Lecture 1: Intro, G-modules

1. • Handout Syllabus
   • Discuss texts.
2. Overview:

Defn: Number Theory is the study of $\overset{G}{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})} = \left\{\begin{array}{c}\text{automorphisms} \\ \text{of algebraic} \\ \text{closure of } \mathbb{Q}\end{array}\right\}$, and the sets G naturally acts on.

Example Open Problem: Is every finite group a quotient of G?

Galois Cohomology: Apply homological algebra to study G:

- natural way to classify objects, e.g. "twists of a curve"
- linearizes problems (define new invariants; reveal hidden structure)

This course:

Part 1: Group Cohomology: apply homo. algebra to modules over groups.

- general interest outside number theory!
- Solve problems like:

  Given G = group
  $\overset{G}{A}$ = abelian group

  Find all "extensions of G by A":

$$0 \to A \to E \to G \to 1.$$

Part 2: Galois Cohomology: apply group cohomology to number theory.

- You will get absolutely nowhere in most algebraic number theory from last 30 years without mastering Galois cohomology. "Flip Wiles' Proof"

3. More Details:

Part 1: Group Cohomology.

Cover basic theory with most proofs. Basically no number theory.

- G-modules
- cocycles /coboundaries
- basic homological algebra
- dimension shifting
- inflation restriction
- cup products

etc.

Part 2: Galois Cohomology

Less proofs. More examples. Number theory.

- Profinite groups (and cohomology) /topological groups
- Hilbert 90 (examples)
- Kummer theory
- Descent of field of definition of variety
- Twists of algebraic curve
- Brauer groups (= classes of central simple algebras)
- Elliptic curves
- Duality:
  - Tate Local Duality
  - Pouitou-Tate Global Duality
- Lang's Theorem
- Shafarevich–Tate Group
- Étale Cohomology.

We will follow $\boxed{\text{Ch VII of Serre's "Local Fields"}}$ for a while.

§4.

G-modules:

G = any group

A = abelian group with a G-action

$$G \times A \longrightarrow A$$

$$1.a = a$$
$$s.(a+a') = s.a + s.a'$$
$$(st).a = s.(t.a).$$

$$\Lambda = \mathbb{Z}[G] = \left\{ \sum_{g\in G} n_g g \;:\; n_g \in \mathbb{Z}, \text{ all but finitely many } n_g = 0 \right\}$$ – noncommutative ring!

A is a Λ-module. "a G-module"

$\mathrm{Mod}_G = \{ A : A \text{ is a } G\text{-module} \}$ is an abelian category.

so we have:
direct sums, Kernels, cokernels,

Defn:

- Exact sequence:

$$(\cdots \to) A \xrightarrow{f} B \xrightarrow{g} C \qquad f, g \text{ homomorphism}$$

is exact at B if $\mathrm{im}(f) = \ker(g)$.

- Short exact sequence:

$0 \to A \to B \to C \to 0$ is exact at A, B, C.

- A functor (= "morphism between categories")

$$\mathrm{Mod}_G \longrightarrow \text{Abelian Groups}$$

$$A \longmapsto A^G = \{ a \in A : g.a = a \text{ all } g \in G \}$$

Let $H^0(G,A) = A^G$.

<u>Prop</u>: If $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ is an exact sequence of G-modules, then

$$0 \to A^G \to B^G \to C^G$$

is exact at A^G and B^G.

<u>Proof</u>: Suppose $b \in B^G$ and $g(b) = 0$.
There exists $a \in A$ s.t. $f(a) = b$.
But for any $s \in G$,

$$f(s.a) = s f(a) = sb = b$$

so $f(s.a) = f(a)$ hence $a \in A^G$, since f is injective.

Etc.

<u>Defn</u>: We say $A \longmapsto A^G$ is "<u>left exact</u>".

Formally one can define functors $H^q(G,-) : \mathrm{Mod}_G \to \mathrm{AbGrp}$ for all $q \geq 0$ s.t. if $0 \to A \to B \to C \to 0$ is exact then have

<u>long exact sequence</u>:

$$0 \to A^G \to B^G \to C^G \to H^1(G,A) \to H^1(G,B) \to H^1(G,C) \to$$
$$\to H^2(G,A) \to H^2(G,B) \to H^2(G,C) \to \cdots.$$