We proved representability of two moduli functors so far:

$$N \geq 3, \quad (p, N) = 1 \qquad S \in Sch/_{\mathbb{Z}[\frac{1}{N}]}$$

$$\mathcal{M}_N(S) := \{(E, \alpha) \mid E/S \text{ EC}, \ \alpha: \underline{\mathbb{Z}/N}_S^{\oplus 2} \xrightarrow{\cong} E[N]\}/_{\cong}$$

$$\mathcal{M}_{N,p}(S) := \{(E, \alpha, C) \mid (E,\alpha) \in \mathcal{M}_N(S)$$
$$C \subseteq E \text{ subgroup s.th. } C \to S \text{ fin. loc. free deg } p\}/_{\cong}$$

Our next aim is to better understand the structure of these schemes. We begin with $\mathcal{M}_N$.

§ Properties of $\mathcal{M}_N$

<u>Thm</u> $\mathcal{M}_N$ is an affine scheme. The structure map

$$\mathcal{M}_N \longrightarrow \operatorname{Spec} \mathbb{Z}[\tfrac{1}{N}] \text{ is smooth of rel dim } 1.$$

<u>Proof</u> Affineness follows from construction:

:) Recall that we showed (by hand) that $\mathcal{M}_3$ is representable by open affine $\subseteq \mathbb{A}^1_{\mathbb{Z}[\frac{1}{3}, \zeta_3]}$

:) Then we passed to $\mathcal{M}_{3N} \longrightarrow \mathcal{M}_3[\frac{1}{N}]$, which we established on finite étale cover. In ptic, $\mathcal{M}_{3N}$ affine.

·) Then we showed

$$\mathcal{M}_N[\tfrac{1}{3}] \cong \ker\left(GL_2(\mathbb{Z}/3N) \to GL_2(\mathbb{Z}/N)\right) \backslash \mathcal{M}_{3N}.$$

Since $G \backslash \operatorname{Spec} A = \operatorname{Spec} A^G$, thus quotient is affine

·) Similar arguments apply to $\mathcal{M}_N[\tfrac{1}{2}]$ (omitted).

Hence $\mathcal{M}_N \to \operatorname{Spec} \mathbb{Z}[\tfrac{1}{N}]$ affine morphism to affine scheme.

$\Rightarrow$ $\mathcal{M}_N$ affine.

Finite presentation (= fin. type since $\mathbb{Z}[\tfrac{1}{N}]$ noetherian)

1st proof (constructional)

$\mathcal{M}_3$ fin. pres $\Rightarrow$ $\mathcal{M}_{3N}$ fin pres. (same $\mathcal{M}_4$)

Prop [AV Lect 14] X/S affine, finite type

G/S fin loc free, $G \curvearrowright X$. Then $G \backslash X \to S$ fin type. $\square$

Apply this to $\mathcal{M}_N[\tfrac{1}{3}] = K \backslash \mathcal{M}_{3N}$.

<u>2nd proof</u> <u>Prop</u> [Stacks 01ZC] For $f: X \to S$ equiv:

1) f locally fin. presentation

2) $\forall$ inverse systems of affine S-schemes $(T_i)_{i \in I}$,

$$\varinjlim_{i \in I} X(T_i) \xrightarrow{\ \cong\ } X\big(\varprojlim_{i \in I} T_i\big)$$

In our lecture on noetherian approximation, we showed that this is satisfied for $X = \mathcal{M}_N$.

<u>Smoothness</u>

<u>1st proof</u> (Lifting Criterion) To show: Existence of dotted arrow locally on S.

$S_0 = V(I)$

$I^2 = 0$

$$\begin{array}{ccc} S_0 & \xrightarrow{x_0} & \mathcal{M}_N \\ {\scriptstyle f}\downarrow & \overset{\exists}{\nearrow} & \downarrow \\ S & \longrightarrow & \operatorname{Spec} \mathbb{Z}[\tfrac{1}{N}] \end{array}$$

<u>Translation</u> Let $x_0 \leftrightarrow (E_0, \alpha_0)/S_0$.

To show: Zariski-locally on S, there is (E, α) s.t.

$$S_0 \times_S (E, \alpha) \cong (E_0, \alpha_0).$$

wlog, $S = \operatorname{Spec} R$ affine, $S_0 = \operatorname{Spec} R_0$

Recall Hodge bundle $\omega_{E_0/S_0} = e^* \Omega^1_{E_0/S_0}$.

Seen at beginning: If ω_{E_0/S_0} trivial, E_0 has Weierstraß description

$$E_0 \cong V_+ (Y^2 Z + \dots) \subseteq \mathbb{P}^2_{R_0}$$

Choose lifts of coefficients to R $\Longrightarrow$ $\exists$ EC E/S

s.th. $S_0 \times_S E \cong E_0$.

<u>Next</u> $E[N] \longrightarrow S$ étale since $N \in \mathcal{O}_S^\times$.

Apply lifting criterion:

$$\begin{array}{ccc} S_0 & \xrightarrow{\alpha} & E[N] \\ \downarrow & \overset{\exists!}{\nearrow} & \downarrow \\ S & = & S \end{array} \quad \Longrightarrow \exists \text{ deformation } (E, \alpha)/S \text{ as demanded.}$$

Relative dimension is 1 since it is so generically.

2nd <u>proof</u> $\mathcal{M}_3, \mathcal{M}_4 \to \operatorname{Spec} \mathbb{Z}$ are smooth by explicit computation.

$\mathcal{M}_{3N} \longrightarrow \mathcal{M}_3$, $\mathcal{M}_{4N} \longrightarrow \mathcal{M}_4$ étale, hence also smooth$/\mathbb{Z}$.

The maps $\mathcal{M}_{3N} \to \mathcal{M}_N[\frac{1}{3}]$, $\mathcal{M}_{4N} \to \mathcal{M}_N[\frac{1}{2}]$ are torsors for the constant group $\ker(GL_2(\mathbb{Z}/k\cdot N) \to GL_2(\mathbb{Z}/N))$ $k = 3, 4$.

(Recall: This is because that group acts freely.)

In partic, $\mathcal{M}_{kN} \to \mathcal{M}_N[\frac{1}{k}]$ are étale surjective.

Smoothness being étale local $\Rightarrow$ $\mathcal{M}_N$ is smooth. $\square$

§ Properties of $\mathcal{M}_{N,p}$

First I recall the construction of $\mathcal{M}_{N,p}$:

Given G/S fin loc free group sch + $d \geq 1$, we considered

$$\mathrm{Sub}_{d,G} : \mathrm{Sch}/S \to \mathrm{Set}$$
$$(u: T \to S) \mapsto \{ H \subseteq T \times_S G \text{ subgroup sch s.th. } H \to S \text{ fin loc free rank } d \}$$

<u>Prop</u> $\mathrm{Sub}_{d,G} \to S$ representable by projective scheme.

<u>Thm</u> (Deligne, cf. Oort - Tate)

Let $G \to S$ be finite loc free <u>commutative</u> group scheme of order n. Then $n G = 0$, i.e.

$n \cdot g = 0 \;\; \forall \; g \in G(T)$, $T \to S$.

Equivalently,
$$\begin{array}{ccc} G & \xrightarrow{[n]} & G \\ & \searrow \quad \nearrow_{e} & \\ & S & \end{array}$$
commutes.

<u>Application</u> $C \subseteq E/S$ subgroup of order p
(i.e. $C \to S$ fin loc free order p)

Then $p \cdot C = 0$, i.e. $C \subseteq E[p]$.

$\Longrightarrow \mathcal{M}_{N,p} = \mathrm{Sub}_{p,\, \mathcal{E}[p]} \longrightarrow \mathcal{M}_N$
where $(\mathcal{E}, \alpha)/\mathcal{M}_N$ universal.

(<u>Rmk</u> Above Thm also conjectured for G not nec commutative. Known for certain cases of S.)

Prop i) $\mathcal{M}_{N,p}[\frac{1}{p}] \to \mathcal{M}_N[\frac{1}{p}]$ is finite étale, deg $p+1$.

ii) $\mathcal{M}_{N,p} \to \mathcal{M}_N$ still finite loc free of deg $p+1$.

Proof Finiteness first. We know $\mathcal{M}_{N,p} \to \mathcal{M}_N$ projective, so quasi-finite suffices.

Given $(E,\alpha) \in \mathcal{M}_N(k)$, $k=\bar{k}$, need to see that there are only fin many $C \subseteq E$ of order p.

3 cases:

char $k \neq p \Rightarrow E[p] \cong (\mathbb{Z}/p)^2 \Rightarrow p+1$ many $C \subseteq E[p]$

char $k = p$, E ordinary

$\Rightarrow E[p] \cong \mu_p \times \mathbb{Z}/p \Rightarrow 2$ possible C: $C = \mathbb{Z}/p$ or μ_p.

char $k = p$ E supersing

$\Rightarrow E[p] \cong \operatorname{Spec} k[\varepsilon]/\varepsilon^{p^2}$

$\Rightarrow$ At most 1 possible C, namely $C \cong \operatorname{Spec} k[\varepsilon]/\varepsilon^p$

(We'll see later that this is indeed a subgroup.)

i) Etaleness of $\mathcal{M}_{N,p}[\frac{1}{p}] \to \mathcal{M}_N[\frac{1}{p}]$:

Given constant group scheme $G = \underline{\Gamma}_S \to S$,

say $\#\Gamma = n$, one finds $\mathrm{Sub}_{d,G} = \underline{\Xi}_S$ with

$$\Xi = \{ H \subseteq \Gamma \text{ subgroup of order } d \}$$

In ptic, $\mathrm{Sub}_{d,G} \to S$ finite étale of degree $\# \Xi$

Moreover, $\mathrm{Sub}_{d,G}$ has the base change property

$$\mathrm{Sub}_{d, T \times_S G} = T \times_S \mathrm{Sub}_{d,G} .$$

(Immediate from its definition.)

Let $\mathcal{E}/\mathcal{M}_N[\frac{1}{p}]$ be universal EC. We know that there exists $U \to \mathcal{M}_N[\frac{1}{p}]$ étale surjective s.th.

$$U \times_{\mathcal{M}_N} \mathcal{E}[p] \cong \underline{(\mathbb{Z}/p)}^{\oplus 2}_U .$$

$$\Longrightarrow \quad U \times_{\mathcal{M}_N} \mathcal{M}_{N,p}[\tfrac{1}{p}] \cong \underline{\mathbb{P}^1(\mathbb{F}_p)}_U$$

is a constant scheme, in ptic fin. étale.

Since being étale is étale local on target,

$\mathcal{M}_{N,p}[\frac{1}{p}] \to \mathcal{M}_N$ itself étale.

ii) $\mathcal{M}_{N,p} \xrightarrow{\pi} \mathcal{M}_N$ fin flat deg $p+1$:

$\mathcal{M}_N$ is smooth over $\mathbb{Z}[\frac{1}{N}]$, in ptic reduced. We aim to apply the following to $\pi_* \mathcal{O}_{\mathcal{M}_{N,p}}$:

<u>Lemma</u> S reduced noetherian, $\mathcal{E}$ coherent $\mathcal{O}_S$-mod s.th. $\dim_{\kappa(s)} \mathcal{E}(s) = n$ $\forall s$. Then $\mathcal{E}$ loc free rk n.

<u>Proof</u> $\bar{e}_1, \dots, \bar{e}_n \in \mathcal{E}(s)$ a $\kappa(s)$ basis.

$e_1, \dots, e_n \in \mathcal{E}_s$ lifts, defined near s.

Then $\mathcal{O}_S^{\oplus n} \xrightarrow{e_i} \mathcal{E}$ surjective near s by Nakayama + noetherian assumpt.

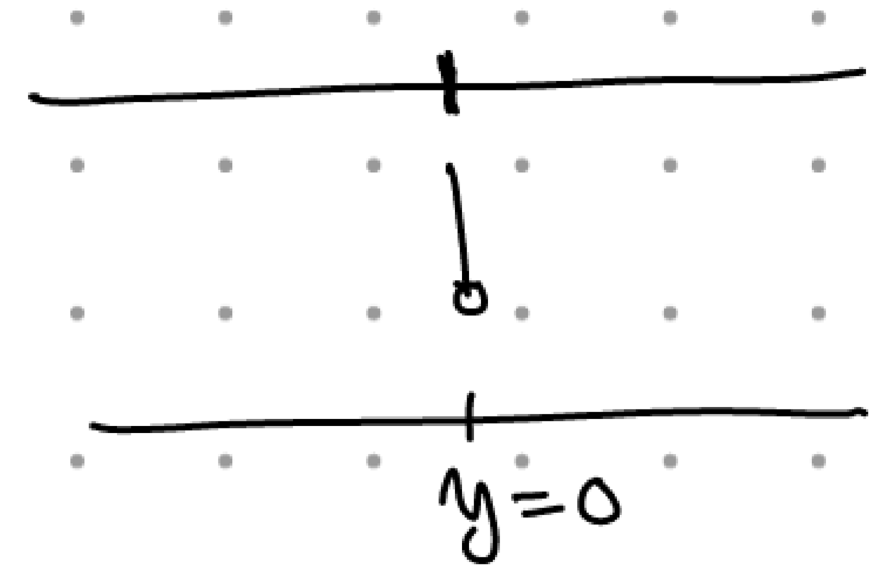
In ptic, $e_i(s') \in \mathcal{E}(s')$ $\kappa(s')$-basis $\forall s'$ near s by assumption.

Thus $\sum \lambda_i e_i = 0 \Rightarrow \lambda_i(s') = 0$ $\forall s'$ near s.

S reduced $\Rightarrow \lambda_i = 0$ near s. $\square$

So we need to show: Each fiber $\operatorname{Spec} k \times_{\mathcal{M}_N} \mathcal{M}_{N,p}$, for $\operatorname{Spec} k \to \mathcal{M}_N$ any, is of order $p+1$.

Intuition



$V(xy, y^2)$

$\downarrow$

$V(y)$

is an iso outside $y=0$, but not flat. Fiber over $y=0$ is of length 2. Such situations we need to exclude.

Prop E/k EC. Then $\mathrm{Sub}_{p, E[p]} \to \operatorname{Spec} k$ of degree $p+1$.

Proof Wlog $k = \bar{k}$.

1) Seen before for char $k \neq p$.

2) char $k = p$, E ordinary

Then $E[p] \cong \mu_p \times \mathbb{Z}/p$ and

$$\mathrm{Sub}_{p, \mu_p \times \mathbb{Z}/p} \cong \operatorname{Spec} k \amalg \mu_p \quad (\text{cf. last lecture})$$

3) char $k = p$, E supersingular

Fact There is a unique non-trivial, p-torsion, self-dual extension of α_p by itself. It equals

$G := \operatorname{Spec} k[x]/x^{p^2}$, $\quad m^*(x) = a + b + F(a^p, b^p)$

where $F(s,t) = \dfrac{s^p + t^p - (s+t)^p}{p} \in \mathbb{Z}[s,t]$

$$= - \sum_{i=1}^{p-1} \frac{\binom{p}{i}}{p} s^i t^{p-i} .$$

and where $a = x \otimes 1$, $b = 1 \otimes x$

Additional Info (cf. Finite Group Schemes lecture by Gebhard Martin)

$k = \bar{k}$. $\exists$ 4 extensions of α_p by itself up to iso:

·) $\alpha_p \oplus \alpha_p$

·) $\alpha_{p^2} := \ker \left(G_a \xrightarrow{x \mapsto x^p} G_a \right)$

·) $\alpha_{p^2}^\vee$

·) above G.

$E[p]$, E supersingular, has 1-dimensional Lie algebra and is self-dual because of Weil pairing

$\Longrightarrow E[p] \cong G$.

Prop G as above. Then $\mathrm{Sub}_{p,G} \cong \mathrm{Spec}\, k[a]/a^{p+1}$.

·) A any k-algebra, $H \overset{i}{\subseteq} \mathbb{A}^1_A$ any closed subscheme s.th. $H/\mathrm{Spec}\, A$ fin loc free deg d.

Write $H = \mathrm{Spec}\, B$, $i^*: A[x] \twoheadrightarrow B$.

Then $x = i^*(x)$ generates B.

Assume first B free as A-module (holds locally on $\mathrm{Spec}\, A$.)

Obtain that $x^d, x^{d-1}, \dots, 1$ are lin dependent since $\mathrm{rk}_A B = d$.

$\multimap$ $\exists$ relation $\sum_i a_i x^i = 0$.

Since $\dim_{\kappa(s)} B(s) = d$ $\forall$ $s \in \mathrm{Spec}\, A$, $a_d \in A^\times$.

$\multimap$ wlog $a_d = 1$, which determines a_i <u>uniquely</u>.

Uniqueness implies extension to case where B only loc. free.

<u>Note</u> In our case $d = p$ and $H \subseteq \mathrm{Spec}\, A[x]/x^{p^2}$

$\Leftrightarrow \left(x^p + \sum_i a_i x^i \right) \mid x^{p^2}$.

Claim On G, $[n]^*(x) = n\cdot x \quad \forall n \geq 1$

Proof By induction, $n=1$ being ok.

Consider $G \xrightarrow{([n], id)} G\times G \xrightarrow{m} G$ on rings:

$$m^*(x) = a+b+F(a^p, b^p)$$

$$\xmapsto{([n],id)^*} nx + x + \underbrace{F((nx)^p, x^p)}$$

$$= -\sum_{i=1}^{p-1} \frac{\binom{p}{i}}{p} \underbrace{\left((nx)^i x^{p-i}\right)^p}_{\text{divided by } x^{p^2}=0}$$

$$=0$$

□

·) So consider $H = V(x^p - \sum_{i=0}^{p-1} a_i x^i) \subseteq A[x]/_{x^{p^2}}$

that is a subgroup. Then stable under all $[n]$,

$$\Rightarrow x^p - \sum n^{i-p} a_i x^i = x^p - \sum a_i x^i \quad \forall n.$$

Thus $a_i = 0$ except for $i=1$,

$$H = V(x^p - cx)$$

·) Using polynomial division, one obtains

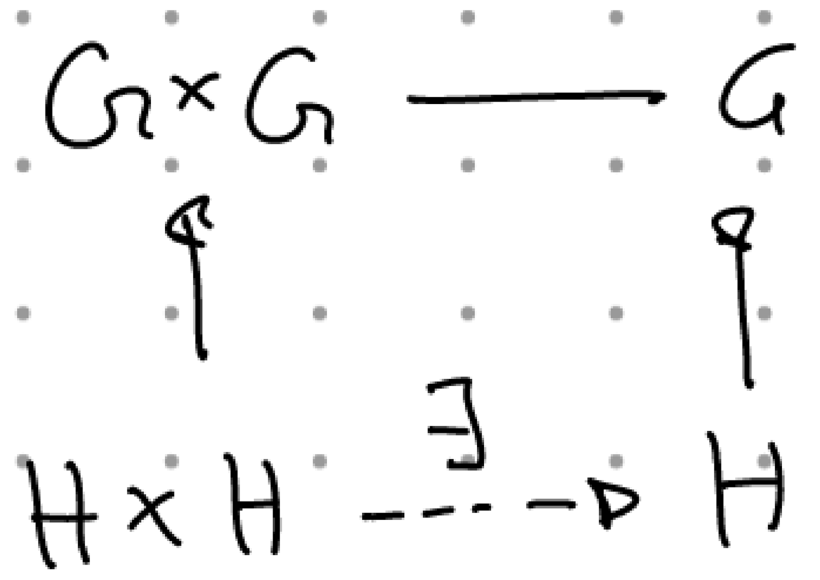
$$x^{p^2} = (x^p - cx)\left(\sum_{i=0}^{p} c^i \, x^{p^2 - i(p-1) - p}\right) + c^{p+1}x.$$

and hence $\quad x^p - cx \mid x^{p^2} \iff c^{p+1} = 0.$

<u>Final Claim</u>

Any $H = V(x^p - cx) \subseteq A \otimes_k G$ is a subgroup.

<u>Proof</u> Need to see factorization



<u>Equivalently</u> $\quad m^*(x^p - cx) \in (a^p - ca) \otimes_k A[b]/b^{p^2}$

$$+ \; A[a]/a^{p^2} \otimes_k (b^p - cb)$$

Compute:

$$m^*(x^p - cx) = \underbrace{a^p + b^p - ca - cb}_{\equiv 0} + \underbrace{F(a^{p^2}, b^{p^2})}_{=0} - cF(a^p, b^p)$$

$$cF(a^p, b^p) \equiv cF(ca, cb)$$

$$= - c \sum_{i=1}^{p-1} \frac{\binom{p}{i}}{p} c^p a^i b^{p-i} \equiv 0$$

∎

Rmk It follows that $\mathcal{M}_{N,p} \longrightarrow \operatorname{Spec} \mathbb{Z}[\frac{1}{N}]$ is flat, which is not at all immediate from definitions.