Galois Cohomology (Study Group)

1 Cohomology of Local Fields (by Pedro Lemos)

Notation.

- For a field K, G_K will be the absolute Galois group
- If K is a non-archimedean local field (characteristic 0), write $G_K^{\mathrm{unr}} = \mathrm{Gal}(K_{\mathrm{unr}}/K)$

1.1 Finiteness of Cohomology and Tate's Duality

Definition 1.1. If G is a group (respectively profinite groups), the *cohomological dimension* of G is the smallest non-negative integer m such that $H^i(G, A) = 0$ for all $i > m$, for all A G-module (respectively discrete G-modules). We denote this by $\mathrm{cd}G$

For a prime p, we define the *cohomological p-dimension* of G to be the smallest non-negative integer m such that $H^i(G, A)(p) = 0$ for all $i > m$, for all A G-module (respectively discrete G-modules). We denote this by $\mathrm{cd_p}G$

Theorem 1.2. *Let K be a non-archimedean local field of characteristic 0.*

1. *For any prime p, we have $\mathrm{cd}_p G_K = 2$.* Also, if L/K is of degree p^∞ then $\mathrm{cd}_p G_L \leq 1$.
2. $H^i(G_K, \mu_m) = \begin{cases} K^*/(K^*)^m & i = 1 \\ \frac{1}{m}\mathbb{Z}/\mathbb{Z} & i = 2 \\ 0 & i \geq 3 \end{cases}$
3. *If A is a finite G_K-module, then $H^i(G_K, A)$ is finite, for all $i \geq 0$.*

Given a non-archimedean local field K, set $A^* = \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$ and $A' = \mathrm{Hom}(A, \mu)$.

Theorem 1.3 (Tate's Duality)**.** *Let K be a finite field extension of $\mathbb{Q}_p$ and A a finite G_K-module. Then the cup product gives us $H^i(K, A') \times H^{2-i}(K, A) \xrightarrow{\cup} H^2(K, \mu) \cong \mathbb{Q}/\mathbb{Z}$ which, for $i \in \{0, 1, 2\}$, induces an isomorphism $H^i(K, A') \to H^{2-i}(K, A)^*$.*

We have a representation $\rho : G_K \to \mathrm{Aut}(A)$. We say that this representation is *unramified* if the inertia subgroup I of G_K is contained in $\ker \rho$. Equivalently $A^I = A$. Notice that $I \cong \mathrm{Gal}(\overline{K}, K_{\mathrm{unr}})$.

Definition 1.4. For a G_K-module A, we define $H^i_{\mathrm{unr}}(K, A) = \mathrm{im}\left(H^i(G_K^{\mathrm{unr}}, A^J) \xrightarrow{\mathrm{inf}} H^i(G_K, A)\right)$. We call this group the *ith unramified cohomology group.*

Remark. We have $H^0_{\mathrm{unr}}(K, A) = H^0(K, A)$.

Theorem 1.5. *Let A be a finite G_K-module with $|A|$ coprime with the characteristic of the residue field, where K is a finite field extension of $\mathbb{Q}_p$. Then the groups $H^i_{\mathrm{unr}}(K, A')$ and $H^{2-i}_{\mathrm{unr}}(K, A')$ annihilate each others in the pairing $H^i(K, A') \times H^{2-i}(K, A) \xrightarrow{\cup} H^2(K, \mu) \cong \mathbb{Q}/\mathbb{Z}$. Moreover, they are mutually orthogonal complements.*

1.2 Euler - Poincaré characteristic

Set $h^i(K,A) = \left|H^i(K,A)\right|$.

Definition 1.6. The *Euler - Poincaré characteristic of* A is given by $\chi(K,A) = \prod_i h^i(K,A)^{(-1)^i}$.

Remark. In our case $\chi(K,A) = \frac{h^0(K,A)h^2(K,A)}{h^1(K,A)}$

Theorem 1.7 (Tate)**.** *For any finite G_K-module A of order a, we have $\chi(K,A) = |a|_K$, where $|\ |_K$ is a normalised absolute value on K.*

1.3 Tate modules of Elliptic curves

Definition 1.8. If E is an elliptic curve over K, and we take l to be a prime with $l \neq \mathrm{char} K$. The *l-adic Tate module* of E is $T_l(E) = \varprojlim_n E(\overline{K})[l^n]$.

If $m \neq \mathrm{char}K$, we know that $E(\overline{K})[m] \cong (\mathbb{Z}/m\mathbb{Z})$. We get a continuous representation $\rho : G_K \to \mathrm{GL}\left(\underbrace{T_l(E) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l}_{V_l(E)}\right) \cong \mathrm{GL}_2(\mathbb{Q}_l)$.

Aim: To study the cohomology of $V_l(E)$.

Let us look at an elliptic curve over $\mathbb{F}_p$. $G_{\mathbb{F}_p}$ is topologically generated by the Frobenius automorphism ϕ_p.

Fact. *The characteristic polynomial of $\rho(\phi_p)$ is $x^2 - a_p(E)x + p$, where $a_p(E) = p + 1 - |E(\mathbb{F}_p)|$. We know that $|a_p(E)| \leq 2\sqrt{p}$.*

So, $H^0(\mathbb{F}_p, V_l(E)) = V_l(E)^{\phi_p} = 0$. We have $H^1(C_m, A) \cong \frac{\ker N}{(g-1)A}$ where $N : A \to A$ is defined by $a \mapsto \sum_{\sigma \in G} \sigma a$. We compute $H^1(\mathbb{F}_p, V_l(E)) \cong \frac{\ker N}{(\phi_p - 1)V_l(E)} \cong V_l(E)/V_l(E) = 0$. Finally $H^i(\mathbb{F}_p, V_l(E)) = 0$ for $i \geq 2$.

Consider E an elliptic curve of good reduction over $\mathbb{Q}_p$. We have $H^i_{\mathrm{unr}}(G_{\mathbb{Q}_p}, V_l(E)) = 0$ for $i \in \{0,1,2\}$, this is due to the fact $H^i_{\mathrm{unr}}(G_{\mathbb{Q}_p}, V_l(E)) = H^i(G^{\mathrm{unr}}_{\mathbb{Q}_p}, V_l(E))$.

$H^0(G_{\mathbb{Q}_p}, V_l(E)) = H^0_{\mathrm{unr}}(G_{\mathbb{Q}_p}, V_l(E))$.

Theorem 1.9 (Néron - Ogg - Shaferenich)**.** *t For an elliptic curve E over $\mathbb{Q}_p$, E has good reduction if and only if there exists a prime $l \neq p$ such that $T_l E$ is unramified.*

We let l and p be primes for the rest of this section

Theorem 1.10. *Let V be a finite $G_{\mathbb{Q}_l}$-module which is also a $\mathbb{Q}_l$ -vector space. Then $H^i(\mathbb{Q}_p, V)$ is finite dimensional $\forall i \geq 0$ and $H^i(\mathbb{Q}_p, V) = 0$ for all $i \geq 3$.*

We define $\mathbb{Q}_l(1) := \mathbb{Q}_l \otimes_{\mathbb{Z}_l} \mathbb{Z}_l(1)$.

Theorem 1.11. *Let V be as above. The cup product gives us again an isomorphism $H^i(\mathbb{Q}_p, V') \xrightarrow{\sim} H^{2-i}(\mathbb{Q}_p, V)^*$, where $V' = \mathrm{Hom}(V, \mathbb{Q}_l(1))$ and $V^* = \mathrm{Hom}(V, \mathbb{Q}_l)$. Furthermore, $H^1_{\mathrm{unr}}(\mathbb{Q}_p, V')$ and $H^1_{\mathrm{unr}}(\mathbb{Q}_p, V)$ are mutually orthogonal.*

Euler - Binearo characteristic. $\chi(\mathbb{Q}_p, V) = \sum_i (-1)^i \dim_{\mathbb{Q}_l} H^i(\mathbb{Q}_p, V)$**.**

Theorem 1.12. *Let V be as above, then for $l \neq p$ we have $\chi(\mathbb{Q}_p, V) = 0$.*

Let E be an elliptic curve over $\mathbb{Q}_p$ with good reduction, and $l \neq p$ be a prime. We have $H^0(G^{\mathrm{unr}}_{\mathbb{Q}_p}, V_l(E)) = H^0(G_{\mathbb{F}_p}, V_l(\overline{E})) = 0$, $H^0(\mathbb{Q}_p, V_l(E)) = H^0_{\mathrm{unr}}(\mathbb{Q}_p, V_l(E)) = 0$.

There is a pairing (Weil pairing) $V_l(E) \times V_l(E) \to \mathbb{Q}_l(1)$, which is non-degenerate, Galois invariant, bilinear. This means that $V_l(E) \cong V_l(E)'$. So

$$\begin{aligned} 0 &= H^0(\mathbb{Q}_p, V_l(E)) \\ &= H^0(\mathbb{Q}_p, V_l(E)') \\ &\cong H^2(\mathbb{Q}_p, V_l(E))^* \\ &\Rightarrow H^2(\mathbb{Q}_p, V_l(E)) = 0 \end{aligned}$$

So the Euler - Poincaré implies $H^1(\mathbb{Q}_p, V_l(E)) = 0$.

Hence: If E is an elliptic curve over $\mathbb{Q}_p$ with good reduction, then $H^i(\mathbb{Q}_p, V_l(E)) = 0$ for all $i \geq 0$.

Now consider an elliptic curve E over $\mathbb{Q}_p$ with split multiplicative reduction. We have $\dim_{\mathbb{Q}_l} H^o(\mathbb{Q}_p, V_l(E)) \leq 1$. The reduction mod p induces a map $\alpha : V_l(E) \to V_l(\overline{E}_{\mathrm{ns}})$. We know that $\overline{E}_{\mathrm{ns}}(\overline{\mathbb{F}}_p) \cong \overline{\mathbb{F}}_p^*$, $\overline{E}_{\mathrm{ns}}(\overline{\mathbb{F}}_p)[l^m] \cong \overline{\mathbb{F}}_p^*[l^m] \cong \mu_{l^m}$, hence we have $V_l(\overline{E}_{\mathrm{ns}}) \cong \mathbb{Q}_l(1)$. We have a map $V_l(E) \to \mathbb{Q}_l(1)$, the cyclotomic character $\chi_l : G_{\mathbb{Q}_p} \to \mathbb{Q}_l^*$ and $V_l(E)/\ker \alpha \cong \mathbb{Q}_l(1)$. Turns out that the determinant of $\rho : G_{\mathbb{Q}_p} \to \mathrm{GL}(V_l(E))$ is also χ_l. So $\dim_{\mathbb{Q}_l} H^0(\mathbb{Q}_p, V_l(E)) = 1$. By Tate's duality, $\dim H^2(\mathbb{Q}_p, V_l(E)) = 1$ and by Euler - Poincaré: $\dim H^1(\mathbb{Q}_p, V_l(E)) = 2$.

Remark. For any other case of bad reduction we have $H^i(\mathbb{Q}_p, V_l(E)) = 0$ for all $i \geq 0$.