

EULER SYSTEMS AND BSD

PHILIPP WIEDEMANN

CONTENTS

1.	Continuous Profinite Group Cohomology	1
2.	Selmer groups	2
2.1.	Bloch–Kato Selmer Structure	2
2.2.	Global Duality	3
3.	Euler Systems	4
3.1.	Applications to elliptic curves	4

1. CONTINUOUS PROFINITE GROUP COHOMOLOGY

Let G be a profinite group and let M be a topological G -module. There is a chain complex

$$0 \xrightarrow{d^{-1}} \mathrm{Maps}_{\mathrm{cts}}(\{*\}, M) \xrightarrow{d^0} \mathrm{Map}_{\mathrm{cts}}(G, M) \xrightarrow{d^1} \mathrm{Map}_{\mathrm{cts}}(G^2, M) \xrightarrow{d^2} \dots$$

where the coboundary maps d^i are defined in the usual way. We define the *continuous i th G -cohomological functor* as

$$H^i(G, M) := \frac{\ker d^i}{\mathrm{im} \, d^{i-1}}$$

for $i \geq 0$.

For some M we can do homological algebra.

Lemma 1.1. *Let G be a profinite group. Suppose we have a short exact sequence of topological G -modules*

$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$$

If this short exact sequence admits a continuous (set-theoretic) section, then there is a long exact sequence in continuous G -cohomology.

Remark 1.2. The hypotheses of the above lemma is always satisfied if:

- (1) C is discrete, as in Serre’s Galois cohomology;

Date: October 8, 2026.

- (2) A is open in B (in which case C is discrete);
- (3) B is a f.g. $\mathbb{Z}_p$ -module;
- (4) B is a f.g. $\mathbb{Q}_p$ -module.

2. SELMER GROUPS

Fix a field K . Let p be a rational prime and let T be a p -adic representation of G_K , by which we mean a free $\mathcal{O}$ -module of finite rank with a continuous $\mathcal{O}$ -linear action of G_K , where $\mathcal{O}$ is the ring of integers of some finite field extension $\Phi/\mathbb{Q}_p$. Let $V := T \otimes_{\mathcal{O}} \Phi$ and $W := V/T = T \otimes \Phi/\mathcal{O}$.

By the previous remark, we can talk about the Galois cohomology of T , V and W , use spectral sequences etc.

Let A be a subquotient of V (e.g. $A = T$ or $A = W$). We call a family of submodules of local cohomology groups

$$(\mathcal{F}, A) := \{H_{\mathcal{F}}^1(K_v, A) \subset H^1(K_v, A)\}_{v \text{ a place of } K}$$

a *Selmer structure for A* . Given a Selmer structure $(\mathcal{F}, A)$ we define $\mathcal{F}$ -Selmer group of A to be

$$H_{\mathcal{F}}^1(K, A) := \ker \left(H^1(K, A) \rightarrow \prod_{v \in K} \frac{H^1(K_v, A)}{H_{\mathcal{F}}^1(K_v, A)} \right)$$

Remark 2.1. A Selmer structure for A induces Selmer structures for subquotients of A by functoriality.

2.1. Bloch–Kato Selmer Structure. We define the *Bloch–Kato Selmer structure* $\mathcal{F}_{\text{BK}}$ of V by

$$H_{\mathcal{F}_{\text{BK}}}^1(K_v, V) := \begin{cases} \ker(H^1(K, V) \rightarrow H^1(K_v^{\text{nr}}, V)) & \text{if } v \nmid p \\ \ker(H^1(K, V) \rightarrow H^1(K_v, V \otimes B_{\text{cris}})) & \text{if } v \mid p \\ 0 & \text{if } v \text{ is Archimedean} \end{cases}$$

Theorem 2.2. *Let A be an abelian variety over K . Then*

$$H_{\mathcal{F}_{\text{BK}}}^1(K, A[p^n]) = \text{Sel}_{p^n}(K, A)$$

for each $n \geq 0$.

Given a Selmer-structure $(\mathcal{F}, A)$ and a set of places Σ of K , we define new Selmer structures

$$H_{\mathcal{F}_{\Sigma}}^1(K_v, A) := \begin{cases} H^1(K_v, A) & \text{if } v \in \Sigma \\ H_{\mathcal{F}}^1(K_v, A) & \text{if } v \notin \Sigma \end{cases}$$

$$H_{\mathcal{F}_{\Sigma}}^1(K_v, A) := \begin{cases} 0 & \text{if } v \in \Sigma \\ H_{\mathcal{F}}^1(K_v, A) & \text{if } v \notin \Sigma \end{cases}$$

Selmer structures have a partial order $\leq$ in the obvious way.

Remark 2.3. For any Selmer structure $\mathcal{F}$ and sets of places $\Sigma \subset \Sigma'$ we have

$$\mathcal{F}_\Sigma \leq \mathcal{F}_{\Sigma'} \leq \mathcal{F} \leq \mathcal{F}^\Sigma \leq \mathcal{F}^{\Sigma'}$$

We define the Cartier dual of A a subquotient of V is defined as

$$\mathrm{Hom}_{\mathcal{O}}(A, \mathcal{O}(1))$$

where $\mathcal{O}(1) := \mathcal{O}_{\varepsilon_{\mathrm{cyc}}}$.

Remark 2.4.

$$(T/p^n)^* = T^*[p^n]$$

Fix $n \geq 0$.

Given a Selmer structure $(\mathcal{F}, T/p^n)$ we can define a *dual* Selmer structure $(\mathcal{F}, T/p^n)^* := (\mathcal{F}^*, T^*[p^n])$ by taking exact orthogonal complements on local cohomology, i.e.

$$H_{\mathcal{F}^*}^1(K_v, T^*[p^n]) := \ker [H^1(K_v, T^*[p^n]) \rightarrow \mathrm{Hom}(H^1(K_v, T/p^n), \Phi/\mathcal{O}) \rightarrow \mathrm{Hom}(H_{\mathcal{F}}^1(K_v, T/p^n), \Phi/\mathcal{O})]$$

by taking appropriate limits we can define canonical Selmer structures

$$\begin{aligned} (\mathcal{F}, V)^* &:= (\mathcal{F}^*, V^*) & H_{\mathcal{F}^*}^1(K_v, V^*) &:= \ker [H^1(K_v, V^*) \rightarrow \mathrm{Hom}(H_{\mathcal{F}}^1(K_v, V), \Phi)] \\ (\mathcal{F}, T)^* &:= (\mathcal{F}^*, W^*) & H_{\mathcal{F}^*}^1(K_v, W^*) &:= \varinjlim_n H_{\mathcal{F}^*}^1(K_v, T^*/p^n) \\ (\mathcal{F}, W)^* &:= (\mathcal{F}^*, T^*) & H_{\mathcal{F}^*}^1(K_v, T^*) &:= \varprojlim_n H_{\mathcal{F}^*}^1(K_v, /T^*p^n) \end{aligned}$$

Example 2.5. $(\mathcal{F}^\Sigma)^* = (\mathcal{F}^*)_\Sigma$

Proposition 2.6 (Local Tate Duality). *Let $A \in \{T, V, W, T/p^n\}$, then*

$$((\mathcal{F}, A)^*)^* = (\mathcal{F}, A)$$

Remark 2.7. If $\mathcal{F}_1 \leq \mathcal{F}_2$, then $\mathcal{F}_2^* \leq \mathcal{F}_1^*$.

Proposition 2.8. *For $A \in \{T, V, W, T/p^n, T[p^n]\}$ we have $\mathcal{F}_{\mathrm{BK}}^* = \mathcal{F}_{\mathrm{BK}}$.*

Proof. For $\ell \nmid p$ this comes from the orthogonality of unramified cohomology. $\square$

2.2. Global Duality.

Theorem 2.9 (Global Poitou-Tate duality). *Let $\mathcal{F}_1 \leq \mathcal{F}_2$ be two Selmer structures on $A \in \{T, W, T/p^n, T[p^n]\}$ (not V) which differ in finitely many places $v \in \mathfrak{S}$. Then we have an exact sequence*

$$0 \rightarrow H_{\mathcal{F}_1}^1(K) \rightarrow H_{\mathcal{F}_2}^1(K) \rightarrow \bigoplus_{v \in \mathfrak{S}} \frac{H_{\mathcal{F}_1}^1(K_v)}{H_{\mathcal{F}_2}^1(K_v)} \rightarrow \mathrm{Hom}(H_{\mathcal{F}_1}^1(K), \Phi/\mathcal{O}) \rightarrow \mathrm{Hom}(H_{\mathcal{F}_2}^1(K), \Phi/\mathcal{O}) \rightarrow 0$$

3. EULER SYSTEMS

Let $K = \mathbb{Q}$.

Let T be a p -adic representation of $G_{\mathbb{Q}}$ and suppose the set of places where T ramifies Π_T is finite. Let $\mathcal{K}$ be the maximal p -subextension of the compositum of the unique $\mathbb{Z}_p$ -extension $\mathbb{Q}_{\mathbb{Z}_p}$ of $\mathbb{Q}$ with all extensions $\mathbb{Q}(\zeta_\ell)/\mathbb{Q}$ such that $\ell \notin \Pi_T$. We define the $\mathbb{Z}_p[[G_{\mathbb{Q}}^{\text{ab}}]]$ -module of Euler systems to be the projective limit of cohomology groups

$$\text{ES}_T := \varprojlim_{F, F'} \left\{ \begin{array}{ccc} H^1(F', T) & & \\ \text{cor} \downarrow & & \\ H^1(F, T) & \xleftarrow{\prod_w \det(1 - \text{Frob}_w^{-1} x | T^*) \mid_{x := \text{Frob}_w^{-1}}} & H^1(F, T) \end{array} \right\}$$

where F, F' range over finite subextensions of $\mathcal{K}/\mathbb{Q}$, and for each such F, F' , the product occurs over primes w of F' such that $w|_F$ ramifies in F'/F . In other words, an Euler system $\{\mathbf{c}_F\}_F \in \text{ES}_T$ is a collection of cohomology classes such that

$$\text{cor}_F^{F'} \mathbf{c}_{F'} = \left(\prod_w \det[1 - \text{Frob}_w^{-1} x | T^*] \mid_{x := \text{Frob}_w^{-1}} \right) \mathbf{c}_F$$

Theorem 3.1. *Suppose T is a p -adic representation (not equal to the trivial representation $\mathbb{Z}_p$) such that:*

- *there is a $\tau \in G_{\mathbb{Q}}$ such that τ , linear with respect to all p -power roots of -1 , with $\dim_{\mathbb{Q}_p}(V/(\tau - 1)) = 1$,*
- *V is irreducible over $\mathbb{Q}_p$.*

Suppose $\text{ES}_T \rightarrow \prod_F H^1(F, T)_{\text{tf}}$ admits a nonzero image (where F ranges over finite subextensions of $\mathbb{Q}_{\mathbb{Z}_p}/\mathbb{Q}$), then $H_{\mathcal{F}_{\text{BK}}, \Sigma_p}^1(\mathbb{Q}, W^)$ is finite order.*

3.1. Applications to elliptic curves. Fix an elliptic curve E over $\mathbb{Q}$. By the self-duality of E/p^n , the dual Selmer structure on $T_p E$ is $W_p E := T_p E \otimes \mathbb{Q}_p/\mathbb{Z}_p$.

Proposition 3.2. *There exists a map $\exp_{\omega_E}^*$ called the dual exponential map which induces a commutative diagram*

$$\begin{array}{ccc} \frac{H^1(\mathbb{Q}_p, V_p E)}{H_{\mathcal{F}_{\text{BK}}}^1(\mathbb{Q}_p, V_p E)} & \xrightarrow[\sim]{\exp_{\omega_E}^*} & \mathbb{Q}_p \\ \uparrow & & \uparrow \\ \frac{H^1(\mathbb{Q}_p, T_p E)}{H_{\mathcal{F}_{\text{BK}}}^1(\mathbb{Q}_p, T_p E)} & \xrightarrow{\sim} & \mathbb{Z}_p \end{array}$$

Proof. By ω_E we denote the invariant differential of E with respect to some fixed minimal Weierstrass model of E . We have a commutative diagram of isomorphisms

$$\begin{array}{ccccc} \mathrm{Tan}(E/\mathbb{Q}) & \xrightarrow{\exp_E} & E(\mathbb{Q}_p) \otimes \mathbb{Q}_p & \xrightarrow{\sim} & H_{\mathcal{F}_{\mathrm{BK}}}^1(\mathbb{Q}_p, V_p E) \\ \omega_E^* \uparrow & & \uparrow & & \\ \mathbb{Q}_p & \xleftarrow{\lambda_E} & \widehat{E}(p\mathbb{Z}_p) \otimes \mathbb{Q}_p & \xrightarrow{\sim} & E_1(\mathbb{Q}_p) \otimes \mathbb{Q}_p \end{array}$$

where $\mathrm{Tan}(E/\mathbb{Q}_p)$ is the tangent space of $E(\mathbb{Q}_p)$ at the identity with dual basis ω_E^* induced by ω_E , $\lambda_E : \widehat{E} \rightarrow \mathbb{G}_a$ is the formal group logarithm, and $\exp_E$ is the Lie group exponential map. $\square$

Corollary 3.3. *For any elliptic curve E over $\mathbb{Q}$, the canonical inclusion*

$$H_{\mathcal{F}_{\mathrm{BK}, \Sigma_p}}^1(\mathbb{Q}, W_p E) \hookrightarrow H_{\mathcal{F}_{\mathrm{BK}}}^1(\mathbb{Q}, W_p E)$$

has finite order cokernel if and only if

$$H_{\mathcal{F}_{\mathrm{BK}}^{\Sigma_p}}^1(\mathbb{Q}, T_p E) \xrightarrow{\mathrm{res}_p} \frac{H^1(\mathbb{Q}_p, T_p E)}{H_f^1(\mathbb{Q}_p, T_p E)}$$

is not the zero map, for at least one (or any) prime p .

Proof. Poitou–Tate duality gives an exact sequence

$$\begin{array}{ccccccc} 0 & \longrightarrow & H_{\mathcal{F}_{\mathrm{BK}}}^1(\mathbb{Q}, T_p E) & \longrightarrow & H_{\mathcal{F}_{\mathrm{BK}}^{\Sigma_p}}^1(\mathbb{Q}, T_p E) & & \\ & & & & \swarrow \mathrm{res}_p & & \\ & & & & \frac{H^1(\mathbb{Q}_p, T_p E)}{H_{\mathcal{F}_{\mathrm{BK}}}^1(\mathbb{Q}_p, T_p E)} & & \\ & & \swarrow & & & & \\ H_{\mathcal{F}_{\mathrm{BK}}}^1(\mathbb{Q}, W_p E)^\vee & \longrightarrow & H_{\mathcal{F}_{\mathrm{BK}, \Sigma_p}}^1(\mathbb{Q}, W_p E)^\vee & \longrightarrow & 0 & & \end{array}$$

from which the result follows by the previous lemma. $\square$

Theorem 3.4 (Kato). *There exists an Euler system $\mathbf{c} \in \mathrm{ES}_{T_p E}$ such that*

$$\exp_{\omega_E}^* \circ \mathrm{res}_p(\mathbf{c}_{\mathbb{Q}}) = r_E L_{Np}(E, 1) / \Omega_E$$

where r_E is a positive integer, independent of p , $L_{Np}(E, s)$ is the Np -truncated Hasse–Weil function of E where N is the conductor of E , and Ω_E is the fundamental period of E . Furthermore, if E does not have CM, then ES_T satisfies the hypotheses of the Euler system theorem.

Corollary 3.5. *If $E/\mathbb{Q}$ is not CM then $L(E, 1) \neq 0$ if and only if $E(\mathbb{Q})$ and $\mathrm{III}(\mathbb{Q}, E)$ are both finite order.*

Proof. The local factors of $L(E, s)$ do not vanish at $s = 1$, so we have $L_{Np}(E, 1) \neq 0$. It follows by Kato's Euler system that $\text{res}_p \neq 0$, hence we have an embedding of finite order modules

$$H_{\mathcal{F}_{\text{BK}, \Sigma_p}}^1(\mathbb{Q}, W_p E) \hookrightarrow H_{\mathcal{F}_{\text{BK}}}^1(\mathbb{Q}, W_p E)$$

by the exact sequence above. The result follows from the short exact sequence

$$0 \longrightarrow E(\mathbb{Q}) \otimes \mathbb{Q}_p / \mathbb{Z}_p \longrightarrow H_{\mathcal{F}_{\text{BK}}}^1(\mathbb{Q}, W_p E) \longrightarrow \text{III}(\mathbb{Q}, E)(p) \longrightarrow 0$$

□