subgroup of even permutations of G. Prove that under the isomorphism $H^1(F, C_2) = H^1(F, \mu_2)$, we have that $\Delta(K)$ coincides with the square class of the usual discriminant $(d_{K/F}) \in F^\times/F^{\times 2}$.

Finally, for an étale algebra A, define $\Delta(A)$ by it's decomposition into a product of finite separable field extensions $\Delta(K_1 \times \cdots \times K_r) = \Delta(K_1) \cdots \Delta(K_r)$, where here, you can either think of this product in the abelian group $H^1(F, C_2)$ or in $F^\times/F^{\times 2}$.

(b) Prove that the induced map $H^1(F, S_3) \to H^1(F, C_2)$ on Galois cohomology has the interpretation $[A] \mapsto [\Delta(A)]$ on étale algebras. Conclude, from the longish exact sequence, a standard result from Galois theory: a cubic field extension is cyclic if and only if its discriminant is a square.

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