16.7.2024

An example of bad reduction of modular curves: level $\Gamma_0(p)$ over $\mathbb{Z}_{(p)}$

In this chapter we will study an example of "bad reduction", i.e. a modular curve over (an open part of) $\operatorname{Spec}\mathbb{Z}$ whose fiber over $\mathbb{F}_p$ (p a fixed prime) is singular.

So fix a prime number p.

We want to consider level structure "of type $\Gamma_0(p)$".

Recall (for any $N \geq 1$):

$$\Gamma_0(N)\backslash\mathcal{H} \overset{1:1}{\longleftrightarrow} \{(E,H);\ E/\mathbb{C} \text{ ell. curve},\ H \leq E[N] \text{ cyclic of order } N\}/\cong$$

This makes sense* over an arbitrary base scheme S.

Since for us $N=p$ will be a prime number, "cyclic" is automatic (also in the relative setting).

* when understood correctly, i.e., scheme-theoretically,

The first result we will show is that

$$\mathcal{M}_0(p) : (\mathrm{Sch}/\mathbb{Z})^{op} \longrightarrow (\mathrm{Sets})$$

$$S \longmapsto \{(E, H);\ E/S \text{ elliptic curve}$$

$$H \subset E[p] \text{ finite loc. free subgroup scheme of order } p\}/\cong$$

$(\text{order of } H := \mathrm{rk}_S\, \Gamma(S, \mathcal{O}_H))$

is relatively representable over $\mathcal{M}$.

However, every (E, H) has non-trivial automorphism (at least $[-1]$), so $\mathcal{M}_0(p)$ is not representable.

Instead, we will consider some $N \geq 3$, $p \nmid N$, and

$$\mathcal{M}_0(p) \times_{\mathcal{M}} \mathcal{M}_N = \{(E, \alpha, H)\}/\cong \qquad (/\mathbb{Z}[\tfrac{1}{N}])$$

α: level-N str.; H: $\subset E[p]$ as above

and the finite flat (see below) morphism

$$\underbrace{\mathcal{M}_0(p) \times_{\mathcal{M}} \mathcal{M}_N} \longrightarrow \mathcal{M}_N$$

Remark

Theorem - If a commutative finite locally free group scheme over some scheme S.
Then multiplication by $\deg(H)$ is $\equiv 0$ on H.

Therefore we can write $M_0(p)$ alternatively as

$$S \mapsto \{(E, E', \varphi : E \to E');$$
$$E, E'/S \text{ elliptic curves}$$
$$\varphi \text{ isogeny of degree } p\}/\cong .$$

Theorem (relative representability of $\Gamma_0(N)$-level str.)

Let $N \geq 1$.

Let S be a scheme (we do not require that N is invertible on S),

Let E/S be an elliptic curve.

The functor $\mathrm{Subgp}(E[N])$ given by

$$(\mathrm{Sch}/S)^{\mathrm{op}} \to (\mathrm{Sets})$$

$$T \longmapsto \{H \subset E_T[N] \text{ subgp scheme of order } N, \underline{\text{cyclic}}\}$$

is representable by a finite flat S-scheme (even finite étale if N invertible on S).

(automatic if N is a prime number)

Proof To simplify assume $N = p$ prime.

The representability of the Sub$_p$ functor holds quite generally, as the following lemma shows.

Lemma Let S be a scheme, G/S a finite locally free group scheme, $d \geq 1$.

Then the functor

$$\mathrm{Sub}_d(G) : (\mathrm{Sch}/S)^{\mathrm{op}} \longrightarrow (\mathrm{Sets})$$

$$T \longmapsto \{ H \subseteq G_T \text{ finite locally free subgroup scheme of order } d \}$$

is representable by a projective S-scheme.

(But note that in general Sub_d need not be finite nor flat over S.)

Proof. Shrinking S, if necessary, we may assume that $S = \operatorname{Spec} R$, R connected, $G = \operatorname{Spec} A$, A a finite free R-module. Let $n = \mathrm{rk}_R A$ and choose an isomorphism $A \cong R^n$.

Obtain

$$\mathrm{Sub}_d(G) \longrightarrow \mathrm{Grass}_{n-d,n}$$

$$H \longmapsto \ker\left(\mathcal{O}^n \twoheadrightarrow \Gamma(H, \mathcal{O}_H) \right)$$

We will show that this morphism Δ factors through representable by a closed immersion (this implies that Subd is representable by a closed subscheme of $\mathrm{Grass}_{n-d,n}$ and hence proves the Lemma).

So let $T \to \mathrm{Grass}_{n-d,n}$ be a morphism (this is the same as a loc.-free quotient $\mathcal{O}_T^n \twoheadrightarrow \mathcal{Q}$ of rank d).

We need to show:

$$\mathrm{Subd} \times_{\mathrm{Grass}_{n-d,n}} T \longrightarrow T$$

is a closed immersion scheme, or in other words:

there exists a (necessarily unique) closed subscheme $Z \subseteq T$ s.t. a morphism $T' \to T$ factors through Z if and only if $\mathcal{O}_{T'}^n \twoheadrightarrow \mathcal{Q}_{|T'}$ is the quotient by an ideal sheaf of $\mathcal{O}_{T'}^n$ $(= \mathcal{O}_{\mathbb{A} \times_S T'})$ and defines a subgroup scheme of $\mathbb{A} \times_S T'$.

Explicitly, this means that the dashed arrows in the following diagrams need to exist:

- multiplication:

$$\begin{array}{ccc} \mathcal{O}_{G\times T} \underset{\mathcal{O}_T}{\otimes} \mathcal{O}_{G\times T} & \longrightarrow & \mathcal{O}_{G\times T} \\ \downarrow{\scriptstyle \varphi\otimes\varphi} & & \downarrow{\scriptstyle \varphi} \\ \mathcal{Q} \underset{\mathcal{O}_T}{\otimes} \mathcal{Q} & \dashrightarrow & \mathcal{Q} \end{array}$$

- comultiplication ($\hat{=}$ mult. $H\times H \to H$)

$$\begin{array}{ccc} \mathcal{O}_{G\times T} & \longrightarrow & \mathcal{O}_{G\times T} \underset{\mathcal{O}_T}{\otimes} \mathcal{O}_{G\times T} \\ \varphi\downarrow & & \downarrow{\scriptstyle \varphi\otimes\varphi} \\ \mathcal{Q} & \dashrightarrow & \mathcal{Q} \underset{\mathcal{O}_T}{\otimes} \mathcal{Q} \end{array}$$

- counit ($\hat{=}$ neutral elt η H)

$$\begin{array}{ccc} \mathcal{O}_{G\times T} & \twoheadrightarrow & \mathcal{O}_T \\ \downarrow & \nearrow & \\ \mathcal{Q} & & \end{array}$$

- coinverse ($\hat{=}$ inverse elts for H)

(automatic since finite gp schemes [check on functors]; but could be expressed by similar diagram)

The result then follows from the following lemma.

Lemma Let T be a scheme.

(1) Let $\mathcal{E} \xrightarrow{\alpha} \mathcal{F}$ be a homom of finite loc. free $\mathcal{O}_T$-modules. Then there exists a (unique) closed subscheme $Z \subseteq T$ such that a morphism $T' \xrightarrow{f} T$ factors through Z if and only if $f^*(\alpha) = 0$.

(2) Let
$$\begin{array}{ccc} \mathcal{E} & \xrightarrow{\alpha} & \mathcal{E}' \\ \downarrow & & \downarrow \\ \mathcal{Q} & & \mathcal{Q}' \end{array}$$
be a diagram of finite locally free $\mathcal{O}_T$-modules (where the vertical arrows are surjective). Then there exists a (unique) closed subscheme $Z \subseteq T$ such that $f: T' \to T$ factors through Z if and only if $f^*\alpha$ induces a homom. $f^*\mathcal{Q} \to f^*\mathcal{Q}'$ making the diagram commutative.

Proof (1) Since Z (if it exists) is clearly unique, we may work locally on T and thus assume that $\mathcal{E}$ and $\mathcal{F}$ are free, so that (after choosing bases) α is given by a matrix. We then define Z as the closed subscheme of T with ideal the ideal generated by the entries of this matrix.

(2) Apply Part (1) to $\operatorname{Ker}(\mathcal{E} \to \mathcal{Q}) \to \mathcal{E}' \to \mathcal{Q}'$.

We now come back to the case $G = E[p]$.
We still need to show that $\mathrm{Sub}_p(E[p])$ is finite flat of degree $p+1$. We start by looking at the étale case.

Example Let G/S be finite étale.
Then $\mathrm{Sub}_d(G)$ is finite étale $/S$.

In fact, we may check this after a finite étale base change $S' \to S$ and thus may assume that G is constant. But then every subgroup scheme of G (also after pullback) is constant (if S is connected) and thus

$$\mathrm{Sub}_d(G) = \coprod_H S,$$ the union ranging over the finite set of subgroups of the abstract group G.

For $\mathrm{Sub}_p(E[p])$ over $\mathbb{Z}[\frac{1}{p}]$ we obtain that after a finite étale base change $\mathrm{Sub}_p(E[p]) \cong \mathrm{Sub}_p(\mathbb{Z}/p^2)$

of degree $p+1$ over S, $\cong \coprod_{GL_2(\mathbb{Z}/p)/B} S$

as desired.

Next: $\mathrm{Sub}_p(E[p])$ is finite.

We know already that $\mathrm{Sub}_p(E[p])$ is projective, so it is enough to show that $\mathrm{Sub}_p(E[p])$ is quasi-finite.

In other words we need to show that for E an elliptic curve over an algebraically closed field k, $E[p]$ has only finitely many subgroup schemes of order p.

[Note: $\mathrm{char}\, k = p > 0 \rightsquigarrow \mathrm{Sub}_p(\alpha_p^2) \cong \mathbb{P}^1_k$, not finite!]

Case 1 p invertible in k. Then $E[p] \cong \mathbb{Z}/p^2$ has $p+1$ subgp schemes of order p, see above.

E ordinary: $E[p] \cong \mu_p \times \mathbb{Z}/p$

Case 2 $\mathrm{char}\, k = p$, $\rightsquigarrow$ only p: μ_p, $\mathbb{Z}/p$

E ordinary.

Then $E[p](k) = \mathbb{Z}/p$, so topologically $E[p]$ has p points, and the connected component $E[p]^\circ$ of the neutral element of $E[p]$ has order p.

Then not hard to show that $E[p] \cong \mathbb{Z}/p \times E[p]^\circ$.

Now let $H \subset E[p]$ be a subgp scheme of order p.

If H^0 is non-trivial, then (since $H^0 \subseteq E[p]^0$ and the latter has order p) $H^0 = E[p]^0$.
On the other hand, if H^0 is trivial (i.e., $= \operatorname{Spec} k$), then H is étale and necessarily $H \cong \underline{\mathbb{Z}/p}$.

Thus $\operatorname{Sub}_k(E[p])$ has 2 points in this case.
(One can show, and we will use below, that $E[p]^\circ \cong \mu_p$.)

Case 3 $\operatorname{char} k = p$, E supersingular.

$\rightsquigarrow$ $E[p](k) = \{0\}$, $E[p] = E[p]^\circ$ connected, $\dim_k T_0 E(p) = 1$

$\rightsquigarrow$ as a scheme, $E[p] \cong \operatorname{Spec} k[X]/(X^{p^2})$

Therefore, $E[p]$ has a unique closed subscheme that is finite loc. free with structure sheaf $\cong$ such p, namely $\operatorname{Spec} k[X]/(X^p)$.

[This is in fact a subgroup scheme.]

17.7.2024

By the following lemma:

Lemma Let S be a reduced scheme, $\mathcal{F}$ a quasi-coherent $\mathcal{O}_S$-module of finite type and $r \geq 0$ such that

$$\dim_{\kappa(s)} \mathcal{F}(s) = r \quad \text{for all } s \in S.$$

Then $\mathcal{F}$ is locally free of rank r.

(See [Mumford, Abelian Varieties, §5, Lemma 1] or [GW1] Cor 11.19.)

the remaining part of "finite flat of degree $p+1$" will follow (since M_N reduced which allows us to reduce to the universal case), if we can show that for every alg. closed field k and elliptic curve E/k, the scheme $\mathrm{Sub}_p(E[p])$ has degree $p+1$ over k, i.e., $\dim_k \Gamma(\mathrm{Sub}_p(E[p]), \mathcal{O}_{\mathrm{Sub}_p(E[p])}) = p$.

Case 1 $\mathrm{char}(k) \neq p$. Have already seen that (k being alg. cl.)

$$\mathrm{Sub}_p(E[p]) = \mathrm{Sub}_p\left((\mathbb{Z}/p)^2\right) = \coprod_{\mathbb{P}^1(\mathbb{F}_p)} \mathrm{Spec}\, k \text{ has degree } p+1 \text{ /} k.$$

As a preparation for Case 2, note that we can list the subgroups $H \subset (\mathbb{Z}/p)^2$ as $0 \times (\mathbb{Z}/p)$, $\langle (1, i) \rangle$, $i = 0, \ldots, p-1$.

In other words, given a subgp $H \subset (\mathbb{Z}/p)^2$ different from $0 \times \mathbb{Z}/p$, $H \cap (\{1\} \times \mathbb{Z}/p)$ is a singleton and its unique elt is a generator of H.

Case 2 $\mathrm{char}\, k = p$, E ordinary.

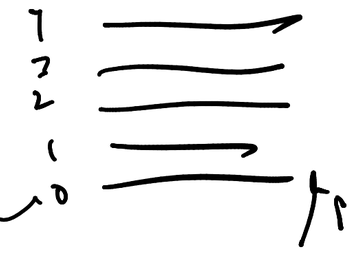
(connected component of the neutral elt.)

As stated above, $E[p] \cong \underline{\mathbb{Z}/p} \times E[p]^\circ$.

Further, we can show that the Weil pairing induces an isomorphism between $E[p]^\circ$ and the "Cartier dual" of $\underline{\mathbb{Z}/p}$: $E[p]^\circ \cong \mu_p$, the gp scheme of p-th roots of unity / k (i.e. $\mu_p := \ker(\mathbb{G}_{m,k} \longrightarrow \mathbb{G}_{m,k},\ z \mapsto z^p)$).

Note that when $\mathrm{char}\, k \neq p$, k alg. cl., then $\mu_{p,k} \cong \underline{\mathbb{Z}/p}$, so the same description for $E[p]$ holds. ∎

So we need to determine, for



k alg. cl. of char $p > 0$, $\mathrm{Sub}_p(\overline{\mathbb{Z}/p \times \mu_p})$ the scheme of subgroup schemes of order p.

We write $\mathrm{Sub}_p(\mathbb{Z}/p \times \mu_p) = \underline{\{\{0\} \times \mu_p\}} \cup \underline{U}$

open complement

$\cong \mathrm{Spec}\, k$,

closed pt

Claim $U \cong \mu_{p,k}$.

Proof of claim For $H \in U(S)$, all $H \cap (\{i\} \times \mu_p)$, $i \in \mathbb{Z}/p$, are isomorphic (take $i \neq 0$ s.t. the intersection is non-empty and use the group structure).

Since H has rk p of order p, each of these intersections is rk 1 over S, so $\cong S$. Thus

$H \cap (\{1\} \times \mu_p)$ defines $S \to \mu_p$ so get $U \to \mu_{p,k}$

Conversely, $S \xrightarrow{h} \mu_p$ defines $H = \bigcup_{i \in \mathbb{Z}/p} \{i\} \times (i \cdot h(S))$.

Since U/k finite, we see that $U \subseteq \mathrm{Sub}_p(\mathbb{Z}/p \times \mu_p)$ is closed, so the decomposition $\mathrm{Sub}_p(\mathbb{Z}/p \times \mu_p) = \mathrm{Spec}\, k \amalg \mu_{p,k}$ is the compos. into (two) conn. comp. Also see: degree is $p+1$.

Remark. Note that we cannot "control the factors" in this argument:

If V denotes the (open) complement of the closed point $\mathbb{Z}/p \times \{\zeta\}$, we do not get a map

$$V(S) \ni H \longmapsto H \cap \textcircled{?}$$

no way to invert the closed embedding.

Case 3 $\mathrm{char}\, k = p$, E supersingular

We skip this case. See the lecture notes by Mihatsch, Lecture 17: One can write down $E[p]$ explicitly and then explicitly compute the scheme $\mathrm{Sub}_p(E[p])$.

Remark In [Katz-Mazur] the flatness part of the theorem is shown by a different approach: They first prove that the moduli problem $\mathcal{M}_1(p)$ with $\Gamma_1(p)$-level (+ auxiliary level-N structure) $p \nmid N$ is representable by a scheme that is finite flat over $\mathcal{M}_N$. Since the forgetful morphism $\mathcal{M}_1(p) \to \mathcal{M}_0(p)$ can be shown to be faithfully flat, it follows that $\mathcal{M}_0(p)$ is flat $/\mathcal{M}_N$.

Moreover they show that $\mathcal{M}_1(p)$ is a regular scheme. Since $\mathcal{M}_1(p) \to \mathcal{M}_0(p)$ is finite flat, this implies that $\mathcal{M}_0(p)$ is regular, too.

Note that the flatness of $\mathcal{M}_0(p)$ over $\mathcal{M}$ has the following non-obvious corollary:

Cor. Let $N \geq 3$, $p \nmid N$. Then $\mathcal{M}_0(p) \underset{\mathcal{M}}{\times} \mathcal{M}_N$ is flat over $\mathbb{Z}[\frac{1}{N}]$.

Finally, let us analyze the geometry of the "fiber at p" of $\mathcal{M}_0(p)$ more precisely.

We fix an integer $N \geq 3$, $p \nmid N$, and redefine $\mathcal{M}_0(p) := \mathcal{M}_0(p) \underset{\mathcal{M}}{\times} \mathcal{M}_N = \{(E, \alpha, H)\}/\simeq$

ell. c. str. | level-N str. | $\subset E[p]$ of order p

With $\overline{\cdot}$ for $\cdot \otimes_{\mathbb{Z}[\frac{1}{N}]} \mathbb{F}_p$.

Note that $\overline{\mathcal{M}_N}$ is smooth/$\mathbb{F}_p$, but could consist of several connected components. We sometimes implicitly restrict to one connected component in the discussion below.

Let S be a scheme of characteristic p, i.e. $p = 0 \in \mathcal{O}_S$.

E/S ell. c. $\rightsquigarrow$ $F_{E/S} : E \to E^{(p)}$ (rel.) Frobenius,

$V_{E/S} : E^{(p)} \to E$ "Verschiebung",

defined as $V_{E/S} := F^{\vee}_{E/S} = "\frac{1}{p} F_{E/S}"$

the unique elt $V \in \mathrm{Hom}_S(E^{(p)}, E)$ s.t. $VF = p$.

Both $F_{E/S}, V_{E/S}$ are isogenies of degree p.

One computes that $\ker(F_{E/S}) = V(I^p)$, where I denotes the ideal sheaf defining the neutral element (viewed as a closed subscheme $\subset E$).

From this we obtain a section $\overline{\Phi}$ to the forgetful morphism $\overline{\mathcal{M}_0(p)} \xrightarrow{\pi} \overline{\mathcal{M}_N}$, defined by

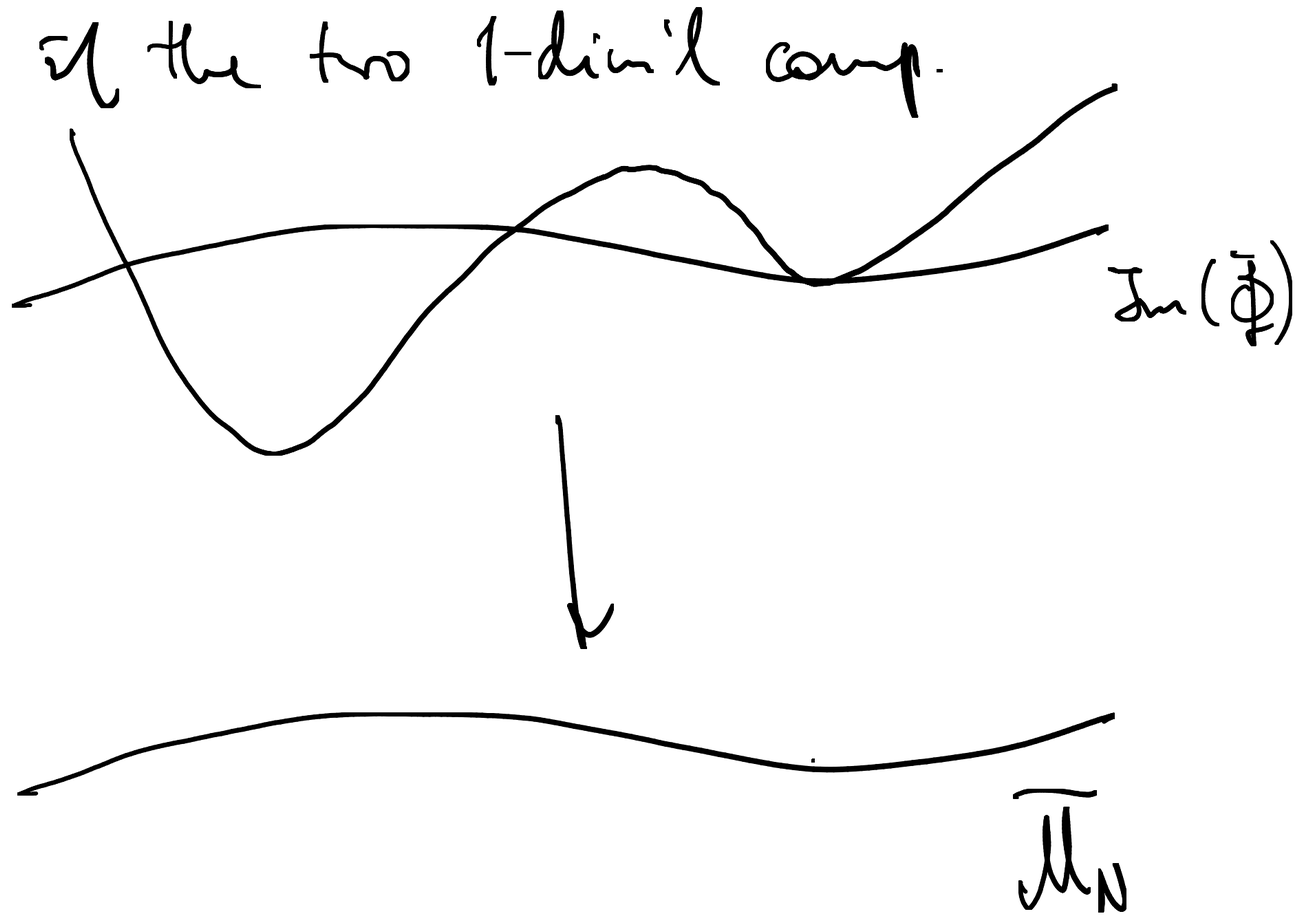
$$\overline{\Phi} : \overline{\mathcal{M}_N} \to \overline{\mathcal{M}_0(p)}, \quad (E, \alpha) \mapsto (E, \alpha, \ker(F_{E/S})).$$

Since $\pi \circ \overline{\Phi} = \mathrm{id}$, $\overline{\Phi}$ is a closed immersion.

Since $\dim \overline{\mathcal{M}_0(p)} = \dim \overline{\mathcal{M}_N} = 1$, $\mathrm{Im}(\overline{\Phi})$ is an irreducible component of $\overline{\mathcal{M}_0(p)}$.

Now $\overline{\mathcal{M}_0(p)} \to \overline{\mathcal{M}_N}$ is finite flat with fibers consisting of 1 or 2 points (and "2" actually occurs).

Therefore $\overline{\mathcal{M}_0(p)}$ must contain exactly one other 1-dimensional irreducible component (and possibly further 0-dimensional comp.), which the two 1-dim'l comp. intersect over ordinary points).



(the 1-pt fibers live over the supersingular points of $\overline{\mathcal{M}_N}$)

The locus where the fiber cardinality is 1 is closed in $\overline{\mathcal{M}_N}$, hence finite. Since any elliptic curve admits at most finitely many level-N structures, this proves (again, cf. Problem 33(1)) that there exist at most finitely many supersingular elliptic curves $/\overline{\mathbb{F}}_p$.

To better understand the "ascent" in the component of $\overline{\mathcal{M}_0(p)}$, consider the following map:

$$\omega : \mathcal{M}_0(p) \longrightarrow \mathcal{M}_1(p)$$

$$(E, \alpha, H) \longmapsto (E/H, \alpha', E[p]/H)$$

- living (E,H) as a degree p isogeny $E \to E/H =: E'$, this
- maps $E \to E'$ to the dual
- isogeny $E' \to E$.

where

$$\begin{array}{ccccc} (\mathbb{Z}/N)^2 & \xrightarrow{\sim} & E[N] & \subset & E \to E/H \\ & \searrow^{\sim} & & & \downarrow \wr \\ & \alpha' & \longrightarrow & & (E/H)[N] \end{array}$$

Then $\omega^2 : (E, \alpha, H) \longmapsto (E, p\alpha, H)$ is an automorphism, hence ω itself is an automorphism of $\mathcal{M}_0(p)$ $\uparrow$ $(p \nmid N)$

Now consider the composition

$$\overline{\omega} \circ \Phi : \overline{\mathcal{M}_N} \longrightarrow \overline{\mathcal{M}_0(p)}, \quad (E, \alpha) \mapsto \left(E^{(p)}, F_{E/S} \circ \alpha, \ker(V_{E/S})\right)$$

Since ω is an automorphism, $\overline{\omega} \circ \Phi$ is a closed immersion, too.

Claim $\overline{\mathrm{Ims}(\varphi)} = \mathrm{Im}(\overline{\Phi}) \cup \mathrm{Im}(w \circ \overline{\Phi})$

and $\mathrm{Im}(\overline{\Phi}) \cap \mathrm{Im}(w \circ \overline{\Phi}) = \{(E, \alpha, H);\ E \text{ supersingular}\}$ (as sets)

Proof of claim As explained above, it is enough to check the second claim.

'$\supseteq$' must hold since each of $\mathrm{Im}(\overline{\Phi})$, $\mathrm{Im}(w \circ \overline{\Phi})$ projects onto $\overline{\mathcal{M}_N}$ but the fibers over supersingular points in $\overline{\mathcal{M}_N}$ contain only one point.

'$\subseteq$' Let k be alg. closed and consider a k-point in the intersection

$\rightsquigarrow$ $(E, \alpha, \ker(F_{E/k})) \cong (E'^{(p)}, \alpha', \ker(V_{E'/k}))$

$\rightsquigarrow$ $\ker(V_{E'/k})$ topologically has only one point

$\rightsquigarrow$ $V_{E'/k}$ purely inseparable

Thus E' is supersingular. (Since being supersingular is preserved under isogenies, the same holds for E.)

Have shown now:

- $\overline{\mathcal{M}_0(p)}$ is the union of two copies of $\overline{\mathcal{M}_N}$, and the two copies intersect precisely in the supersingular points
- One of the two copies projects down to $\overline{\mathcal{M}_N}$ via the identity morphism (since Φ is a section).

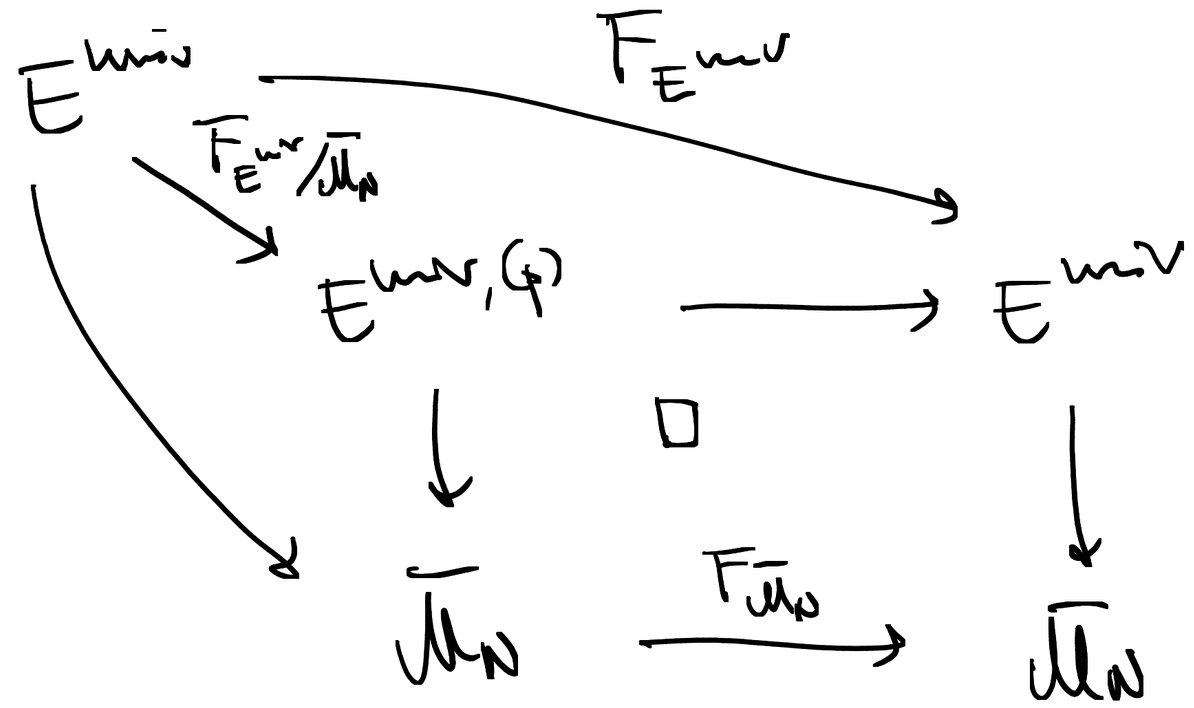
Since $\overline{\mathcal{M}_0(p)}$ is finite flat of degree $p+1$ over $\overline{\mathcal{M}_N}$, the other component has degree p over $\overline{\mathcal{M}_N}$, i.e. the restriction of $\overline{\mathcal{M}_0(p)} \to \overline{\mathcal{M}_N}$ to $\mathrm{Im}(\omega \circ \Phi)$ is given by a degree p morphism $\overline{\mathcal{M}_N} \to \overline{\mathcal{M}_N}$.

We will show next that this is the Frobenius morphism $F_{\overline{\mathcal{M}_N}}$ $(= F_{\overline{\mathcal{M}_N}/\mathbb{F}_p})$ of $\overline{\mathcal{M}_N}$.

<u>Lemma</u> We have a commutative diagram

$$\begin{array}{ccc} \overline{\mathcal{M}_0(p)} & \xrightarrow{\overline{\omega}} & \overline{\mathcal{M}_0(p)} \\ \downarrow & & \downarrow \\ \overline{\mathcal{M}_N} & \xrightarrow{F_{\overline{\mathcal{M}_N}}} & \overline{\mathcal{M}_N} \end{array}$$

Proof of Lemma. Consider $E^{univ} \to \overline{\mathcal{M}}_N$ univ. ell. curve and



$\rightsquigarrow E^{univ,(p)} \cong E^{univ}/\ker F_{E^{univ}/\overline{\mathcal{M}}_N}$.

For any $\mathbb{F}_p$-scheme S, the map

$F_{\overline{\mathcal{M}}_N} : \overline{\mathcal{M}}_N(S) \to \overline{\mathcal{M}}_N(S)$

is given by (ignoring the level structure to simplify the notation; since all maps here induce isomorphisms on the N-torsion there is no problem with this):

$$S \xrightarrow{f} \overline{\mathcal{M}}_N \quad \widehat{\cong} \quad E/S = E^{univ} \times_{\overline{\mathcal{M}}_N, f} S \longmapsto E^{univ,(p)} \times_{\overline{\mathcal{M}}_N, f} S$$

$$= E^{univ} \times_{\overline{\mathcal{M}}_N, F_{\overline{\mathcal{M}}_N}} \overline{\mathcal{M}}_N \times_{\overline{\mathcal{M}}_N, f} S = E^{univ} \times_{\overline{\mathcal{M}}_N, F_{\overline{\mathcal{M}}_N} \circ f} S$$

$$= E^{univ} \times_{\overline{\mathcal{M}}_N, f \circ F_S} S = E^{(p)}.$$

$F_{\overline{\mathcal{M}}_N} \circ f = f \circ F_S$

"Frobenius commutes with any morphism"

I.e., $\overline{\mathcal{M}}_N(S) \longrightarrow \overline{\mathcal{M}}_N(S)$

$(E, \alpha) \longmapsto (E^{(p)}, \alpha^{(p)})$

pullback of α

and this proves the lemma.

Remark (The ordinary locus)

Let $\overline{\mathcal{M}}_N^{ord} = \overline{\mathcal{M}}_N \setminus \{(E,\alpha);\ E \text{ supersing.}\}$ ← finite set of closed pts

$\subset \overline{\mathcal{M}}_N$ open

and let $\overline{\mathcal{M}_0(p)}^{ord}$ be the inverse image of $\overline{\mathcal{M}}_N^{ord}$ in $\overline{\mathcal{M}_0(p)}$ $(= \overline{\mathcal{M}_0(p)} \setminus \{(E,\alpha,H);\ E \text{ supersing.}\})$

↑ finite set of closed pts

Then $\overline{\mathcal{M}_0(p)}^{ord}$ consists of two connected components, each of which is isomorphic to $\overline{\mathcal{M}}_N^{ord}$.

One of the components maps to $\overline{\mathcal{M}}_N^{ord}$ via the identity morphism. This component can be characterized by "(all fibres of) H are connected".

The other component maps to $\overline{\mathcal{M}}_N^{ord}$ via the Frobenius morphism. It can be characterized by "H étale".

The key point one needs to show here is that these two conditions are open conditions (for "étale" this is more or less clear; then apply Grothendieck duality).

The map ι exchanges these two connected components of $\overline{M_0(\varphi)}^{ord}$.

This description shows in particular that $\overline{M_0(\varphi)}^{ord}$ is smooth / $\mathbb{F}_q$. Hence $M_0(\varphi) \setminus \{(E,\alpha,H);\ E \text{ supersingular}\}$ is smooth / $\mathbb{Z}[\frac{1}{N}]$.

With more effort one can show that in the supersingular points the two irreducible components of $\overline{M_0(\varphi)}$ intersect transversally, so these points are "ordinary double points".

Moreover, $M_0(\varphi)$ can be shown to be a regular scheme. (NB $M_0(\varphi)$ is not smooth / $\mathbb{Z}[\frac{1}{N}]$, $\overline{M_0(\varphi)}$ is not regular (in fact not even normal))

References.
[Deligne-Rapoport]
[Mihatsch, Lecture Notes]