Arithmetic of the twisted L-values of elliptic curves

Alberto Angurel Andrés

University of Nottingham

04/07/2025

Introduction

BSD conjecture

$$r_{\mathrm{alg}} := \mathrm{rank} E(\mathbb{Q}) = \mathrm{ord}_{s=1} L(E,s) =: r_{\mathrm{an}}$$

Introduction

BSD conjecture

$$r_{\mathrm{alg}} := \mathrm{rank} E(\mathbb{Q}) = \mathrm{ord}_{s=1} L(E,s) =: r_{\mathrm{an}}$$

Today

We consider the set of special values of the twisted L-functions, where

$$L(E,\chi,s) := \sum_{n\geq 1} \frac{\chi(n)a_n}{n^s} = \prod_{q \text{ prime}} \frac{1}{1-\chi(q)a_q q^{-s} + \mathbf{1}_N(q)\chi^2(q)q^{1-2s}}$$

for every Dirichlet character χ.

Introduction

BSD conjecture

$$r_{\mathrm{alg}} := \mathrm{rank} E(\mathbb{Q}) = \mathrm{ord}_{s=1} L(E,s) =: r_{\mathrm{an}}$$

Today

We consider the set of special values of the twisted L-functions, where

$$L(E,\chi,s) := \sum_{n\geq 1} \frac{\chi(n)a_n}{n^s} = \prod_{q \text{ prime}} \frac{1}{1-\chi(q)a_q q^{-s} + \mathbf{1}_N(q)\chi^2(q)q^{1-2s}}$$

for every Dirichlet character χ.

Under the assumption of Ш being finite, we will see that the set

$$\{L(E,\chi,1) : \ \chi \text{ Dirichlet character}\}$$

determines r_{alg} and the group structure of Ш.

Introduction

BSD conjecture

$$r_{\mathrm{alg}} := \mathrm{rank} E(\mathbb{Q}) = \mathrm{ord}_{s=1} L(E,s) =: r_{\mathrm{an}}$$

Today

We consider the set of special values of the twisted L-functions, where

$$L(E,\chi,s) := \sum_{n\geq 1} \frac{\chi(n)a_n}{n^s} = \prod_{q \text{ prime}} \frac{1}{1-\chi(q)a_q q^{-s} + \mathbf{1}_N(q)\chi^2(q)q^{1-2s}}$$

for every Dirichlet character χ.

Under the assumption of Ш being finite, we will see that the set

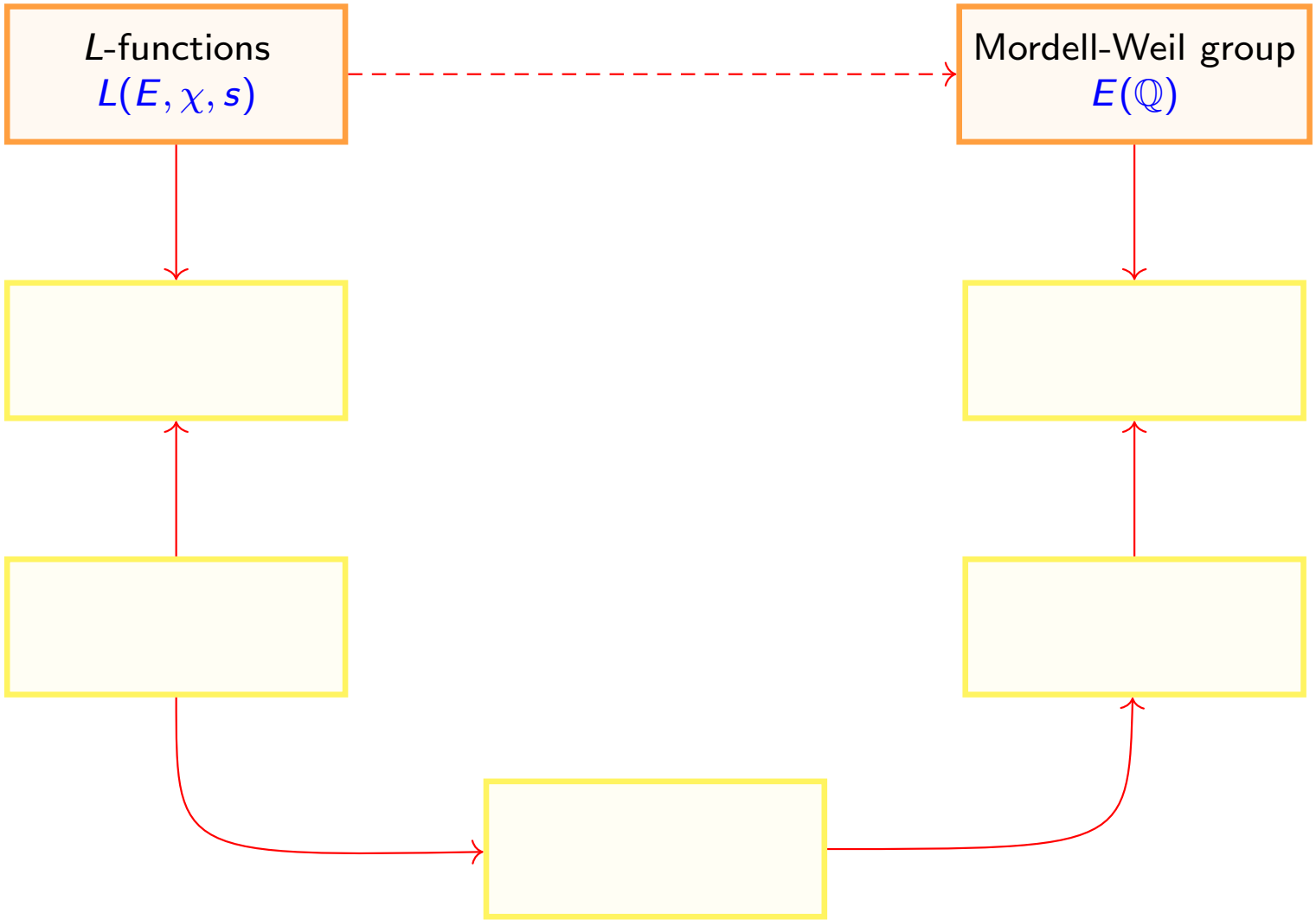
$$\{L(E,\chi,1) : \ \chi \text{ Dirichlet character}\}$$

determines r_{alg} and the group structure of Ш.

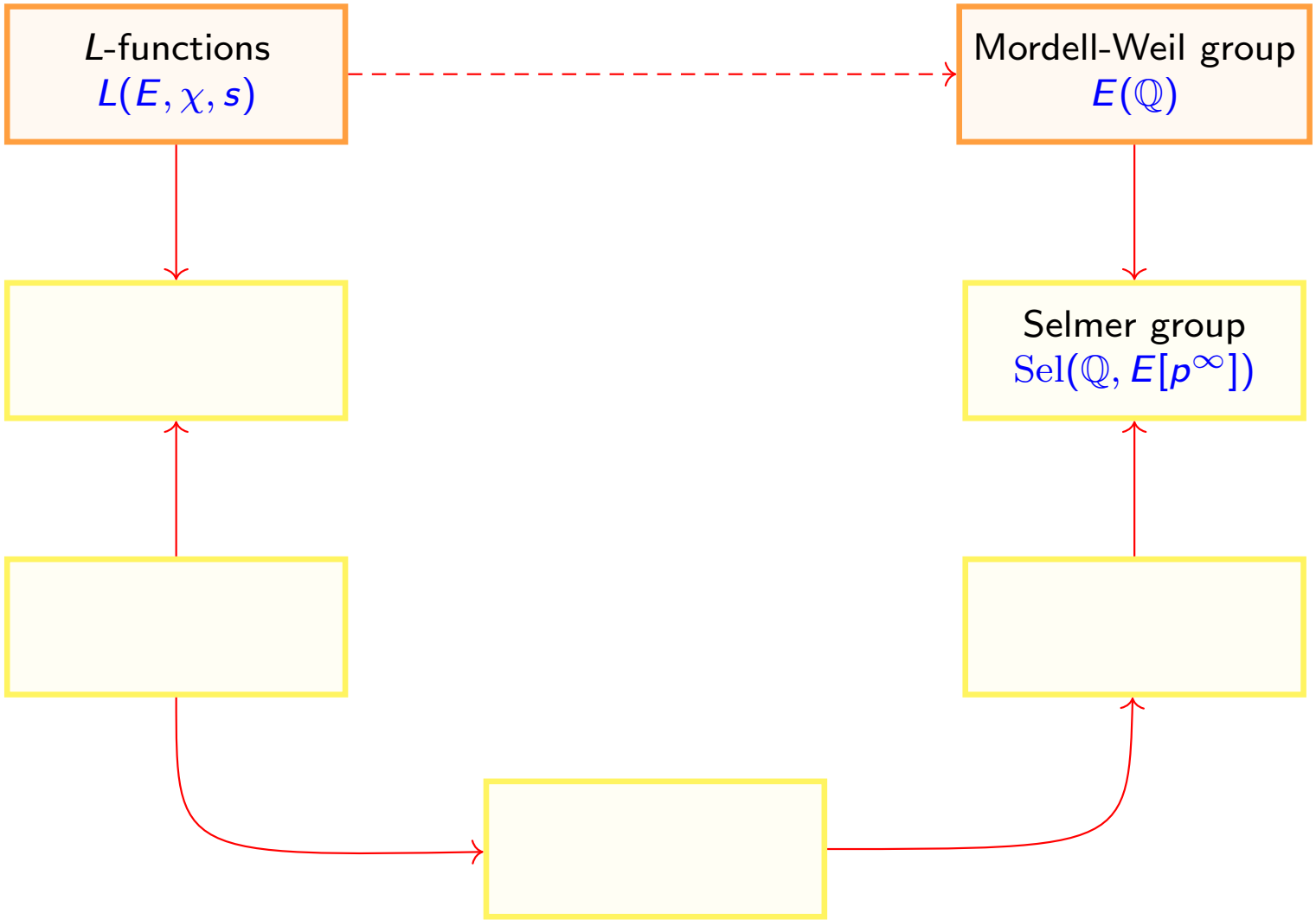
Generalisation to abelian extensions

The above mentioned set also determines the rank of $E(K)$ and the Galois structure of $Ш(E/K)$ for most abelian extensions $K/\mathbb{Q}$.

General picture



Selmer group



Selmer group

- Fix a prime $p \geq 5$. The p-Selmer group is a subgroup of $H^1(\mathbb{Q}, E[p^\infty])$.

Selmer group

- Fix a prime $p \geq 5$. The p-Selmer group is a subgroup of $H^1(\mathbb{Q}, E[p^\infty])$.

- It fits in the exact sequence

$$0 \longrightarrow E(\mathbb{Q}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \mathrm{Sel}(\mathbb{Q}, E[p^\infty]) \longrightarrow Ш(E)[p^\infty] \longrightarrow 0$$

Selmer group

- Fix a prime $p \geq 5$. The p-Selmer group is a subgroup of $H^1(\mathbb{Q}, E[p^\infty])$.
- It fits in the exact sequence

$$0 \longrightarrow E(\mathbb{Q}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \mathrm{Sel}(\mathbb{Q}, E[p^\infty]) \longrightarrow Ш(E)[p^\infty] \longrightarrow 0$$

- Conjecturally, $Ш(E)$ is a finite group, so $\mathrm{Sel}(\mathbb{Q}, E[p^\infty])$ detects r_{alg}:

$$E(\mathbb{Q}) \otimes \mathbb{Q}_p/\mathbb{Z}_p = (\mathbb{Q}_p/\mathbb{Z}_p)^{r_{\mathrm{alg}}}; \quad \mathrm{Sel}(\mathbb{Q}, E[p^\infty]) = (\mathbb{Q}_p/\mathbb{Z}_p)^{r_{\mathrm{sel}}} \oplus (\text{finite})$$

Selmer group

- Fix a prime $p \geq 5$. The p-Selmer group is a subgroup of $H^1(\mathbb{Q}, E[p^\infty])$.
- It fits in the exact sequence

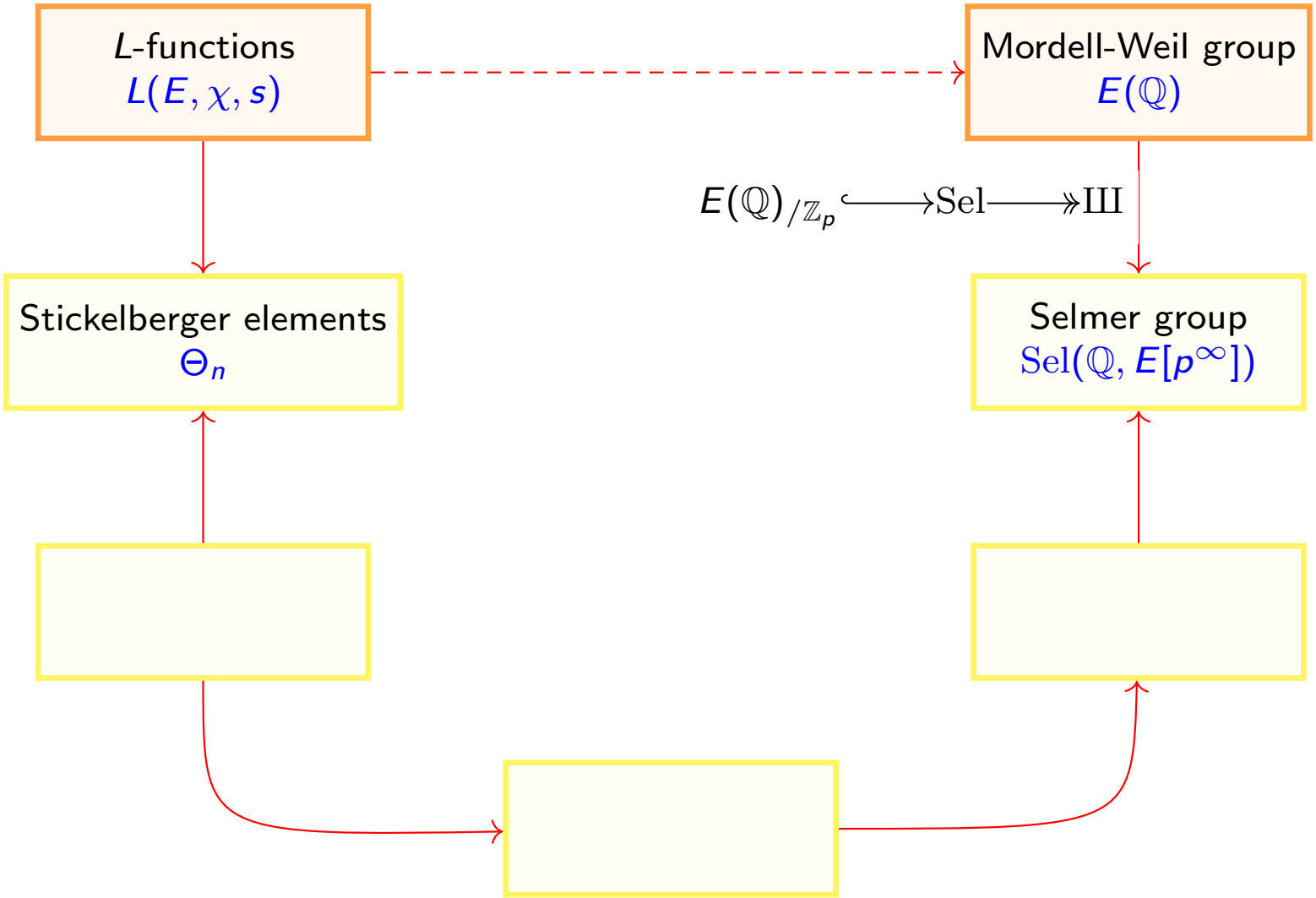
$$0 \longrightarrow E(\mathbb{Q}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \mathrm{Sel}(\mathbb{Q}, E[p^\infty]) \longrightarrow Ш(E)[p^\infty] \longrightarrow 0$$

- Conjecturally, $Ш(E)$ is a finite group, so $\mathrm{Sel}(\mathbb{Q}, E[p^\infty])$ detects r_{alg}:

$$E(\mathbb{Q}) \otimes \mathbb{Q}_p/\mathbb{Z}_p = (\mathbb{Q}_p/\mathbb{Z}_p)^{r_{\mathrm{alg}}}; \quad \mathrm{Sel}(\mathbb{Q}, E[p^\infty]) = (\mathbb{Q}_p/\mathbb{Z}_p)^{r_{\mathrm{sel}}} \oplus (\text{finite})$$

- In this talk, we will assume that $Ш(E)$ is finite, so $r_{\mathrm{alg}} = r_{\mathrm{sel}}$.

Stickelberger elements



Stickelberger elements

- The goal is to group the L-values in an element of a group algebra.

Stickelberger elements

- The goal is to group the L-values in an element of a group algebra.
- Let χ be a Dirichlet character modulo n:

$$\chi : \ (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$$

- We consider χ as a character of $\mathcal{G}_n := \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ via the identification:

$$a \mod n \leftrightarrow \sigma_a : \zeta_n \mapsto \zeta_n^a$$

Stickelberger elements

- The goal is to group the L-values in an element of a group algebra.
- Let χ be a Dirichlet character modulo n:

$$\chi : \ (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$$

- We consider χ as a character of $\mathcal{G}_n := \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ via the identification:

$$a \mod n \leftrightarrow \sigma_a : \zeta_n \mapsto \zeta_n^a$$

- We define the idempotent element

$$e_\chi := \sum_{a \in (\mathbb{Z}/c)^\times} \chi(a)\sigma_a \in \overline{\mathbb{Q}}_p[\mathcal{G}_n]$$

Stickelberger elements

- The goal is to group the L-values in an element of a group algebra.
- Let χ be a Dirichlet character modulo n:

$$\chi : \ (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$$

- We consider χ as a character of $\mathcal{G}_n := \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ via the identification:

$$a \mod n \leftrightarrow \sigma_a : \zeta_n \mapsto \zeta_n^a$$

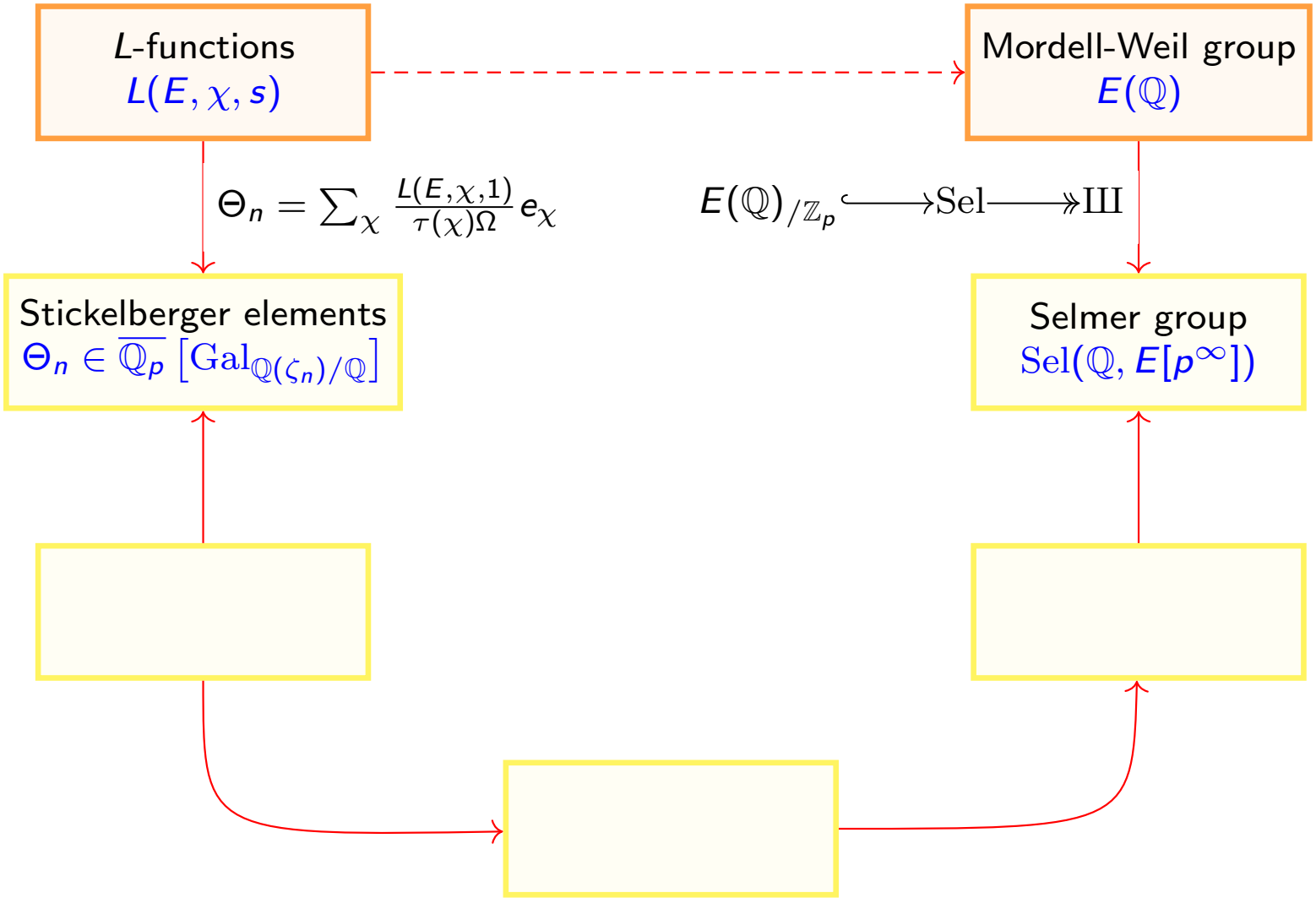
- We define the idempotent element

$$e_\chi := \sum_{a \in (\mathbb{Z}/c)^\times} \chi(a)\sigma_a \in \overline{\mathbb{Q}}_p[\mathcal{G}_n]$$

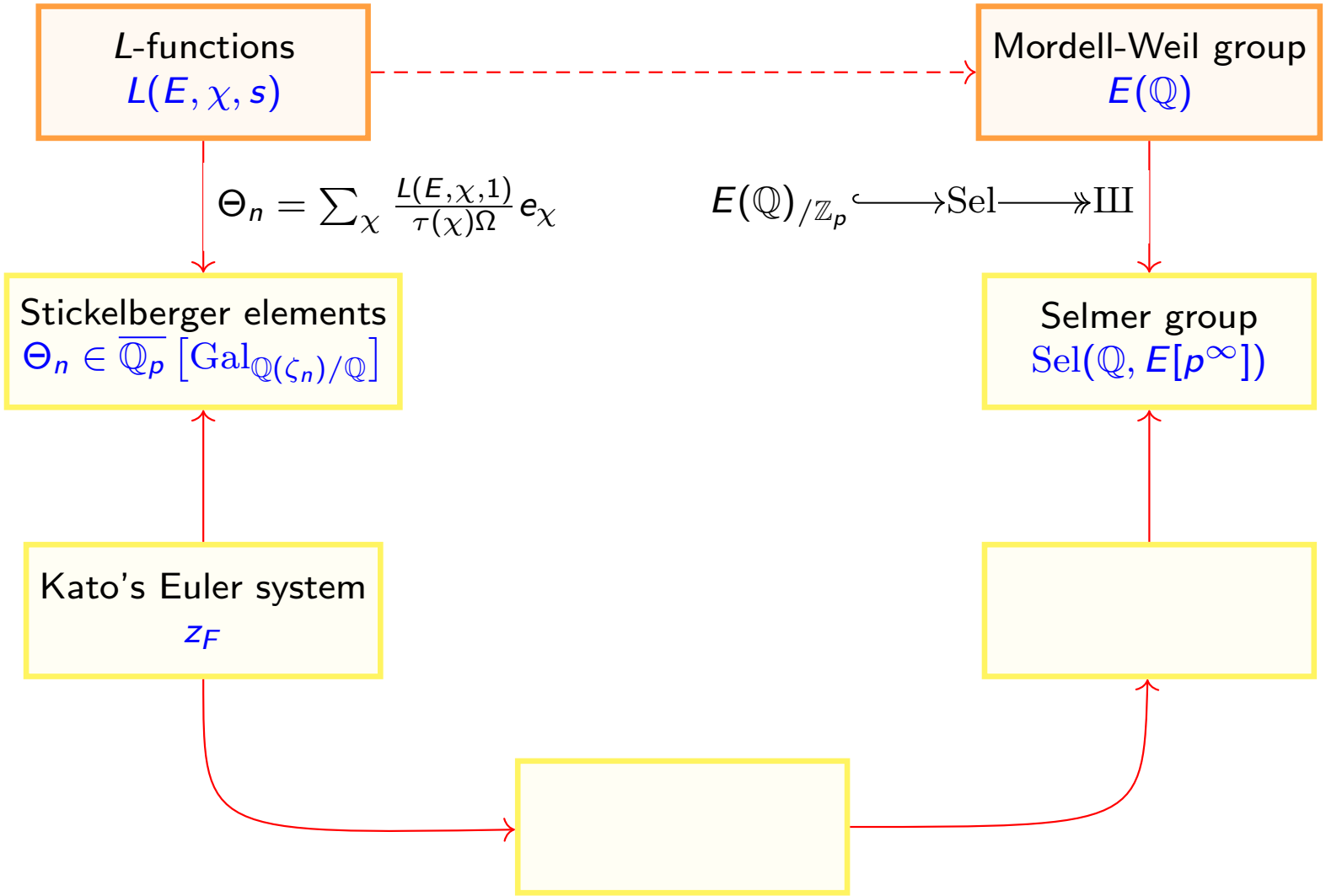
Stickelberger element

$$\Theta_n := \sum_{\chi \bmod n} \frac{L(E,\chi,1)}{\tau(\chi)\Omega^{\pm}} e_\chi \in \overline{\mathbb{Q}}_p[\mathcal{G}_n]$$

Stickelberger elements



Kato's Euler system



Kato's Euler system

Euler systems

An Euler system is a collection

$$\{z_F \in H^1(F, T_pE) : \ F/\mathbb{Q} \text{ finite}\}$$

satisfying the following condition:

Kato's Euler system

Euler systems

An Euler system is a collection

$$\{z_F \in H^1(F, T_pE) : \ F/\mathbb{Q} \text{ finite}\}$$

satisfying the following condition: for every F'/F, there is a corestriction map

$$\mathrm{cor} : \ H^1(F', T_pE) \to H^1(F, T_pE)$$

Kato's Euler system

Euler systems

An Euler system is a collection

$$\{z_F \in H^1(F, T_pE) : \ F/\mathbb{Q} \text{ finite}\}$$

satisfying the following condition: for every F'/F, there is a corestriction map

$$\mathrm{cor} : \ H^1(F', T_pE) \to H^1(F, T_pE)$$

We impose

$$\mathrm{cor}(z_{F'}) = \left(\prod_{\ell \in \mathrm{Ram}(F'/\mathbb{Q}) \setminus \mathrm{Ram}(/\mathbb{Q})} \mathrm{Euler}(\ell) \right) z_F$$

Kato's Euler system

Euler systems

An Euler system is a collection

$$\{z_F \in H^1(F, T_pE) : \ F/\mathbb{Q} \text{ finite}\}$$

satisfying the following condition: for every F'/F, there is a corestriction map

$$\mathrm{cor} : \ H^1(F', T_pE) \to H^1(F, T_pE)$$

We impose

$$\mathrm{cor}(z_{F'}) = \left(\prod_{\ell \in \mathrm{Ram}(F'/\mathbb{Q}) \setminus \mathrm{Ram}(/\mathbb{Q})} \mathrm{Euler}(\ell) \right) z_F$$

Kato's zeta elements

Kato constructed zeta elements $z_F \in H^1(F, T_pE)$ satisfying the Euler systems relation.

Kato's Euler system

Euler systems

An Euler system is a collection

$$\{z_F \in H^1(F, T_pE) : \ F/\mathbb{Q} \text{ finite}\}$$

satisfying the following condition: for every F'/F, there is a corestriction map

$$\mathrm{cor} : \ H^1(F', T_pE) \to H^1(F, T_pE)$$

We impose

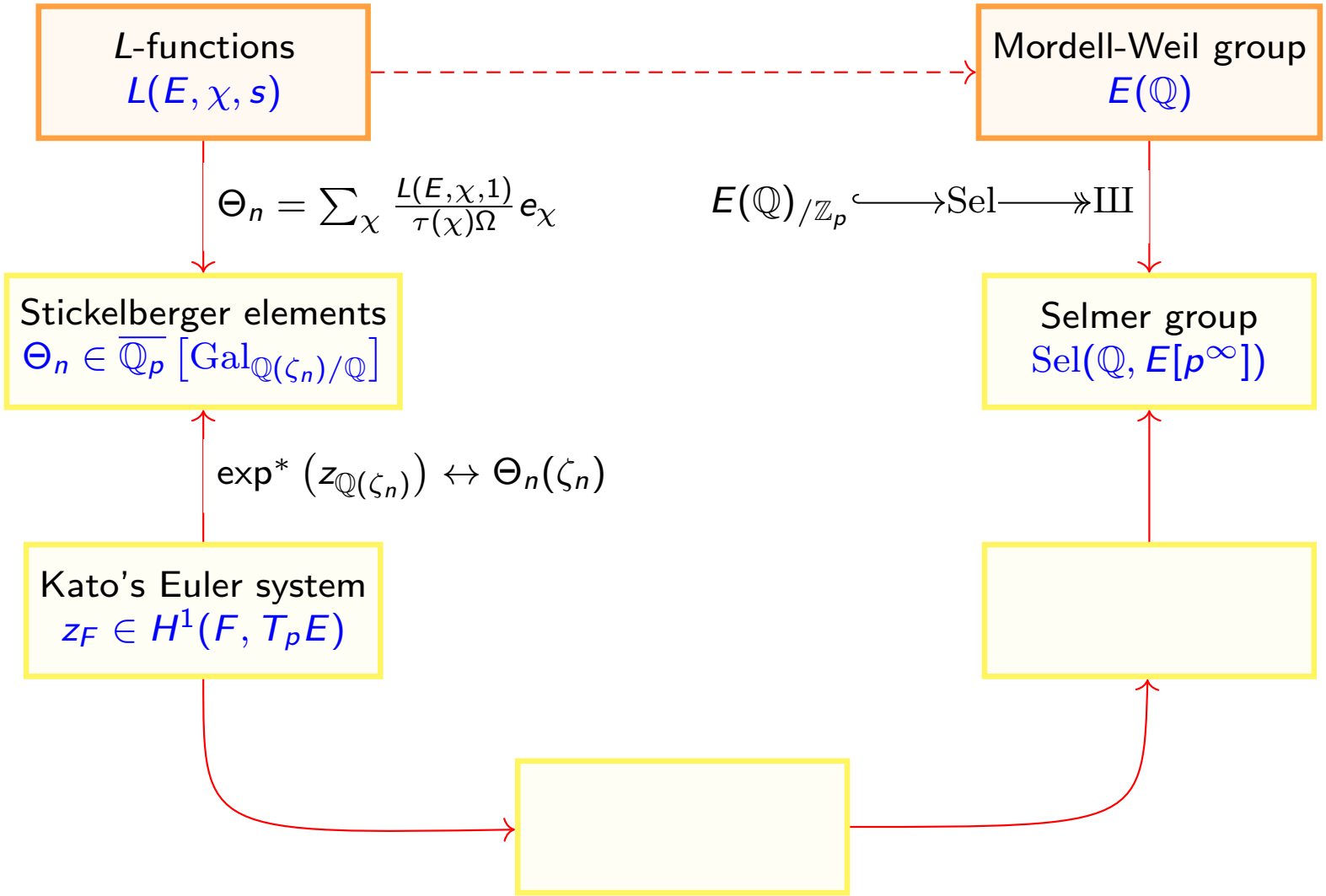
$$\mathrm{cor}(z_{F'}) = \left(\prod_{\ell \in \mathrm{Ram}(F'/\mathbb{Q}) \setminus \mathrm{Ram}(/\mathbb{Q})} \mathrm{Euler}(\ell) \right) z_F$$

Kato's zeta elements

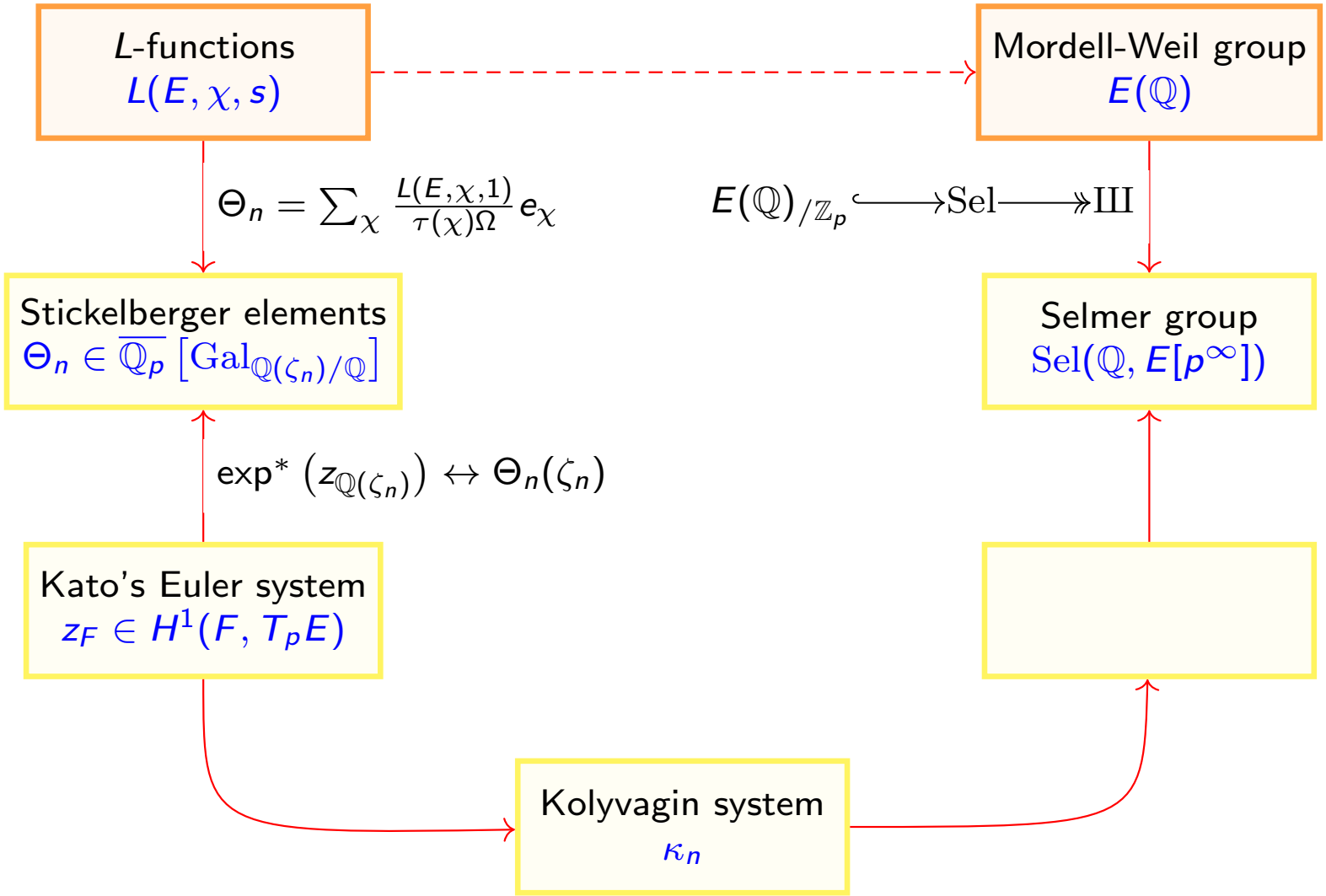
Kato constructed zeta elements $z_F \in H^1(F, T_pE)$ satisfying the Euler systems relation. They are linked to the special L-values via the dual exponential map. For $F = \mathbb{Q}(\zeta_n)$, we have

$$\exp^* : H^1(F, T_pE) \to \mathbb{Q}(\zeta_n), \quad \boxed{z_{\mathbb{Q}(\zeta_n)} \mapsto (*)\Theta_n(\zeta_n)}$$

Kato's Euler system



Kolyvagin systems



Kolyvagin systems

- Euler systems: collection of cohomology classes in a tower of number fields.

Kolyvagin systems

- Euler systems: collection of cohomology classes in a tower of number fields.
- Kolyvagin systems: collection of cohomology classes, all of them in $H^1(\mathbb{Q}, T_p E)$.

Kolyvagin systems

- Euler systems: collection of cohomology classes in a tower of number fields.
- Kolyvagin systems: collection of cohomology classes, all of them in $H^1(\mathbb{Q}, T_pE)$.
- For every square-free n, there is a $\kappa_n \in H^1(\mathbb{Q}, T_pE)$ such that

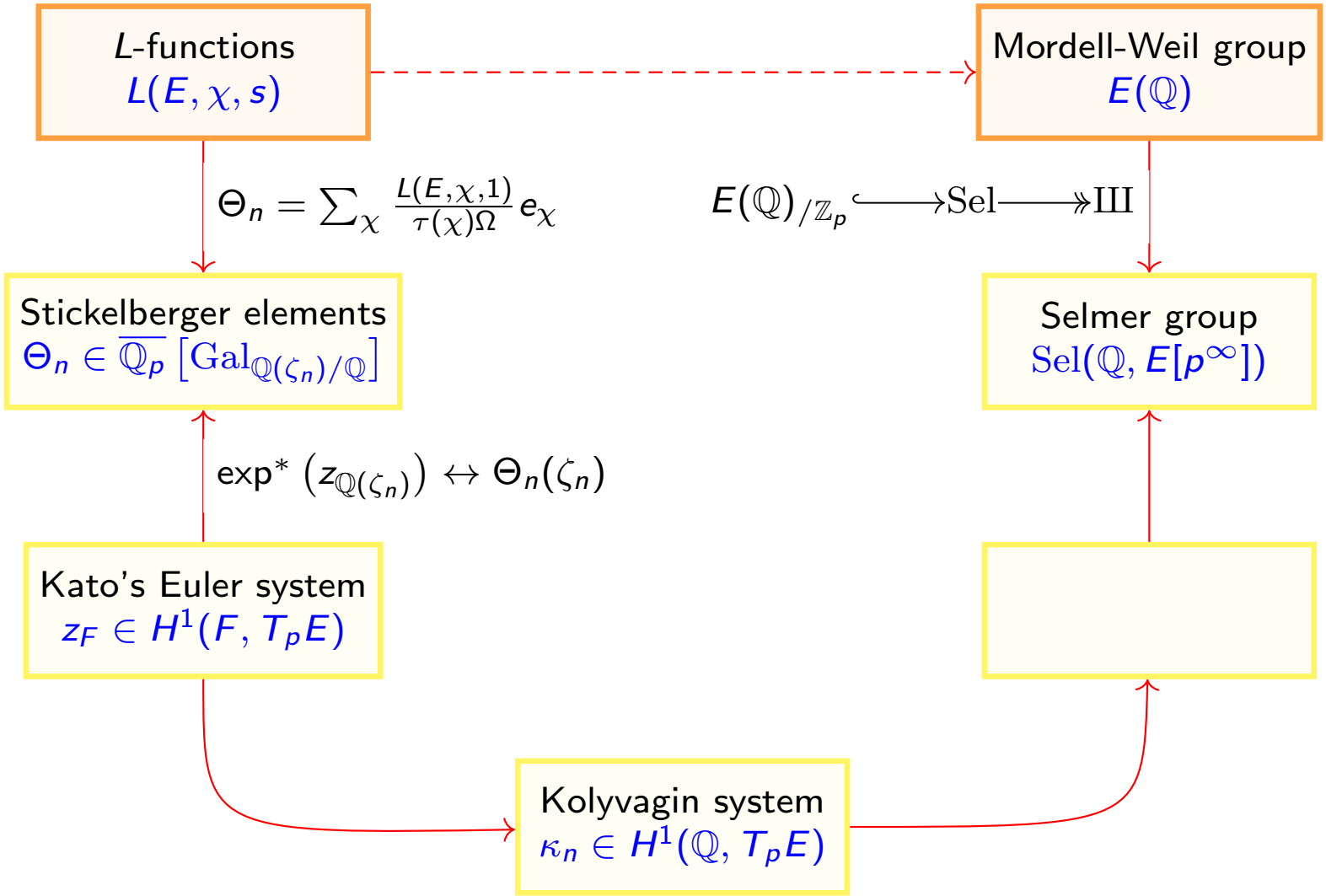
Kolyvagin systems

- Euler systems: collection of cohomology classes in a tower of number fields.
- Kolyvagin systems: collection of cohomology classes, all of them in $H^1(\mathbb{Q}, T_pE)$.
- For every square-free n, there is a $\kappa_n \in H^1(\mathbb{Q}, T_pE)$ such that
  - κ_n is unramified for good reduction primes not dividing np.
  - For every n and every prime ℓ not dividing n, we impose a condition $\kappa_n \leftrightarrow \kappa_{n\ell}$.

Kolyvagin systems

- Euler systems: collection of cohomology classes in a tower of number fields.
- Kolyvagin systems: collection of cohomology classes, all of them in $H^1(\mathbb{Q}, T_pE)$.
- For every square-free n, there is a $\kappa_n \in H^1(\mathbb{Q}, T_pE)$ such that
  - κ_n is unramified for good reduction primes not dividing np.
  - For every n and every prime ℓ not dividing n, we impose a condition $\kappa_n \leftrightarrow \kappa_{n\ell}$.
- These conditions are very rigid: there is only one Kolyvagin system up to constant.

Kolyvagin systems



Kolyvagin derivatives

- Kolyvagin derivative: descent machinery to obtain cohomology classes over $\mathbb{Q}$.

Kolyvagin derivatives

- Kolyvagin derivative: descent machinery to obtain cohomology classes over $\mathbb{Q}$.
- For every prime ℓ, fix a generator $\sigma_\ell \in \mathrm{Gal}(\mathbb{Q}(\zeta_\ell)/\mathbb{Q}) =: \mathcal{G}_\ell$. The Kolyvagin derivative operator is defined as

$$D_\ell := \sum_{i=1}^{\ell-1} i\sigma_\ell^i \in \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\zeta_\ell/\mathbb{Q}))]$$

Kolyvagin derivatives

- Kolyvagin derivative: descent machinery to obtain cohomology classes over $\mathbb{Q}$.
- For every prime ℓ, fix a generator $\sigma_\ell \in \mathrm{Gal}(\mathbb{Q}(\zeta_\ell)/\mathbb{Q}) =: \mathcal{G}_\ell$. The Kolyvagin derivative operator is defined as

$$D_\ell := \sum_{i=1}^{\ell-1} i\sigma_\ell^i \in \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\zeta_\ell/\mathbb{Q}))]$$

- For a square-free integer n, let

$$D_n := \prod_{\ell \mid n} D_\ell$$

Kolyvagin derivatives

- Kolyvagin derivative: descent machinery to obtain cohomology classes over $\mathbb{Q}$.
- For every prime ℓ, fix a generator $\sigma_\ell \in \mathrm{Gal}(\mathbb{Q}(\zeta_\ell)/\mathbb{Q}) =: \mathcal{G}_\ell$. The Kolyvagin derivative operator is defined as

$$D_\ell := \sum_{i=1}^{\ell-1} i\sigma_\ell^i \in \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\zeta_\ell/\mathbb{Q}))]$$

- For a square-free integer n, let

$$D_n := \prod_{\ell|n} D_\ell$$

- 'Fact': $D_n z_{Q(\zeta_n)} \in H^1(\mathbb{Q}(\zeta_n), T_pE)^{\mathcal{G}_n}$

Kolyvagin derivatives

- Kolyvagin derivative: descent machinery to obtain cohomology classes over $\mathbb{Q}$.
- For every prime ℓ, fix a generator $\sigma_\ell \in \mathrm{Gal}(\mathbb{Q}(\zeta_\ell)/\mathbb{Q}) =: \mathcal{G}_\ell$. The Kolyvagin derivative operator is defined as

$$D_\ell := \sum_{i=1}^{\ell-1} i\sigma_\ell^i \in \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\zeta_\ell/\mathbb{Q}))]$$

- For a square-free integer n, let

$$D_n := \prod_{\ell \mid n} D_\ell$$

- 'Fact': $D_n z_{Q(\zeta_n)} \in H^1(\mathbb{Q}(\zeta_n), T_pE)^{\mathcal{G}_n}$
- $H^1(\mathbb{Q}, T_pE) \xrightarrow{\mathrm{res}} H^1(\mathbb{Q}(\zeta_n), T_pE)^{\mathcal{G}_n}$ is an isomorphism (under assumptions).

Kolyvagin derivatives

- Kolyvagin derivative: descent machinery to obtain cohomology classes over $\mathbb{Q}$.
- For every prime ℓ, fix a generator $\sigma_\ell \in \mathrm{Gal}(\mathbb{Q}(\zeta_\ell)/\mathbb{Q}) =: \mathcal{G}_\ell$. The Kolyvagin derivative operator is defined as

$$D_\ell := \sum_{i=1}^{\ell-1} i\sigma_\ell^i \in \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\zeta_\ell/\mathbb{Q}))]$$

- For a square-free integer n, let

$$D_n := \prod_{\ell | n} D_\ell$$

- 'Fact': $D_n z_{Q(\zeta_n)} \in H^1(\mathbb{Q}(\zeta_n), T_pE)^{\mathcal{G}_n}$
- $H^1(\mathbb{Q}, T_pE) \xrightarrow{\mathrm{res}} H^1(\mathbb{Q}(\zeta_n), T_pE)^{\mathcal{G}_n}$ is an isomorphism (under assumptions).
-

$$\boxed{\kappa_n := \mathrm{res}^{-1}\left(D_n z_{\mathbb{Q}(\zeta_n)}\right)}$$

Kolyvagin derivatives

- Kolyvagin derivative: descent machinery to obtain cohomology classes over $\mathbb{Q}$.
- For every prime ℓ, fix a generator $\sigma_\ell \in \mathrm{Gal}(\mathbb{Q}(\zeta_\ell)/\mathbb{Q}) =: \mathcal{G}_\ell$. The Kolyvagin derivative operator is defined as

$$D_\ell := \sum_{i=1}^{\ell-1} i\sigma_\ell^i \in \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\zeta_\ell/\mathbb{Q}))]$$

- For a square-free integer n, let

$$D_n := \prod_{\ell \mid n} D_\ell$$

- 'Fact': $D_n z_{Q(\zeta_n)} \in H^1(\mathbb{Q}(\zeta_n), T_pE)^{\mathcal{G}_n}$
- $H^1(\mathbb{Q}, T_pE) \xrightarrow{\mathrm{res}} H^1(\mathbb{Q}(\zeta_n), T_pE)^{\mathcal{G}_n}$ is an isomorphism (under assumptions).
-

$$\boxed{\kappa_n := \mathrm{res}^{-1}\left(D_n z_{\mathbb{Q}(\zeta_n)}\right)}$$

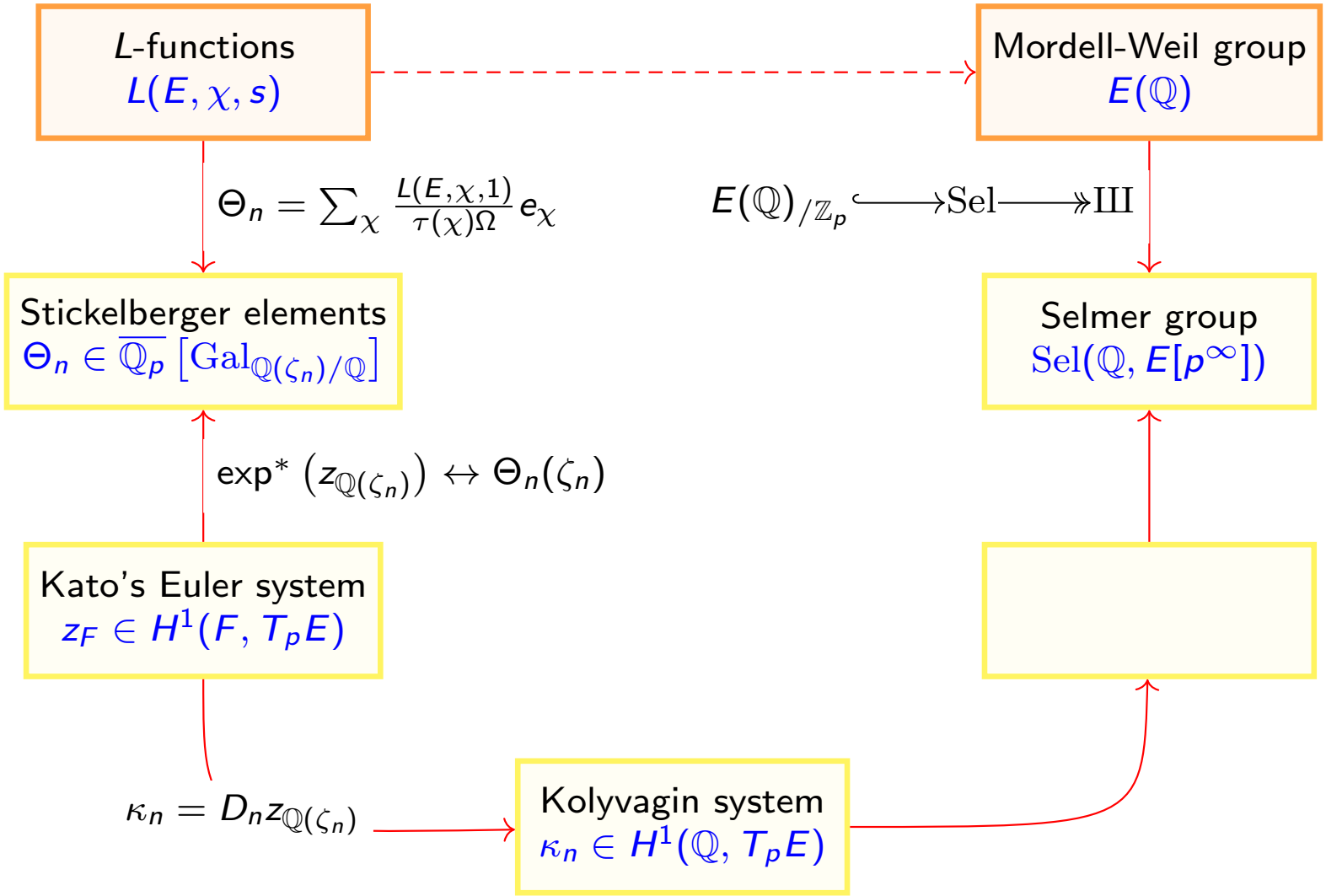
From Euler systems to Kolyvagin systems

The Kolyvagin derivative defines a map

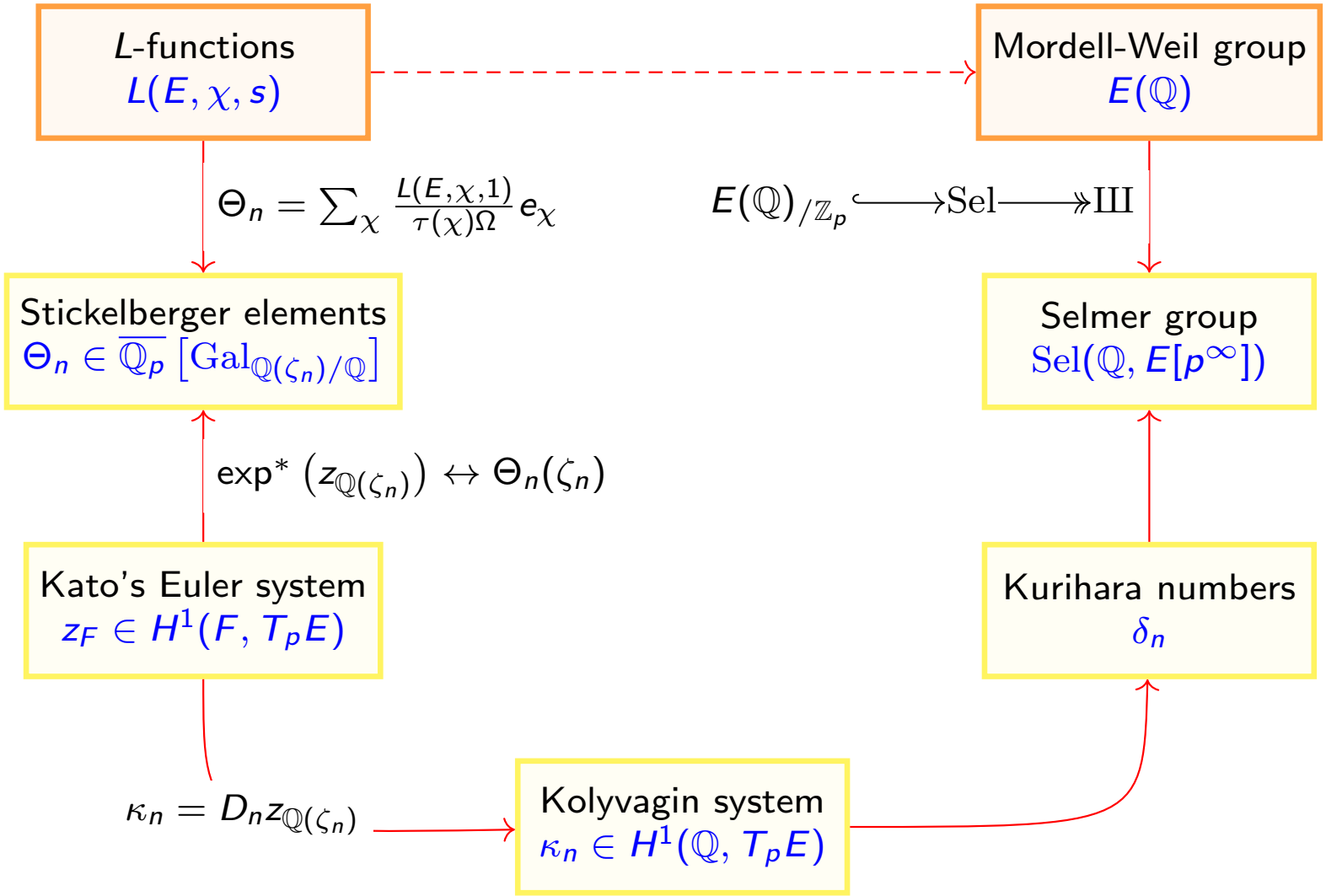
$$\Phi : \{\text{Euler systems}\} \to \{\text{Kolyvagin systems}\}$$

satisfying that, if $\Phi(z) = \kappa$, then $\kappa_1 = z_{\mathbb{Q}}$.

Kolyvagin derivatives



Kurihara numbers



Kurihara numbers

- By the general theory of Kolyvagin systems

$$H^1(\mathbb{Q}, T_pE) \xrightarrow{\text{loc}} H^1(\mathbb{Q}_p, T_pE) \xrightarrow{\sim} \mathbb{Z}_p$$

Kurihara numbers

- By the general theory of Kolyvagin systems

$$H^1(\mathbb{Q}, T_pE) \xrightarrow{\text{loc}} H^1(\mathbb{Q}_p, T_pE) \xrightarrow{\sim} \mathbb{Z}_p$$

- We can use $p^\alpha \exp^*$ for some integer α, which is related to the Euler factor at p.

Kurihara numbers

- By the general theory of Kolyvagin systems

$$H^1(\mathbb{Q}, T_pE) \xrightarrow{\text{loc}} H^1(\mathbb{Q}_p, T_pE) \xrightarrow{\sim} \mathbb{Z}_p$$

- We can use $p^\alpha \exp^*$ for some integer α, which is related to the Euler factor at p.
- By the interpolation property of Kato's Euler system,

$$\delta_n := p^\alpha \exp^*(\kappa_n) = D_n\Theta_n(\zeta_n)$$

Kurihara numbers

- By the general theory of Kolyvagin systems

$$H^1(\mathbb{Q}, T_pE) \xrightarrow{\text{loc}} H^1(\mathbb{Q}_p, T_pE) \xrightarrow{\sim} \mathbb{Z}_p$$

- We can use $p^\alpha \exp^*$ for some integer α, which is related to the Euler factor at p.
- By the interpolation property of Kato's Euler system,

$$\delta_n := p^\alpha \exp^*(\kappa_n) = D_n\Theta_n(\zeta_n)$$

- Explicitly, fix a primitive root η_ℓ of $(\mathbb{Z}/\ell)^\times$ for every prime divisor ℓ of n. Then

$$\boxed{\delta_n = \sum_{a\in(\mathbb{Z}/n)^\times} \left[\frac{a}{n}\right]^+ \prod_{\ell\mid n} \left(\log_{\eta_\ell}(a)\right) \in \mathbb{Z}_{(p)}}$$

Kurihara numbers

- By the general theory of Kolyvagin systems

$$H^1(\mathbb{Q}, T_pE) \xrightarrow{\text{loc}} H^1(\mathbb{Q}_p, T_pE) \xrightarrow{\sim} \mathbb{Z}_p$$

- We can use $p^\alpha \exp^*$ for some integer α, which is related to the Euler factor at p.
- By the interpolation property of Kato's Euler system,

$$\delta_n := p^\alpha \exp^*(\kappa_n) = D_n\Theta_n(\zeta_n)$$

- Explicitly, fix a primitive root η_ℓ of $(\mathbb{Z}/\ell)^\times$ for every prime divisor ℓ of n. Then

$$\boxed{\delta_n = \sum_{a\in(\mathbb{Z}/n)^\times} \left[\frac{a}{n}\right]^+ \prod_{\ell\mid n} \left(\log_{\eta_\ell}(a)\right) \in \mathbb{Z}_{(p)}}$$

- These quantities are known as Kurihara numbers.

Kurihara numbers

- By the general theory of Kolyvagin systems

$$H^1(\mathbb{Q}, T_pE) \xrightarrow{\text{loc}} H^1(\mathbb{Q}_p, T_pE) \xrightarrow{\sim} \mathbb{Z}_p$$

- We can use $p^\alpha \exp^*$ for some integer α, which is related to the Euler factor at p.
- By the interpolation property of Kato's Euler system,

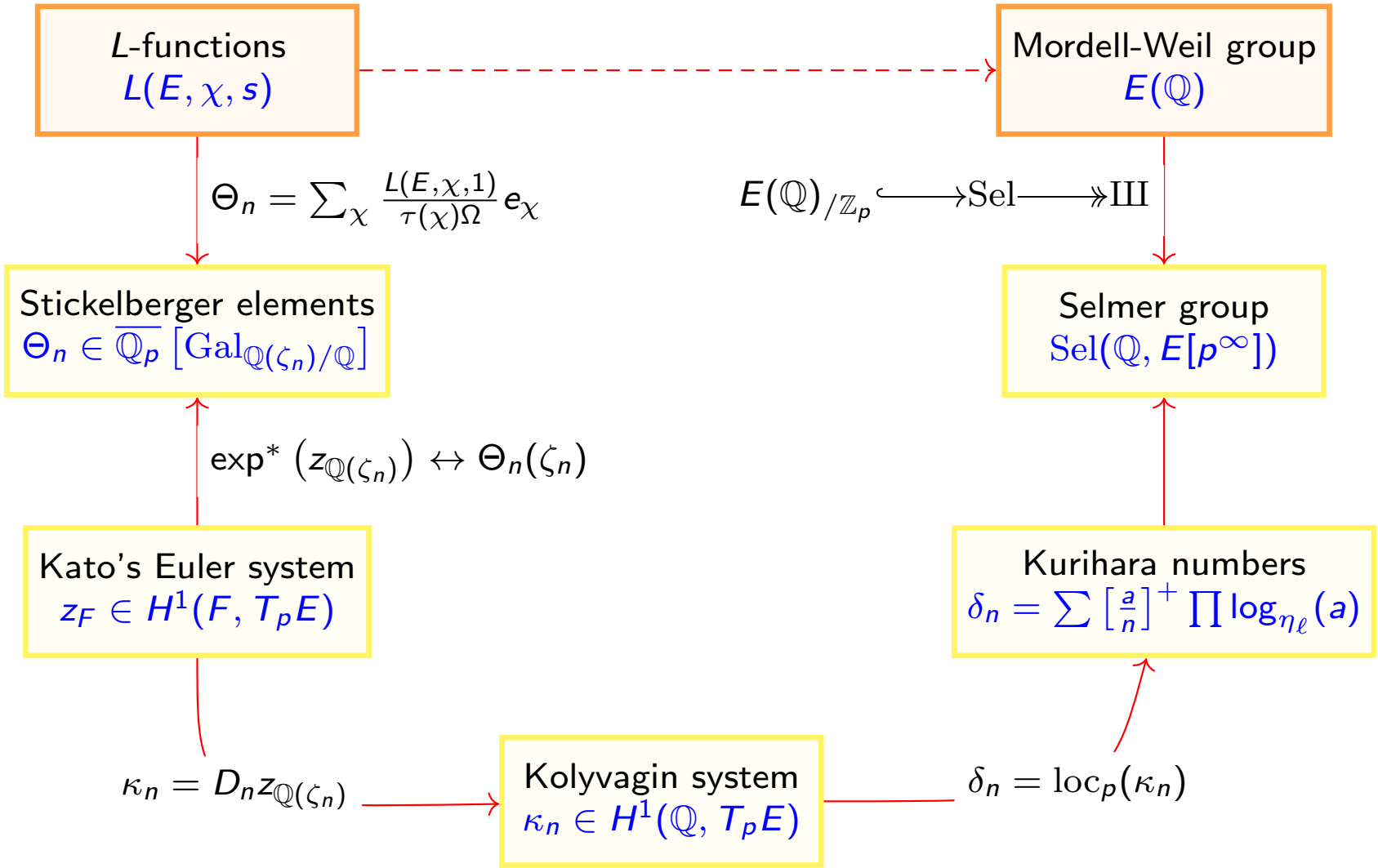
$$\delta_n := p^\alpha \exp^*(\kappa_n) = D_n\Theta_n(\zeta_n)$$

- Explicitly, fix a primitive root η_ℓ of $(\mathbb{Z}/\ell)^\times$ for every prime divisor ℓ of n. Then

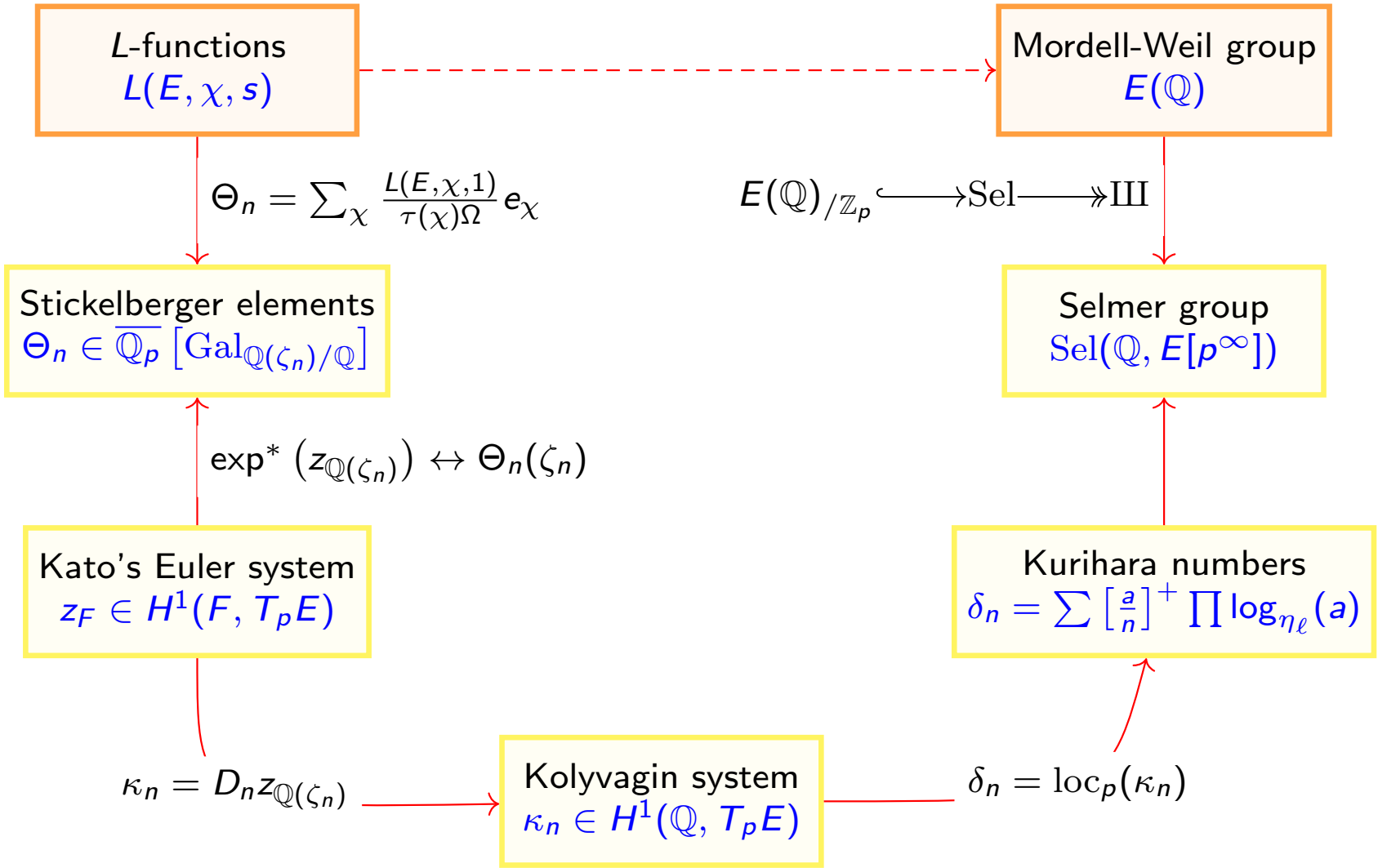
$$\boxed{\delta_n = \sum_{a\in(\mathbb{Z}/n)^\times} \left[\frac{a}{n}\right]^+ \prod_{\ell\mid n} \left(\log_{\eta_\ell}(a)\right) \in \mathbb{Z}_{(p)}}$$

- These quantities are known as Kurihara numbers.
- They depend on η_ℓ, but their p-adic valuation is independent of these choices.

Kurihara numbers



Structure of the Selmer group



Structure of the Selmer group

- For every square-free n, we denote by $\nu(n)$ the number of prime divisors of n.

Structure of the Selmer group

- For every square-free n, we denote by $\nu(n)$ the number of prime divisors of n.
- For every $i \in \mathbb{Z}_{\geq 0}$, define

$$\theta_i = \langle \{\delta_n : \ \nu(n) = i\} \rangle \subset \mathbb{Z}_p$$

Structure of the Selmer group

- For every square-free n, we denote by $\nu(n)$ the number of prime divisors of n.
- For every $i \in \mathbb{Z}_{\geq 0}$, define

$$\theta_i = \langle \{\delta_n : \ \nu(n) = i\} \rangle \subset \mathbb{Z}_p$$

- These ideals are related to the Fitting ideals of the Selmer group.

Structure of the Selmer group

- For every square-free n, we denote by $\nu(n)$ the number of prime divisors of n.
- For every $i \in \mathbb{Z}_{\geq 0}$, define

$$\theta_i = \langle \{\delta_n : \ \nu(n) = i\} \rangle \subset \mathbb{Z}_p$$

- These ideals are related to the Fitting ideals of the Selmer group.

Structure of the Selmer group

- For every square-free n, we denote by $\nu(n)$ the number of prime divisors of n.
- For every $i \in \mathbb{Z}_{\geq 0}$, define

$$\theta_i = \langle \{\delta_n : \ \nu(n) = i\} \rangle \subset \mathbb{Z}_p$$

- These ideals are related to the Fitting ideals of the Selmer group.

Fitting ideals

Let M be a finitely generated $\mathbb{Z}_p$-module. The structre theorem gives an isomorphism

$$M \cong \mathbb{Z}/p^{\alpha_1} \times \cdots \times \mathbb{Z}/p^{\alpha_r}$$

where $\alpha_i \in \mathbb{N} \cup \infty$. Assume $\alpha_1 \leq \cdots \leq \alpha_r$.

Structure of the Selmer group

- For every square-free n, we denote by $\nu(n)$ the number of prime divisors of n.
- For every $i \in \mathbb{Z}_{\geq 0}$, define

$$\theta_i = \langle \{\delta_n : \ \nu(n) = i\} \rangle \subset \mathbb{Z}_p$$

- These ideals are related to the Fitting ideals of the Selmer group.

Fitting ideals

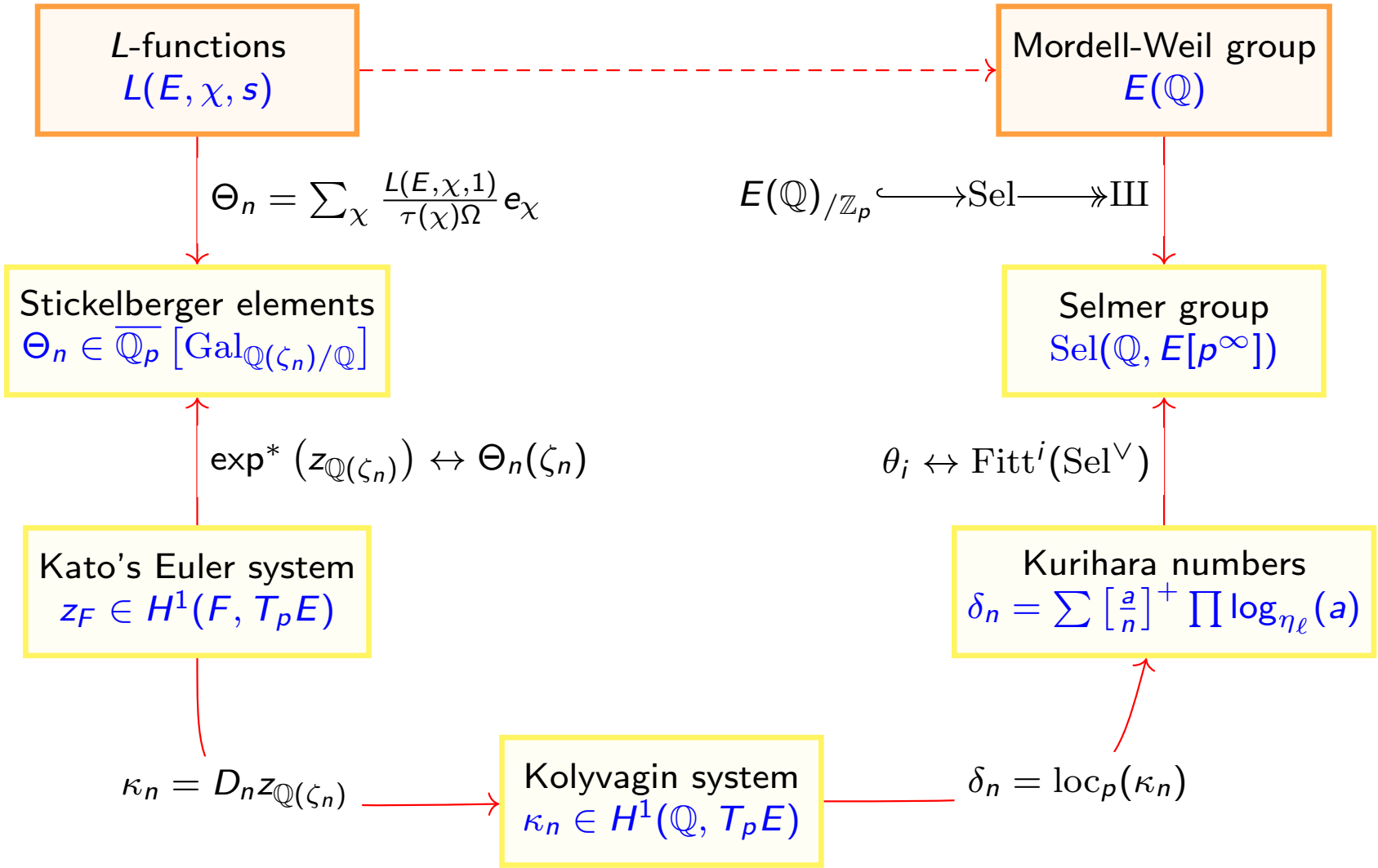
Let M be a finitely generated $\mathbb{Z}_p$-module. The structre theorem gives an isomorphism

$$M \cong \mathbb{Z}/p^{\alpha_1} \times \cdots \times \mathbb{Z}/p^{\alpha_r}$$

where $\alpha_i \in \mathbb{N} \cup \infty$. Assume $\alpha_1 \leq \cdots \leq \alpha_r$. Then

$$\begin{cases} \mathrm{Fitt}^i(M) = \prod_{k=1}^{r-i} p^{\alpha_k} & \text{if } 0 \leq i < r \\ \mathrm{Fitt}^i(M) = \mathbb{Z}_p & \text{if } i \geq r \end{cases}$$

Structure of the Selmer group



Main result

Theorem (C-H. Kim, 2025)

Let $p \geq 5$ satisfying that

- $G_{\mathbb{Q}}$ acts surjectively on $T_p E$.
- p divides neither the Tamagawa numbers nor the Manin constant
- $E(\mathbb{Q}_p)$ contains no p-torsion.
- The Iwasawa main conjecture (IMC) holds for E.

Main result

Theorem (C-H. Kim, 2025)

Let $p \geq 5$ satisfying that

- $G_{\mathbb{Q}}$ acts surjectively on $T_p E$.
- p divides neither the Tamagawa numbers nor the Manin constant
- $E(\mathbb{Q}_p)$ contains no p-torsion.
- The Iwasawa main conjecture (IMC) holds for E.

Then,

$$\begin{cases} \theta_i = \mathrm{Fitt}^i(\mathrm{Sel}(\mathbb{Q}, E[p^\infty])^\vee) & \text{if } (-1)^i = \omega(E) \\ \theta_i = 0 & \text{if } (-1)^i \neq \omega(E) \end{cases}$$

Main result

Theorem (C-H. Kim, 2025)

Let $p \geq 5$ satisfying that

- $G_{\mathbb{Q}}$ acts surjectively on T_pE.
- p divides neither the Tamagawa numbers nor the Manin constant
- $E(\mathbb{Q}_p)$ contains no p-torsion.
- The Iwasawa main conjecture (IMC) holds for E.

Then,

$$\begin{cases} \theta_i = \mathrm{Fitt}^i(\mathrm{Sel}(\mathbb{Q}, E[p^\infty])^\vee) & \text{if } (-1)^i = \omega(E) \\ \theta_i = 0 & \text{if } (-1)^i \neq \omega(E) \end{cases}$$

Remark

The above theorem, together with the Cassels-Tate pairing, can determine the full structure of the Selmer group.

Main result

Theorem (C-H. Kim, 2025)

Let $p \geq 5$ satisfying that

- $G_{\mathbb{Q}}$ acts surjectively on T_pE.
- p divides neither the Tamagawa numbers nor the Manin constant
- $E(\mathbb{Q}_p)$ contains no p-torsion.
- The Iwasawa main conjecture (IMC) holds for E.

Then,

$$\begin{cases} \theta_i = \mathrm{Fitt}^i(\mathrm{Sel}(\mathbb{Q}, E[p^\infty])^\vee) & \text{if } (-1)^i = \omega(E) \\ \theta_i = 0 & \text{if } (-1)^i \neq \omega(E) \end{cases}$$

Remark

The above theorem, together with the Cassels-Tate pairing, can determine the full structure of the Selmer group.

Remark

If $Ш(E)$ is finite, the algebraic rank is the minimal i such that there exists a square-free n_0 such that $\delta_{n_0} \neq 0$ and $\nu(n_0) = i$.

Main result

Theorem (C-H. Kim, 2025)

Let $p \geq 5$ satisfying that

- $G_{\mathbb{Q}}$ acts surjectively on T_pE.
- p divides neither the Tamagawa numbers nor the Manin constant
- $E(\mathbb{Q}_p)$ contains no p-torsion.
- The Iwasawa main conjecture (IMC) holds for E.

Then,

$$\begin{cases} \theta_i = \mathrm{Fitt}^i(\mathrm{Sel}(\mathbb{Q}, E[p^\infty])^\vee) & \text{if } (-1)^i = \omega(E) \\ \theta_i = 0 & \text{if } (-1)^i \neq \omega(E) \end{cases}$$

Remark

The above theorem, together with the Cassels-Tate pairing, can determine the full structure of the Selmer group.

Remark

If $Ш(E)$ is finite, the algebraic rank is the minimal i such that there exists a square-free n_0 such that $\delta_{n_0} \neq 0$ and $\nu(n_0) = i$. In this situation, $\#Ш(E)[p^\infty] \sim \delta_{n_0}$.

Main result

Theorem (C-H. Kim, 2025)

Let $p \geq 5$ satisfying that

- $G_{\mathbb{Q}}$ acts surjectively on T_pE.
- p divides neither the Tamagawa numbers nor the Manin constant
- $E(\mathbb{Q}_p)$ contains no p-torsion.
- The Iwasawa main conjecture (IMC) holds for E.

Then,

$$\begin{cases} \theta_i = \mathrm{Fitt}^i(\mathrm{Sel}(\mathbb{Q}, E[p^\infty])^\vee) & \text{if } (-1)^i = \omega(E) \\ \theta_i = 0 & \text{if } (-1)^i \neq \omega(E) \end{cases}$$

Remark

The above theorem, together with the Cassels-Tate pairing, can determine the full structure of the Selmer group.

Remark

If $Ш(E)$ is finite, the algebraic rank is the minimal i such that there exists a square-free n_0 such that $\delta_{n_0} \neq 0$ and $\nu(n_0) = i$. In this situation, $\#Ш(E)[p^\infty] \sim \delta_{n_0}$.

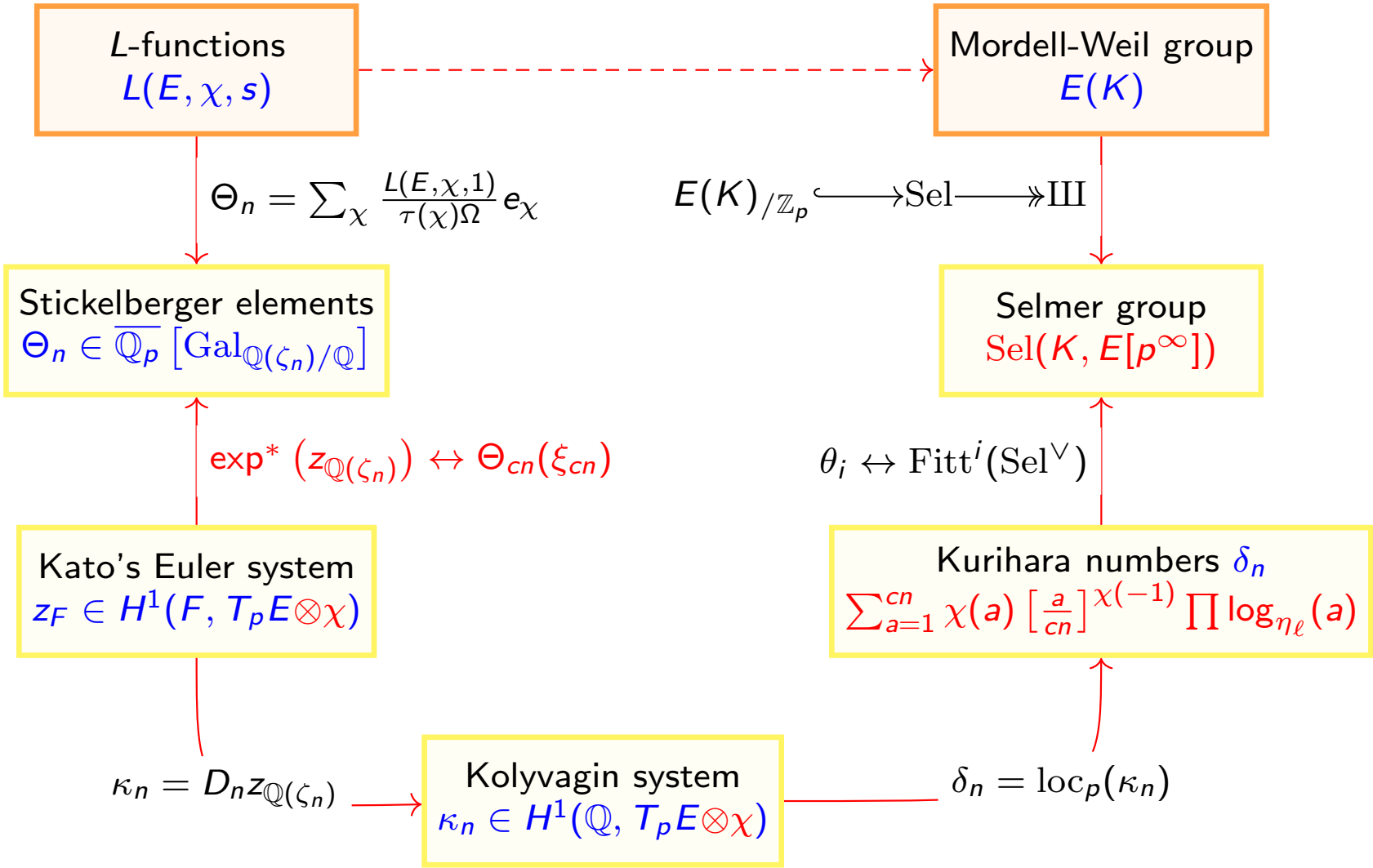
The values δ_n for other square-free n will determine the group structure of $Ш(E)[p^\infty]$.

Arithmetic over an abelian extension $K/\mathbb{Q}$

Assumptions on $K/\mathbb{Q}$

- The degree $[K:\mathbb{Q}]$ is prime to p.
- $K/\mathbb{Q}$ is unramified at p and at every bad prime of E.
- We call c the conductor of $K/\mathbb{Q}$.

Arithmetic over an abelian extension $K/\mathbb{Q}$



Arithmetic over an abelian extension $K/\mathbb{Q}$

Assumptions on $K/\mathbb{Q}$

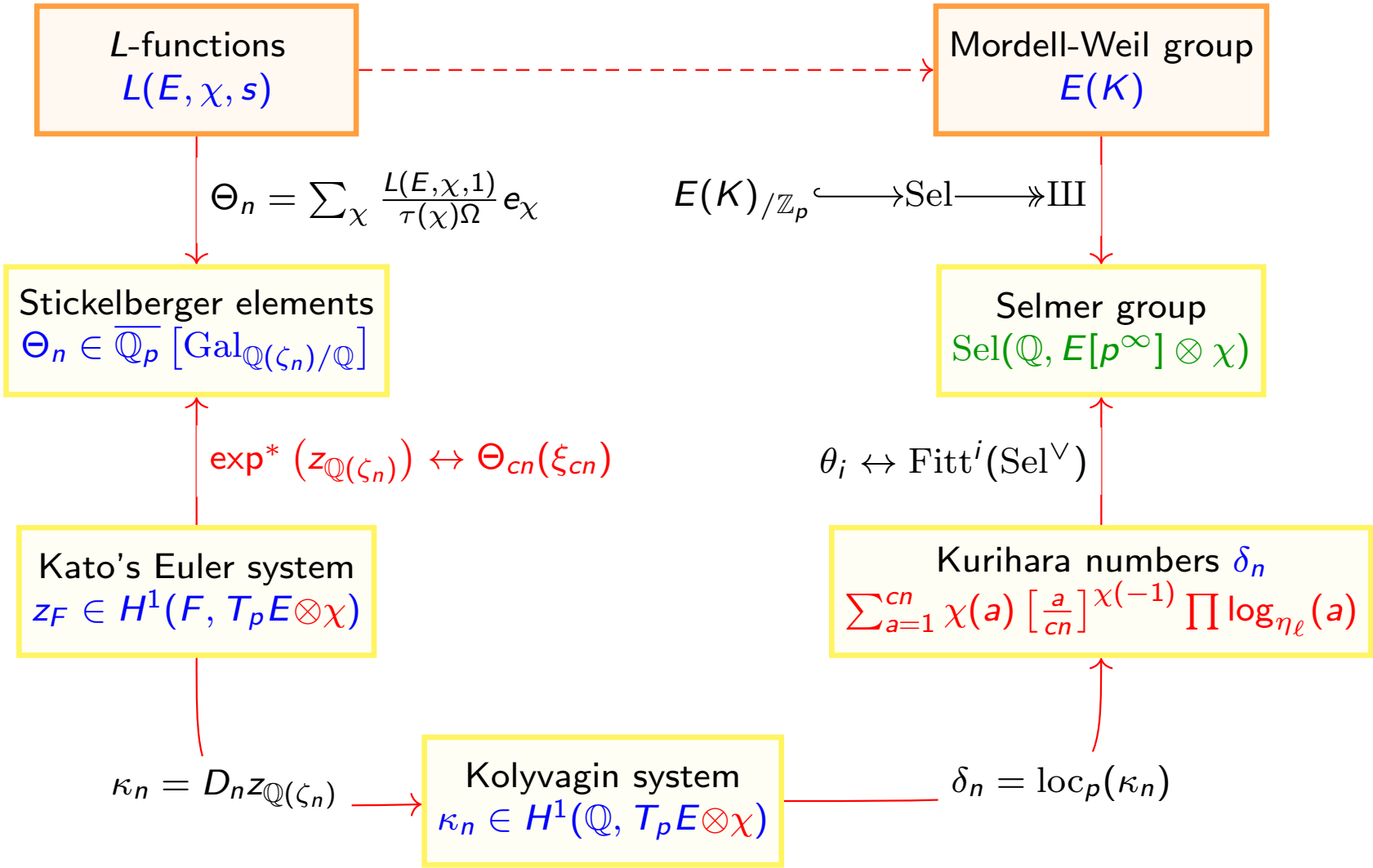
- The degree $[K:\mathbb{Q}]$ is prime to p.
- $K/\mathbb{Q}$ is unramified at p and at every bad prime of E.
- We call c the conductor of $K/\mathbb{Q}$.

Splitting the Selmer group

$$\mathrm{Sel}(K, E[p^\infty]) =' \bigoplus_{\chi} Sel(\mathbb{Q}, E[p^\infty] \otimes \chi)$$

We can study the different χ-parts independently.

Arithmetic over an abelian extension $K/\mathbb{Q}$



Arithmetic over an abelian extension $K/\mathbb{Q}$

Assumptions on $K/\mathbb{Q}$

- The degree $[K:\mathbb{Q}]$ is prime to p.
- $K/\mathbb{Q}$ is unramified at p and at every bad prime of E.
- We call c the conductor of $K/\mathbb{Q}$.

Splitting the Selmer group

$$\mathrm{Sel}(K, E[p^\infty]) =' \bigoplus_{\chi} Sel(\mathbb{Q}, E[p^\infty] \otimes \chi)$$

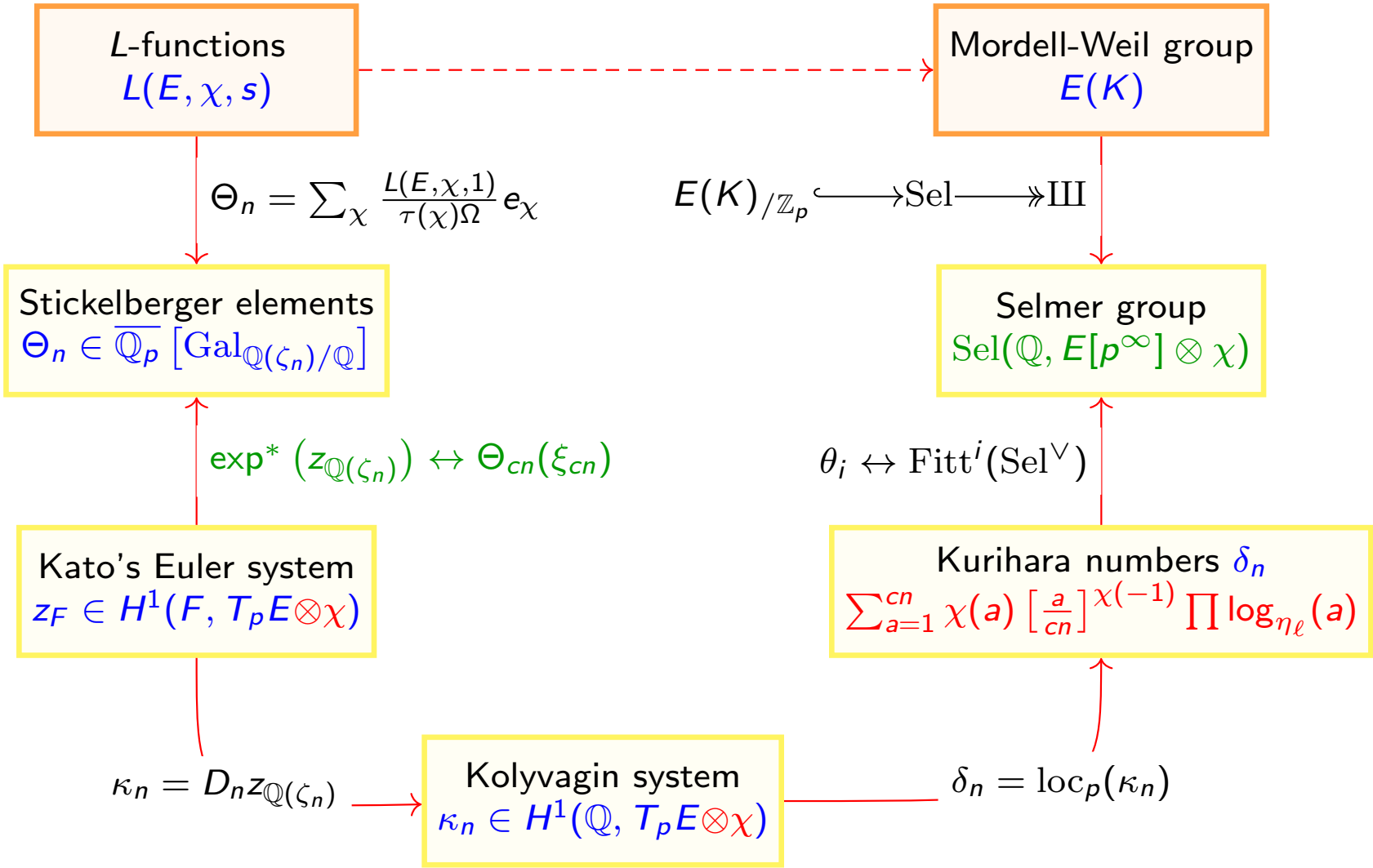
We can study the different χ-parts independently.

Generator of $\mathrm{Gal}(\mathbb{Q}(\zeta_{cn})/\mathbb{Q})$

- Problem: when c is not square-free, then ζ_{cn} do not generate $\mathbb{Q}(\zeta_{cn})$ as a $\mathbb{Q}_p[\mathcal{G}_{cn}]$-module.
- Solution: Substitute

$$\zeta_{cn} \mapsto \sum_{\widetilde{cn}|d|cn} \zeta_d$$

Arithmetic over an abelian extension $K/\mathbb{Q}$



Arithmetic over an abelian extension $K/\mathbb{Q}$

Splitting the Selmer group

$$\mathrm{Sel}(K, E[p^\infty]) =' \bigoplus_{\chi} Sel(\mathbb{Q}, E[p^\infty] \otimes \chi)$$

We can study the different χ-parts independently.

Generator of $\mathrm{Gal}(\mathbb{Q}(\zeta_{cn})/\mathbb{Q})$

- Problem: when c is not square-free, then ζ_{cn} do not generate $\mathbb{Q}(\zeta_{cn})$ as a $\mathbb{Q}_p[\mathcal{G}_{cn}]$-module.
- Solution: Substitute

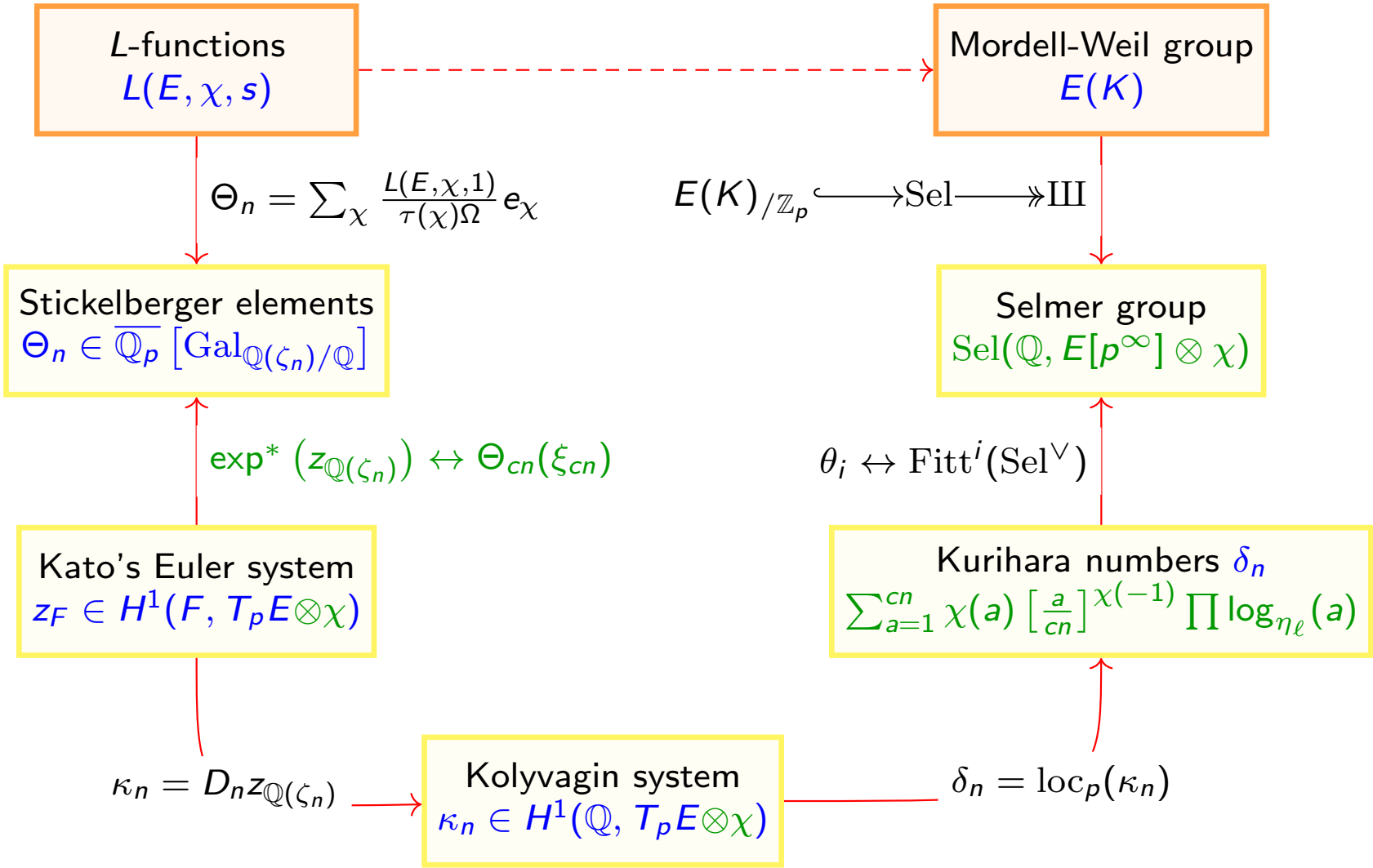
$$\zeta_{cn} \mapsto \sum_{\widetilde{cn}|d|cn} \zeta_d$$

Twisted Kurihara numbers

Twisted Kato's Euler system $\rightarrow$ twisted Kurihara numbers

$$\delta_{n,\chi} = \sum_{a \in (\mathbb{Z}/cn)^*} \chi(a) \left[\frac{a}{n}\right]^{\chi(-1)} \prod \left(\log_{\eta_\ell}(a)\right)$$

Arithmetic over an abelian extension $K/\mathbb{Q}$



Main result over abelian extensions

Theorem (A., 2025)

Let $p \geq 5$ satisfying that

- $K/\mathbb{Q}$ has degree prime to p and is unramified at every bad prime of E.
- $G_{\mathbb{Q}}$ acts surjectively on T_pE.
- p divides neither the Tamagawa numbers (over K) nor the Manin constant
- $E(K_{\mathfrak{p}})$ contains no p-torsion for every $\mathfrak{p} \mid p$.
- The Iwasawa main conjecture (IMC) holds for f_χ.

Main result over abelian extensions

Theorem (A., 2025)

Let $p \geq 5$ satisfying that

- $K/\mathbb{Q}$ has degree prime to p and is unramified at every bad prime of E.
- $G_{\mathbb{Q}}$ acts surjectively on T_pE.
- p divides neither the Tamagawa numbers (over K) nor the Manin constant
- $E(K_{\mathfrak{p}})$ contains no p-torsion for every $\mathfrak{p} \mid p$.
- The Iwasawa main conjecture (IMC) holds for f_χ.

We want to compute the Fitting ideals of the χ-part of $\mathrm{Sel}(K, E[p^\infty])^\vee$. We have two cases:

Main result over abelian extensions

Theorem (A., 2025)

Let $p \geq 5$ satisfying that

- $K/\mathbb{Q}$ has degree prime to p and is unramified at every bad prime of E.
- $G_{\mathbb{Q}}$ acts surjectively on T_pE.
- p divides neither the Tamagawa numbers (over K) nor the Manin constant
- $E(K_{\mathfrak{p}})$ contains no p-torsion for every $\mathfrak{p} \mid p$.
- The Iwasawa main conjecture (IMC) holds for f_χ.

We want to compute the Fitting ideals of the χ-part of $\mathrm{Sel}(K, E[p^\infty])^\vee$. We have two cases:

- $\boxed{\chi = \overline{\chi}}$

$$\begin{cases} \theta_i = \mathrm{Fitt}^i(\mathrm{Sel}(\mathbb{Q}, E[p^\infty])^\vee_\chi) & \text{if } (-1)^i = \omega(E) \\ \theta_i = 0 & \text{if } (-1)^i \neq \omega(E) \end{cases}$$

Main result over abelian extensions

Theorem (A., 2025)

Let $p \geq 5$ satisfying that

- $K/\mathbb{Q}$ has degree prime to p and is unramified at every bad prime of E.
- $G_{\mathbb{Q}}$ acts surjectively on T_pE.
- p divides neither the Tamagawa numbers (over K) nor the Manin constant
- $E(K_{\mathfrak{p}})$ contains no p-torsion for every $\mathfrak{p} \mid p$.
- The Iwasawa main conjecture (IMC) holds for f_χ.

We want to compute the Fitting ideals of the χ-part of $\mathrm{Sel}(K, E[p^\infty])^\vee$. We have two cases:

- $\boxed{\chi = \overline{\chi}}$

$$\begin{cases} \theta_i = \mathrm{Fitt}^i(\mathrm{Sel}(\mathbb{Q}, E[p^\infty])^\vee_\chi) & \text{if } (-1)^i = \omega(E) \\ \theta_i = 0 & \text{if } (-1)^i \neq \omega(E) \end{cases}$$

- $\boxed{\chi \neq \overline{\chi}}$

$$\theta_i = \mathrm{Fitt}^i(\mathrm{Sel}(, E[p^\infty])^\vee_\chi) \ \forall i$$

Thank you for your attention!