

Big picture



Special case



§ Zeta- and L-functions

(1) Riemann $\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} = \prod_p \frac{1}{1-p^{-s}} = \prod_p \frac{1}{F_p(p^{-s})}$; $F_p(T) = 1-T$
degree $d=1$

Dedekind ζ_K , K num. field

$\zeta_K(s) = \sum_{0 \neq \mathfrak{a} \subseteq \mathcal{O}_K} \frac{1}{N\mathfrak{a}^s} = \prod_p \frac{1}{1-Np^{-s}} = \prod_p \frac{1}{F_p(p^{-s})}$; $F_p(T) = \prod_{\mathfrak{p}|p} (1-T^{f_{\mathfrak{p}}})$
degree $[K:\mathbb{Q}]$

(2) $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$ character

$L(\chi, s) = \sum_{n \geq 1} \frac{\chi(n)}{n^s}$; $F_p(T) = 1-\chi(p)T$ degree 1

(3) E/\mathbb{Q} ell. curve

$L(E, s) = \sum_{n \geq 1} \frac{a_n}{n^s} = \prod_p \frac{1}{F_p(p^{-s})}$; $F_p(T) = \begin{cases} 1-a_pT+pT^2 & \text{if } E \text{ has good red. at } p \\ 1-T & \text{split mult.} \\ 1+T & \text{non-split mult.} \\ 1 & \text{additive} \end{cases}$

(4) $f \in S_k(\Gamma_0(N))$ cusp form

$f = \sum_{n \geq 1} a_n q^n$ \rightsquigarrow $L(f, s) = \sum \frac{a_n}{n^s}$

degree 2

Standard conjectures each $L(s)$

- has meromorphic continuation to \mathbb{C}
- \exists conductor N , weight k , Hodge numbers $\lambda_1, \dots, \lambda_d \in \mathbb{Z}$ such that

$\hat{L}(s) = \left(\frac{N}{\pi^d}\right)^{s/2} \Gamma\left(\frac{s+\lambda_1}{2}\right) \dots \Gamma\left(\frac{s+\lambda_d}{2}\right) L(s)$

satisfies functional equation

$\hat{L}(k-s) = w \cdot \hat{L}(s)$

	N	k	λ_i	w
Riemann	1	1	0	1
Dedekind	$ \mathcal{O}_K $	1	$f_{\mathfrak{p}}^2$ 0's $f_{\mathfrak{p}}$'s	1
χ	N	1	0 X even 1 X odd	$\frac{1}{2}$
E/\mathbb{Q}	N	2	0, 1	w

- zeroes of $L(s)$ are on $\text{Re } s = \frac{1}{2}$ (RH)
- special value conjectures at $s \in \mathbb{Z}$
(BSD, Stark, Deligne-Beilinson, Bloch-Kato, ...)

Goal

num. fields \rightarrow
characters \rightarrow
ell. curves \rightarrow
cusp forms \rightarrow

Galois representations
 $\rho: G_{\mathbb{Q}} \rightarrow GL_d(\mathbb{C})$

$$L(\rho, s) = \prod_p \frac{1}{F_p(p^{-s})}$$

$$F_p(T) = \det(1 - T \text{Frob}_p^{-1} | \rho^{\mathbb{Z}_p})$$

$$N = N_p = \prod_p N_p$$

$$W = W_p = \prod_p W_p$$

Notation: $G_K = \text{Gal}(\bar{K}/K)$.

§ Galois representations

(1) $[K:\mathbb{Q}] = d$

$\Sigma = \{ \text{embeddings } K \hookrightarrow \mathbb{C} \} \subset G_{\mathbb{Q}}$
 $|\Sigma| = d$

$\mathbb{C}[\Sigma] \subset G_{\mathbb{Q}} \rightsquigarrow \rho_K: G_{\mathbb{Q}} \rightarrow GL_d(\mathbb{C})$ Gal. rep.

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

$\rho_{\chi}: G_{\mathbb{Q}} \rightarrow \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^{\times} \xrightarrow{\chi} \mathbb{C}^{\times}$ Gal. rep.

Note $K = \mathbb{Q}(\zeta_n)$
 $\rho_{\chi} \in \text{reg. rep. of } \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$
 $\rho_K = \bigoplus_{\chi} \rho_{\chi}$

Generally $\rho_K = \bigoplus$ Artin representations

(3) E/\mathbb{Q} ell. curve

$y^2 = x^3 + Ax + B$ $A, B \in \mathbb{Q}$

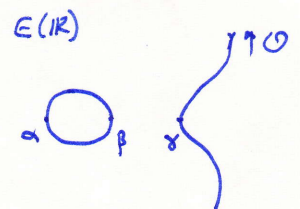
$E[n] := \{ P \in E(\bar{\mathbb{Q}}) \mid nP = \mathcal{O} \}$ n torsion
 $\cong (\mathbb{Z}/n\mathbb{Z})^2 \subset G_{\mathbb{Q}}$

Ex $E[2] = \{ \mathcal{O}, (x, 0), (-x, 0), (x, 0) \} \subset G_{\mathbb{Q}}$

For m, n coprime

$E(mn) \cong E(m) \times E(n)$

enough to look at $n = \ell^k$



$E(\mathbb{C}) \cong \mathbb{C}/\Lambda \cong (\mathbb{R}/\mathbb{Z})^2$
as Lie gp.

$$\rightarrow E[\ell^k] \xrightarrow{(\ell)} E[\ell^{k-1}] \xrightarrow{(\ell)} \dots \xrightarrow{(\ell)} E[\ell]$$

Def Tate module $T_\ell E = \varprojlim_k E[\ell^k] \cong (\mathbb{Z}_\ell)^2 \supset G_\mathbb{Q}$

$$\forall \ell \in E = T_\ell E \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \cong (\mathbb{Q}_\ell)^2 \supset G_\mathbb{Q}$$

Linear action of $G_\mathbb{Q}$ on torsion pts \Rightarrow

$$\bar{\rho}_n : G_\mathbb{Q} \rightarrow \text{GL}_2(\mathbb{Z}/n\mathbb{Z})$$

$$G_\mathbb{Q} \rightarrow \text{GL}_2(\mathbb{Z}_\ell)$$

$$\rho_\ell : G_\mathbb{Q} \rightarrow \text{GL}_2(\mathbb{Q}_\ell) \hookrightarrow \text{GL}_2(\mathbb{C}) \quad \text{Gal. rep. (for every } \ell)$$

Weil pairing $\cong (\mathbb{Z}/\ell^n) \times E[n] \rightarrow \mu_{\ell^n}$

$$\det \rho_\ell = \chi_\ell \quad \text{cyclotomic character} \quad G_\mathbb{Q} \rightarrow \varprojlim_n \text{Aut } \mu_{\ell^n} = \varprojlim_n (\mathbb{Z}/\ell^n \mathbb{Z})^\times = \mathbb{Z}_\ell^\times$$

In general

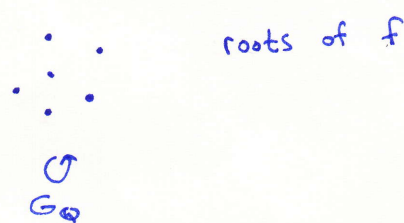
X/\mathbb{Q} non-sing. projective variety $\rightarrow H^i = H_{\text{ét}}^i(X, \mathbb{Q}_\ell)$ étale coh. groups
 \mathbb{Q}_ℓ -vector spaces

• $H^i \otimes_{\mathbb{Q}_\ell} \mathbb{C} = H_{\text{top}}^i(X(\mathbb{C}))$ [$\Rightarrow 0$ for $i > 2 \dim X$]

• $H^i \supset G_\mathbb{Q}$

Ex K/\mathbb{Q} number field, $K = \mathbb{Q}(x)/f(x)$

$X = \text{Spec } K$



$\xrightarrow{1:1}$ embeddings $K \hookrightarrow \mathbb{C}$
 Σ

$$H^0 = \mathbb{Q}_\ell[\Sigma]$$

$$H^i = 0 \quad (i > 0)$$



$$E(\mathbb{C}) = \mathbb{C}/\Lambda$$

Ex E/\mathbb{Q} ell. curve

$$H^0 = \mathbb{Q}_\ell$$

$$H^1 = T_\ell E^*$$

$$H^2 = \chi_\ell$$

1-dim

2-dim

1-dim

$$[E[\ell^n] = \ell^n\text{-coverings } E \rightarrow E \\ T_\ell E = \Pi_{\text{ét}}^1(E)_\ell = H_1^{\text{ét}}(E, \mathbb{Z}_\ell) = (H^1)^*]$$

Ex C/\mathbb{Q} curve

$$\begin{aligned} H^0 &= \mathbb{Q}_\ell & 1\text{-dim} \\ H^1 &= H^1(\text{Jac } C) = T_\ell(\text{Jac } C)^* & 2g\text{-dim.} \\ H^2 &= X_\ell & 1\text{-dim} \end{aligned}$$

Ex A/\mathbb{Q} abelian variety

$$H^i = \bigwedge^i H^1 \quad ; \quad H^1 = (T_\ell A)^*$$

(4) Ex f cusp form of weight k level N

$$\left. \begin{aligned} \underline{k=2} & \text{ Eichler-Shimura} \\ p_f & \subseteq H^1(X_0(N)) \\ \underline{k>2} & \text{ Deligne} \\ \underline{k=1} & \text{ Deligne-Serre} \end{aligned} \right\} p_f \text{ Gal. rep.}$$

Summary: Algebraic varieties $X/\mathbb{Q} \rightsquigarrow$ large source of Galois representations: $H_{\text{ét}}^i(X, \mathbb{Q}_\ell)$ & their direct summands ("motives")
(Dirichlet character, Artin reps, p_f)

§ Local invariants of Galois representations

Galois rep $\rho \rightsquigarrow$ L-function $L(\rho, s)$

local factors $\prod_p \text{F}_p(T)$
conductor $N = \prod_p p^{n_p}$
root number $w = \prod_p w_p$

Fix a prime p ,

$$\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p \quad \Rightarrow \quad G_{\mathbb{Q}_p} \xrightarrow{\text{Res}} G_{\mathbb{Q}}$$

decomposition subgroup

Study $\rho|_{G_{\mathbb{Q}_p}}$. $(\Rightarrow \text{F}_p(T), n_p, w_p)$

Structure of $G_{\mathbb{Q}_p}$:

$$G_{\mathbb{Q}_p} \begin{cases} \overline{\mathbb{Q}}_p \\ | \\ I = I_{\mathbb{Q}_p} \text{ inertia subgroup} \\ \mathbb{Q}_p^{\text{nr}} = \bigcup_{p \nmid n} \mathbb{Q}_p(\sqrt[n]{p}) \\ | \\ G_{\mathbb{F}_p} \\ | \\ \mathbb{Q}_p \end{cases}$$

$$1 \longrightarrow I \longrightarrow G_{\mathbb{Q}_p} \xrightarrow{\sigma \mapsto \bar{\sigma}} G_{\mathbb{F}_p} \longrightarrow 1$$

$\langle x \mapsto x^p \rangle \cong \hat{\mathbb{Z}}$

Def $I = \{ \sigma \in G_{\mathbb{Q}_p} \mid \bar{\sigma} = 1 \} \triangleleft G_{\mathbb{Q}_p}$

$\text{Frob}_p =$ any elt of $G_{\mathbb{Q}_p}$ reducing to $x \mapsto x^p$

A $G_{\mathbb{Q}_p}$ module M is unramified if I acts trivially on M

$(\Rightarrow G_{\mathbb{F}_p}$ -module)

Main example: torsion points on elliptic curves

Ex $K = \mathbb{Q}_5$

$E_1: y^2 = x^3 - 1$

$E_2: y^2 = (x-1)(x^2-5)$

$E_3: y^2 = x^3 - 5^2$

$\tilde{E}_1/\mathbb{F}_5: y^2 = x^3 - 1$

$\tilde{E}_2/\mathbb{F}_5: y^2 = x^3 - x^2$

$\tilde{E}_3/\mathbb{F}_5: y^2 = x^3$



elliptic curve (good reduction)

multiplicative reduction
 $[y^2 + x^2 = x^3$ tangent lines at $(0,0)$
 $y = \sqrt{-1}x, y = -\sqrt{-1}x$ defined $(\mathbb{F}_5$
 \Rightarrow split multiplicative red.)

additive reduction
 [becomes good or multiplicative after a finite extension]

Recall $E[2] = \{0, (\alpha, 0), (\beta, 0), (\gamma, 0)\}$

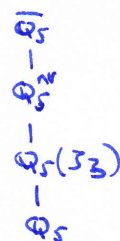
$E_1[2] = \{0, (1, 0), (\sqrt{3}, 0), (\sqrt{3}^2, 0)\}$

$E_2[2], E_3[2]$ ramified

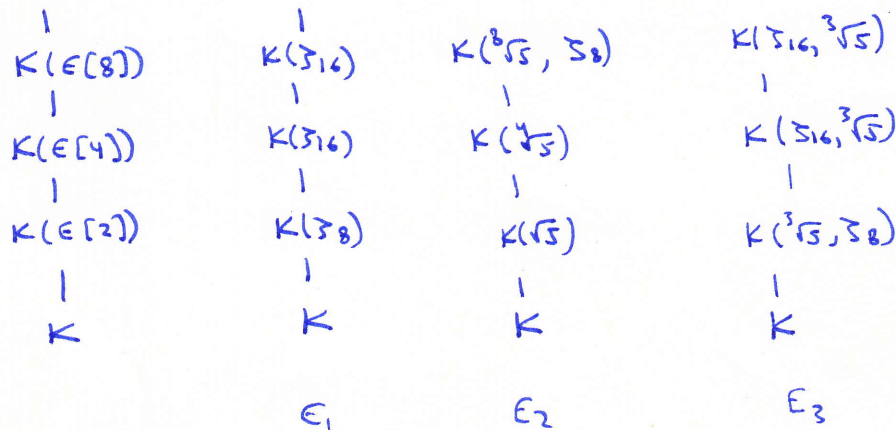
α, β, γ roots of cubic

unramified

involve $\sqrt{5}, \sqrt[3]{5}$



Computation \Rightarrow for these 3 curves



NB
 $\mathbb{Q}_5(\sqrt{3}) = \mathbb{Q}_5(\sqrt{8}) =$
 $\mathbb{Q}_5(\sqrt[24]{5}) = \mathbb{Q}_5(\sqrt{-3})$
 unique quad. unramified ext. of \mathbb{Q}_5

Residue degree: Weil pairing $\Rightarrow \mathbb{M}_{2^n} \subseteq K(E[2^n])$

\Rightarrow residue degree $\rightarrow \infty$

Ramification: Guess?

E_1 all unramified

E_2 regularly growing ramification

E_3 finite ramification

[Yes! \Leftrightarrow good reduction

\Leftrightarrow (pot.) mult. red.

\Leftrightarrow additive pot. good. red.

§ Good reduction

Thm (Néron-Ogg-Shafarevich) E/\mathbb{Q}_p elliptic, $L \neq p$.

E has good reduction $\Leftrightarrow E[\ell^n]$ unramified $\forall n \geq 1$
 $(\Leftrightarrow T_\ell E, V_\ell E$ unramified)

[similarly /K, K/\mathbb{Q}_p finite]

In this case

$\rho_\ell(\mathbb{I}) = 1$

$\rho_\ell(\text{Frob}_p) = 2 \times 2$ matrix with char poly $T^2 - aT + p$, $d = p+1 = \#\tilde{E}(\mathbb{F}_p)$

Here

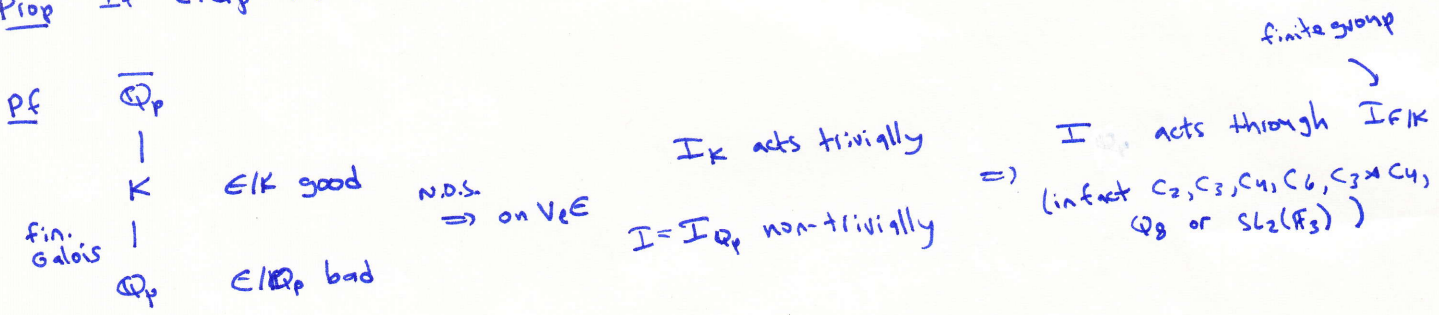
$(V_\ell E^*)^\mathbb{I} = V_\ell E^*$ (unramified), so $\boxed{F_\ell(T) = 1 - aT + pT^2}$

Ex $E_1/\mathbb{Q}_5 : y^2 = x^3 - 1$ good red.
 $\tilde{E}_1/\mathbb{F}_5 : y^2 = x^3 - 1$ has 6 pts $(0, (0, \pm 2), (1, 0), (3, \pm 2))$
 $T^2 - aT + p = T^2 + 5$, $\underline{F(T) = 1 + 5T^2}$

Here $\rho_\ell : G_{\mathbb{Q}_p} \longrightarrow GL_2(\mathbb{Q}_\ell) \hookrightarrow GL_2(\mathbb{C})$
 $\mathbb{I} \longrightarrow 1$
 $\text{Frob}_p \longrightarrow \begin{pmatrix} 0 & -5 \\ 1 & 0 \end{pmatrix}$ in some basis.

§ Additive pot. good reduction \rightsquigarrow Exc.

Prop If E/\mathbb{Q}_p has additive pot. good reduction, then $\boxed{F_\ell(T) = 1}$



$\dim V_\ell E^{\mathbb{I}} < 2 \Rightarrow 0$ or 1

If 1, then \mathbb{I} acts as $\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$
 $\det = \chi_\ell^{-1} = 1$ on $\mathbb{I}_K \rightarrow \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ \leftarrow infinite order! contradiction.

So $V^\mathbb{I} = \{0\}$, $F(T) = \det(\dots | (V_\ell E^*)^\mathbb{I}) = 1$ ■

§ Multiplicative reduction

For E/\mathbb{C}

$$E(\mathbb{C}) \cong \mathbb{C}/\mathbb{Z} + i\mathbb{Z} \xrightarrow[\cong]{\exp(2\pi i \cdot)} \mathbb{C}^*/q\mathbb{Z} \quad q = e^{2\pi i z} \quad \left[\cong \text{ given by transcendental fn's} \right]$$

as complex Lie groups.

Thm (Tate) If E/\mathbb{Q}_p has multiplicative reduction, then

- $\exists! q \in p\mathbb{Z}_p$ s.t.

$$E \cong E_q : y^2 + xy = x^3 + a_4(q)x + a_6(q)$$

← Tate curve [with Tate parameter q]

$$a_4(q) = -5 \sum_{n \geq 1} \frac{n^3 q^n}{1 - q^n}$$

$$a_6(q) = \frac{1}{12} \left[a_4 q + 7 \sum_{n \geq 1} \frac{n^5 q^n}{1 - q^n} \right]$$

$$\Delta(q) = q \prod_{n=1}^{\infty} (1 - q^n)^{24}$$

$$j(q) = \frac{1}{q} + 744 + 196884q + \dots$$

- $E(\overline{\mathbb{Q}_p}) \cong \overline{\mathbb{Q}_p}^*/q\mathbb{Z}$ as $G_{\mathbb{Q}_p}$ -modules $\left[\Rightarrow E(\mathbb{Q}_p) \cong \mathbb{Q}_p^*/q\mathbb{Z} \right]$

↳ given by power series $(x(q;u), y(q;u)) \leftarrow u$

Cor $E[\ell] \cong \langle M_{\ell}, q^{1/\ell} \rangle$
 $E[\ell^n] \cong \langle M_{\ell^n}, q^{1/\ell^n} \rangle$ as $G_{\mathbb{Q}_p}$ -modules

Ex $E_2/\mathbb{Q}_5 : y^2 = (x-1)(x^2-5)$
 $j = \frac{2^7}{5}, \Delta = 2^{10} \cdot 5 \Rightarrow q = 5 \times \text{unit.}$

$$\mathbb{Q}_p(E[2^n]) \cong \mathbb{Q}_p(\sqrt[n]{5}, M_{2^n})$$

Action of I on $\forall \ell \in E$

$$\begin{pmatrix} 1 & \psi \\ 0 & 1 \end{pmatrix}$$

$$\psi: I \rightarrow \mathbb{Z}_\ell$$

$$\sigma \mapsto \left(\frac{\sigma(p^{1/\ell^n})}{p^{1/\ell^n}} \right)_{n \geq 1} \in \varprojlim M_{\ell^n} \cong \mathbb{Z}_\ell \quad \text{tame character}$$

Action of Frob_p on $\forall \ell \in E$

$$\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$$

On $\forall \ell \in E^*$

invariants

$$I: \begin{pmatrix} 1 & 0 \\ \psi & 1 \end{pmatrix} \quad \text{Frob}_p: \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$$

$$F_p(T) = \det(1 - \text{Frob}_p^{-1} T | (\forall \ell \in E^*)^{\mathbb{Z}_p}) = \boxed{1 - T}$$

§ Non-split multiplicative reduction

Unramified quad twist of split mult. reduction: $I: \begin{pmatrix} 1 & 0 \\ \psi & 1 \end{pmatrix}$ $\text{Frob}_p: \begin{pmatrix} -1/p & 0 \\ 0 & -1 \end{pmatrix}$

$F_p(T) = 1 + T$

§ Additive reduction

Becomes good or multiplicative after a finite (ramified) extension.

Exc $\Rightarrow (V_e \in^*)^I = 0$ and so $F_p(T) = 1$

Summary E/\mathbb{Q}_p elliptic curve, $L \neq p$

$F_p(T) = \det(1 - \text{Frob}_p^{-1} T | (V_e \in^*)^I) = \begin{cases} 1 - q_p T + p T^2 & \in \text{good} \\ 1 - T & \in \text{split mult.} \\ 1 + T & \in \text{non-split mult.} \\ 1 & \in \text{additive} \end{cases}$ independent of l

Same defn for $H^i(X)$ for any nonsingular projective X (or any other)

Galois representation $\rho: G_{\mathbb{Q}} \rightarrow GL_d(\mathbb{Q})$:

compatible system of l -adic representations

Def $F_p(T) = \det(1 - \text{Frob}_p^{-1} T | \rho^I(p))$ local factor

$L(\rho, s) = \prod_p \frac{1}{F_p(p^{-s})}$ global L-function

Ex E/\mathbb{Q} elliptic curve

$L(H^0(E), s) = \prod_p \frac{1}{1 - p^{-s}} = \zeta(s)$

$L(H^1(E), s) = \prod_{p|D} \frac{1}{1 - q_p^{-s}} \prod_{p \nmid D} \frac{1}{1 - q_p^{-s} + p^{1-2s}}$ $\leftarrow L(E, s)$

$L(H^2(E), s) = \prod_p \frac{1}{1 - p \cdot p^{-s}} = \zeta(s-1)$

Thm (Grothendick Monodromy Thm) X/\mathbb{Q}_p non-singular projective variety

After a fin. ext. K/\mathbb{Q}_p , I acts on $H^i(X, \mathbb{Q}_\ell)$ as $I_d + \psi \cdot N$,

$\psi: G_{\mathbb{Q}_p} \rightarrow \mathbb{Z}_\ell$ tame character as before, N nilpotent matrix.

Rmk Such representations are called Weil-Deligne representations, and Weil representations if $N = 0$.

Ex E/\mathbb{Q}_p good (or potentially good) $\Rightarrow N = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ $\forall \ell \in$ Weil rep.

E/\mathbb{Q}_p multiplicative (or pot. mult.) $\Rightarrow N = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ $\forall \ell \in$ Weil-Deligne.