SELMER GROUPS FOR p-ADIC GALOIS REPRESENTATIONS

RALPH GREENBERG
NOTES BY SUBONG LIM

In these lectures we discuss the definition of Selmer groups for elliptic curves and then explain how one can extend the definition to much more general situations, e.g., modular forms, symmetric powers of elliptic curves, etc. Part of the motivation comes from Iwasawa theory and the question of formulating a main conjecture.

1. First Lecture

1.1. **Selmer groups for elliptic curves.** Let F be a number field. Let E be an elliptic curve defined over F.

Theorem 1. (Mordell-Weil) *$E(F)$ is a finitely generated abelian group. That is, $E(F) \cong \mathbb{Z}^r \times$ (a finite group), where $r = \mathrm{rank}(E(F)) \geq 0$.*

One crucial ingredient in the proof: For some $n \geq 2$, $E(F)/nE(F)$ is finite. In fact, $E(F)/nE(F)$ is finite for all $n \geq 1$. This is the so-called "weak Mordell-Weil Theorem".

Regard F as a subfield of $\bar{\mathbb{Q}}$, an algebraic closure of $\mathbb{Q}$. Let $G_F = \mathrm{Gal}(\bar{\mathbb{Q}}/F)$. The Kummer homomorphism: For any $n \geq 1$, consider $E[n] = E(\bar{\mathbb{Q}})[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$. In general, if A is an abelian group then $A[n] = \{a \in A |\ na = 0_A\}$. Then G_F acts on $E[n]$. That is, there is a homomorphism

$$G_F \to \mathrm{Aut}(E[n]) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

One defines a map $\kappa_n : E(F)/nE(F) \to \mathrm{H}^1(G_F, E[n])$. There are two ways to define this map:

(1) Let $P \in E(F)$. Pick $Q \in E(\bar{\mathbb{Q}})$ such that $nQ = P$. Note that $E(\bar{\mathbb{Q}})$ and $\bar{\mathbb{Q}}^*$ are divisible groups. If $Q' \in E(\bar{\mathbb{Q}})$ satisfies $nQ' = P$, then $Q' - Q \in E[n]$. Let $g \in G_F$. Then $nQ = P$ implies that $ng(Q) = g(P) = P$. Hence $g(Q) - Q \in E[n]$. Define $\psi : G_F \to E[n]$ by $\psi(g) = g(Q) - Q$ for all $g \in G_F$. We define

$$\kappa_n(P + nE(F)) = [\psi] \text{ in } \mathrm{H}^1(G_F, E[n]).$$

(2) Consider the exact sequence

$$0 \to E[n] \to E(\bar{\mathbb{Q}}) \xrightarrow{n} E(\bar{\mathbb{Q}}) \to 0.$$

We get the corresponding cohomology sequence which is exact

$$\mathrm{H}^0(F, E[n])(= \mathrm{H}^0(G_F, E[n])) \to \mathrm{H}^0(F, E(\bar{\mathbb{Q}})) \to \mathrm{H}^0(F, E(\bar{\mathbb{Q}})) \to \mathrm{H}^1(F, E[n]) \to \mathrm{H}^1(F, E(\bar{\mathbb{Q}})).$$

We obtain an exact sequence

$$E(F) \xrightarrow{n} E(F) \to \mathrm{H}^1(F, E[n]).$$

Hence we obtain an injective map

$$\kappa_n : E(F)/nE(F) \to \mathrm{H}^1(F, E[n]).$$

One shows that $E(F)/nE(F)$ is finite by showing that $\mathrm{Im}(\kappa_n)$ is contained in a certain finite subgroup of $\mathrm{H}^1(F, E[n])$.

Define $E_{\mathrm{Tors}} = E(\bar{\mathbb{Q}})_{\mathrm{Tors}} = \varinjlim_n E[n] \cong (\mathbb{Q}/\mathbb{Z})^2$. G_F acts on E_{Tors} by a homomorphism

$$G_F \to \mathrm{Aut}(E_{\mathrm{Tors}}) \cong \mathrm{Aut}((\mathbb{Q}/\mathbb{Z})^2) \cong \varprojlim_n \mathrm{Aut}(E[n]) \cong \varprojlim_n \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \cong \mathrm{GL}_2(\hat{\mathbb{Z}}) \cong \prod_p \mathrm{GL}_2(\mathbb{Z}_p)$$

where p varies over the primes.

Define $\kappa : E(F) \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z}) \to \mathrm{H}^1(F, E_{\mathrm{Tors}})$ by $\kappa(P \otimes (\frac{1}{n} + \mathbb{Z})) = \kappa_n(P)$ where $P \in E(F)$. Note that $E(F) \otimes_{\mathbb{Z}} (\frac{1}{n}\mathbb{Z}/\mathbb{Z}) \cong E(F)/nE(F)$.

Remark that:

(1) $E(F) \cong \mathbb{Z}^r \times$ (a finite group). This implies that $E(F) \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} \cong (\mathbb{Q}/\mathbb{Z})^r$.
(2) κ is injective.

1.2. **Definition of** $\mathrm{Sel}_E(F)$**.** Let v be a place of F. Let F_v be the completion of F at v. Pick an embedding $\bar{\mathbb{Q}} \hookrightarrow \overline{F_v}$ extending the embedding $F \hookrightarrow F_v$.

$$\begin{array}{ccc} \bar{\mathbb{Q}} & \hookrightarrow & \bar{F}_v \\ \uparrow & & \uparrow \\ F & \hookrightarrow & F_v \end{array}$$

We have the restriction homomorphism $G_{F_v} \hookrightarrow G_F$. We have a Kummer map

$$\kappa_v : E(F_v) \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z}) \to \mathrm{H}^1(F_v, E(\bar{F}_v)_{\mathrm{Tors}}).$$

Also we have a commutative diagram

$$\begin{array}{ccc} E(F) \otimes (\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\kappa} & \mathrm{H}^1(F, E_{\mathrm{Tors}}) \\ \downarrow & & \downarrow \\ E(F_v) \otimes (\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\kappa_v} & \mathrm{H}^1(F_v, E(\bar{F}_v)_{\mathrm{Tors}}) \end{array}$$

This is the definition of the Selmer group:

$$\begin{aligned} \mathrm{Sel}_E(F) &= \ker(\mathrm{H}^1(F, E_{\mathrm{Tors}}) \to \prod_v \frac{\mathrm{H}^1(F_v, E_{\mathrm{Tors}})}{\mathrm{Im}\,(\kappa_v)}) \\ &= \{[\varphi] \in \mathrm{H}^1(F, E_{\mathrm{Tors}}) |\ [\varphi|_{G_{F_v}}] \in \mathrm{Im}\,(\kappa_v)\}. \end{aligned}$$

We have

$$\kappa : E(F) \otimes \mathbb{Q}/\mathbb{Z} \to \mathrm{H}^1(F, E_{\mathrm{Tors}}).$$

Remark that $\mathrm{Im}\,(\kappa) \subset \mathrm{Sel}_E(F)$. Define $Ш_E(F) = \mathrm{Sel}_E(F)/\mathrm{Im}\,(\kappa)$. We call $Ш_E(F)$ the Tate-Shafarevich group for E over F. Note that $\mathrm{Im}\,(\kappa) \cong E(F) \otimes \mathbb{Q}/\mathbb{Z} \cong (\mathbb{Q}/\mathbb{Z})^r$. It is conjectured that

$Ш_E(F)$ is a finite group. If this conjecture is true, then $\mathrm{Im}\,(\kappa) = \mathrm{Sel}_E(F)_{\mathrm{div}}$ where $\mathrm{Sel}_E(F)_{\mathrm{div}}$ is the maximal divisible subgroup of $\mathrm{Sel}_E(F)$.

Let p be a prime. Take the p-primary subgroup of everything. If A is an abelian group, then $A_p = \cup_n A[p^n]$ is the p-primary subgroup of A. Then $(E_{\mathrm{Tors}})_p = \cup_m E[p^m] = E[p^\infty] \cong (\mathbb{Q}/\mathbb{Z})_p^2 \cong (\mathbb{Q}_p/\mathbb{Z}_p)^2$ where $E[p^m] = E(\bar{\mathbb{Q}})[p^m]$. And G_F acts on these groups.

2. Second Lecture

Let p be a prime. Then

(1) $(E_{\mathrm{Tors}})_p = \cup_n E[p^n] = E[p^\infty] \cong (\mathbb{Q}_p/\mathbb{Z}_p)^2$,
(2) $\mathrm{H}^1(F, E_{\mathrm{Tors}})_p = \mathrm{H}^1(F, E[p^\infty])$,
(3) $\kappa_p : E(F) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \to \mathrm{H}^1(F, E[p^\infty])$,
(4) $\kappa_{v,p} : E(F_v) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \to \mathrm{H}^1(F_v, E[p^\infty])$,
(5) $\mathrm{Sel}_E(F)_p = \ker(\mathrm{H}^1(F, E[p^\infty]) \to \prod_v \mathrm{H}^1(F_v, E[p^\infty])/\mathrm{Im}\,(\kappa_{v,p}))$.

Here v varies over all primes of F.

It turns out that $\mathrm{Sel}_E(F)_p[p]$ is a finite group. As a consequence

$$\mathrm{Sel}_E(F)_p \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{s_p} \times \text{ (a finite abelian } p\text{-group)}$$

where $s_p \geq 0$. s_p is called the $\mathbb{Z}_p$-corank of $\mathrm{Sel}_E(F)_p$ and $s_p = s_p(E, F)$.

We have an exact sequence

$$0 \to E(F) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \xrightarrow{\kappa_p} \mathrm{Sel}_E(F)_p \to Ш_E(F)_p \to 0.$$

In fact, $s_p = r + \mathrm{corank}_{\mathbb{Z}_p}(Ш_E(F)_p)$ where $r = \mathrm{rank}(E(F))$. We have $s_p \geq r$. Conjecturally we should have $s_p = r$ for all primes p.

Before going on, I will mention other Galois modules:

(1) $T_p(E) = \varprojlim_n E[p^n] \cong \mathbb{Z}_p^2$ and G_F acts on this. The map $E[p^m] \to E[p^n]$ for $m \geq n$ is just multiplication by p^{m-n}.
(2) $V_p(E) = T_p(E) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong \mathbb{Q}_p^2$ and G_F acts.
(3) $E[p^\infty] = V_p(E)/T_p(E)$ as G_F-modules.

The action G_F on $T_p(E)$ is given by homomorphism $G_F \to \mathrm{Aut}_{\mathbb{Z}_p}(T_p(E)) \cong \mathrm{GL}_2(\mathbb{Z}_p)$.

Theorem 2. (Faltings) *Let E_1 and E_2 be elliptic curves defined over F. Suppose that $V_p(E_1) \cong V_p(E_2)$ as $\mathbb{Q}_p$-representation spaces for G_F for some prime p. Then there exists an isogeny $\varphi : E_1 \to E_2$ defined over F. Furthermore, if $T_p(E_1) \cong T_p(E_2)$, then one can choose φ so that $|\ker(\varphi)|$ is not divisible by p*

This is the philosophy: Arithmetic information about E which is unchanged by an isogeny defined over F should *somehow* be determined by the isomorphism class of $V_p(E)$ as a representation space for G_F for any prime p. Furthermore, information which is unchanged by an F-isogeny of degree prime to p should be determined *somehow* by the isomorphism class of $T_p(E)$. We can do this for $\mathrm{Sel}_E(F)_p$.

We can describe $\mathrm{Sel}_E(F)_p$ entirely in terms of $E[p^\infty] \cong V_p(E)/T_p(E)$. Recall that

$$\mathrm{Sel}_E(F)_p = \ker(\mathrm{H}^1(F, E[p^\infty]) \to \prod_v (\mathrm{H}^1(F_v, E[p^\infty])/\mathrm{Im}\,(\kappa_{v,p}))).$$

We must show that $\mathrm{Im}\,(\kappa_{v,p})$ has a description just in terms of the G_F-module $E[p^\infty]$.

Proposition 3. *Suppose v does not lie over p. Then* $\mathrm{Im}\,(\kappa_{v,p}) = 0$.

Proof Suppose v is nonarchimedean. Suppose v lies over l, where $l \neq p$. It is known that $E(F_v)$ has a subgroup of finite index isomorphic to $\mathbb{Z}_l^{[F_v:\mathbb{Q}_l]}$. If $\mathcal{F}_E$ is the formal group for E over F_v, then for any $t \geq 1$, $\mathcal{F}_E(\mathfrak{m}_v^t)$ is a subgroup of $E(F_v)$ of finite index. Here $\mathfrak{m}_v$ is the maximal ideal in $\mathcal{O}_{F_v}$. The $\log_{\mathcal{F}_E}$ defines an isomorphism $\mathcal{F}_E(\mathfrak{m}_v^t) \tilde{\to} \mathfrak{m}_v^t$ as a subgroup of $\mathcal{O}_{F_v}$ of finite index for $t \gg 0$. And $\mathfrak{m}_v^t \cong \mathbb{Z}_l^{[F_v:\mathbb{Q}_l]}$ as a $\mathbb{Z}_l$-module. We have an exact sequence

$$0 \to \mathbb{Z}_l^{[F_v:\mathbb{Q}_l]} \to E(F_v) \to A \to 0$$

where A is finite. $\mathbb{Z}_l \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = 0$ because $p\mathbb{Z}_l = \mathbb{Z}_l$ for $p \neq l$. And $A \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = 0$. Hence $E(F_v) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = 0$ and so $\mathrm{Im}\,(\kappa_{v,p}) = 0$.

Here is another argument: One can show $\mathrm{H}^1(F_v, E[p^\infty])$ is finite if v is nonarchimedean and $v \nmid p$. Note that

$$\kappa_{v,p} : E(F_v) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \to \mathrm{H}^1(F_v, E[p^\infty])$$

and $E(F_v) \otimes (\mathbb{Q}_p/\mathbb{Z}_p)$ is divisible and $\mathrm{H}^1(F_v, E[p^\infty])$ is finite. Hence $\mathrm{Im}\,(\kappa_{v,p}) = 0$.

If v is archimedean, then $F_v \cong \mathbb{R}$ or $\mathbb{C}$. And $E(F_v) \cong \mathbb{R}/\mathbb{Z}$ or $\mathbb{R}/\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z}$ or $(\mathbb{R}/\mathbb{Z})^2$. One again sees that $E(F_v) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = 0$.

Suppose $v|p$. Assume that E has a good reduction at v and that the reduced elliptic curves are ordinary. Let $\tilde{E}_v$ be the reduction of E modulo v which is an elliptic curve defined over the residue field f_v for prime v of E. The field f_v is a finite field of characteristic p and $f_v \cong \mathbb{F}_q$ where q is a power of p. Then

$$\tilde{E}_v[p^\infty] = \begin{cases} \mathbb{Q}_p/\mathbb{Z}_p & \text{if } \tilde{E}_v \text{ is ordinary,} \\ 0 & \text{if } \tilde{E}_v \text{ is supersingular.} \end{cases}$$

We have a surjective homomorphism $E(\bar{F}_v) \to \tilde{E}_v(\bar{f}_v)$, which is a reduction modulo v. This induces a surjective homomorphism $E[p^\infty] \to \tilde{E}_v[p^\infty]$. This map is G_{F_v}-equivariant. Let I_v be the inertia subgroup of G_{F_v}. Then I_v acts trivially on $\tilde{E}_v[p^\infty]$.

Proposition 4. *With the above notation and assumption that $\tilde{E}_v$ is ordinary, we have*

$$\mathrm{Im}\,(\kappa_{v,p}) = \ker(\mathrm{H}^1(F_v, E[p^\infty]) \to \mathrm{H}^1(F_v, E[p^\infty]_{I_v}))_{\mathrm{div}}.$$

3. Third Lecture

Note that

(1) $\mathrm{Sel}_E(F)_p = \ker(\mathrm{H}^1(F, E[p^\infty]) \to \prod_v \mathrm{H}^1(F_v, E[p^\infty]/\mathrm{Im}\,(\kappa_{v,p})))$.
(2) $\mathrm{Im}\,(\kappa_{v,p}) = 0$ if $v \nmid p$.

(3) Assume $v|p$ and E has good ordinary reduction at p. In other words, $\tilde{E}_v$ is ordinary. Then $\mathrm{Im}\,(\kappa_{v,p}) = (\ker(\mathrm{H}^1(F_v, E[p^\infty]) \to \mathrm{H}^1(F_v, E[p^\infty]_{I_v})))_{\mathrm{div}}$.

What do these groups look like? Recall that

$$\kappa_{v,p} : E(F_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{H}^1(F_v, E[p^\infty])$$

and $\kappa_{v,p}$ is injective. $E(F_v)$ contains $\mathcal{F}_E(\mathfrak{m}_v^t)$ for any $t \geq 1$ as a subgroup of finite index. Here $\mathcal{F}_E$ is the formal group of E over F_v. And $\mathcal{F}_E(\mathfrak{m}_v^t) \cong \mathbb{Z}_p^{[F_v:\mathbb{Q}_p]}$ if t is sufficiently large. Then, $\mathbb{Z}_p \otimes \mathbb{Q}_p/\mathbb{Z}_p = \mathbb{Q}_p/\mathbb{Z}_p$. This implies that

$$E(F_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{[F_v:\mathbb{Q}_p]}.$$

And $\mathrm{H}^1(F_v, E[p^\infty]) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{2[F_v:\mathbb{Q}_p]} \times E(F_v)_p$ where $E(F_v)_p$ is the p-primary part of $E(F_v)$ and it is actually finite. Reference is Chapter 2 of [2]. Also, Tate's duality theorem implies the above isomorphism. And $\mathrm{corank}(\mathrm{Im}\,(\kappa_{v,p})) = [F_v : \mathbb{Q}_p]$ and $\mathrm{corank}(\mathrm{H}^1(F_v, E[p^\infty])) = 2[F_v : \mathbb{Q}_p]$. We have an exact sequence

$$0 \to \mathcal{F}_E[p^\infty] \to E[p^\infty] \to \tilde{E}_v[p^\infty] \to 0$$

where $\mathcal{F}_E[p^\infty]$ denotes $\mathcal{F}_E(\bar{\mathfrak{m}}_v)[p^\infty]$ and $\bar{\mathfrak{m}}_v$ is the maximal ideal in $O_{\bar{F}_v}$. Note that

(1) $E[p^\infty] = (\mathbb{Q}_p/\mathbb{Z}_p)^2$,
(2) $\tilde{E}_v[p^\infty] \cong \mathbb{Q}_p/\mathbb{Z}_p$,
(3) $\mathcal{F}_E[p^\infty] \cong \mathbb{Q}_p/\mathbb{Z}_p$.

And $E[p^\infty]_{I_v} \cong \tilde{E}_v[p^\infty]$ since $\mathcal{F}_E[p^\infty] \cong \mu_{p^\infty}$ for the action of I_v. Thus

$$\mathrm{H}^1(F_v, E[p^\infty]_{I_v}) \cong \mathrm{H}^1(F_v, \tilde{E}_v[p^\infty]) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{[F_v:\mathbb{Q}_p]} \times \text{ (a finite group).}$$

The last isomorphism comes from the Poitou-Tate theorem. And

$$\ker(\mathrm{H}^1(F_v, E[p^\infty]) \to \mathrm{H}^1(F_v, E[p^\infty]_{I_v})) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{[F_v:\mathbb{Q}_p]} \times \text{ (a finite group)}$$

where the corank of $\mathrm{H}^1(F_v, E[p^\infty])$ is $2[F_v : \mathbb{Q}_p]$ and the corank of $\mathrm{H}^1(F_v, E[p^\infty]_{I_v})$ is $[F_v : \mathbb{Q}_p]$. This kernel is isomorphic to the image of

$$\mathrm{H}^1(F_v, \mathcal{F}_E[p^\infty]) \xrightarrow{\alpha} \mathrm{H}^1(F_v, E[p^\infty])$$

by the cohomology exact sequence. Since $\ker(\alpha) = \mathrm{H}^0(G_{f_v}, \tilde{E}_v[p^\infty])$ is finite,

$$\mathrm{H}^1(F_v, \mathcal{F}_E[p^\infty]) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{[F_v:\mathbb{Q}_p]} \times \text{ (a finite group).}$$

Hence

$$\ker(\mathrm{H}^1(F_v, E[p^\infty]) \to \mathrm{H}^1(F_v, E[p^\infty]_{I_v})) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{[F_v:\mathbb{Q}_p]} \times \text{ (a finite group).}$$

It suffices to prove that $\mathrm{Im}\,(\kappa_{v,p}) \subset \ker(\mathrm{H}^1(F_v, E[p^\infty]) \to \mathrm{H}^1(F_v, \tilde{E}_v[p^\infty]))$.

3.1. **Proof of the inclusion.**

$$\begin{array}{ccc} E(F_v)\otimes \mathbb{Q}_p/\mathbb{Z}_p & \xrightarrow{\kappa_{v,p}} & \mathrm{H}^1(F_v, E[p^\infty]) \\ \downarrow & & \downarrow \\ \tilde{E}_v(f_v)\otimes \mathbb{Q}_p/\mathbb{Z}_p & \xrightarrow{\tilde{\kappa}_{v,p}} & \mathrm{H}^1(F_v, \tilde{E}_v[p^\infty]) \end{array}$$

is a commutative diagram of G_{F_v}-equivariant maps. Since $\tilde{E}_v(f_v)$ is finite, $\tilde{E}_v(f_v)\otimes \mathbb{Q}_v/\mathbb{Z}_p = 0$ and hence $\mathrm{Im}\,(\kappa_{v,p}) \subset \ker(\mathrm{H}^1(F_v, E[p^\infty]) \to \mathrm{H}^1(F_v, \tilde{E}_v[p^\infty]))$.

This is a remark: What if $v \nmid p$ has a split multiplicative reduction at v? We have an exact sequence

$$0 \to \mu_{p^\infty} \to E[p^\infty] \to \mathbb{Q}_p/\mathbb{Z}_p \to 0.$$

This is G_{F_v}-equivariant. The above descriptions of $\mathrm{Im}\,(\kappa_{v,p})$ are still valid. What if E has a supersingular reduction at v? That means $\tilde{E}_v[p^\infty] = 0$. We still have the exact sequence

$$0 \to \mathcal{F}_E[p^\infty] \to E[p^\infty] \to \tilde{E}_v[p^\infty] \to 0.$$

$\mathrm{Im}\,(\kappa_{v,p}) = (\mathbb{Q}_p/\mathbb{Z}_p)^{[F_v:\mathbb{Q}_v]}$ and $\ker(\mathrm{H}^1(F_v, E[p^\infty]) \to \mathrm{H}^1(F_v, E[p^\infty]_{I_v})) = \mathrm{H}^1(F_v, E[p^\infty])$. The last equality comes from the fact that $E[p^\infty]_{I_v} = \tilde{E}_v[p^\infty] = 0$. And $\ker(\mathrm{H}^1(F_v, E[p^\infty]) \to \mathrm{H}^1(F_v, E[p^\infty]_{I_v}))$ has $\mathbb{Z}_p$-corank $2[F_v : \mathbb{Q}_p]$. The above description of $\mathrm{Im}\,(\kappa_{v,p})$ for $v|p$ is obviously not valid in this case.

In fact, $\mathrm{Im}\,(\kappa_{v,p})$ was described by Bloch-Kato. Consider the map

$$\mathrm{H}^1(F_v, V_p(E)) \to \mathrm{H}^1(F_v, V_p(E)\otimes_{\mathbb{Q}_p} B_{\mathrm{cris}})$$

where B_{cris} is an infinite dimensional $\mathbb{Q}_p$-algebra with action of G_{F_v}. This is done by Fontaine. Consider the kernel of the above map. We call this $\mathrm{H}^1_f(F_v, V_p(E))$. We have a map $V_p(E) \to E[p^\infty]$. Then Bloch-Kato proved that $\mathrm{Im}\,(\kappa_{v,p})$ coincides with the image of $\mathrm{H}^1_f(F_v, V_p(E))$ under the map $\mathrm{H}^1(F_v, V_p(E)) \to \mathrm{H}^1(F_v, E[p^\infty])$ induced from the map $V_p(E) \twoheadrightarrow E[p^\infty]$.

Assume also that F_v is a p-adic Lie extension of $\mathbb{Q}_p$. Assume $F_v/\mathbb{Q}_p$ is infinitely ramified. Then

$$\mathrm{Im}\,(\kappa_{v,p}) = \ker(\mathrm{H}^1(F_v, E[p^\infty]) \to \mathrm{H}^1(F_v, \tilde{E}_v[p^\infty]))$$

under the assumption that E has a good reduction at v. When E has a supersingular reduction, $\mathrm{Im}\,(\kappa_{v,p}) = \mathrm{H}^1(F_v, E[p^\infty])$. Remark that the above equality is far from true when $[F_v : \mathbb{Q}_v] < \infty$.

4. Fourth Lecture

This lecture is about "modular forms". Let E be an elliptic curve defined over $\mathbb{Q}$. It can be extended to general number field F. Let p be a prime where E has a good reduction, i.e., $p \nmid N_E$ where N_E is the conductor of E. Let $\tilde{E}_p$ be the reduced curve mod p over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Define $a_p = 1 + p - |\tilde{E}_p(\mathbb{F}_p)|$. That is in $\mathbb{Z}$. There is a criterion: $\tilde{E}_p$ is ordinary if and only if $p \nmid a_p$ and $\tilde{E}_p$ is supersingular if and only if $p|a_p$. Remark that if E has CM and $\mathrm{End}(E) = \mathbb{Q}(\sqrt{-d})$, then $\tilde{E}_p$ is ordinary if and only if $(\frac{-d}{p}) = 1$. If E does not have CM, then

$$\lim_{x\to\infty} |\{p \le x|\ \tilde{E}_p \text{ is ordinary}\}|/\pi(x) = 1.$$

The left-hand side is called "Dirichlet density". But note that $\{p|\ \tilde{E}_p$ is supersingular$\}$ is infinite. It is proved by Elkies. Remark that $|a_p| \leq 2\sqrt{p}$ (Hasse). If $p \geq 5$, then $p|a_p$ if and only if $a_p = 0$. However, if $p = 2$ or 3, then $a_p \in \{0, \pm p\}$, and all three values occur. Consider $1 - a_pX + pX^2$. This is related to the Euler factor of Hasse-Weil L-function $L(E/\mathbb{Q}, s)$, i.e., $(1 - a_pp^{-s} + pp^{-s})^{-1}$. Write $1 - a_pX + pX^2 = (1 - \alpha_pX)(1 - \beta_pX), \alpha_p, \beta_p \in \bar{\mathbb{Q}}_p$. Note that $\alpha_p + \beta_p = a_p, \alpha_p\beta_p = p$, and $(Y - \alpha_p)(Y - \beta_p) = Y^2 - a_pY + p$. And $|\tilde{E}_p(\mathbb{F}_p)| = 1 + p - a_p = (1 - \alpha_p)(1 - \beta_p)$. It is known that $|\tilde{E}_p(\mathbb{F}_{p^n})| = (1 - \alpha_p^n)(1 - \beta_p^n)$. Recall that

$$\tilde{E}_p(\tilde{\mathbb{F}}_p)[p^\infty] = \begin{cases} \mathbb{Q}_p/\mathbb{Z}_p & \tilde{E}_p \text{ is ordinary,} \\ 0 & \tilde{E}_p \text{ is supersingular.} \end{cases}$$

This implies that

$$\begin{aligned} & \tilde{E}_p \text{ is ordinary} \\ \iff\ & \tilde{E}_p[p] \neq 0 \\ \iff\ & |\tilde{E}_p(\mathbb{F}_{p^n})| \text{ is divisible by } p \text{ for some } n \\ \iff\ & p|(1 - \alpha_p^n)(1 - \beta_p^n) \text{ for some } n. \end{aligned}$$

Let $\mathrm{ord}_p : \bar{\mathbb{Q}}_p^* \to \mathbb{Q}$ be normalized so that $\mathrm{ord}_p(p) = 1$. From $(Y - \alpha_p)(Y - \beta_p) = Y^2 - a_pY + p$, we deduce that

$$\begin{aligned} p|a_p \implies & \mathrm{ord}_p(\alpha_p) = \mathrm{ord}_p(\beta_p) = \frac{1}{2}, \\ p \nmid a_p (i.e., \alpha_p \in \mathbb{Z}_p^*) \implies & \mathrm{ord}_p(\alpha_p) = 0, \mathrm{ord}_p(\beta_p) = 1 \text{ or the reverse.} \end{aligned}$$

And $\tilde{E}_p$ is ordinary if and only if $p \nmid a_p$. Note that since α_p is p-adic unit, $1 - \alpha_p^n$ is divisible by p and hence $p \mid |\tilde{E}_p(\mathbb{F}_{p^n})|$. If $\tilde{E}_p$ is ordinary, then consider $V_p(E)$ as a $\mathbb{Q}_p$-representation space for $G_{\mathbb{Q}_p}$. Then V_p is reducible. We have a homomorphism, which is $G_{\mathbb{Q}_p}$-equivariant,

$$\begin{aligned} E[p^\infty] &\longrightarrow \tilde{E}_p[p^\infty] \text{ surjective,} \\ T_p[E] &\longrightarrow T_p(\tilde{E}_p) \text{ finite cokernel,} \\ V_p[E] &\longrightarrow V_p(\tilde{E}_p) \text{ surjective.} \end{aligned}$$

Let $W_p(E) = \ker(V_p(E) \to V_p(\tilde{E}_p))$. Note that $\dim_{\mathbb{Q}_p} W_p(E) = 1$ and W_p is $G_{\mathbb{Q}_p}$-equivariant. The action of $G_{\mathbb{Q}_p}$ is given by

$$\begin{array}{ccc} \rho : G_{\mathbb{Q}_p} & \longrightarrow & \mathrm{Aut}_{\mathbb{Q}_p}(V_p(E)) \\ & \searrow^{\chi} & \downarrow \det \\ & & \mathbb{Q}_p^* \end{array}$$

where χ is a cyclotomic character. $\chi : G_{\mathbb{Q}_p} \twoheadrightarrow \mathbb{Z}_p^*$ gives the action on μ_{p^∞}. $I_{\mathbb{Q}_p}$ acts on $V_p(E)/W_p(E)$ by χ^0 because $V_p/W_p \cong \tilde{E}_p[p^\infty]$. $I_{\mathbb{Q}_p}$ acts on $W_p(E)$ by χ. We have a filtration of $V_p(E)$ given by $F^0V_p = V_p, F^1V_p = W_p, F^2V_p = 0$.

Definition 5. *Suppose that V_p is a $\mathbb{Q}_p$-representation space for $G_{\mathbb{Q}_p}$. Assume* $\dim_{\mathbb{Q}_p} V_p$ *is finite. V_p is ordinary if there exists $G_{\mathbb{Q}_p}$-invariant $\mathbb{Q}_p$-subspaces F^iV_p with the following properties*

(1) $F^{i+1}V_p \subset F^iV_p$ *for* $i \in \mathbb{Z}$,
(2) $I_{\mathbb{Q}_p}$ *acts on* $F^iV_p/F^{i+1}V_p$ *by* χ^i,
(3) $F^iV_p = 0$ *for some* i, $F^jV_p = V_p$ *for some* $j \in \mathbb{Z}$.

If $V_p = V_p(E)$ and $\tilde{E}_p$ is ordinary, then we can take $F^jV_p = V_p$ for $j \leq 0$, $F^1V_p = W_p(E)$, $F^jV_p = 0$ for $j \geq 2$. Remark that above discussion on ordinary representation can be generalized to general algebraic variety over $\mathbb{Q}_p$. Consider $\Delta = \Delta(z) = \sum_{n=1}^{\infty} \tau(n)q^n = q\prod_{m=1}^{\infty}(1-q^m)^{24}$, $q = e^{2\pi iz}$. Then Δ is a modular form of weight 12 for $\mathrm{SL}_2(\mathbb{Z})$. In fact, it is a cusp form and $\tau(1) = 1$. For every prime p, there is a 2-dimensional $\mathbb{Q}_p$-representation space, which we call $V_p(\Delta)$ for $G_{\mathbb{Q}}$ with the following properties: Let $\rho_{\Delta,p} : G_{\mathbb{Q}} \to \mathrm{Aut}_{\mathbb{Q}_p}(V_p(\Delta))$ be the corresponding homomorphism. Note that

(1) $\rho_{\Delta,p}$ is continuous,
(2) $\rho_{\Delta,p}|_{G_{\mathbb{Q}_l}}$ is unramified for all $p \neq l$,
(3) If $l \neq p$, then Frob_l, the element of $G(\mathbb{Q}_l^{\mathrm{ur}}/\mathbb{Q}_l)$ satisfies

$$\mathrm{Tr}(\rho_{\Delta,p}(\mathrm{Frob}_l)) = \tau(l)$$

and

$$\det(\rho_{\Delta,p}(\mathrm{Frob}_l)) = l^{11}.$$

The existence was conjectured by Serre in [3]. Proof of existence can be found in [4]. Ramanujan conjecture $|\tau(p)| \leq 2p^{\frac{11}{2}}$ implies that $L(\Delta, s) := \sum_{n=1}^{\infty} \frac{\tau(n)}{n^s}$ converges for $\Re(s) > \frac{11}{2}$. This is a criterion for $V_p(\Delta)$ to be ordinary as a representation space for $G_{\mathbb{Q}_p}$:

$$V_p(E) \text{ is ordinary if and only if } p \nmid \tau(p).$$

And $\{p | p \text{ divides } \tau(p)\} = \{2, 3, 5, 7, 7758337633, \cdots\}$. Next time we will describe $V_p(\Delta)$ and filtrations and Selmer group.

5. Fifth Lecture

Let

$$\Delta = \Delta(z) = q\prod_{m=1}^{\infty}(1-q^m)^{24} = \sum_{m=1}^{\infty}\tau(m)q^m,\ q = e^{2\pi iz}.$$

Then Δ is a cusp form of level 1 and weight 12. Define $L(\Delta, s) = \sum_{n=1}^{\infty} \frac{\tau(n)}{n^s}$. It converges for $\Re(s) > \frac{13}{2}$ because $|\tau(n)| < d(n)n^{\frac{11}{2}}$ where d is the number of divisors. Remarkable properties of $L(\Delta, s)$ discovered by Ramanujan is that

$$L(\Delta, s) = \prod_p (1 - \tau(p)p^{-s} + p^{11}p^{-2s}) \text{ for } \Re(s) > \frac{13}{2}.$$

Consider $1 - \tau(p)X + p^{11}X^2 = (1 - \alpha_p X)(1 - \beta_p X)$ where $\alpha_p + \beta_p = \tau(p), \alpha_p\beta_p = p^{11}$. And $|\alpha_p| = |\beta_p| = p^{11/2}$ by Deligne. Therefore $|\tau(p)| < 2p^{11/2}$. And $L(\Delta, s)$ is entire and has a functional equation

$$\pi^{-(12-s)}\Gamma(12 - s)L(\Delta, 12 - s) = \pi^{-s}\Gamma(s)L(\Delta, s).$$

Riemann Hypothesis is that all nontrivial zeros lie on $\Re(s) = 6$. Trivial zeros are $s = 0, -1, -2, \cdots$. It is forced by the functional equation and they are all simple zeros. Critical values in the sense of Deligne is the following:

$$\begin{aligned} & \{L(\Delta, m)|\ m :\ \text{integer},\ \Gamma(12 - s) \text{ and } \Gamma(s) \text{ don't have a pole at } s = m\} \\ = \ & \{L(\Delta, m)|\ m = 1, 2, \cdots, 11\}. \end{aligned}$$

More generally, consider $L(\Delta \otimes \varphi, s)$ where φ is a quadratic character. It is possible that $L(\Delta \otimes \varphi, 6) = 0$. We will generalize the conjecture that

$$\mathrm{ord}_{s=1}L(E/\mathbb{Q}, s) = \mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}(E/\mathbb{Q})_p).$$

Conjecture involves a Selmer group defined in terms of $V_p(\Delta)$. The analogue of $E[p^\infty]$ is $V_p(\Delta)/T_p(\Delta)$ where $T_p(\Delta)$ is a $G_\mathbb{Q}$-invariant $\mathbb{Z}_p$-lattice in $V_p(\Delta)$. Thus, $T_p(\Delta) \cong \mathbb{Z}_p^2$. Define $D_p = V_p(\Delta)/T_p(\Delta) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^2$. $G_\mathbb{Q}$ acts on D_p. We want to define $\mathrm{Sel}(D_p/\mathbb{Q})$ in the following way:

$$\mathrm{Sel}(D_p/\mathbb{Q}) = \ker(\mathrm{H}^1(\mathbb{Q}, D_p) \to \prod_l \mathrm{H}^1(\mathbb{Q}_l, D_p)/K_l(D_p))$$

where $K_l(D_p) = 0$ if $l \neq p$. For $l = p$, we will assume that $p \nmid \tau(p)$. Then $V_p(\Delta)$ is ordinary. More precisely $V_p(\Delta)$ contains a 1-dimensional subspace $W_p(\Delta)$ which is $G_{\mathbb{Q}_p}$-invariant and $I_{\mathbb{Q}_p}$ acts on $V_p(\Delta)/W_p(\Delta)$ by χ^0 and on $W_p(\Delta)$ by χ^{11}.

Remark that the determinant of $\det(\rho_{\Delta,p}(\mathrm{Frob}_l)) = l^{11}$. We have a filtration $F^jV_p(\Delta) = V_p(\Delta)$ for $j \leq 0$, $F^1V_p(\Delta) = \cdots = F^{11}V_p(\Delta) = W_p(\Delta)$, $0 = F^{12}V_p(\Delta) = F^{13}V_p(\Delta) = \cdots$. Similarly, $V_p(\Delta) \otimes \varphi$ is ordinary where φ is a quadratic character which is unramified at p. And we have a similar result for $V_p(\Delta) \otimes \chi^t$ where χ is a p-power cyclotomic character and $t \in \mathbb{Z}$. Although χ is highly ramified, it is also ordinary with a different filtration.

Let $L(\Delta, s)$ be a L-function associated to $V_p(\Delta)$ and let $L(\Delta, \varphi, s)$ be a L-function associated to $V_p(\Delta) \otimes \varphi$ which is defined by

$$L(\Delta, \varphi, s) = \sum_{n=1}^{\infty} \frac{\tau(n)\varphi(n)}{n^s}.$$

Frob_l has eigenvalues α_l and β_l in $V_p(\Delta)$ and $\varphi(l)\alpha_l$ and $\varphi(l)\beta_l$ in $V_p(\Delta) \otimes \varphi$. The trace is $\tau(l)\varphi(l)$. Then

$$\begin{aligned} & L(\Delta, s - t) \\ = \ & \prod_l (1 - \tau(l)l^{-s+t} + l^{11}l^{-2(s-t)})^{-1} \\ = \ & \prod_l (1 - \tau(l)l^{-s}l^t + l^{11}l^{-2s}l^{2t})^{-1} \end{aligned}$$

is the L-function associated to $V_p(\Delta)\otimes\chi^t$. The eigenvalues of Frob_l are $\alpha_l l^t, \beta_l l^t$. And let

$$K_p(D_p) := \ker(\mathrm{H}^1(\mathbb{Q}_p, D_p) \to \mathrm{H}^1(\mathbb{Q}_p, (D_p)_{I_{\mathbb{Q}_p}}))_{\mathrm{div}}.$$

Note that $V_p(\Delta)/W_p(\Delta)$ is unramified for $G_{\mathbb{Q}_p}$. Let F^+D_p be the image of $F^1V_p(\Delta) = W_p(\Delta)$ in $D_p = V_p/T_p$. Then

$$K_p(D_p) = \ker(\mathrm{H}^1(\mathbb{Q}_p, D_p) \to \mathrm{H}^1(\mathbb{Q}_p, D_p/F^+D_p))_{\mathrm{div}}.$$

It is conjectured that

$$\mathrm{ord}_{s=1}(L(\Delta, s)) = \mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}(D_p/\mathbb{Q})).$$

That means $\mathrm{Sel}(D_p/\mathbb{Q})$ is finite. It is proved by Kato. Consider $L(\Delta, s-t)$ which corresponds to $V_p(\Delta)\otimes\chi^t$. It is conjectured that

$$\mathrm{ord}_{s=1}(L(\Delta, s-t)) = \mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}(D_p\otimes\chi^t/\mathbb{Q})).$$

We should have the filtration $F^+D_p\otimes\chi^t = F^{1-t}(D_p\otimes\chi^t)$. And we have

$$\begin{aligned} & 1 \le 1-t \le 11 \\ \iff\ & -10 \le t \le 0 \\ \iff\ & F^+(V_p\otimes\chi^t) = (F^{1-t}V_p)\otimes\chi^t \\ \iff\ & F^+(V_p\otimes\chi^t) = W_p\otimes\chi^t. \end{aligned}$$

6. Sixth Lecture

Let $\Delta = \sum_{n=1}^{\infty}\tau(n)q^n \in S_{12}(1)$. And consider $V_p(\Delta)$ and $\rho_{\Delta,p} : G_{\mathbb{Q}} \to \mathrm{Aut}_{\mathbb{Q}_p}(V_p(\Delta))$. We define

$$L(\Delta, s) = \sum_{n=1}^{\infty}\frac{\tau(n)}{n^s} = L(V_p(\Delta), s).$$

The Euler factor $(1-\tau(l)l^{-s}+11^{11}l^{2s})^{-1}$ can be recovered from $V_p(\Delta)$ for all primes l. Let φ be a quadratic character. Assume that the conductor is prime to p. Then

$$L_p(V_p(\Delta)\otimes\varphi, s) = \sum_{n=1}^{\infty}\frac{\tau(n)\varphi(n)}{n^s}.$$

Critical values in the sense of Deligne occur for $s = 1, 2, \cdots, 11$. And $\mathrm{ord}_{s=n}(L(V_p(\Delta)\otimes\varphi, s)) = 1$ if $m \in \{0, -1, -2, \cdots\}$. $V_p(\Delta)$ is an ordinary $G_{\mathbb{Q}_p}$-representation space if and only if $p \nmid \tau(p)$.

We will consider analogy with the elliptic curve case. Let E be an elliptic curve over $\mathbb{Q}$ and let N_E be a conductor of E. Then

$$L(E/\mathbb{Q}, s) = \sum_{n=1}^{\infty}\frac{a_n}{n^s} = L(V_p(E), s).$$

Here $V_p(E)$ recovers all Euler factor. And $\sum_{n=1}^{\infty}a_nq^n \in S_2(N_E)$. This is a deep result but it is known.

Assume $p \nmid N_E$. Then $V_p(E)$ is ordinary if and only if $p \nmid a_p$. Then the question is: can one prove

$$p \nmid \tau(p) \Longleftrightarrow V_p \text{ is ordinary}$$

by interpreting $(1-\alpha_p^m)(1-\beta_p^m)$ for $m \geq 1$ where $1-\tau(p)X+p^{11}X^2 = (1-\alpha_p X)(1-\beta_p X)$? We don't know yet.

Assume $p \nmid \tau(p)$. Then $\rho_{\Delta,p}|_{G_{\mathbb{Q}_p}}$ is ordinary. There is an 1-dimensional $G_{\mathbb{Q}_p}$-invariant subspace which I call $W_p(\Delta)$ such that $I_{\mathbb{Q}_p}$ acts on $V_p(\Delta)/W_p(\Delta)$ by χ^0 and on $W_p(\Delta)$ by χ^{11}. Let $t \in \mathbb{Z}$. Then $V_p(\Delta)\otimes\varphi\chi^t \supset W_p(\Delta)\otimes\varphi\chi^t$. And $I_{\mathbb{Q}_p}$ acts on $V_p(\Delta)\otimes\varphi\chi^t/W_p(\Delta)\otimes\varphi\chi^t$ by χ^t. Also $I_{\mathbb{Q}_p}$ acts on $W_p(\Delta)\otimes\varphi\chi^t$ by χ^{11+t}. Note that $F^+(V_p(\Delta)\otimes\varphi\chi^t)$ is the first positive term in filtration and it is given by

$$F^+(V_p(\Delta)\otimes\varphi\chi^t) = \begin{cases} W_p(\Delta)\otimes\varphi\chi^t & \text{if } t \in \{0,-1\cdots,-10\}, \\ V_p(\Delta)\otimes\varphi\chi^t & \text{if } t > 0, \\ 0 & \text{if } t \leq -11. \end{cases}$$

Let $D_p\otimes\varphi\chi^t = V_p(\Delta)\otimes\varphi\chi^t/T_p(\Delta)\otimes\varphi\chi^t \cong (\mathbb{Q}_p/\mathbb{Z}_p)^2$. And let $F^+(D_p\otimes\varphi\chi^t)$ be the image of $F^+(V_p(\Delta)\otimes\varphi\chi^t)$. Then

$$\operatorname{corank}(F^+(D_p\otimes\varphi\chi^t)) = \begin{cases} 1 & 0 \geq t \geq -10, \\ 2 & t \geq 1, \\ 0 & t \leq -11 \end{cases}$$

and

$$\operatorname{corank}(D_p\otimes\varphi\chi^t/F^+(D_p\otimes\varphi\chi^t)) = \begin{cases} 2 & 0 \geq t \geq -10, \\ 0 & t \geq 1, \\ 1 & t \leq -11. \end{cases}$$

Note that

$$K_p(D_p\otimes\varphi\chi^t) = \ker(\mathrm{H}^1(\mathbb{Q}_p, D_p\otimes\varphi\chi^t) \to \mathrm{H}^1(\mathbb{Q}_p, D_p\otimes\varphi\chi^t/F^+(D_p\otimes\varphi\chi^t))_{\mathrm{div}}.$$

Here $\operatorname{corank}_{\mathbb{Z}_p}(\mathrm{H}^1(\mathbb{Q}_p, D_p\otimes\varphi\chi^t)) = 2$ and $\operatorname{corank}_{\mathbb{Z}_p}(\mathrm{H}^1(\mathbb{Q}_p, D_p\otimes\varphi\chi^t/F^+(D_p\otimes\varphi\chi^t)) = \operatorname{corank}_{\mathbb{Z}_p}(\frac{D_p\otimes\varphi\chi^t}{F^+(D_p\otimes\varphi\chi^t)})$. And we have

$$\operatorname{corank} K_p(D_p\otimes\varphi\chi^t) = \begin{cases} 1 & 0 \geq t \geq -10, \\ 2 & t \geq 1, \\ 0 & t \leq -11 \end{cases}$$

and

$$\operatorname{corank}_{\mathbb{Z}_p} \frac{\mathrm{H}^1(\mathbb{Q}_p, D_p\otimes\varphi\chi^t)}{K_p(D_p\otimes\varphi\chi^t)} = \begin{cases} 1 & 0 \geq t \geq -10, \\ 0 & t \geq 1, \\ 2 & t \leq -11. \end{cases}$$

Note that

$$\begin{aligned}\mathrm{Sel}_{D_p\otimes\varphi\chi^t}(\mathbb{Q}) &= \ker(\mathrm{H}^1(\mathbb{Q}, D_p\otimes\varphi\chi^t) \to \frac{\mathrm{H}^1(\mathbb{Q}_p, D_p\otimes\varphi\chi^t)}{K_p(D_p\otimes\varphi\chi^t)} \times \prod_{l\neq p} \mathrm{H}^1(\mathbb{Q}_l, D_p\otimes\varphi\chi^t))\\ &= \ker(\mathrm{H}^1(\mathbb{Q}_{\Sigma_\varphi}/\mathbb{Q}, D_p\otimes\varphi\chi^t) \to \mathrm{H}^1(\mathbb{Q}_p, D_p\otimes\varphi\chi^t)/K_p(D_p\otimes\varphi\chi^t) \times \prod_{\substack{l\in\Sigma_\varphi\\ l\neq p}} \mathrm{H}^1(\mathbb{Q}_l, D_p\otimes\varphi\chi^t))\end{aligned}$$

where $\Sigma_\varphi = \{\infty,$ primes divides conductor of $\varphi\}$ and $\mathbb{Q}_{\Sigma_\varphi}$ is the maximal extension of $\mathbb{Q}$ which is unramified outside Σ_φ.

Remark that

(1) $\mathrm{corank}_{\mathbb{Z}_p}(\mathrm{H}^1(\mathbb{Q}_{\Sigma_\varphi}/\mathbb{Q}, D_p\otimes\varphi\chi^t)) \geq 1$,
(2) $\mathrm{corank}_{\mathbb{Z}_p}$ depends on t for $\mathrm{H}^1(\mathbb{Q}_p, D_p\otimes\varphi\chi^t)/K_p(D_p\otimes\varphi\chi^t)$. For $l\in\Sigma_\varphi$, $\mathrm{H}^1(\mathbb{Q}_l, D_p\otimes\varphi\chi^t)$ is finite.

$\mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}(D_p\otimes\varphi\chi^t/\mathbb{Q}))$ can be 0 if $0\geq t\geq -10$ or $t\leq -11$ and is ≥ 1 if $t\geq 1$.

And note that

$$L(V_p(\Delta)\otimes\varphi\chi^t, s) = L(V_p(\Delta)\otimes\varphi, s-t)$$

has order of vanishing at $s=1$ as $\begin{cases}0 & \text{if } t\neq -5, 0\geq t\geq -10,\\ 1 & \text{if } t\geq 1,\\ 0 & \text{if } t\leq -11.\end{cases}$

Remark that for $t=-5$ $\det(\rho_{\Delta,p}\otimes\chi^{-5}) = \chi^{11}(\varphi\chi^{-5})^2 = \chi$ where φ is a quadratic character. This means that $V_p(\Delta)\otimes\varphi\chi^{-s} \bigwedge V_p(\Delta)\varphi\chi^{-5} \cong \mathbb{Q}_p(1)$. This is an analogue of Weil pairing.

By Poitou-Tate duality

$$\begin{aligned}&\mathrm{Hom}(V_p(\Delta)\otimes\varphi\chi^t, \mathbb{Q}_p(1))\\ =\ &\mathrm{Hom}(V_p(\Delta), \mathbb{Q}_p\otimes\varphi\chi^{1-t})\\ =\ &\mathrm{Hom}(V_p(\Delta), \mathbb{Q}_p\otimes\chi^{11})\otimes\varphi\chi^{-10-t}\\ =\ &V_p(\Delta)\otimes\varphi\chi^{-10-t}.\end{aligned}$$

This give two sides of functional equation between $L(V_p(\Delta)\otimes\varphi, 1-t)$ and $L(V_p(\Delta)\otimes\varphi, 11+t)$.

References

[1] R.Greenberg: *Iwasawa Theory for p-adic Representations;* Advanced Studies in Pure Mathematics 17 (1989), 97-137.

[2] R.Greenberg: *Introduction to Iwasawa Theory for Elliptic Curves;* IAS/Park City Mathematics Series 9 (2001), 407-464.

[3] J.P.Serre: *An interpretation of some congruences concerning Ramanujan's tau-function;* in Serre's Collected Works in French or on the internet in English.

[4] B.Conrad: *Modular Forms and the Ramanujan Conjecture;* a new book which should be available soon.

[5] S.Bloch, K.Kato: *Tamagawa Numbers of Motives;* in the Grothendieck Festschrift, vol. 1, Progress in Mathematics 89, Birkhauser, 1990.