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

Group Work # 2 (Thursday, April 26)

Reading: [GS] §1.1-1.2, 2.1-2.2, 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. Let A be an (associative unital) F-algebra. We say that an F-linear map $\overline{} : A \to A$ 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 $\overline{}$ 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 $\overline{}$ is a standard involution on an F-algebra A, define the **(involution) trace** $t : A \to F$ by $a \mapsto a + \overline{a}$ and the **(involution) norm** $n : A \to F$ by $a \mapsto a\overline{a}$. Prove that any $a \in A$ satisfies $a^2 - t(a)a + n(a) = 0$. This is an analogue of the Cayley–Hamilton theorem and one often calls $x^2 - t(a)x + n(a) \in F[x]$ the involution 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.

2. About division algebras.

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

(b) Let $\mathbb{C}(t)$ be the rational function field over the complex numbers. Then $\mathbb{C}(t)$ is an infinite dimensional division $\mathbb{C}$-algebra (but clearly far from central). Where does your previous argument break down for A? **Remark.** it turns out that there are no nontrivial central division $\mathbb{C}(t)$-algebras, this is a consequence of Tsen's Theorem. Can you find a new proof of this fact?

(c) The **Weyl algebra** is the unital associative $\mathbb{C}$-algebra generated by t and ∂_t, with the relation (coming from the chain rule) $t\,\partial_t - \partial_t\,t = 1$. This algebra acts by differential operators, with t acting by multiplication and ∂_t acting by taking the formal derivative with respect to t, on the polynomial ring $\mathbb{C}[t]$, e.g., $(\partial_t\,t)f(t) = \partial_t(tf(t)) = f(t)+tf'(t)$. Prove that the Weyl algebra is an infinite dimensional central simple $\mathbb{C}$-algebra. Where does the argument in part (a) break down?

(d) Prove that if A is a 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. Show that $M_2(F)$ contains any quadratic extension K/F as an F-subalgebra.

(e) Read the proof of [GS] Theorem 2.2.1, really Lemma 2.2.2. This was not as easy as I made it appear in class!

3. 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 $\varphi : G \to \mathrm{Aut}(A)$. Thus we can form the semidirect product $F = A \rtimes_\varphi G$ with respect to this action, i.e., F is the set $A \times G$ with operation $(a, g) \cdot (a', g') = (a\, g(a'), gg')$. Let $f : F \to G$ be the projection homomorphism. 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) Prove that $Z^1(G, A)$ is an abelian group under the usual addition of maps. Show that the map $d : A \to Z^1(G, A)$ defined by $c \mapsto (\sigma \mapsto c - \sigma(c))$ is a well-defined homomorphism and denote by $B^1(G, A) \subset Z^1(G, A)$ its image. Prove that $H^1(G, A) \cong Z^1(G, A)/B^1(G, A)$, hence is an abelian group.

(b) 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. Conclude that this provides a bijection between $Z^1(G, A)$ and the set of splittings of F.

(c) 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 this provides a bijection between $H^1(G, A)$ and the the set of equivalence classes of splittings of F.

(d) More generally, consider any group 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 (why does this condition not depend on the choice of lift?). An automorphism of the extension is an automorphism $\phi : F \to F$ that restricts to an automorphism $\phi|_A : A \to A$. 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 right coset space $\mathrm{Out}(f) = \mathrm{Inn}(f)\backslash\mathrm{Aut}(f)$, equivalently, the set of equivalence classes of automorphisms of the extension, where automorphisms 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 $(\alpha.\phi)(x) = \alpha(f(x))\, \phi(x)$ 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. Conclude that $H^1(G, A)$ and $\mathrm{Out}(f)$ have the same cardinality.

(e) Now let $G = A = C_2$ be the cyclic group of order 2. Let G act on A trivially. Prove that $H^1(C_2, C_2)$ is cyclic of order 2. You know that the two extensions of C_2 by C_2 are

$$1 \to C_2 \to V_4 \to C_2 \to 1$$
$$1 \to C_2 \to C_4 \to C_2 \to 1$$

where V_4 is the Klein four group. Explicitly describe the automorphism groups of these two extensions as subgroups of the automorphism groups $\mathrm{Aut}(V_4) = \mathrm{GL}_2(\mathbb{F}_2)$ and $\mathrm{Aut}(C_4) = \{\pm 1\}$, and show how the outer automorphism groups of the extensions explicitly correspond to $H^1(C_2, C_2)$.

Thus "the first cohomology group of G with coefficients in A corresponds to automorphisms of any group extension of G by A."

4. Let F be a field, Alg_F be the category of commutative unital F-algebras, and Set the category of sets. We introduce **projective n-space** $\mathbb{P}^n$ over F as the functor $\mathsf{Alg}_F \to \mathsf{Set}$ defined on objects $R \in \mathsf{Alg}_F$ as the set $\mathbb{P}^n(R)$ of pairs (L, i) where L is a projective R-module of rank 1 and $i : L \to R^{n+1}$ is a direct summand R-module homomorphism, i.e., there exists a projective R-module P of rank n (called the complement of L) and an R-module homomorphism $p : P \to R^{n+1}$ so that $i + p : L \oplus P \to R^{n+1}$ is an R-module isomorphism, and where we consider (L, i) equivalent to (L', i') if $i = i' \circ l$ for some R-module isomorphism $l : L \to L'$. On morphisms $\varphi : R \to S$, the functor is defined by $\mathbb{P}^n(\varphi)(L, i) = (L \otimes_R S, i \otimes_R \mathrm{id}_S)$. I don't begrudge you if this appears to be a crazy definition!

(a) A **unimodular row** over R is a vector $a = (a_0, \ldots, a_n) \in R^{n+1}$ such that there exists $b = (b_0, \ldots, b_n) \in R^{n+1}$ with $\sum_{i=0}^n a_i b_i = 1$. Prove that if $a \in R^{n+1}$ is a unimodular row, then $Ra \subset R^{n+1}$ is a free rank 1 direct summand, hence the (R, i_a) gives an element of $\mathbb{P}^n(R)$ where $i_a : R \to R^{n+1}$ is the given by scalar multiplying a. (**Hint.** Use b to define a surjection $R^{n+1} \to R$, whose kernel will be the complement.) Prove that two unimodular rows $a, b \in R^{n+1}$ give the same element of $\mathbb{P}^n(R)$ if and only if $a = \lambda b$ for some $\lambda \in R^\times$. Letting $\mathrm{Um}_{n+1}(R)$ be the set of unimodular rows over R, this gives a well-defined map $\mathrm{Um}_{n+1}(R)/R^\times \to \mathbb{P}^n(R)$.

(b) Show that for any field extension K/F, the map $\mathrm{Um}_{n+1}(K)/K^\times \to \mathbb{P}^n(K)$ is a bijection and that $\mathbb{P}^n(K)$ is in bijection with the set of lines through the origin in K^{n+1}. This recovers the usual notion of projective space $\mathbb{P}^n(K) = (K^{n+1} \smallsetminus \{0\})/K^\times$.

(c) Let $R = \mathbb{R}[x, y]/(x^2 + y^2 - 1)$ and consider the ideal $L = (1 + x, y) \subset R$. Prove that L^2 is a principal ideal but that L is not principal. (**Hint.** You may want to use the norm on the quadratic ring extension $R[x] \subset R = R[x][\sqrt{1 - x^2}]$. **Remark.** Evidently, R is not a PID, though it turns out to be a Dedekind domain, and you can see the nonunique factorization $(1 + x)(1 - x) = y^2$.) Consider the 2×2 matrix

$$M = \frac{1}{2}\begin{pmatrix} 1 + x & y \\ y & 1 - x \end{pmatrix}$$

and the associated R-module homomorphism $M : R^2 \to R^2$ defined by matrix multiplication. Prove that the map $i : L \to R^2$ defined by $i(u) = (u, \frac{1-x}{y} u)$ is well-defined and determines an R-module isomorphism $L \to \mathrm{im}(M)$. Prove that there is a direct sum decomposition $\mathrm{im}(M) \oplus \ker(M) = R^2$, and that $\ker(M) = \mathrm{im}(I - M)$ is also isomorphic to L. (**Hint.** Use that $M^2 = M$.) In partiular, L is a projective R-module of rank 1 that is not free. Conclude that $(L, i) \in \mathbb{P}^1(R)$ but is not determined by a unimodular row over R. **Remark.** Geometrically, L corresponds to the Möbius line bundle on the circle.

(d) Consider the two localizations $R_1 = R[\frac{1}{1+x}]$ and $R_2 = R[\frac{1}{y}]$, and for $j = 1, 2$ let $L_j \subset R_j$ be the ideal extended from $L \subset R$ and $i_j : L_j \to R_j^2$ the inclusion extended from $i : L \to R^2$. Prove that each L_j is principal and find a unimodular row $a_j \in \mathrm{Um}_2(R_j)$ that corresponds to the point $(L_j, i_j) \in \mathbb{P}^1(R_j)$. Letting $R_{12} = R[\frac{1}{1+x}, \frac{1}{y}]$, prove that under the functorial maps $\mathbb{P}^1(R_j) \to \mathbb{P}^1(R_{12})$ the images of (L_j, i_j) agree and verify that the your unimodular rows a_1 and a_2 become equal in $\mathrm{Um}_2(R_{12})/R_{12}^\times$. This gives an example where unimodular rows on R_1 and R_2 that agree (up to scaling) over R_{12} can fail to come from a unimodular row over R, whereas this property holds for the functor $\mathbb{P}^1$. **Remark.** In other words the functor $R \mapsto \mathrm{Um}_2(R)$ is a presheaf but not a sheaf, whereas $\mathbb{P}^1$ is a sheaf, which provides some motivation for the crazy definition of $\mathbb{P}^n$.