

2. Galois stable lattices + their mod p reduction.

Lemma let $V \in \text{Rep}_E G_K$

$\Rightarrow \exists$ a Galois stable lattice $T \subset V$ i.e.

a free \mathcal{O}_E -module $T \subset V$ that is stable under G_K -action s.t. $T \otimes_{\mathcal{O}_E} E \cong V$.

proof) $\because G_K$ is compact. + Exercise.

Lemma let $V \in \text{Rep}_E G_K$, and T_1, T_2 be Galois stable lattices of V .

$\Rightarrow \text{J.H.}(\overline{T}_1) = \text{J.H.}(\overline{T}_2)$, where $\overline{T}_i := T_i \otimes_{\mathcal{O}_E} \mathbb{F}$.

Lemma let $V \in \text{Rep}_E G_K$.

If mod p reduction of V is irreducible, then

\exists a unique Galois stable lattice of V up to homothety.

proof) Exercise. \rightarrow

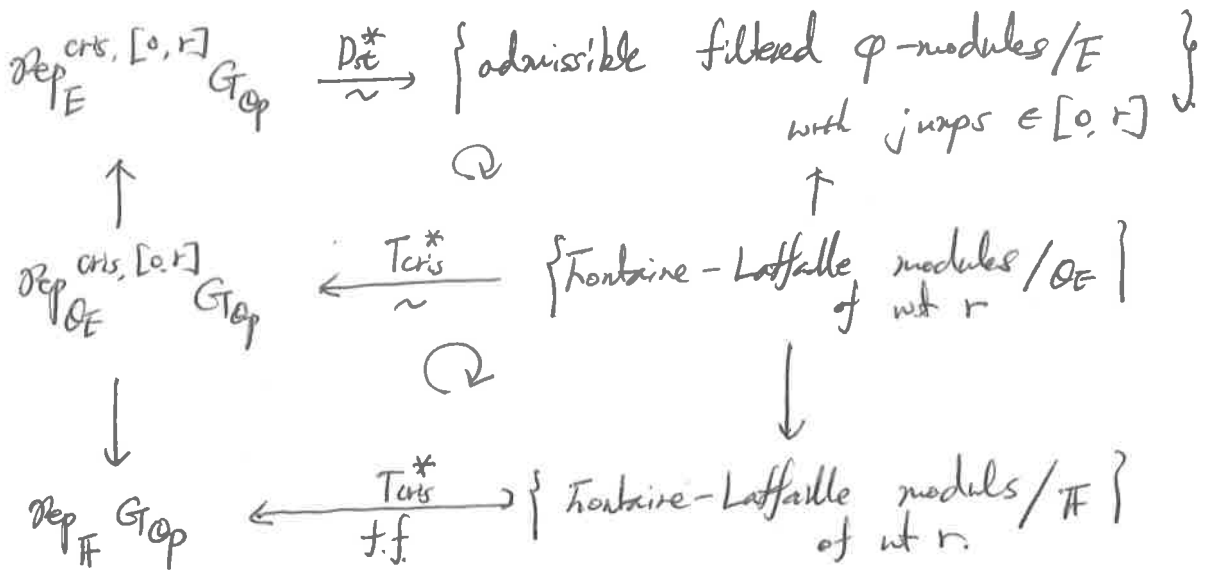
Lemma let $\overline{V} \in \text{Rep}_{\mathbb{F}} G_K$ be an irred. rep'n.

$\Rightarrow P_K$ acts on \overline{V} trivially.

proof) Exercise. $\because P_K = \text{pro-}p \text{ group} \triangleleft G_K$.

* Fontaine - Laffaille Theory

Assume $0 < r < p-1$.



Def . A Fontaine-Laffaille module \mathcal{M} of weight r is a free \mathcal{O}_E -module M of finite rank together with $(\{ \text{Fil}^i M \}_{i \in \mathbb{Z}_1}, \{ \phi_i \}_{i \in \mathbb{Z}_1})$,

where

- a decreasing filtration $\{ \text{Fil}^i M \}_{i \in \mathbb{Z}_1}$ by \mathcal{O}_E -submodules s.t. $\text{Fil}^{i+1} M$ is a \mathbb{Z}_p -direct summand of $\text{Fil}^i M$ for all i , and $\text{Fil}^0 M = M$ and $\text{Fil}^{r+1} M = 0$.

- \mathcal{O}_E -linear maps $\phi_i: \text{Fil}^i M \rightarrow M$ s.t.

$$\phi_i|_{\text{Fil}^{i+1} M} = p \cdot \phi_i \quad \text{and} \quad \sum_{i=0}^r \phi_i(\text{Fil}^i M) = M$$

• Morphisms are \mathcal{O}_E -linear maps compatible with ϕ_i and filtration.

Thm \exists an exact, anti-equivalence of categories

$$T_{cris}^* : \left\{ \begin{array}{l} \text{H.-L. modules}/\mathcal{O}_E \\ \text{of wt } r \end{array} \right\} \xrightarrow{\sim} \text{Rep}_{\mathcal{O}_E}^{cris, [0, r]} \text{Group}$$

that fits the diagram.

Def. A Torsten-Laffaille module/ \mathbb{F} of weight r is a \mathbb{F} -v.s. M of finite dimension together with $(\{F_i M\}_{i \in \mathbb{Z}_1}, \{\phi_i\}_{i \in \mathbb{Z}_1})$

where

- a decreasing filtration $\{F_i M\}_{i \in \mathbb{Z}_1}$ by \mathbb{F} -subspaces
 - st. \bullet $F_{i+1} M$ is a \mathbb{F}_p -direct summand of $F_i M$ for all $i \in \mathbb{Z}_1$, and
 - \bullet $F_0 M = M$ and $F_{r+1} M = 0$.
- \mathbb{F} -linear map $\phi_i : F_i M \rightarrow M$ st.
 - $F_{i+1} M \subset \text{Ker } \phi_i$ and $\sum_{i=0}^r \phi_i(F_i M) = M$.
- Morphisms are \mathbb{F} -linear maps compatible with ϕ_i and filtration.

Thm \exists an exact, fully faithful contravariant functor

$$T_{cris}^* : \left\{ \begin{array}{l} \text{TL modules}/\mathbb{F} \\ \text{of weight } r \end{array} \right\} \longrightarrow \text{Rep}_{\mathbb{F}} \text{Group}$$

ex.) Consider the example (I) - (C) + assume $0 < r < p$.

$M := \mathcal{O}_E(e_1, e_2)$

$$\pi_i^* M := M \cap \pi_i^* D = \begin{cases} M & i \leq 0 \\ \mathcal{O}_E e_1 & 0 < i \leq r \\ 0 & r < i \end{cases}$$

$\phi_i := \frac{1}{p_i} \phi : \pi_i^* M \rightarrow M.$

$\Rightarrow \phi_0 = \phi : \pi_0^* M \rightarrow M$
 $e_1 \mapsto \lambda e_2$
 $e_2 \mapsto -e_1 + \lambda e_2$

$\phi_1 : \mathcal{O}_E e_1 \rightarrow M$
 $e_1 \mapsto \frac{\lambda}{p} e_2$

$\phi_r : \mathcal{O}_E e_1 \rightarrow M$
 $e_1 \mapsto \frac{\lambda}{p^r} e_2$

$\bar{M} = \mathbb{F}(e_1, e_2)$

$$\pi_i^* \bar{M} = \begin{cases} \bar{M} & i \leq 0 \\ \mathbb{F} e_1 & 0 < i \leq r \\ 0 & r < i \end{cases}$$

$\phi_i : \pi_i^* \bar{M} \rightarrow \bar{M} \Rightarrow \phi_0 : e_1 \mapsto 0$
 $e_2 \mapsto -e_1$

$\phi_1 : e_1 \mapsto 0$

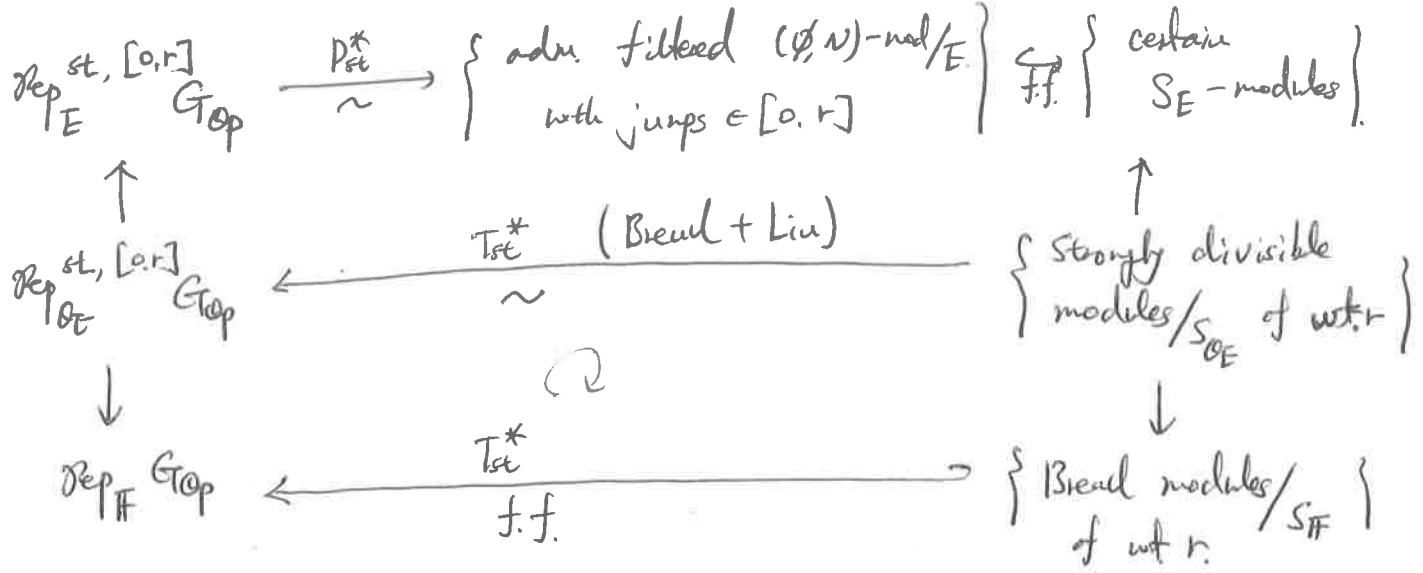
$\phi_r : e_1 \mapsto \left(\frac{\lambda}{p^r}\right) e_2$

Exercise: $\text{Tensor}^*(\bar{M})$ is irreducible

In fact; $\bar{P}|_{\mathbb{I}_{\mathbb{A}^p}} \sim \omega_{\downarrow}^+ \oplus \omega_{\downarrow}^{pr}$ where $\bar{P} := \text{Tensor}^*(M).$

* Strongly divisible modules

Assume $0 < r < p-1$.



Warning!! The bottom T_{st}^* is only faithful, in general.
 Known fully faithful when $e \cdot r < p-1$, where $e := [K:K_0]$.
 (Cassida).

Let $E(u) := u - p \in \mathbb{Z}_p[u]$.

$$S := \widehat{\mathbb{Z}_p \left[\frac{u^i}{i!} \mid i \in \mathbb{N} \right]} \quad (\widehat{\quad} \text{p-adic completion})$$

$$= \left\{ \sum_{i=0}^{\infty} w_i \cdot \frac{E(u)^i}{i!} \mid w_i \in \mathbb{Z}_p, w_i \rightarrow 0 \right\}$$

$\Rightarrow S$ has additional structure:

- $\phi: S \rightarrow S$ is a \mathbb{Z}_p -linear map with $\phi(u) = u^p$.
- $N: S \rightarrow S$ is a \mathbb{Z}_p -linear ~~map~~ derivation s.t. $N(u) = -u$.
- a decreasing filtration $\{ \pi^i S \mid i \in \mathbb{Z}_{\geq 0} \}$, where

$$\pi^i S := \widehat{\sum_{j=i}^{\infty} \frac{E(u)^j}{j!} S}$$

Ex) $N\phi = p\phi N$ on S

$\phi(\pi^i S) \subset p^i S$ for $0 \leq i \leq p-1$.

Def $S_{OE} := S \otimes_{\mathbb{Z}_p} O_E$

$$S_E := S_{OE} \otimes_{\mathbb{Z}_p} O_p = S \otimes_{\mathbb{Z}_p} E.$$

Extend the definitions of $\phi, \nu, \{\tau l^i S\}_{i \in \mathbb{Z}_{\geq 0}}$
to S_{OE} and S_E by O_E -linearity and E -linearity.

Def A filtered (ϕ, ν) -module $/ S_E$ is a free S_E -module \mathcal{D} of finite rank together with

- a $\phi \otimes 1$ -semilinear morphism $\phi: \mathcal{D} \rightarrow \mathcal{D}$

s.t. $\det \phi$ is invertible in S_{O_p}

w.r.t. a S_{O_p} -basis.

- a decreasing filtration on \mathcal{D} by S_E -modules $\{\tau l^i \mathcal{D}\}_{i \in \mathbb{Z}}$

with $\cdot \tau l^i \mathcal{D} = \mathcal{D}$ if $i \leq 0$

$$\cdot \tau l^i S_E \cdot \tau l^j \mathcal{D} \subseteq \tau l^{i+j} \mathcal{D}$$

- an ~~\mathbb{Z}_p~~ E -linear map $N: \mathcal{D} \rightarrow \mathcal{D}$ s.t.

$$\cdot N(sx) = N(s) \cdot x + s \cdot N(x) \quad \forall s \in S_E, \forall x \in \mathcal{D}$$

$$\cdot N\phi = \rho\phi N$$

$$\cdot N(\tau l^i \mathcal{D}) \subseteq \tau l^{i-1} \mathcal{D} \quad \forall i \in \mathbb{Z}.$$

• Let D be an adm. filtered (ϕ, ν) -module/ E with $\text{Fil}^0 D = D$.

$$\Rightarrow - \mathcal{D} := S \otimes_{\mathbb{Z}_p} D \in S_E\text{-module}$$

$$- \phi := \phi \otimes \phi : \mathcal{D} \rightarrow \mathcal{D}$$

$$- \nu := \nu \otimes 1 + 1 \otimes \nu : \mathcal{D} \rightarrow \mathcal{D}$$

- $\text{Fil}^0 \mathcal{D} = \mathcal{D}$ and, by induction,

$$\text{Fil}^{i+1} \mathcal{D} := \left\{ x \in \mathcal{D} \mid \nu(x) \in \text{Fil}^i \mathcal{D} \text{ and } f_p(x) \in \text{Fil}^{i+1} D \right\}$$

where $f_p : \mathcal{D} \rightarrow D$ is defined by $s(u) \otimes x \mapsto s(p) \cdot x$.

Thm (Breuil) $D \mapsto \mathcal{D} := S \otimes_{\mathbb{Z}_p} D$ gives a fully faithful ~~functor~~ functor from the category of adm. filtered (ϕ, ν) -mod/ E with $\text{Fil}^0 D = D$ to the " of filtered (ϕ, ν) -modules/ S_E .

Lemma Consider the example (2), and assume $r=2$

$$\Rightarrow \cdot \text{Fil}^0 \mathcal{D} = \mathcal{D}$$

$$\cdot \text{Fil}^1 \mathcal{D} = S_E(e_1 + 2e_2) + \text{Fil}^1 S_E \cdot \mathcal{D}$$

$$\cdot \text{Fil}^2 \mathcal{D} = S_E(e_1 + 2e_2 + \frac{u^p}{p} e_2) + \text{Fil}^2 S_E \cdot \mathcal{D}$$

$$\cdot \text{Fil}^i \mathcal{D} = \text{Fil}^{i-2} S_E(e_1 + 2e_2 + \frac{u^p}{p} e_2) + \text{Fil}^i S_E \cdot \mathcal{D} \quad \forall i \geq 2.$$

proof) Exercise.

Tip!! $\nu(e_1 + 2e_2 + \frac{u^p}{p} e_2) = e_1 + 0 - \frac{u}{p} e_2 = -\frac{u^p}{p} e_2 \in \text{Fil}^2 \mathcal{D}$.

Def) A strongly divisible module / S_{OE} of weight r is
 a free S_{OE} -module \underline{M} of finite rank
 with - an S_{OE} -submodule $\tau l^r \underline{M}$
 - additive maps $\phi, \nu: \underline{M} \rightarrow \underline{M}$

- s.t.
- $\tau l^r S_{OE} \cdot \underline{M} \subseteq \tau l^r \underline{M}$
 - $\tau l^r \underline{M} \cap I \cdot \underline{M} = I \cdot \tau l^r \underline{M} \quad \forall I \in \text{ideal } S_{OE}$
 - $\phi(sx) = \phi(s) \cdot \phi(x) \quad \forall s \in S_{OE}, \forall x \in \underline{M}$.
 - $\phi(\tau l^r \underline{M}) \subseteq p^r \underline{M}$ and generate it over S_{OE} .
 - $\nu(sx) = \nu(s) \cdot x + s \cdot \nu(x) \quad \forall s \in S_{OE}, \forall x \in \underline{M}$
 - $\nu \phi = p \phi \nu$
 - $E(\nu) \cdot \nu(\tau l^r \underline{M}) \subseteq \tau l^r \underline{M}$.

Thm let $0 \leq r < p-1$



fits that fits the diagram.

- Breuil proved G_{Op} -case + conjectured G_{TK} -case
- Liu proved G_{TK} -case.

• Let \underline{M} be a strongly div. module/ $S_{\mathbb{A}^1}$ of rank r .

$$\Rightarrow \mathcal{D} := \underline{M} \left[\frac{1}{P} \right] = \underline{M} \otimes_{S_{\mathbb{A}^1}} \mathcal{O}_P, \quad \text{Fil}^r \mathcal{D} := \text{Fil}^r \underline{M} \left[\frac{1}{P} \right].$$

$$\cdot \phi, \nu \subset \mathcal{D}$$

$$\cdot \text{Fil}^i \mathcal{D} := \begin{cases} \mathcal{D} & \text{if } i \leq 0 \\ \{x \in \mathcal{D} \mid E(u)^{r-i} x \in \text{Fil}^r \mathcal{D}\} & \text{if } 0 < i \leq r \\ \sum_{j=0}^{i-1} (\text{Fil}^{i-j} S_{\mathbb{A}^1}) (\text{Fil}^j \mathcal{D}) & \text{if } i > r, \text{ inductively} \end{cases}$$

$\Rightarrow \mathcal{D}$ is a filtered (ϕ, ν) -module/ $S_{\mathbb{A}^1}$

$$\Rightarrow \text{Let } \begin{array}{ccc} S_0: S_{\mathbb{A}^1} & \rightarrow & \mathcal{O}_P \\ u & \mapsto & 0 \end{array} \quad \begin{array}{ccc} S_P: S_{\mathbb{A}^1} & \rightarrow & \mathcal{O}_P \\ u & \mapsto & P. \end{array}$$

$$\cdot D := \mathcal{D} \otimes_{S_{\mathbb{A}^1}, S_0} \mathcal{O}_P = \mathcal{D} \otimes_{S_{\mathbb{A}^1}, S_P} \mathcal{O}_P$$

$$\begin{array}{c} \hookrightarrow \\ \phi, \nu \end{array}$$

$$\text{Fil}^i D := \text{Fil}^i \mathcal{D} \otimes_{S_{\mathbb{A}^1}, S_P} \mathcal{O}_P.$$

$\Rightarrow D$ is an admissible filtered (ϕ, ν) -module/ E .

with jumps $\in [0, r]$.

\therefore We have an alternative definition of

strongly div. modules from the data

of adm. filtered (ϕ, ν) -modules.

Def Let D be an admi. filtered (ϕ, ν) -mod/ E
 with $\text{Fil}^0 D = D$ and $\text{Fil}^{r+1} D = 0$.

A strongly div. module \mathcal{D} in \mathcal{S}_E of weight r .
 $\mathcal{D} := S \otimes_{\mathbb{F}_p} D$ is
 a free $S_{\mathbb{F}_p}$ -submodule $\underline{\mathcal{M}}$ of \mathcal{D} of finite rank
 with $\underline{\mathcal{M}}[\frac{1}{p}] \cong \mathcal{D}$.

s.t. - $\underline{\mathcal{M}}$ is stable under ϕ and ν .

- $\phi(\text{Fil}^r \underline{\mathcal{M}}) \subseteq p^r \underline{\mathcal{M}}$, where

$$\text{Fil}^r \underline{\mathcal{M}} := \underline{\mathcal{M}} \cap \text{Fil}^r \mathcal{D}$$

eg.) Consider example (2) + assume $r=2$.

$$E(u) := (u-p) \in S.$$

$$\gamma := \frac{(u-p)^p}{p} \in S$$

$$\Rightarrow \cdot \phi(\gamma) = \frac{(u^p-p)^p}{p} \in p^{p-1} \cdot S.$$

$$\cdot \gamma^{-1} \equiv \frac{u^p-p}{p} \pmod{pS}$$

$$\Rightarrow \phi(E(u)) = u^p - p \equiv p(\gamma^{-1}) \pmod{p^2 S}$$

$$\cdot \nu(\gamma) = -u(u-p)^{p-1}$$

$$= -p[\gamma + (u-p)^{p-1}] \in p \cdot S.$$

• let D be an admi. filtered (ϕ, N) -module/ E
 in example (2) with $r=2$. ($\Rightarrow v_p(\lambda) = \frac{1}{2}$)

Prop $\underline{M} := S_{\mathcal{O}_E}(E_1, E_2)$ is a str. div. mod. in $\mathcal{D} := S_{\mathbb{Z}_p} D$

where ① if $v_p(\lambda-1) \geq \frac{1}{2}$

$$E_1 = p e_1 + \lambda e_2 + (\lambda-1) e_2$$

$$E_2 = \lambda e_2$$

② if $v_p(\lambda-1) < \frac{1}{2}$

$$E_1 = p e_1 + \lambda e_2 + (\lambda-1) e_2 - \frac{p f}{\lambda-1} (\lambda-1)^2 e_2$$

$$E_2 = \lambda (\lambda-1) e_2$$

Here, f is defined as follows: assume $v_p(\lambda-1) < \frac{1}{2}$

• Define a sequence

$$G_0 := 1, \quad G_{n+1} := \frac{(\lambda-1)^2}{(\lambda-1)^2 - p G_n} \in E.$$

$\Rightarrow \{G_n\}$ converges to an element in $1 + \underline{M}_E$, ~~denoted~~ denoted by f .

$$\therefore G_{n+1} = 1 + \frac{p G_n}{(\lambda-1)^2 - p G_n} \in 1 + \underline{M}_E.$$

$$G_{n+2} - G_{n+1} = \frac{p(\lambda-1)^2}{[(\lambda-1)^2 - p G_{n+1}][(\lambda-1)^2 - p G_n]} (G_{n+1} - G_n)$$

$\Rightarrow \{G_n\}$ is Cauchy.

$\Rightarrow \{G_n\}$ converges in $1 + \underline{M}_E$ \square

• f satisfies $\boxed{p f^2 - (\lambda-1)^2 f + (\lambda-1)^2 = 0.}$

We prove the case ② by a series of lemmas.

lemma . $\phi(E_1) \equiv E_1 \pmod{m_E \cdot \mathcal{M}}$

. $\phi(E_2) \equiv 0 \pmod{\text{---}}$

. $\nu(E_2) \equiv 0 \pmod{\text{---}}$

. $\nu(E_1) = 0.$

proof) . $\phi(E_1) = p\lambda e_1 + \lambda z e_2 + \lambda(\phi(\gamma)-1)e_2 - \frac{\lambda p \delta}{z-1} (\phi(\gamma)-1)^2 e_2$

$$= p\lambda \left[E_1 - \frac{z}{\lambda(z-1)} E_2 - \frac{\gamma-1}{\lambda(z-1)} E_2 + \frac{p\delta}{\lambda(z-1)^2} (\gamma)^2 E_2 \right]$$

$$+ \frac{\lambda z}{\lambda(z-1)} E_2 + \frac{\phi(\gamma)-1}{z-1} E_2 - \frac{p\delta}{(z-1)^2} (\phi(\gamma)-1)^2 E_2$$

$$= p\lambda E_1 + \frac{\phi(\gamma) + (z-1) - p(\delta+z-1)}{z-1} E_2$$

$$- \frac{p\delta(\phi(\gamma)-1)^2 - p^2\delta(\gamma)^2}{(z-1)^2} E_2 \equiv E_1 \pmod{m_E \cdot \mathcal{M}}$$

. $\nu(E_1) = p e_1 - u(\nu p)^M e_2 - \frac{p\delta}{z-1} z \cdot (\delta-1) (-u(\nu p)^M) e_2$

$$= p \left[1 - \cancel{u(\nu p)^M} [\gamma + (\nu p)^M] e_2 + \frac{z p \delta}{z-1} (\delta-1) [\delta + (\nu p)^M] e_2 \right]$$

$$= \frac{p}{\lambda(z-1)} \left[1 - [\gamma + (\nu p)^M] \left(1 - \frac{z p \delta}{z-1} (\delta-1) \right) \right] E_2$$

$$\equiv 0 \pmod{m_E \cdot \mathcal{M}}$$

. Check $\phi(E_2), \nu(E_2)$ □

Lemma $\text{Fil}^2 \mathcal{M} = \langle \mathcal{H}_1, \mathcal{H}_2 \rangle + \text{Fil}^2 S_{\mathbb{E}} \cdot \mathcal{M}$, where

$$\mathcal{H}_1 := \lambda E_1 - E_2 + \frac{p\delta}{(\lambda-1)^2} E_2 + \frac{p\lambda}{\lambda-1} E_2 + (np) \left(\frac{\lambda\delta}{\lambda-1} E_1 + \frac{p\delta\lambda}{(\lambda-1)^2} E_2 \right)$$

$$\mathcal{H}_2 := (np) \left(\lambda\delta E_1 - E_2 + \frac{p\delta\lambda}{\lambda-1} E_2 \right) \bullet$$

proof). Recall: $\text{Fil}^2 \mathcal{D} = S_{\mathbb{E}} (e_1 + \lambda e_2 + \frac{np}{p} e_3) + \text{Fil}^2 S_{\mathbb{E}} \cdot \mathcal{D}$.

\Rightarrow Modulo $\text{Fil}^2 S_{\mathbb{E}}$, ~~every~~ every element in $\text{Fil}^2 \mathcal{D}$ is written as

$$x \equiv c_0 \left(e_1 + \lambda e_2 + \frac{np}{p} e_3 \right) + c_1 (np) (e_1 + \lambda e_2) \text{ for } c_i \in \mathbb{E}.$$

Recall: $\text{Fil}^2 \mathcal{M} := \mathcal{M} \cap \text{Fil}^2 \mathcal{D}$.

$$\begin{aligned} \Rightarrow x &\equiv c_0 \left[\frac{1}{p} \left(E_1 - \frac{\lambda}{\lambda(\lambda-1)} E_2 + \frac{1}{\lambda(\lambda-1)} E_2 + \frac{p\delta}{\lambda(\lambda-1)^2} E_2 \right) + \frac{\lambda}{\lambda(\lambda-1)} E_2 + (np) \frac{1}{p\lambda(\lambda-1)} E_2 \right] \\ &\stackrel{\text{mod}}{\text{Fil}^2 S_{\mathbb{E}} \cdot \mathcal{D}} + c_1 (np) \left[\frac{1}{p} \left(E_1 - \frac{\lambda}{\lambda(\lambda-1)} E_2 + \frac{1}{\lambda(\lambda-1)} E_2 + \frac{p\delta}{\lambda(\lambda-1)^2} E_2 \right) + \frac{\lambda}{\lambda(\lambda-1)} E_2 \right] \\ &= c_0 \left(\frac{1}{p} E_1 - \frac{1}{p\lambda} E_2 + \frac{\delta}{\lambda(\lambda-1)^2} E_2 + \frac{\lambda}{\lambda(\lambda-1)} E_2 \right) \\ &\quad + (np) \left[c_1 \left(\frac{1}{p} E_1 - \frac{1}{p\lambda} E_2 + \frac{\delta}{\lambda(\lambda-1)^2} E_2 + \frac{\lambda}{\lambda(\lambda-1)} E_2 \right) + \frac{c_0}{p\lambda(\lambda-1)} E_2 \right] \\ &= c_0 \left(\frac{1}{p} E_1 - \frac{1}{p\lambda} E_2 + \frac{\delta}{\lambda(\lambda-1)^2} E_2 + \frac{\lambda}{\lambda(\lambda-1)} E_2 \right) \\ &\quad + (np) \left(\frac{c_1}{p} E_1 + \frac{(\lambda-1)c_0 + p\lambda(\lambda-1)c_1 - [(\lambda-1)^2 - p\delta]c_1}{p\lambda(\lambda-1)^2} E_2 \right) \end{aligned}$$

Recall: $p\delta^2 - (\lambda-1)^2\delta + (\lambda-1)^2 = 0$

$$\Rightarrow \frac{(\lambda-1)c_0 - [(\lambda-1)^2 - p\delta]c_1}{p\lambda(\lambda-1)^2} = \frac{\delta c_0 - (\lambda-1)c_1}{p\lambda\delta(\lambda-1)}$$

$$x \equiv C_0 \left(\frac{1}{p} E_1 - \frac{(z-1)^2 - p\delta - pz(z-1)}{p\lambda(z-1)^2} E_2 \right)$$

$$+ (wp) \left(\frac{c_1}{p} E_1 + \frac{pz c_1}{p\lambda(z-1)} E_2 + \frac{\delta C_0 - (z-1)C_1}{p\lambda\delta(z-1)} E_2 \right)$$

Since $z > 1$

$$\Rightarrow \cdot v_p(C_0) \geq v_p(p\lambda) = \frac{z}{2}$$

$$\cdot v_p(c_1) \geq 1$$

$$\cdot v_p(\delta C_0 - (z-1)C_1 + p\delta z C_1) \geq v_p(p\lambda(z-1))$$

$$\Leftrightarrow v_p(\delta C_0 - (z-1)C_1) \geq v_p(p\lambda(z-1))$$



Since $C_1 = \frac{p\delta}{z-1} \cdot \frac{C_0}{p\lambda} - \frac{p\delta(z-1)}{z-1} \cdot \frac{\delta C_0 - (z-1)C_1}{p\lambda\delta(z-1)}$,

$$x \equiv \frac{C_0}{p\lambda} \left(\lambda E_1 - \frac{(z-1)^2 - p\delta - pz(z-1)}{(z-1)^2} E_2 \right)$$

$$+ (wp) \left(\frac{p\lambda\delta}{z-1} \frac{C_0}{p\lambda} - \frac{p\lambda\delta(z-1)}{z-1} \cdot \frac{\delta C_0 - (z-1)C_1}{p\lambda\delta(z-1)} \right) \left(\frac{1}{p} E_1 + \frac{pz}{p\lambda(z-1)} E_2 \right)$$

$$+ (wp) \frac{\delta C_0 - (z-1)C_1}{p\lambda\delta(z-1)} E_2$$

$$\equiv \frac{C_0}{p\lambda} \left[\underbrace{\lambda E_1 - \frac{(z-1)^2 - p\delta - pz(z-1)}{(z-1)^2} E_2}_{= F_1} + (wp) \left(\frac{\lambda\delta}{z-1} E_1 + \frac{p\delta z}{(z-1)^2} E_2 \right) \right]$$

$$- \frac{\delta C_0 - (z-1)C_1}{p\lambda\delta(z-1)} (wp) \underbrace{\left(\lambda\delta E_1 - E_2 + \frac{p\delta z}{z-1} E_2 \right)}_{= F_2}$$

Cor $\pi_1 \equiv -E_1 \pmod{m_E \cdot \mathcal{M}}$

$\pi_2 \equiv \dots \pmod{\dots}$
 $-u E_2$

proof obvious

Lemma $\phi(\pi_1) \equiv p\lambda^2 E_1 \pmod{p^2 m_E \cdot \mathcal{M}}$

$\phi(\pi_2) \equiv 0 \pmod{\dots}$

proof) Using our computation of $\phi(E_1), \phi(E_2)$

$$\phi(\pi_1) = p\lambda^2 E_1 + \frac{\lambda[\phi(\gamma) - p(\gamma)]}{\alpha - 1} E_2 - \frac{p\lambda\delta[\phi(\gamma)(\phi(\gamma) - 1) - p(\gamma)^2]}{(\alpha - 1)^2} E_2$$

$$+ (u^p - p) \left(\frac{p\lambda^2\delta}{\alpha - 1} E_1 + \frac{\lambda\delta(\phi(\gamma) + \alpha - 1 - p(\gamma))}{(\alpha - 1)^2} E_2 - \frac{p\lambda\delta^2((\phi(\gamma) - 1)^2 - p(\gamma)^2)}{(\alpha - 1)^3} E_2 \right)$$

$$\equiv p\lambda^2 E_1 - \frac{p\lambda(\gamma)}{\alpha - 1} E_2 + \frac{p^2\lambda\delta(\gamma)^2}{(\alpha - 1)^2} E_2$$

$$+ \frac{(u^p - p)}{p} \left(\frac{p\lambda\delta(\alpha - 1 - p(\gamma))}{(\alpha - 1)^2} E_2 - \frac{p^2\lambda\delta^2}{(\alpha - 1)^3} E_2 \right)$$

$\phi\delta^2 - (\alpha - 1)\delta + (\alpha - 1)^2$
 $\stackrel{0}{\equiv}$

$$\stackrel{0}{\equiv} p\lambda^2 E_1 - \frac{p\lambda(\gamma)}{\alpha - 1} E_2 + \frac{p^2\lambda\delta(\gamma)^2}{(\alpha - 1)^2} E_2$$

$$+ \frac{u^p - p}{p} \left(\frac{p\lambda}{\alpha - 1} E_2 - \frac{p^2\lambda\delta(\gamma)}{(\alpha - 1)^2} E_2 \right)$$

$$= p\lambda^2 E_1 - \frac{p\lambda}{\alpha - 1} \left[(\gamma) - \frac{u^p - p}{p} \right] E_2 + \frac{p^2\lambda\delta(\gamma)}{(\alpha - 1)^2} \left[(\gamma) - \frac{u^p - p}{p} \right] E_2$$

$$\equiv p\lambda^2 E_1 \pmod{p^2 m_E \cdot \mathcal{M}}$$

$\phi(\pi_2) = \text{exercise}$

