

§1 Torsors [BLR 6.4]

General concept: G/S group scheme, $X, Y/S$ schemes

$G \curvearrowright X$, $X \rightarrow Y$ G -invariant.

Def $X \rightarrow Y$ G -torsor def

1) $G \times_S X \xrightarrow{\cong} X \times_Y X$

2) \exists covering $Y' \rightarrow Y$ + section $Y' \times_Y X$
 \downarrow
 Y'

usually split.

Idea Given $T \xrightarrow{y} Y$, (1) says that any
two lifts $T \xrightarrow{x_1, x_2} X$

differs by unique $g \in G(T)$ i.e. $x_2 = g x_1$.

In other words: $\{x \in X(T) \text{ lifting } y\}$

is \emptyset or $\cong G(T)$.

(2) says: \exists covering $T' \rightarrow T$ + $x \in X(T')$ lifting y .

(Exclude e.g. situation $X = \emptyset$.)

"Covering" has to be specified, usually split.

Example 1) $X = \text{Spec } L \longrightarrow Y = \text{Spec } K$

finite Galois w/ Gal. grp. $\Gamma \subset X$

↳ torsor for étale topology:

$$L \otimes_K X = \text{Spec} \left(L \otimes_K L \right) = \Gamma \times_{\mathbb{C}} \text{Spec } L$$

Γ acts by translation.

2) $X \longrightarrow Y$ Spec Γ ~~group~~ of ab vars w/ kernel K .

$$K \times_{\text{Spec}} X \xrightarrow{\cong} X \times_Y X$$

So 1) satisfied. 2) satisfied w/ prof topology

& $Y' = X$ itself.

3) Thm (AV Lect 14) G/S fin loc free, X/S sep.

$G \subset X$ freely (i.e. $G \times_S X \hookrightarrow X \times_S X$ d. immers.)

Assume \exists affine G -stable cover of X

Then Quotient Y exists, $X \longrightarrow Y$ is fin loc free

and $G \times_S X \xrightarrow{\cong} X \times_Y X$. In other words,

$X \longrightarrow Y$ is G -torsor for prof topology.

§2 Gm-torsors Fact: $X \rightarrow Y$ G_m -torsor

for ét/parf/parc top, then \exists Zariski covering

$Y = \cup U_i$ s.t. $X(U_i) \neq \emptyset$.

(This is a consequence of spqc descent for vector bundles. It means torsors for different topologies coincide.)

$\{ \text{Gm-torsors } X \xrightarrow{\pi} Y \} \xrightarrow{\cong} \text{Pic}(Y)$

$\text{Spec } \bigoplus_{i \in \mathbb{Z}} \mathcal{L}^{\otimes i} \longrightarrow \mathcal{L}$

$X \longmapsto \{ \mathcal{L} \in \pi_* \mathcal{O}_X \mid \mu^*(\mathcal{L}) = f^* \mathcal{L} \}$

Setting $X = \text{Spec } A$, $G_m \text{ C } X \longrightarrow A = \bigoplus_{i \in \mathbb{Z}} A_i$
(over $S = \text{Spec } \mathbb{R}$)

Action free $\stackrel{\text{def}}{=} G_m \times X \longrightarrow X \times X$ closed immersion.

Prop If action free, quotient $q: X \rightarrow Y = \text{Spec } A_0$

\rightarrow a G_m -torsor. More precisely, A_1 is a line

bundle / A_0 and $A = \bigoplus_{i \in \mathbb{Z}} A_1^{\otimes i}$ as mng .

Proof $\sum [t^{\pm 1}] \otimes A \xrightarrow{\cong} A \otimes A$
 $f^d \otimes a_i b \xrightarrow{\cong} a \otimes b \quad \deg(a) = d$

being surjective $\Rightarrow f \otimes 1$ is surjective, i.e.

$\exists e_1, \dots, e_r \in A_1, f_1, \dots, f_r \in A_{-1}$

s.t. $1 = \sum e_i f_i \quad u_i = e_i f_i$

Note $\deg(u_i) = 0$, so $\text{Spec } A_0 = \cup D(u_i)$

Claim $D(u_i) \times_Y X \cong_{\text{lim}} D(e_i f_i)$

lim-equivalently.

Proof u_i invertible $\Rightarrow e_i, f_i$ invertible

Given $a \in A_1 [u_i^{-1}]$ may write

$$a = a \left(\sum e_j f_j \right) = a \cdot \underbrace{\left(\sum \frac{e_j f_j}{e_i} \right)}_{\in A_0} \cdot e_i$$

So $A_1 [u_i^{-1}] = A_0 [u_i^{-1}] e_i$ Since e_i invertible in $A [u_i^{-1}]$,

even $A_0 [u_i^{-1}] \xrightarrow{\cdot e_i} A_1 [u_i^{-1}]$

$\Rightarrow A_1$ l.b. over A_0 , trivialized by e_i over $D(u_i)$.

Given $a \in A_d[u_i^{-1}]$, $a = (a \cdot e_i^{-d}) \cdot e_i^d$
 $\in A[u_i^{-1}] \cdot e_i^d$,

Thus the natural map

$$\bigoplus_{i \in \mathbb{Z}} A_{-i} \longrightarrow A \quad \text{is an iso.} \quad \square$$

Important consequence:

$X \rightarrow Y$ has Zariski locally sections
 & these are unique up to G_m -action.

Example $\tilde{M} \rightarrow G_m \backslash \tilde{M} = \text{Spec } \mathbb{Z}[\frac{1}{6}, j]$

does not have sections everywhere

Recall first that if K field, $j \in K$, then \exists

E/K with $j(E) = j$.

$\implies \exists E/\mathbb{Q}(j)$ with $j(E) = j$.

It extends to an open $U \subseteq \mathbb{A}_{\mathbb{Z}}^1 \setminus \{0\}$

Claim $\exists E/R$ $R = \mathbb{Q}(j)_{(j)}$ s.t. $j(E) = j$.

($R =$ local ring at $j=0$ in $\mathbb{A}_{\mathbb{Q}}^1$)

Proof \mathbb{R} local, so E would be given by Weierstrass eqn

$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{R}.$$

Then $\Delta = (\text{const} \neq 0) + \text{higher}$ in $\hat{\mathbb{R}} = \mathbb{Q}[[j]]$

as it lies in $\hat{\mathbb{R}}^*$.

But $j = 1728 \frac{4a^3}{\Delta}$ has no solution in $\hat{\mathbb{R}}$. \square

Rank $j=0 \iff y^2 = x^3 + 1$

has extra auto $x \mapsto \zeta_3 x$
 $y \mapsto y$ / $\mathbb{Q}(\zeta_3)$

CM by $\mathbb{Z}[\zeta_3]$.

Similar argument works at

$$j=1728 \iff y^2 = x^3 + x$$

has auto $x \mapsto -x$
 $y \mapsto iy$ / $\mathbb{Q}(i)$

CM by $\mathbb{Z}[i]$.

§3 Level structure $n \geq 1, n \in \mathcal{O}_S(S)^\times$.

$E \rightarrow S$ ét. Then $E[n] \rightarrow S$ fin. ét. order n^2 .

Two important principles:

1) $X \xrightarrow{f} Y$ fin. ét. Then f open & closed

·) closed since finite

·) open since flat, loc. fin. pres. maps are open
(Stacks 01UA.)

2)
$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ & \searrow u & \swarrow v \\ & S & \end{array}$$
 u, v fin. ét. $\implies f$ fin. étale.

Example $X \rightarrow S$ fin. ét. of deg d .

Then $\exists S' \rightarrow S$ fin. ét. s.t. $S' \times_S X \cong \coprod S'$

Proof by induction on d , $d=1$ being $X=S$.

$\Delta: X \rightarrow X \times_S X$ fin. ét. by principle 2),

hence $X \times_S X = \Delta \coprod (\text{orb})$ by principle 1). \square

Prop $n \in \mathbb{O}_S(S)^\times$, $E/S \in \mathcal{C}$. Then $\exists S' \rightarrow S$

fu et. s.t. $S' \times_S E[n] \cong (\mathbb{Z}/n)^{\oplus 2} S'$.

Proof of Prop Example yields $S' \rightarrow S$ fu. et.

$$S' \times_S E[n] \cong \coprod_{i \in I} S' \quad |I| = n^2$$

Denote sections by t_i , $i \in I$.

For $a, b \in \mathbb{Z}/n$, $S'_{a,b,i,j} = (at_i + bt_j) \cap e(S') \subseteq S'$

is open + closed, since $(at_i + bt_j) \cap e(S') \rightarrow e(S')$
is fu. étale.

$$\Rightarrow S' = S'_{a,b,i,j} \sqcup S'_{a,b,r,j}$$

Now given $s \in S'$, we know $\text{Spec } \mathcal{O}_S(S) \times_S E[n] = (\mathbb{Z}/n)^{\oplus 2}$.

Pick i, j s.t. t_i, t_j provide basis at s .

Only for many a, b exist

$$\Rightarrow \exists S' = S'_{i,j} \sqcup S'_{i,j}^c \text{ where}$$

$$t_i t_j: \mathbb{Z}/n^{\oplus 2} S'_{i,j} \xrightarrow{\cong} S'_{i,j} \times_S E[n]$$

Varying s finishes the proof. \square

Prop E/S as before. The functor

$$L_{E,n} : \mathcal{S}/S \rightarrow \mathcal{S}b$$

$$T/S \longmapsto \left\{ \alpha : \underline{\mathbb{Z}/n}_{\mathbb{T}}^{\oplus 2} \xrightarrow{\cong} T \times_S E[n] \right\}$$

\Rightarrow representable + fin. étale $/S$. $L_{E,n} \rightarrow S$ is

a $GL_2(\mathbb{Z}/n)$ -torsor (for étale topology).

Remark 1) Group homo $\alpha : \underline{\mathbb{Z}/n}_{\mathbb{T}}^{\oplus 2} \rightarrow T \times_S E[n]$ is

same as two $\alpha_1, \alpha_2 \in E[n](\mathbb{T})$.

2) $GL_2(\mathbb{Z}/n) \subset L_{E,n}$ as $g \cdot \alpha = \alpha \circ g$.

Proof Consider $X := E[n] \times_S E[n]$.

Then $X(\tau) = \text{Hom}(\underline{\mathbb{Z}/n}_{\tau}^{\oplus 2}, \tau \times_S E[n])$

If $a, b \in (\mathbb{Z}/n)^2 \setminus \{(0,0)\}$, have

$$m_{a,b} : X \rightarrow E[n]$$

$$(\alpha_1, \alpha_2) \mapsto (a\alpha_1, b\alpha_2)$$

It is finite étale. Then

$$B_{a,b} := X \times_{m_{a,b}, E[n], e} S \rightarrow X$$

is open and closed.

$B_{a,b} = \text{locus}$
where a, b
give non-trivial
dependence relation
of α_1, α_2 .

$X \setminus \bigcup_{(a,b) \neq (0,0)} B_{a,b} = L_{E,n}$ is
dense for space.

We know $\exists T \rightarrow S$ for étale s.k.

$$\tau \times_S E[n] \cong \underline{\mathbb{Z}/n}_{\tau}^{\oplus 2}$$

So $\tau \times_S \text{Iso}(\underline{\mathbb{Z}/n}_S^{\oplus 2}, E[n])$ giving tensor
property.

$$\cong \text{Iso}(\underline{\mathbb{Z}/n}_{\tau}^{\oplus 2}, \underline{\mathbb{Z}/n}_{\tau}^{\oplus 2}) \cong \underline{\text{GL}}_2(\mathbb{Z}/n)_{\tau}, \quad \square$$

Def Iso of ECs w/ level- n -str $(E, \alpha), (E', \alpha')$

def Iso $\phi: E_1 \xrightarrow{\cong} E_2$ s.t. $\alpha_2 = \phi \circ \alpha_1$

$$M_n: \text{Sch}/\mathbb{Z}[\frac{1}{n}]^{\text{op}} \longrightarrow \text{Set}$$

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

$$\tilde{M}_n: \text{Sch}/\mathbb{Z}[\frac{1}{6n}]^{\text{op}} \longrightarrow \text{Set}$$

$$S \longmapsto \{(E, \alpha, \pi) \mid \begin{array}{l} (E, \pi) \in \tilde{M}(S) \\ \alpha \in L_{E,n}(S) \end{array}\} / \cong$$

Cor \tilde{M}_n is an affine scheme

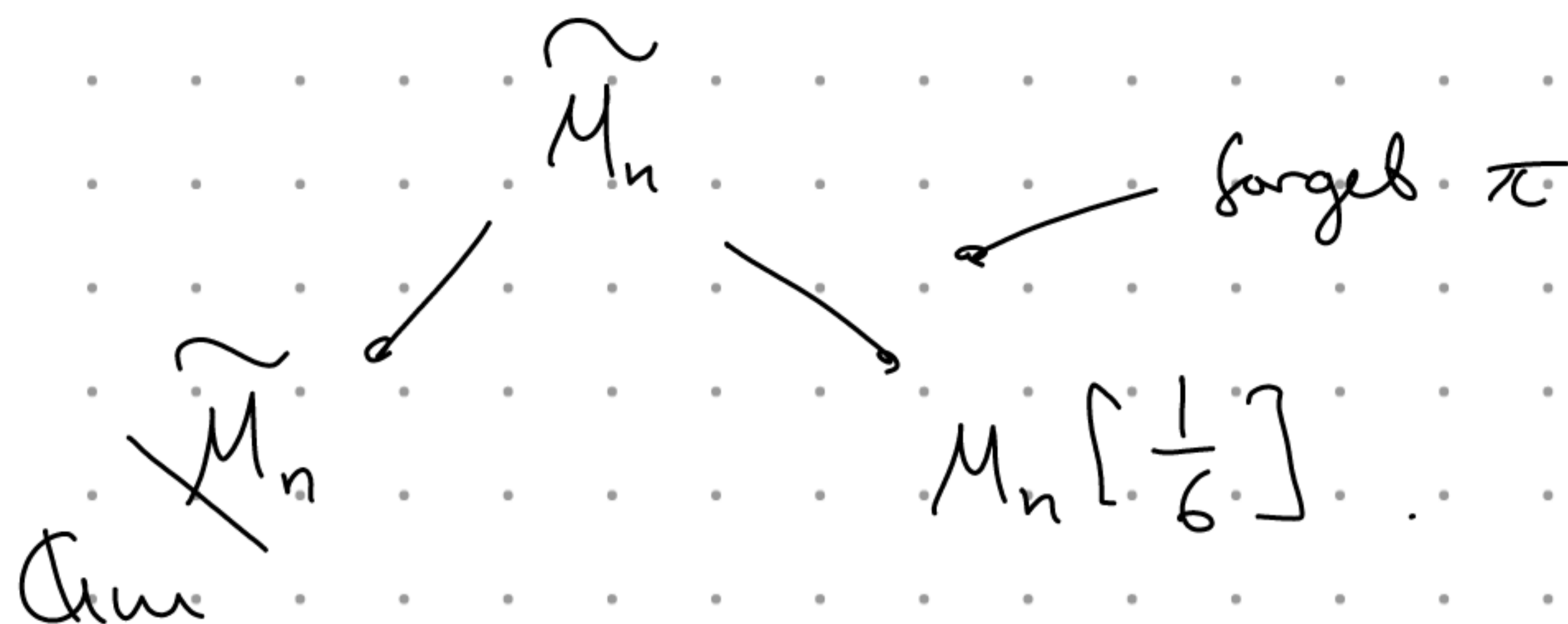
Proof $\tilde{M}_n = L_{E,n} \rightarrow \tilde{M}[\frac{1}{n}]$, $(E, \pi)/\tilde{M}$ universal curve
 \Rightarrow representable. (Even $\text{Gal}_2(\mathbb{Z}/n)$ -torsor.) \square

Remark Def makes sense in char p , $p \nmid n$, too,

but produces empty functor since there

$E[n]$ is never stable.

Obtain



Thm Assume $n \geq 3$. Then $\widetilde{M}_n \cong M_n[\frac{1}{6}]$.

In ptic, M_n is representable by an affine scheme.

Following prop explains why this is plausible:

Prop $n \geq 3$, $(E, \alpha)/S$ EC + level- n -str.

Then $\text{Aut}(E, \alpha) = \{ \text{id} \}$.

1st Proof First observe: If S connected, $\phi: E \rightarrow E'$

map of ECs over S s.t. $\phi(s) = 0$ for some $s \in S$,

then $\phi = 0$ by Rigidity. \rightarrow wlog $S = \text{Spec } k$
check t, n .

To see: $n \geq 3 \Rightarrow \text{End}(E) \xrightarrow{r} \text{End}(E[t])(k)$

\ni injective on $\text{Aut}(E)$.

Let $\phi \in \text{Aut}(E)$. Classif. of $\text{End}(E)$

$\Rightarrow \mathbb{Z}[\phi] \in \{ \mathbb{Z}, \mathbb{Z}[i], \mathbb{Z}[\sqrt{3}] \}$

with $\phi \in \{1, -1\}$ or $\{\pm i\}$ or $\left\{ \begin{smallmatrix} \pm 1 \\ 3 \end{smallmatrix} \right\}, \left\{ \begin{smallmatrix} \pm 1 \\ 6 \end{smallmatrix} \right\}$.

If $\phi = -1$, then $\tau(\phi) = -1$, which is $\neq 1$ mod n , so we are good in case $\phi \in \mathbb{Z}$.

Assume $\mathbb{Z}[\phi] =: R$ is quadratic.

Claim $E[n](k) \cong R/nR$ as R -module.

Proof Seen last term:

$$\mathbb{Z}_\ell \otimes_{\mathbb{Z}} R \hookrightarrow \text{End}_{\mathbb{Z}_\ell}(T_\ell E)$$

Our R is also the max order, i.e. normal,

so $\mathbb{Z}_\ell \otimes_{\mathbb{Z}} R = \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ or DVR.

Any torsion-free finite module over DVR is

free, so $T_\ell E$ is free (necessarily rank 1)

over $\mathbb{Z}_\ell \otimes_{\mathbb{Z}} R$.

Truncating, we find $E[\ell^e](k) \cong R/\ell^e$.

CRT \Rightarrow \square Claim.

Now $1 \neq \pm i \pmod{n \cdot \mathbb{Z}[i]}$ because

$(n=2^e)$ $\mathbb{Z}[i]$ ramified at 2, $1 \pm i$ are unramified

$(2 \neq p | n)$ primitive k -th roots of 1, $p \nmid k$,
different in $\overline{\mathbb{F}_p}$

Similarly $1 \neq \zeta_3^{\pm 1}, \zeta_6^{\pm 1} \pmod{n \cdot \mathbb{Z}[\zeta_3]}$ because

$(n=3^e)$ $\mathbb{Z}[\zeta_3]$ ramified at 3, $1 - \zeta_3^{\pm 1}, \zeta_6^{\pm 1} - 1$
unramified

$(3 \neq p | n)$ same argument. \square

2nd Proof Assume $\phi | E[n] = 1$, i.e. $E[n] \subset \ker(\phi - 1)$.

Consider
$$0 \rightarrow E[n] \rightarrow E \xrightarrow{\cdot n} E \xrightarrow{\cong} E/E[n] \rightarrow 0$$

as seen last term
$$\begin{array}{c} \phi - 1 \downarrow \\ E \end{array} \xrightarrow{\gamma} E/E[n]$$

by quotient property.

i.e. $(\phi - 1) = n \cdot \gamma$. Then

$$\begin{aligned} n^2 \deg(\gamma) &= (\phi - 1)(\phi^* - 1) = \deg \phi - (\phi + \phi^*) + 1 \\ &= 2 - (\phi + \phi^*). \end{aligned}$$

Classification of $\text{End}(E) \Rightarrow |\phi + \phi^*| \leq 2$

So $n^2 \deg \gamma \leq 4$.

This forces $\gamma = 0$ if $n \geq 3$. \square

§ 4 Proof of Thm $n \geq 3$, over $\mathbb{Z}[\frac{1}{6n}]$

Observe If $M_n[\frac{1}{6}]$ representable, then

$\tilde{M}_n \rightarrow M_n$ is \mathbb{G}_m -torsor since

1) $\mathbb{G}_m \times \tilde{M}_n \xrightarrow{\cong} \tilde{M}_n \times_{M_n} \tilde{M}_n$

2) $\tilde{M}_n \rightarrow M_n$ has Zariski local sections

(initialize ω_E ,

(E, α) universal curve)

\rightarrow Necessarily $M_n = \mathbb{G}_m \backslash \tilde{M}_n$!

Assume we know $\mathbb{G}_m \subset \tilde{M}_n$ freely. Then

$q: \tilde{M}_n \rightarrow \mathbb{G}_m \backslash \tilde{M}_n$ is \mathbb{G}_m -torsor (§2),

hence has local sections, unique up to \mathbb{G}_m .

$$\begin{array}{ccc} \mathbb{G}_m \backslash \tilde{M}_n & \xrightarrow{\Phi} & M_n \\ & \xleftarrow{\Psi} & \end{array}$$

1) $y \in (\mathbb{G}_m \backslash \tilde{M}_n)(S)$ $\Phi(y)$: Pick $S = S_i$
 + (E_i, α_i, π_i) lifting $y|_{S_i}$

Torsor-property $\Rightarrow (E_i, \alpha_i, \pi_i)|_{S_{ij}} = (E_j, \alpha_j, \pi_j)|_{S_{ij}}$

for unique $\lambda_{ij} \in \mathcal{O}_S(S_{ij})^\times$

Translation: $\exists! \phi_{ij}: (E_i, \alpha_i)|_{S_{ij}} \xrightarrow{\cong} (E_j, \alpha_j)|_{S_{ij}}$

cycle condition satisfied since $\text{Aut}(E, \alpha) = \{id\}$
(use $n \geq 3$)

\Rightarrow glue to $\Phi(y) := (E, \alpha) \in M_n(S)$.

2) $(E, \alpha) \in M_n(S)$ $\bar{\Gamma}(E, \alpha)$: Pick $S = S_i$ s.t.

$\omega_E|_{S_i} \cong \mathcal{O}_{S_i}$, lift $(E, \alpha, \pi_i) \in \widehat{M}_n(S_i)$.

Since φ \mathbb{Q}_m -invariant, $\{\varphi(E, \alpha, \pi_i)\}_i$

agree on overlaps, define $S \rightarrow \mathbb{Q}_m \backslash \widehat{M}_n$.

3) $\bar{\Gamma} \circ \Phi = id_{\mathbb{Q}_m \backslash \widehat{M}_n}$, $\bar{\Gamma} \circ \bar{\Gamma} = id_{M_n}$

Given y & lift (E_i, α_i, π_i) gluing to (E, α) ,

the (E_i, α_i, π_i) lift (E, α) and glue to y .

Other identity similar. \square

§5 Weil extension Thm

To see: $\mathbb{A}_m \times \tilde{\mathcal{M}}_n \longrightarrow \tilde{\mathcal{M}}_n \times_{\mathbb{Z}[\frac{1}{6n}]} \tilde{\mathcal{M}}_n \hookrightarrow$

closed immersion, i.e. proper monomorphism

[Stacks 04XV]

Monomorphism $\lambda, \lambda' \in \mathbb{A}_m(S)$, $(E, \alpha, \pi), (E', \alpha', \pi') \in \tilde{\mathcal{M}}_n(S)$.

Then $(E, \alpha, \pi) \cong_{\phi} (E', \alpha', \pi')$
& $(E, \alpha, \lambda\pi) \cong_{\psi} (E', \alpha', \lambda'\pi')$ $\} \Rightarrow \lambda = \lambda'$

Proof $n \geq 3 \Rightarrow \phi = \psi$ since $\exists_{\leq 1} \text{ iso } (E, \alpha) \xrightarrow{\cong} (E', \alpha')$.

So $\phi^*(\pi') = \pi$ & $\lambda' \phi^*(\pi') = \lambda\pi$

$\Rightarrow \lambda = \lambda'$ \square

Proposition To show \mathbb{R} DVR, $K = \text{Frac } \mathbb{R}$.

$(E, \alpha, \pi), (E', \alpha', \pi') \in \tilde{\mathcal{M}}_n(\mathbb{R})$

s.t. \exists iso $\phi_K: (E, \alpha)_K \xrightarrow{\cong} (E', \alpha')_K$ with
 $\phi^*(\pi') = \lambda \cdot \pi \quad \lambda \in K^\times$

Then ϕ_K lifts uniquely to $(E, \alpha) \rightarrow (E', \alpha')$ & $\lambda \in R^x$.

Then (Weil extension Thm) S Dedekind scheme, connected, η gen pt.
 $E, E'/S$ ECs. Then

$$\text{Hom}(E, E') \xrightarrow{\cong} \text{Hom}(E_\eta, E'_\eta)$$

Proof E_η, E'_η are schematically dense & E' separated,
 \Rightarrow injectivity is immediate. Surjectivity is the real statement here.

Injective derived property $\phi: E \rightarrow E'$ the unique lift of ϕ_K . (Is iso since also ϕ_K^{-1} lifts.)

Then $\phi \circ \alpha = \alpha'$ since $E[\eta]_K, E'[\eta]_K, \underline{(\mathbb{Q})}_K^{\oplus 2}$ are schematically dense and $\phi_K \circ \alpha_K = \alpha'_K$.

Also $\phi^*(\pi') = \mu \cdot \pi$ for some $\mu \in R^x$.

Then $\mu = \lambda$ since $\Gamma(E, \Omega'_{E/R}) \hookrightarrow \Gamma(E_K, \Omega'_{E/K})$.