A problem of Tate-Shafarevich groups

Daniel Miller

August 7, 2016

1 Generalities on group cohomology

Let Γ be a profinite group. A *continuous* Γ*-module* (later: just a Γ-module) is a Γ-module M such that the action $\Gamma \times M \to M$ is continuous when M is given the discrete topology. One puts $\mathrm{H}^\bullet(\Gamma, -)$ for the derived functors of $\mathrm{H}^0(\Gamma, -)$, taken in the category of all continuous Γ-modules. We will frequently use the inflation-restriction exact sequence [NSW08, 1.6.7]: let $1 \to \Gamma' \to \Gamma \to \Gamma'' \to 1$ be a short exact sequence of profinite groups, M a Γ-module. Then the following sequence is exact:

$$0 \longrightarrow \mathrm{H}^1(\Gamma'', M^{\Gamma'}) \xrightarrow{\text{inf}} \mathrm{H}^1(\Gamma, M) \xrightarrow{\text{res}} \mathrm{H}^1(\Gamma', M).$$

Lemma 1. *Let* $\Gamma' \subset \Gamma$ *be a closed subgroup of a profinite group. Then the kernel of* $\mathrm{H}^1(\Gamma, M) \xrightarrow{\text{res}} \mathrm{H}^1(\Gamma', M)$ *does not depend on the conjugacy class of* Γ'.

Proof. Let $c : \Gamma \to M$ represent an element of $\mathrm{H}^1(\Gamma, M)$. Elementary manipulations show that $c_{\gamma^{-1}} = -\gamma^{-1} c_\gamma$ for all $\gamma \in \Gamma$. For $\sigma \in \Gamma'$, we compute

$$\begin{aligned} c_{\gamma\sigma\gamma^{-1}} &= \gamma\sigma c_{\gamma^{-1}} + \gamma c_\sigma + c_\gamma \\ &= (1 - \gamma\sigma\gamma^{-1}) c_\gamma + \gamma c_\sigma. \end{aligned}$$

Thus $c|_{\gamma\Gamma'\gamma^{-1}}$ is equivalent to the cocycle

$$\begin{aligned} \gamma\sigma\gamma^{-1} &\mapsto \gamma(\sigma - 1)m \\ &= (\gamma\sigma\gamma^{-1} - 1)\gamma m, \end{aligned}$$

which is a coboundary. We have shown that

$$\ker\left(\mathrm{H}^1(\Gamma, M) \to \mathrm{H}^1(\Gamma', M)\right) \subset \ker\left(\mathrm{H}^1(\Gamma, M) \to \mathrm{H}^1(\gamma\Gamma'\gamma^{-1}, M)\right).$$

To obtain the other inclusion, replace Γ' by $\gamma\Gamma'\gamma^{-1}$ and γ by γ^{-1}. $\square$

2 Galois cohomology of number fields

Let k be a number field, v a place of k. We write $\Gamma_v = \mathrm{Gal}(\overline{k_v}/k)$ for the decomposition group, and assume given a conjugacy class of embeddings $\Gamma_v \hookrightarrow \Gamma$. Let $I_v \subset \Gamma_v$ be the inertia group. If S is a finite set of places, we write $\Gamma^S \subset \Gamma$ for the normal subgroup generated by the images of $I_v \to \Gamma$ ($v \notin S$), and put $\Gamma_S = \Gamma/\Gamma^S$. If M is a Γ_v-module, put

$$\begin{aligned}\mathrm{H}^1_{\mathrm{ur}}(\Gamma_v, M) &= \ker\left(\mathrm{H}^1(\Gamma_v, M) \to \mathrm{H}^1(I_v, M)\right) \\ &= \mathrm{im}\left(\mathrm{H}^1(\widehat{\mathbf{Z}}, M^{I_v}) \to \mathrm{H}^1(\Gamma_v, M)\right).\end{aligned}$$

Lemma 2. *Let M be a Γ-module unramified outside S. Then*

$$\begin{aligned}\mathrm{H}^1(\Gamma_S, M) &\xrightarrow{\sim} \ker\left(\mathrm{H}^1(\Gamma, M) \to \bigoplus_{v\notin S} \frac{\mathrm{H}^1(\Gamma_v, M)}{\mathrm{H}^1_{\mathrm{ur}}(\Gamma_v, M)}\right) \\ &= \ker\left(\mathrm{H}^1(\Gamma, M) \to \bigoplus_{v\notin S} \mathrm{H}^1(I_v, M)\right).\end{aligned}$$

Proof. By the inflation-restriction exact sequence, we know that

$$\mathrm{H}^1(\Gamma_S, M) = \{c \in \mathrm{H}^1(\Gamma, M) : c|_{\Gamma^S} = 0\}.$$

Moreover, we know that the map $\prod_{v\notin S} I_v^{\mathrm{ab}} \to \Gamma^{S,\mathrm{ab}}$ is surjective. Since

$$\begin{aligned}\mathrm{H}^1(\Gamma^S, M) &= \hom(\Gamma^{S,\mathrm{ab}}, M) \\ &\hookrightarrow \prod_{v\notin S} \hom(I_v, M) \\ &= \prod_{v\notin S} \mathrm{H}^1(I_v, M),\end{aligned}$$

it is clear that $c|_{\Gamma^S} = 0$ if and only if $c|_{I_v} = 0$ for all $v \notin S$. □

As before, let M be a Γ-module unramified outside S. Define

$$Ш^1_S(M) = \ker\left(\mathrm{H}^1(\Gamma_S, M) \to \bigoplus_{v\in S} \mathrm{H}^1(\Gamma_v, M)\right).$$

Theorem 1. *If M is unramified outside S and $T \supset S$ is a finite set of places, the image of $Ш^1_S(M)$ under the inflation map $\mathrm{H}^1(\Gamma_S, M) \hookrightarrow \mathrm{H}^1(\gamma_T, M)$ contains $Ш^1_T(M)$.*

Proof. We need to show that if $c \in \mathrm{H}^1(\Gamma, M)$, then

$$\left(\begin{array}{cc} c|_{\Gamma_v} \in \mathrm{H}^1_{\mathrm{ur}}(\Gamma_v, M) & v \notin T \\ c|_{\Gamma_v} = 0 & v \in T \end{array} \right) \Rightarrow \left(\begin{array}{cc} c|_{\Gamma_v} \in \mathrm{H}^1_{\mathrm{ur}}(\Gamma_v, M) & v \notin S \\ c|_{\Gamma_v} = 0 & v \in S \end{array} \right),$$

but this is obvious. $\square$

Note: elliptic curves $E_{/\mathbf{Q}}$ with $Ш(E) \neq 0$ (or failures of the Grunwald-Wang theorem over number fields having no unramified extensions) seemed to be counterexamples to Theorem 1, as in those cases $\Gamma_\varnothing = 1$ but $Ш^1_S \neq 0$. The problem is, in all such cases the module in question is *not* everywhere unramified.

References

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*. Second. Vol. 323. Grundlehren der Mathematischen Wissenschaften. Springer-Verlag, 2008.