Tate's Lemma

Connor Lane

August 2024

1 Introduction

The following is a byproduct of the attempts of Shyam Ravishankar and I to understand Cassels' proof of the Cassels-Tate pairing for Elliptic curves [Cas62]. One section that gave us particular trouble is the following Lemma from section 5 of the paper.

Lemma 1 ([Cas62] Lemma 5.1) *Let k be a number field, q a rational prime, and A a finite G_k-module that is isomorphic to $\mathbb{Z}/q\mathbb{Z} \oplus \mathbb{Z}/q\mathbb{Z}$ as an abelian group. Then $\text{Ш}^2(k, A) = 0$.*

We found the proof in Cassels' paper slightly hard to follow. In particular, it has a typo that took us a while to identify, and it does some slightly unusual things like identifying μ_p and $\mathbb{Z}/p\mathbb{Z}$. This motivated us to try and find an alternative proof of the fact, which we present here.

2 Proof of Tate's Lemma

We will want to use a lemma from [NSW13], which we state the relevant case of for convenience.

Lemma 2 ([NSW13] Thm. 9.1.9(iii)) *Let A be a finite G_k-module and $k(A)$ the trivializing extension of A. If $[k(A)/k)] = lcm\{[k(A)_\mathfrak{p} : k_\mathfrak{p}] : \mathfrak{p}$ is a prime of $k\}$. Then $\text{Ш}^1(k, A) = 0$.*

By Poitout-Tate duality [NSW13, Th. 8.6.7], it is sufficient to prove that $\text{Ш}^1(k, A) = 0$, since if A is isomorphic to $\mathbb{Z}/q\mathbb{Z} \oplus \mathbb{Z}/q\mathbb{Z}$ as an abelian group, then $A' = \hom(A, \mu)$ is also isomorphic to $\mathbb{Z}/q\mathbb{Z} \oplus \mathbb{Z}/q\mathbb{Z}$ as an abelian group.

Proof of Lemma 1. Let $K(A)/K$ be the trivializing extension of A. We know $\text{Gal}(K(A)/A) \subseteq \text{Aut}(A) = \text{GL}_2(q)$. Fix a Sylow-$q$ subgroup $G_K^{(q)}$ of G_K, and let $K^{(q)}$ be its fixed field. Let $K' = K^{(q)} \cap K(A)$ so that K' is a maximal q-free subextension of $K(A)/K$. We have maps $\text{res} : H^1(G_K, A) \to H^1(G_{K'}, A)$ and $\text{cor} : H^1(G_{K'}, A) \to H^1(G_K, A)$, whose composition is $\text{cor} \circ res = [K' : K]$, see [NSW13, Cor. 1.5.7].

Since A is q-torsion, $H^1(K, A)$ is also q-torsion and therefore multiplication by $[K' : K]$ is an isomorphism, which implies that res is an injection.

Since $|\text{GL}_2(q)| = q(q-1)^2(q+1)$, we see that $\text{Gal}(K(A)/K') = q$ or 1. In either case, the group $\text{Gal}(K(A)/K')$ is cyclic and therefore by Chebotarev density, there is a prime $\mathfrak{p}$ of K' such that $[K(A)_\mathfrak{P} : K'_\mathfrak{p}] = [K(A) : K']$. Therefore Lemma 2 applies and the map

$$H^1(K', A) \to \prod_{\mathfrak{P}} H^1(K'_\mathfrak{P}, A)$$

is injective. We have the following diagram of restriction maps

$$\begin{tikzcd} H^1(G_{K'}, A) \arrow[r, hook] & \prod_\mathfrak{P} H^1(G_{K'_\mathfrak{P}}, A) \\ H^1(G_K, A) \arrow[r] \arrow[u, hook] & \prod_\mathfrak{p} H^1(G_{K_\mathfrak{p}}, A) \arrow[u] \end{tikzcd}$$

Since the left and upper map are injective, the bottom map must also be injective and we obtain $\text{Ш}^1(K, A) = 0$. The case of Ш^2 follows by Poitout-Tate duality as mentioned at the beginning of this section.

References

[Cas62] J.W.S. Cassels. Arithmetic on curves of genus 1. iv. proof of the hauptvermutung. *Journal für die reine und angewandte Mathematik*, 1962(211):95–112, 1962.

[NSW13] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of Number Fields*. Comprehensive Studies in Mathematics. Springer-Verlag, 2013.