Galois Cohomology (Study Group)

1 Cohomology of global fields and Poitou-Tate duality (Marc Masdeu)

Notation.

- K is a global field (think number field).
- S a set of places of K containing ∞_K (the infinite place of K) (Mostly S will be finite: if not $H^1(G_{\mathbb{Q}}, \mathbb{Z}/p\mathbb{Z}) = \mathrm{Hom}(G_{\mathbb{Q}}, \mathbb{Z}/2\mathbb{Z})$, which by class field theory, is the dual of $\mathbb{Q}^*/\mathbb{Q}^{*2}$ everywhere finite)
- $K_S \subset \overline{K}$ is the maximal subextension which is unramified outside S. If $S = \{\infty_K\}$ then $K_S = K^{\mathrm{unr}}$, if $S = \mu_K$ then $K_S = \overline{K}$.
- $R_{K,S} = \{a \in K : \mathrm{ord}_\nu(a) \geq 0 \forall \nu \in S\}$. If $S = \{\infty_K\}$ then $R_{K,S} = \mathcal{O}_K$, if $S = \mu_K$ then $R_{K,S} = K$.
- Fix embeddings of $\overline{K} \hookrightarrow \overline{K_\nu}$ for all $\nu \in S$. This gives embeddings $G_{K_\nu} \cong D_\nu \hookrightarrow G_K \to G_S := \mathrm{Gal}(K_S/K)$

1.1 Localisation

Let M be any G_S-module (finite). We have maps $H^r(G_S, M) \to H^r(K_\nu, M)$ for all ν.

Definition 1.1. $P^r_S(K,M) = \prod'_{\nu \in S} H^r(K_\nu, M) = \{(c_\nu) \in \prod_{\nu \in S} H^r(K_\nu, M) : c_\nu \in H^r_{\mathrm{unr}}(K_\nu, M) \,\text{almost all}\, \nu\}$. (Convention for ν archimedean, $(r = 0)$, take $H^0_T = H^0/N_G H^0$ instead (Tate cohomology groups)).

- $P^0_S = \prod_{\nu \in S} H^0(K_\nu, M)$
- $P^1_S = \prod_{\nu \in S} H^1(K_\nu, M)$
- $P^2_S = \oplus_{\nu \in S} H^2(K_\nu, M)$

Since each class in $H^r(G_S, M)$ arises from $H^r(\mathrm{Gal}(L/K), M)$ for some L, localisations induces a map: $\beta^r : H^r(G_S, M) \to P^r_S(K, M)$. We define Ш by the following short exact sequence $0 \to Ш^r_S(K,M) \to H^r(G_S, M) \xrightarrow{\beta^r} P^r_S(K,M)$. Dualising (and if M is finite, $\#M \in R^*_{K,S}$) we get

$$\begin{array}{ccccc} P^2_S(K, M^D)^* & \xrightarrow{\beta^{r*}} & H^{2-r}(G_S, M^D)^* & \longrightarrow & Ш^{2-r}_S(K, M^D)^* \\ {\scriptstyle \text{see Pedro's talk}}\downarrow\cong & \nearrow{\scriptstyle \gamma^n(K,M)} & & & \\ P^r_S(K,M) & & & & \end{array}$$

The upshot is there exists maps:

$$4pc\ P^r_S(K,M) \xrightarrow{\gamma^r(K,M)} H^{2-r}(G_S, M^D)^* \longrightarrow Ш^{2-r}_S(K, M^D) \longrightarrow 0$$

Assume M is finite.

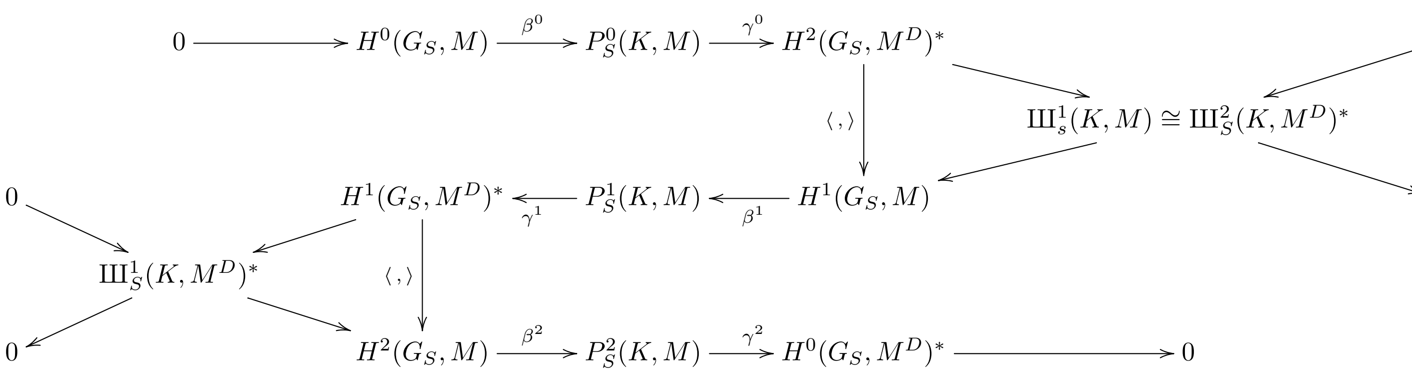
Proposition 1.2. *The map $\beta_1 : H^1(G_S, M) \to P^1_S(K, M)$ is proper (i.e., preimages of compact is compact). (Note the topology in H^1 is the discrete topology and the topology of P^1_S is induced from the product topology)*

Proof. Any compact in P^1_S is contained in some $P_T = \prod_{\nu \in S \setminus T} H^1_{\text{unr}}(K_\nu, M) \times \prod_{\nu \in T} H^1(K_\nu, M)$ (where $T \subset S$ is finite). Let $X_T = (\beta^1)^{-1}(P_T)$, we want X_T is finite. First there exists a finite extension L/K such that $G_L$acts trivially on M, $H^1(G_K, M) \to H^1(G_L, M)$ has finite kernel. Without loss of generality assume M has trivial action. Then $H^1(G_S, M) = \text{Hom}(G_S, M) \ni f$, this gives $L_f = K_S^{\ker(f)}$, so $f \in X_T$ if and only if L_f/K is unramified outside T □

Hermite - Minkowski. *Given n and finite T, there exists finitely many extension L/K such that $[L : K] = n$ and L is unramified outside T.*

Theorem 1.3. *Let M be finite, $\#M \in R^*_{K,S}$.*

1. *There exists a canonical nondegenerate pairing $\langle\, , \rangle : Ш^1_S(K, M) \times Ш^2_S(K, M^D) \to \mathbb{Q}/\mathbb{Z}$.*
2. *For all $r \geq 3$, β^r is a bijection, $\beta^r : H^r(G_S, M) \to \prod_{\nu \text{ arch}} H^r(K_\nu, M)$*
3. *There exists a g-term exact sequence:*



Remark. $Ш^0_S(K, M) = 0$
$Ш^1_S(K, M)$ is finite because it is equal to $(\beta^1)^{-1}(\{1\})$
By duality, $Ш^2_S(K, M)$ is also finite.

1.2 Euler - Poincaré pairing

Warning: $H^r(G_S, M)$ may be non zero for infinitely many r!
So we look at $\chi^*(G_S, M) = \frac{\#H^0(G_S,M)\#H^2(G_S,M)}{\#H^1(G_S,M)}$. We now assume S is finite.

Theorem 1.4. *We have*

$$\chi^*(G_S, M) = \prod_{\nu \text{ inf}} \frac{\#H^0(G_\nu, M)}{|\#M|_\nu} = \begin{cases} 1 & \text{if } K \text{ is function field} \\ \prod_{\nu \text{ inf}} \frac{\#H^0_T(G_\nu, M^D)}{\#H^0(G_\nu, M^D)} & \text{if } K \text{ is a number field} \end{cases}$$

1.3 Applications

Let E be an elliptic curve over $\mathbb{Q}$ and fix a prime $p \geq 3$. S be a finite set containing $\{\infty, 2, p, \text{prime of bad reductions}\}$. Set $G = G_S$ and $V = V_p(E) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \varprojlim_n \underbrace{E[p^n]}_{=:M_n}$. Note that M_n is finite, $\#M_n = p^{2n}$ and $M_n^D = M_n$. We get

$$\begin{aligned} \frac{\#H^0(G, M_n)\#H^2(G, M_n)}{\#H^1(G, M_n)} &= \frac{\#H^0_T(\mathbb{R}, M_n)}{\#H^0(\mathbb{R}, M_n)} \\ &= \frac{1}{\#(1+c)M_n} \\ &= \frac{1}{p^n} \end{aligned}$$

Note that "in the limit" $\#H^0(G, M_n)$ will stabilise. Hence we get $\dim H^1(G, V_p(E)) - \dim H^2(G, V_p(E)) = 1$.

Let us look back at $\langle \, , \, \rangle : Ш^1_S(K, M) \times Ш^2_S(K, M^D) \to \mathbb{Q}/\mathbb{Z}$. Take $a \in Ш^1_S(K, M)$ and $a' \in Ш^2_S(K, M^D)$. So a correspond to $\alpha \in H^1(G_S, M)$, $\alpha_\nu = d\beta_\nu$ for all ν, and a' correspond to $\alpha' \in H^2(G_S, M^D)$, $\alpha'_\nu = 0d\beta'_\nu$ for all ν. Check that $\sum_\nu \mathrm{inv}_\nu(\beta_\nu \cup \alpha'_\nu - \epsilon_\nu) =: \langle a, a' \rangle \in \mathbb{Q}/\mathbb{Z}$, where $\alpha \cup \alpha' = d\epsilon$.