Group cohomology and elliptic curves

Sebastiano Tronto

2021-02-24

G-modules

Let G be a group. A (left) G-module is, equivalently:

- An abelian group M with a linear (left) action of G on M
- An abelian group M with a homomorphism $\rho : G \to \mathrm{Aut}(M)$
- A (left) $\mathbb{Z}[G]$-module M

G-invariants

Fix a group G and a G-module M. Notation: $g \cdot m$.

- A **submodule** of M is a subgroup of M closed under the action of G
- $A^G = \{m \in M \mid g \cdot m = m\}$ is a submodule

For Category Theory fans: $H^1(G, M)$ is the right-derived functor of $(-)^G$.

$H^1(G, M)$, explicitly

- A **cocycle** is a map $\varphi : G \to M$ such that $\varphi(gh) = \varphi(g) + g\varphi(h)$.
- A **coboundary** is a cocycle of the form $\varphi_m : g \mapsto g \cdot m - m$.

Definition

The first cohomology group of G with coefficients in M is

$$H^1(G, M) = \frac{\{\textbf{cocycles}\}}{\{\textbf{coboundaries}\}}$$

$H^n(G, M)$, explicitly

- $C^n(G, M) = \{(\text{continuous}) \text{ maps } \quad f : G^n \to M\}$
- Define $d^{n+1} : C^n(G, M) \to C^{n+1}(G, M)$ by

$$\begin{aligned}\left(d^{n+1}(f)\right)(g_1, \dots, g_{n+1}) = {} & g_1 \cdot f(g_2, \dots, g_{n+1}) + \\ & + \sum_{i=1}^{n} (-1)^i f(g_1, \dots, g_i g_{i+1}, \dots, g_{n+1}) + \\ & + (-1)^{n+1} f(g_1, \dots, g_n)\end{aligned}$$

Definition

The n-th cohomology group of G with coefficients in M is

$$H^n(G, M) = \frac{\ker\left(d^{n+1}\right)}{\operatorname{im}\left(d^n\right)}$$

Long exact sequence

If there is a short exact sequence of G-modules

$$0 \to M \to N \to P \to 0$$

Then there is a **long exact sequence**

$$\begin{aligned} 0 \to M^G \to N^G \to & P^G \to H^1(G,M) \to H^1(G,N) \to \\ & \to H^1(G,P) \to H^2(G,M) \to H^2(G,N) \to \cdots \end{aligned}$$

Applications

Invariants defined in terms of group cohomology:

- Brauer group $\mathrm{Br}(K) = H^2(G_K, \mathbb{G}_m)$
- Weil-Châtelet group $\mathrm{WC}(A/K) = H^1(G_K, A)$
- Tate-Shafarevic group $\text{Ш}(A/K) \subseteq \mathrm{WC}(A/K)$

Setting and Notation

For an elliptic curve E over $\mathbb{Q}$:

- Torsion points:
  - $E[n] = \{\alpha \in E(\overline{\mathbb{Q}}) \mid n\alpha = 0\}$
  - $E[p^\infty] = \bigcup_{d \geq 0} E[p^d]$ for p prime
  - $E[\infty] = \bigcup_{n \geq 1} E[n]$
- For $n \in \mathbb{N}_{\geq 1} \cup \{p^\infty\} \cup \{\infty\}$ we let $G_n = \mathrm{Gal}(\mathbb{Q}(E[n]) \mid \mathbb{Q})$

Divisibility in torsion fields

Definition

We call $\alpha \in E(\mathbb{Q})$ p-indivisible if there is no $\beta \in E(\mathbb{Q})$ such that $p\beta = \alpha$.

Question

If $\alpha \in E(\mathbb{Q})$ is p-indivisible, is it so in $\mathbb{Q}(E[p])$?
If not, how far off is it?

Divisibility and cohomology

Let $L = \mathbb{Q}(E[p])$ and $G_p = \mathrm{Gal}(L \mid \mathbb{Q})$.

Exact sequence of G_p-modules:

$$0 \to E[p] \to E(L) \xrightarrow{\cdot p} pE(L) \to 0$$

Long exact sequence:

$$0 \to E(\mathbb{Q})[p] \to E(\mathbb{Q}) \xrightarrow{\cdot p} E(\mathbb{Q}) \cap pE(L) \to H^1(G_p, E[p])$$

So we get:

$$\frac{E(\mathbb{Q}) \cap pE(L)}{pE(\mathbb{Q})} \hookrightarrow H^1(G_p, E[p])$$

Main Theorem

Theorem (Lombardo, T.)

For every elliptic curve $E/\mathbb{Q}$ the exponent of $H^1(G_\infty, E[\infty])$ divides

$$2^{13} \times 3^8 \times 5^3 \times 7^2 \times 11^2$$

and, if E has CM, it divides 24.

Main Tools

Lemma (Inflation-restriction exact sequence)

For $H \triangleleft G$

$$0 \to H^1(G/H, M^H) \to H^1(G, M) \to H^1(H, M)^G$$

Lemma (Sah)

If $g \in \mathcal{Z}(G)$ *then* $m \mapsto gm - m$ *induces the zero map on* $H^1(G, M)$.

Sah's Lemma - proof

Lemma (Sah)

If $g \in \mathcal{Z}(G)$ then $m \mapsto gm - m$ induces the zero map on $H^1(G, M)$.

Proof.

Let f_g be the induced endomorphism on $H^1(G, M)$. For σ cocycle:

$$\begin{aligned} f_g(\sigma) =& (h \mapsto g\sigma(h) - \sigma(h)) \\ =& (h \mapsto \sigma(gh) - \sigma(h) - \sigma(g)) \\ =& (h \mapsto \sigma(hg) - \sigma(h) - \sigma(g)) \\ =& (h \mapsto h\sigma(g) + \sigma(h) - \sigma(h) - \sigma(g)) \\ =& (h \mapsto h\sigma(g) - \sigma(g)) \end{aligned}$$

which is the coboundary $\varphi_{\sigma(g)}$. $\square$

Applying the tool

- We want to find central elements in G_∞.
- We have a representation:

$$G_\infty \hookrightarrow \mathrm{GL}_2(\hat{\mathbb{Z}}) = \prod_p \mathrm{GL}_2(\mathbb{Z}_p)$$

  So we need **scalar matrices**.
- Problem: working in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ is hard...
- ...but in $\mathrm{GL}_2(\mathbb{Z}_p)$ is doable!

Proof sketch - scalars in G_{p^∞}

- First:

$$E[\infty] \cong \bigoplus_p E[p^\infty] \implies H^1(G_\infty, E[\infty]) \cong \bigoplus_p H^1(G_\infty, E[p^\infty])$$

- Inflation-restriction with $H = \mathrm{Gal}\left(\mathbb{Q}(E[\infty]) \mid \mathbb{Q}(E[p^\infty])\right)$

$$0 \to H^1(G_{p^\infty}, E[p^\infty]^H) \to H^1(G_\infty, E[p^\infty]) \to H^1(H, E[p^\infty])^{G_\infty}$$

Proof sketch (non-CM case)

$H^1(G_{p^\infty}, E[p^\infty]^H)$, we use Sah's lemma:

- If $p > 17, p \neq 37$ we have $-\mathrm{Id} \in G_{p^\infty} \subseteq \mathrm{GL}_2(\mathbb{Z}_p)$
$$\implies H^1(G_{p^\infty}, E[p^\infty]^H) = 0$$
- For small p: case by case work.
- For $p = 2$: Rouse and Zureick-Brown classified all possible G_{2^∞}.

Proof sketch - scalars in G_{p^∞}

Theorem

G_{p^∞} contains all scalar matrices congruent to 1 modulo p^{n_p}, where

$$n_p = \begin{cases} 4 & \text{for } p = 2 \\ 3 & \text{for } p = 3 \\ 1 & \text{for } p = 5, 7, 11, 13, 17, 37 \\ 0 & \text{for } p \geq 19,\ p \neq 37 \end{cases}$$

We take $g = (1 + p^{n_p})\,\mathrm{Id}$ in Sah's Lemma

$$\implies p^{n_p} H^1(G_{p^\infty}, E[p^\infty]^H) = 0$$

(We can actually do better for $p = 13, 17, 37$)

Proof sketch - the other half

Recall $H = \mathrm{Gal}(\mathbb{Q}(E[\infty]) \mid \mathbb{Q}(E[p^\infty]))$

$$\text{Action trivial on } E[p^\infty] \implies H^1(H, E[p^\infty])^{G_\infty} = \mathrm{Hom}(H, E[p^\infty])^{G_\infty}$$

So we need to bound the exponent of $\mathrm{Hom}(H, E[p^\infty])^{G_\infty}$.

Proof sketch - the other half

- Action of $g \in G_\infty$ on $\varphi : H \to E[p^\infty]$:

$$(g\varphi)(x) = g\varphi(g^{-1}xg)$$

- Idea: g lift of $(1 + p^{n_p})\,\mathrm{Id} \in G_{p^\infty}$; **if** $gx = xg$ then:

$$\varphi(x) = (1 + p^{n_p})\varphi(x) \implies p^{n_p}\,\mathrm{Hom}(H, E[p^\infty])^{G_\infty} = 0$$

Proof sketch - last tricks

- Notice: we can work in $\overline{H} \subseteq \prod_p \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$
- Actually in $\overline{H}^{\mathrm{ab}}$
- We can find $a \in \mathbb{Z}$ such that $g^2 x^a = x^a g^2$ in $\overline{H}^{\mathrm{ab}}$ for all g and x

$$\implies p^{n_p + v_p(a)} \operatorname{Hom}(H, E[p^\infty])^{G_\infty} = 0 \qquad (\text{for } p \neq 2)$$

Main Theorem

Theorem (Lombardo, T.)

For every elliptic curve $E/\mathbb{Q}$ the exponent of $H^1(G_\infty, E[\infty])$ divides

$$2^{13} \times 3^8 \times 5^3 \times 7^2 \times 11^2$$

and, if E has CM, it divides 24.

Thank you for your attention!