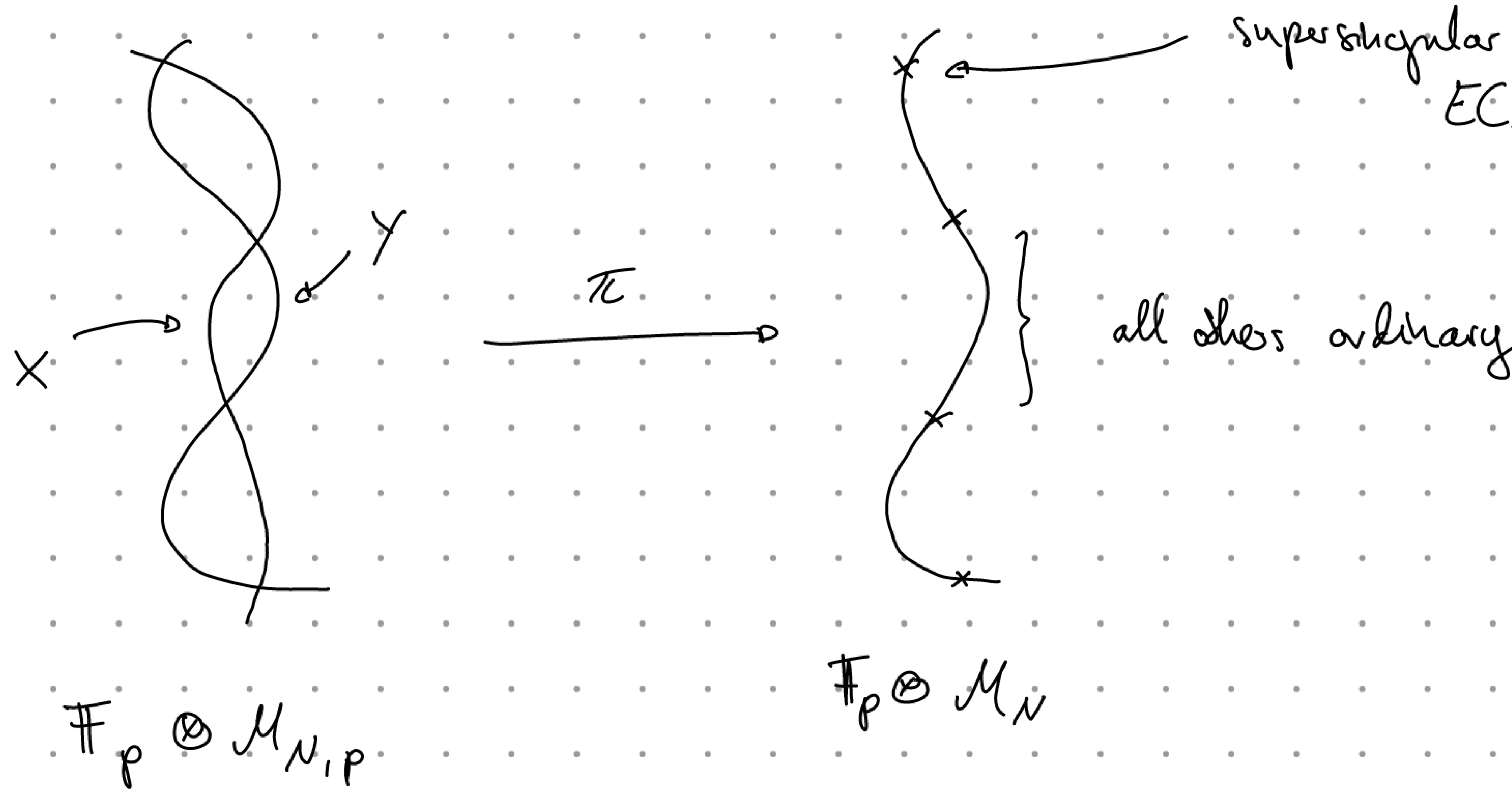
Our next aim is to understand the special fiber $\mathbb{F}_p \otimes_{\mathbb{Z}[\frac{1}{N}]} \mathcal{M}_{N,p}$.

Famous picture:



·) $\mathbb{F}_p \otimes \mathcal{M}_{N,p} = X \cup Y$, both $X, Y \cong \mathbb{F}_p \otimes \mathcal{M}_N$

·) $\pi|_X$ is an isomorphism, $\pi|_Y$ Frobenius

·) X, Y intersect transversally in double points,

there are precisely points above supersingular ECs

·) X^{ord} is locus of (E, α, C) with $C \cong \mu_p$

Y^{ord} —— " —— with $C \cong \mathbb{Z}/p$ $\Big\}$ étale locally.

Note how this picture matches with our computation of fibers of π last lecture.

§ Frobenius & Verschiebung

$X/\mathrm{Spec}\,\mathbb{F}_p$ scheme in char p

$F = F_X : X \to X$ absolute Frobenius defined as

$|F| = \mathrm{id}_{|X|}$, $F^* f = f^p$, $f \in \mathcal{O}_X(U)$.

Given $X \xrightarrow{u} S / \mathrm{Spec}\,\mathbb{F}_p$, obtain diagram

$$\begin{tikzcd}
X \arrow[dr, dashed, "F_{X/S}"] \arrow[drr, bend left, "F_X"] \arrow[ddr, bend right, "u"'] & & \\
& X^{(p)} := S \times_{F,S} X \arrow[r] \arrow[d] \arrow[dr, phantom, "\square"] & X \arrow[d, "u"] \\
& S \arrow[r, "F_S"] & S
\end{tikzcd}$$

<u>Def</u>

$X^{(p)}$ called Frobenius twist of X

$F_{X/S}$ relative Frobenius of X/S

-) If $S = \mathrm{Spec}\,R$, $X = \mathrm{Spec}\,R[t_i]/(f_j)$, then

$X^{(p)} = \mathrm{Spec}\,R[t_i]/(f_j^{(p)})$ $\quad f_j^{(p)} :=$ take coeff of f_j to the p

$F_{X/S}^* : R[t_i]/(f_j^{(p)}) \longrightarrow R[t_i]/(f_j)$, $t_i \longmapsto t_i^p$

Gluing this, we see in particular that

$$(T \times_S X)^{(p)} = T \times_S X^{(p)} \quad \& \quad T \times F_{X/S} = F_{T\times_S X/T}.$$

•) Now consider case of EC in char p, $E \to S$.

Then $F_{E/S} : E \to E^{(p)}$ is a group scheme map since above constructions natural in X.

•) If $S = \operatorname{Spec} k$, one checks that $\deg(F_{E/S}) = p$.

We have the following fibre criterion, cf. Lect. 4 §4.

<u>Prop</u> Assume $E \xrightarrow{f} E'$ homomorph of ECs $/S$ s.th. $\forall s \in S$, $\deg(f(s)) = d$. Then f itself is finite locally free of degree d.

$\Longrightarrow F_{E/S} : E \to E^{(p)}$ is finite loc free of deg p.

$\Longrightarrow \ker(F_{E/S}) \to S$ is finite loc free group sch of order p.

•) Here is a concrete description of $\ker(F_{E/S})$:

<u>Lem</u> Write $e(S) = V(\mathcal{I})$. Then $\ker(F_{E/S}) = V(\mathcal{I}^p)$.

<u>Proof</u> This is a local computation which does not use the fact that E is an elliptic curve.

Let $\mathcal{U} \ni e(s)$ be affine open nbhd of $e(s) \in e(S)$

Assume that $\mathcal{I}|_{\mathcal{U}} \cong \mathcal{O}_{\mathcal{U}} \cdot g$.

(Recall that $\mathcal{I}$ is a Cartier divisor.)

Then $e^{-1}(\mathcal{U}) \subseteq S$ open, cover by $D(f)$, $f \in R$,

replacing S by $D(f)$ and $\mathcal{U}$ by $\mathcal{U} \cap \pi^{-1}(D(f))$,

we end up in a situation

$$\begin{tikzcd} A \arrow[d] \\ R \arrow[u, bend right, "e^*"'] \end{tikzcd} \qquad \mathcal{I} = \ker e^* = (g)$$

Then $e^{(p),*} : A^{(p)} = R \underset{F, R}{\otimes} A \longrightarrow R$

has $\ker e^{(p),*} = (g^{(p)})$ $\quad g^{(p)} = 1 \otimes g$

(If $A = R[t_i]/(f_j)$, then $A^{(p)} = R[t_i]/(f_j^{(p)})$

$$\begin{tikzcd} A \arrow[d, "e^* : t_i \mapsto a_i"] \\ R \end{tikzcd} \qquad \begin{tikzcd} A^{(p)} \arrow[d, "e^{(p),*} : t_i \mapsto a_i^p"] \\ R \end{tikzcd}$$
)

$\ker(F_{E/S}) \cap U$ is now computed by fiber product

$$\begin{tikzcd} A/g^p = ? & R \arrow[l] & r \cdot e^*(a) \\ A \arrow[u] & A^{(p)} \arrow[l] \arrow[u] & r \otimes a \arrow[u, mapsto] \\ r \cdot a^p & r \otimes a \arrow[l, mapsto] & \end{tikzcd}$$

$\square$

<u>Def</u> <u>Verschiebung</u> $V = V_{E/S} : E^{(p)} \longrightarrow E$

is defined as $p \cdot F^{-1} = F^*$

Rosati involution

divided isogeny

It is an isogeny of degree p

<u>Def</u> 1) $w : \mathcal{M}_{N,\rho} \longrightarrow \mathcal{M}_{N,\rho}$

$$(E, \alpha, C) \longmapsto \left(E/C,\ (\mathbb{Z}/N)^{\oplus 2} \xrightarrow{\alpha} E \longrightarrow E/C,\ E[p]/C\right)$$

<u>Note</u> $w^2 = (E, \alpha, C) \longrightarrow (E, p \cdot \alpha, C)$

and $p \cdot \alpha$ again level N-str since $(p, N) = 1$.

2) $\Phi : \overline{\mathcal{M}_N} \longrightarrow \overline{\mathcal{M}_{N,p}}$

$$(E, \alpha) \longmapsto (E, \alpha, \ker F_{E/S})$$

$\Longrightarrow \quad w\Phi : \overline{\mathcal{M}_N} \longrightarrow \overline{\mathcal{M}_{N,p}}$

$(E,\alpha) \longmapsto (E^{(p)}, F_{E/S}\circ\alpha, \ker V_{E/S})$

§ The ordinary locus

AV lecture: If E/k, $\mathrm{char}\, k = p$, is supersingular, then $j(E) \in \mathbb{F}_{p^2}$.

Reason: E supersing $\Longrightarrow E[p] = \ker(F^2_{E/k} : E \longrightarrow E^{(p^2)})$

(E Dedekind $\longrightarrow \exists!$ length p^2 subscheme at e.)

Thus $j(E) = j(E/E[p]) = j(E^{(p^2)}) = j(E)^{p^2}$.

The j-invariant map $j : \overline{M_N} \longrightarrow \mathbb{A}^1_{\mathbb{F}_p}$ is quasi-finite b/c a given EC has at most $|GL_2(\mathbb{Z}/N)|$ many level structures up to isomorphism.

$\Longrightarrow \overline{\mathcal{M}_N} = \overline{\mathcal{M}_N}^{\mathrm{ord}} \cup \overline{\mathcal{M}_N}^{ss}$ (set-theoretically disjoint)

with $\overline{\mathcal{M}_N}^{\mathrm{ord}}$ Zariski open "ordinary locus"

& $\overline{\mathcal{M}_N}^{ss}$ Zariski closed "supersingular locus"

We now study $\underbrace{\mathcal{M}_{N,p} \setminus \overline{\mathcal{M}}_{N,p}^{ss}}_{\text{defined analogously.}} \longrightarrow \mathcal{M}_N \setminus \overline{\mathcal{M}}_N^{ss}$.

Recall that we have Cartier duality

$\star\ \mathcal{C}^{\circ}$ {fin. comm. loc free grp sch G/S }

$G^{\star}(T) = \mathrm{Hom}(G_T, \mathbb{G}_{m,T})$

We know: $\underline{\mathbb{Z}/N}_S^{\star} = \mu_{N,S}$

$\Longrightarrow$ { G/S finite étale }

$= \{ G/S$ s.th. $\exists$ étale surjective $U \to S$ with $U \times_S G \cong \Gamma_U$ some finite $\Gamma \}$

$\underset{\star}{\cong} \{ H/S\ \exists$ such U with $U \times_S H \cong \bigoplus_i \mu_{n_i, U} \}^{op}$

Def Such H/S called <u>multiplicative</u>.

Moreover finite loc free G/S is étale

$\iff \Omega^1_{G/S} = 0$

$\iff \Omega^1_{G/S}(s) = 0 \quad \forall s \in S$

$\iff G(s)$ étale $\forall s \in S$.

(Fiber criterion for étaleness for flat morphisms.)

Thus H/S multiplicative $\iff H(s)$ mult. $\forall s \in S$.

<u>Prop</u> $\overline{\mathcal{M}}^{ord}_{N,p} = A_{N,p} \amalg B_{N,p}$

$A_{N,p} = \{(E, \alpha, C) \mid C \text{ multiplicative}\}$

$B_{N,p} = \{(E, \alpha, C) \mid C \text{ étale}\}$

Each $A_{N,p}$, $B_{N,p}$ is isomorphic to $\overline{\mathcal{M}}^{ord}_{N,p}$. In particular, $\mathcal{M}_{N,p} \setminus \overline{\mathcal{M}}^{ss}_{N,p} \longrightarrow \operatorname{Spec} \mathbb{Z}[\frac{1}{N}]$ is smooth.

<u>Proof</u> We know that for every point $x = (E, \alpha, C) \in \mathcal{M}^{ord}_{N,p}(k)$, C either étale or multiplicative.

Let $(\mathcal{E}, \alpha, \mathcal{C})$ be universal triple.

·) $\mathcal{C}(x)$ étale $\Leftrightarrow$ $\Omega^1_{\mathcal{C}/\overline{M}^{ord}_{N,p}}(x) = 0$

$\Rightarrow$ $\Omega^1 = 0$ in open nbhd of x.
(Supp Ω^1 is closed)

$\Rightarrow$ $\mathcal{C}$ étale above open nbhd of x.

·) $\mathcal{C}(x)$ multipl. $\Leftrightarrow$ $\mathcal{C}^*(x)$ étale, so

similarly an open property.

$\Rightarrow$ $\overline{M}^{ord}_{N,p} = A_{N,p} \sqcup B_{N,p}$ scheme-theoretically disjoint as claimed.

Next, $w: A_{N,p} \xrightarrow{\cong} B_{N,p}$ interchanges two loci

since $H \subseteq E[p]$ infinitesimal (resp. étale)

$\Leftrightarrow$ $E[p]/H$ étale (resp. infinitesimal)

$\forall$ (fibre-wise) ordinary E/S.

Thus enough to show $\overline{M}_N^{ord} \xrightarrow[\cong]{\Phi} A_{N,p}$.

$(E,\alpha)/S \longmapsto (E,\alpha, \ker F_{E/S})$.

This map is injective because composition w/ $A_{N,p} \to \overline{M}_N^{ord}$ is identity.

<u>Claim</u> Also surjective.

E/S ordinary $\Longrightarrow$ $E[p]/\ker F_{E/S}$ étale

Hence unit section $e : S \to E[p]/\ker F_{E/S}$ open + closed.

It follows that there is a <u>unique</u> infinitesimal order p subgroup $C \subseteq E$, namely connected comp of $e(S)$.

If $(E, \alpha, C) \in A_{N,p}(S)$, then both C & $\ker F_{E/S}$ have this property, hence agree.

$\square$ Claim.

We obtain that $A_{N,p}, B_{N,p} \subseteq \overline{M}_N$ are smooth over $\operatorname{Spec} \mathbb{F}_p$.

Smoothness is open $\Longrightarrow$ $M_{N,p} \setminus \overline{M}_{N,p}^{ss}$ smooth over $\mathbb{Z}[\frac{1}{N}]$. $\square$

<u>Cor</u> $\mathcal{M}_{N,p}$ is normal. <u>Proof:</u>

<u>Serre normality criterion</u> [Stacks 0310]

Noetherian ring R normal

$\Leftrightarrow$ $R_{\mathfrak{p}}$ normal $\forall \mathfrak{p} \subseteq R$ of ht 1

& $R_{\mathfrak{p}}$ Cohen-Macaulay $\forall \mathfrak{p} \subseteq R$ of ht 2.

In our case: $\mathcal{M}_{N,p}$ smooth, hence regular, outside $\overline{\mathcal{M}}_{N,p}^{ss}$ which is of codimension 2.

Moreover, $\mathcal{M}_N$ smooth hence regular.

$\mathcal{M}_{N,p} \to \mathcal{M}_N$ finite flat $\Rightarrow$ $\mathcal{M}_{N,p}$ CM

$\Rightarrow$ $\mathcal{M}_{N,p}$ normal. $\square$

($R \to S$ finite flat, R regular, $f_1, \ldots, f_d \in \mathfrak{m}_R$ reg seq of length $d = \dim R$.

$\Rightarrow$ $f_1, \ldots, f_d$ reg seq of length $\dim S$ in S

$\Rightarrow$ S CM.)

<u>Rmk</u> One may define integral models for all levels by normalization. For example:

$$\mathcal{M}_{3\cdot N} / \mathbb{Z}[\tfrac{1}{3}] := \text{integral closure of } \mathcal{M}_3 \text{ in } \mathcal{M}_{3N}[\tfrac{1}{3N}].$$

However, not clear how to work with these spaces since such a definition is very implicit.

Previous corollary shows that for $\mathcal{M}_{N,p}$, two definitions agree.