Correction to last time

Let X/k of fin type, $x_0 \in X$ closed s.th.

$\kappa(x_0)/k$ separable (!)

Then $\coprod_{\substack{x \in X(\bar{k}) \\ |x| = |x_0|}} k_x$ is Galois.

(Proof: Is $\mathrm{Aut}(\bar{k}/k)$-stable composite of separable fields.)

In our application we assumed $\mathrm{char}\, k \nmid n$.

Then $E[n]$, $[n^{-1}](P)$ $P \in E(K)$

are étale k-schemes. $\Longrightarrow$ $\kappa(x_0)/k$ separable $\forall x_0 \in E[n], [n]^{-1}(P)$.

Next aim The extensions $L = K([n]^{-1}E(K))$

we constructed last time are unramified $/K$

away from $\{p \mid n\} \cup \{p$ s.th. E has bad reduction at $p\}$

This requires us to talk about models.

§1 Relative Ellipt. Curves S scheme

Recall Group scheme over S $\overset{=}{\text{def}}$ (G, m) where

$G \to S$ S-scheme

$m: G \times_S G \to G$ multiplication subject to group axioms.

Example $GL_{n,S} = \underline{\mathrm{Spec}}\, \mathcal{O}_S[T_{ij}, S]_{i,j=1}^{n} / (S \cdot \det((T_{ij})_{ij}) - 1)$

$$= S \times_{\mathrm{Spec}\, \mathbb{Z}} GL_{n,\mathbb{Z}}.$$

Yoneda description For $u: T \to S$,

$GL_{n,S}(T) = GL_n(\mathcal{O}_T(T)) = \mathrm{Aut}(\mathcal{O}_T^{\oplus n})$.

Variant $\mathcal{E}/S$ rank n vb. Then

$$GL(\mathcal{E})(T) := \mathrm{Aut}(u^*\mathcal{E})$$

defines a group scheme over S s.th.

$$\mathcal{E}|_U \cong \mathcal{O}_U^{\oplus n} \Rightarrow U \times_S GL(\mathcal{E}) \cong GL_{n,U}.$$

but not necessarily $GL(\mathcal{E}) \cong GL_{n,S}$.

"Twist"

Explicit construction

$S = \cup U_i$ trivializing $\mathcal{E}$, $\phi_i : \mathcal{O}_{U_i}^{\oplus n} \xrightarrow{\cong} \mathcal{E}|_{U_i}$.

$g_{ji} := \phi_j^{-1}\phi_i \in GL_n(\mathcal{O}_S(U_{ij}))$ cocycle.

$G_i := GL_{n,U_i} \to U_i$ constant grp sch.

Glue these along

$$U_{ij} \underset{U_i}{\times} G_i \xrightarrow[\text{conj}(g_{ji})]{\cong} U_{ij} \underset{U_j}{\times} G_j$$

Here, $\text{conj}(h)$ for $h \in GL_n(\mathcal{O}_S(S))$ denotes

$$GL_{n,S} \xrightarrow{(h,\text{id},h^{-1})} GL_{n,S} \times GL_{n,S} \underset{S}{\times} GL_{n,S} \xrightarrow{m} GL_{n,S}.$$

This is a group scheme auto, so $\{G_i\}$ glue to a group scheme $/S$!

<u>Def</u> <u>Ellipt. Curve over S</u> $\overset{=}{\text{def}}$ S-grp scheme (E, m)

s.th. $E \longrightarrow S$ is proper, smooth of dim 1,

has connected fibers.

In prtz

.) Fibers $E(s) = \operatorname{Spec} \varkappa(s) \times_S E \longrightarrow \operatorname{Spec} \varkappa(s)$ ECs

.) $\exists$ unit section $e : S \longrightarrow E$, inverse $i : E \longrightarrow E$

§2 Interlude on Cohom & BC

Setting A noeth, $X \to \operatorname{Spec} A$ proper, $\mathcal{F} \in \mathrm{Coh}_X$.

$\forall A \to B$, have base change map

$$bc^i_B : B \otimes_A H^i(X, \mathcal{F}) \longrightarrow H^i(X_B, \mathcal{F}_B)$$

Concretely: If $(c_J)_J \in \prod_{J \subseteq I, |J| = i+1} \mathcal{F}(U_J)$ represents a Čech cohom class for an open affine covering $X = \bigcup_{i \in I} U_i$, map $1 \otimes (c_J)_J$ to the class of

$$(1 \otimes c_J) \in \prod \mathcal{F}(U_{J,B}) = B \otimes_A \mathcal{F}(U_J).$$

bc^i_B in general neither injective nor surjective, but its information (for all B simultaneously) is encoded in a complex of A-modules:

Thm (AV Lect 7, Stacks Tag 07VL)

Assume $\mathcal{F}(U)$ flat A-module $\forall\, U \subseteq X$. Then $\exists$

$$K^\bullet = 0 \to K^0 \to K^1 \to \cdots \to K^n \to 0$$

complex of finite projective A-modules s.th.

s.th. functorially for all $A \to B$,

$$H^i(X_B, p_X^* \mathcal{F}) = H^i(B \otimes_A K^\bullet). \qquad \square$$

<u>Thm</u> $A, X, \mathcal{F}$ as before.

1) $bc^i_{\kappa(s)}$ surjective $\Rightarrow$ $bc^i_{\kappa(s)}$ is iso

2) If iso for s, then $\exists$ open nbhd $s \in U$ s.th.

$bc^i_{\kappa(t)}$ iso $\forall\, t \in U$.

3) If iso <u>for all s</u>, then bc^i_B iso for all B.

4) If iso for s, then equivalent:

a) bc^{i-1}_s also iso

b) $R^i p_* \mathcal{F}$ is locally free near s.

<u>Proof</u> $K^\bullet$ as in thm, fix i.

$$C^i := \operatorname{coker}(K^{i-1} \to K^i)$$

Defn of N.

Get ex seq

$$0 \to H^i(X, \mathcal{F}) \to C^i \to N \to 0 \qquad (\mathrm{I})$$

$$0 \to N \to K^{i+1} \to C^{i+1} \to 0. \qquad (\mathrm{II})$$

Now apply $\kappa(s) \otimes_A -$

$$\begin{tikzcd}
 & H^i(X,\mathcal{F})(s) \arrow[r, "④"] \arrow[d, "bc^i_{\kappa(s)}"] & C^i(s) \arrow[r] \arrow[d, equal, "①"] & N(s) \arrow[r] \arrow[d, "③"] & 0 \\
0 \arrow[r] & H^i(X(s),\mathcal{F}(s)) \arrow[r, "②"] & C^i(s) \arrow[r] & \ker\left(K^{i+1}(s) \to C^{i+1}(s)\right) &
\end{tikzcd}$$

Ad ① Taking cokernels commutes w/ $B \otimes_A -$, so

$$C^i(s) = \operatorname{Coker}\left(K^{i-1}(s) \to K^i(s)\right)$$

Ad ② This is now defining property of $K^\bullet$.

Ad ③ This $\kappa(s) \otimes_A -$ applied to (II), so

$$\operatorname{Tor}_1^A(K^{i+1}, \kappa(s)) \to \operatorname{Tor}_1^A(C^{i+1}, \kappa(s)) \to N(s) \xrightarrow{③} \cdots$$

is exact. But $= 0$ since K^{i+1} projective.

Ad ④ Kernel is $\operatorname{Tor}_1^A(N, \kappa(s))$ by same arguments for (I)

Statement 1) $bc^i_{\kappa(s)}$ surjective

$\Leftrightarrow$ ③ injective

$\Leftrightarrow$ $\mathrm{Tor}_1^A(C^{i+1}, \kappa(s)) = 0$

Lem (Local criterion for flatness, Stacks 00MK)

$(R, \mathfrak{m})$ local noetherian, M finite type R-mod.

M flat$/R$ $\Leftrightarrow$ $\mathrm{Tor}_1^R(M, R/\mathfrak{m}) = 0$.

Back to proof Above $\Leftrightarrow$ $C^{i+1}_{\mathfrak{p}}$ flat over $A_{\mathfrak{p}}$, $\mathfrak{p} = s$

$\Leftrightarrow$ C^{i+1} free on open nbhd $s \in U$

If these hold, (II) is split exact locally on U,

so $N|_U$ is finite projective

In partic, $\mathrm{Tor}_1^A(N, \kappa(s)) = 0$, so ④ injective,

so $bc^i_{\kappa(s)}$ iso.

Statement 2) Injectivity of ③ in above proof holds

then for all $t \in U$.

Statement 3) Knowing that $bc^i_{x(s)}$ iso $\forall s$

implies N, C^{i+1} loc free, i.e. flat.

Then $Tor_1^A(N, B) = Tor_1^A(C^{i+1}, B) = 0 \quad \forall B$.

Now consider same diagram but for $B \otimes_A -$.

Then ③, ④ are surjective, thus bc^i_B an iso.

Statement 4) Assume $bc^i_{x(s)}$ surjective, U as in

Statement 1).

Have seen that then $N|_U$ is loc free.

Then by (I), locally on U

$$C^i \cong H^i(X, \mathcal{F}) \oplus N^i \quad \text{(non-canonically)}$$

Thus $H^i(X,\mathcal{F})$ loc free $\Leftrightarrow$ C^i loc free

$\overset{\text{Proof of 1)}}{\Leftrightarrow}$ $bc^{i-1}_{x(s)}$ iso. $\square$

§3 Application to ECs   S loc noeth

<u>Thm</u> $E \xrightarrow{p} S$ EC

1) $\mathcal{O}_S \xrightarrow{\cong} p_* \mathcal{O}_E$, $R^1 p_* \mathcal{O}_E$ is l.b. on S

2) $p_* \Omega^1_{E/S}$, $R^1 p_* \Omega^1_{E/S}$ are l.b. on S

3) $\mathcal{L}$ lb on E s.th. $\deg(\mathcal{L}(s)) = d \geq 1$ $\forall s$.

Then $p_* \mathcal{L}$ is vb of rank d on S

$R^1 p_* \mathcal{L} = 0$.

<u>Proof</u> 1) is case $\mathcal{F} = \mathcal{O}_E$.

$\Gamma(E(s), \mathcal{O}_{E(s)}) = \varkappa(s)$ $\forall s$, so the compositions

$$\mathcal{O}_S \longrightarrow p_* \mathcal{O}_E \xrightarrow{bc^0_{\varkappa(s)}} \varkappa(s)$$

are surjective, hence bc^0_s is surjective.

$\xRightarrow{\text{Stmt 1)}}$ $(p_* \mathcal{O}_E)(s) \xrightarrow{\cong} p(s)_* \mathcal{O}_{E(s)}$.

$bc^{-1}_{\varkappa(s)}$ is trivially surjective

$\xRightarrow{\text{Stmt 4)}}$ $p_* \mathcal{O}_E$ is locally free.

Then necessarily a line bundle.

The map $\mathcal{O}_S \longrightarrow p_* \mathcal{O}_E$ is fiber-wise an iso,

hence an iso.

$bc^2_{\mathcal{X}(s)}$ is surjective since $H^2(E(s), -) = 0$.

& $R^2 p_* \mathcal{O}_E = 0$ is loc free

Stmt 4)
$\Longrightarrow$ $bc^1_{\mathcal{X}(s)}$ surjective $\forall s$

Already shown $bc^0_{\mathcal{X}(s)}$ surjective $\forall s$, so

$R^1 p_* \mathcal{O}_E$ is loc. free (Stmt 4))

Since $h^1(E(s), \mathcal{O}_{E(s)}) = 1$ $\forall s$, $R^1 p_* \mathcal{O}_E$

line bundle as claimed.

2) $\Omega^1_{E/S}$ is a line bundle on E, equal to

$p^* e^* \Omega^1_{E/S}$ (property of group schemes).

Working on covering $S = \cup U_i$ s.th. $e^* \Omega^1_{E/S}|_{U_i} \cong \mathcal{O}_{U_i}$,

arguments from 1) apply.

3) Case $\mathcal{F} = \mathcal{L}$

$\deg \mathcal{L}(s) > 0 \Rightarrow H^1(E(s), \mathcal{L}(s)) = 0$

$\Rightarrow bc^1_{\kappa(s)}$ surjective,

hence iso by Stmt 1).

Thus $R^1 p_* \mathcal{L} = 0$ is a vector bundle.

Add to that $bc^{-1}_{\kappa(s)}$ surjective!

$\xrightarrow{\text{stmt 4}}$ $bc^0_{\kappa(s)}$ iso + $p_* \mathcal{L}$ loc free,

then necessarily of rank $h^0(E(s), \mathcal{L}(s)) = \deg \mathcal{L}$. □

Rmk Statement $p_* \mathcal{O}_X \xleftarrow{\cong} \mathcal{O}_S$ holds for all

proper flat $X \to S$ w/ $h^0(X(s), \mathcal{O}_{X(s)}) = 1 \ \forall s$.

This was used last term for families of ab vars.

(Proof is same as in above Thm.)

Rigidity Lem (cf. AV Lect 18)

$$\begin{tikzcd} X \arrow[rr, "f"] \arrow[dr, "p"'] & & Y \arrow[dl, "q"] \\ & S & \end{tikzcd}$$

S connected, $\exists\, s_0$ s.th. $f(X(s_0)) = \{pt\}$

p proper + flat + fin. pres.

$\mathcal{O}_S \xrightarrow{\cong} p_* \mathcal{O}_X$

$\exists$ section $e : S \to X$

q separated + fin. pres.

Then $\exists\ g : S \to Y$ s.th. $f = g \circ p$.

Cor

1) $(E_1, m_1), (E_2, m_2)/S$ ECs

$E_1 \xrightarrow{f} E_2$ map of S-schemes w/ $f \circ e_1 = e_2$.

Then f is group scheme morphism.

2) Any EC E/S is commutative.

3) Given $(E, m)/S$ EC, group str is uniquely determined by $e : S \to E$.

<u>Proof</u> 1) Consider $pr : E_1 \times_S E_1 \longrightarrow E_1$.

We just showed $pr_* \mathcal{O}_{E_1 \times_S E_2} = \mathcal{O}_{E_1}$, so rigidity Lem. may be applied to

$$\begin{tikzcd} E_1 \times_S E_1 \arrow[rr, "\psi"] \arrow[dr, "pr"'] & & E_1 \times_S E_2 \arrow[dl] \\ & E_1 & \end{tikzcd}$$

$$\psi(x, y) = (x, f(x \underset{m_1}{\bullet} y) \underset{m_2}{\bullet} f(y)^{-1} \underset{m_2}{\bullet} f(x)^{-1})$$

(Inverses are for m_2.)

Then $\psi|_{pr^{-1}(e_1)} \equiv (e_1, e_2)$, so $\psi = (id_{E_1}, g) \circ pr$

for some $g : E_1 \longrightarrow E_2$.

But $\psi|_{E_1 \times \{e_1\}} \equiv (e_1, e_2)$ as well, so $g \equiv e_2$.

2) 1) $\Longrightarrow$ $inv : E \longrightarrow E$ is group auto

$\Longrightarrow$ commutative

3) If m' is another grp str. w/ $e = e'$, then

id_E is group iso $(E, m) \cong (E, m')$, so $m = m'$. $\square$

Thm (cf. AV Lect 8)

S loc noeth. There is an equiv of cats

$$\{ECs/S\} \xrightarrow{\cong} \left\{(E,e) \;\middle|\; \begin{array}{l} E \to S \text{ prop smooth,} \\ \text{fib. wise genus } 1 \\ + e: S \to E \end{array}\right\}$$

$$(E,m) \longmapsto (E, e_m)$$

Sketch Fully faithfulness: Previous lecture.

Essential surjectivity: Given (E,e), $x,y \in E(T)$,

$$E_T := T \times_S E \longrightarrow T$$

$\Gamma_x, \Gamma_y, \Gamma_{e_T}$ graph maps

AV Lect. 8: Γ's are closed immersions, images Cartier divisors ("$\dim E_T = \dim T + 1$" since E curve)

$$\mathcal{L} := \mathcal{O}_E([\Gamma_x] + [\Gamma_y] - [\Gamma_{e_T}]) \in \mathrm{Pic}(E_T)$$

is fibre-wise of deg 1.

$\Longrightarrow$ $Q := p_{T,*}\mathcal{L} \in \mathrm{Pic}(T)$ (Thm from prev. lect.)

If $Q|_U = \mathcal{O}_T \cdot q$, then q defines

$$\mathcal{O}_{E_U} \xrightarrow{q} \mathcal{L}|_U$$

AV Lect 8: $\quad E_U \supseteq V(q) \xrightarrow{\cong} U$

so $V(q) = \Gamma_z$ for unique $z : U \to E$

Since $V(\lambda q) = V(q)$ $\forall \lambda \in \mathcal{O}_U^\times$, does not depend on choice q, so glues to $z : T \to E$.

Then put $x + y := z$. $\square$

<u>Ex</u> S any, $2 \in \mathcal{O}_S^\times$, $a, b \in \mathcal{O}_S(S)$, $f(x) = x^3 + ax + b$

$$E := V_+\left(Y^2 Z - \left(X^3 + aXZ^2 + bZ^3\right)\right) \subseteq \mathbb{P}^2_S.$$

Jacobi for $[x:y:z] \in E(k)$ $\quad x(s) \subseteq k, \quad s \in S$

<u>If $z = 1$</u> $\quad \mathrm{rk}\, \mathrm{Jacobi}\left(y^2 - f(x)\right) = \mathrm{rk}\left(2y, -f'(x)\right) = 1$

$\Leftrightarrow$ y invertible or $y = 0$ but $f'(s)(x) \neq 0$

Thus $\mathrm{rk} = 1$ for all $[x:y:1] \in E(k)$

$\Leftrightarrow$ $\Delta(a,b)(s) = \mathrm{disc}(f(s)) = (4a^3 - 27b^2)(s) \neq 0$

If $z=0$ then $x=0$, hence only $[0:1:0]$.

$$\mathrm{Jac}\left(z - x^3 - axz^2 - bz^3\right)$$

$$= \left(\underbrace{-3x^2 - az^2}, \ 1 \underbrace{- axz - bz^2}\right)$$

$= 0$ at $[0:1:0]$, so rank $= 1$.

Conclusion If $\Delta \in \mathcal{O}_S^\times$,

$E \to S$ smooth, proper, fibers genus 1

$e = [0:1:0] : S \longrightarrow E$ section.

Thm $\Longrightarrow$ E is EC

Ex $a=-1$, $b=0$ $\Delta = 4$

$E: \ y^2 = x^3 - x$ defines $EC / \mathbb{Z}[\frac{1}{2}]$

Thm (Tate) $\nexists$ EC / Spec $\mathbb{Z}$

In partic, $\nexists$ EC $\tilde{E} \longrightarrow \operatorname{Spec} \mathbb{Z}_{(2)}$ s.th.

$$\tilde{E}_{\mathbb{Q}} \cong \{ y^2 = x^3 - x \}$$

(Any such $\tilde{E}$ would glue w/ above E to $EC/\mathbb{Z}$.)

However, $\exists$ EC $\tilde{E} \longrightarrow \operatorname{Spec} \mathbb{Z}[i]_{(2)}$ s.th.

$$\tilde{E}_{\mathbb{Q}(i)} \cong \{ y^2 = x^3 - x \}.$$

<u>Rmk</u> Same methods work in char 2,3.

Only difference is one has to use slightly more general cubic equations.

<u>§4 Fiber Criteria</u>

<u>Fiber Crit. for Flatness (Stronger Form)</u>

$R \to S \to S'$ local maps of loc noeth rings, $\mathfrak{m} \subseteq R$ max. ideal.

M S'-module s.th.

1) M finite $/S'$
2) M flat $/R$
3) $M/\mathfrak{m}M$ flat over $S/\mathfrak{m}S$

Then M flat over S. If also

4) $M \neq 0$,

then $R \to S$ is flat.

Proof not difficult, but lengthy. We refer to Stacks OOMP

Ex Consider

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[dr] & Y \arrow[d] \\ & S \end{tikzcd}$$

.) X, Y, S loc noeth

.) $X \to S$ flat.

1) f is flat $\Leftrightarrow$ all fibers $f(s)$ flat,

2) Assume f loc. of fin pres. Then

f smooth $\Leftrightarrow$ all fibers $f(s)$ smooth, $s \in S$

If conditions hold + $X \to Y$ surjective, then $Y \to S$ flat.

Proof For 1) apply Lemma to $\mathcal{O}_{S,s} \to \mathcal{O}_{Y,y} \to \mathcal{O}_{X,x}$

& $M = \mathcal{O}_{X,x}$. $\qquad s \mapsto y \mapsto x$

For 2) also use fiber criterion for smoothness:

f flat, loc of fin pres is smooth

$\Leftrightarrow$ its fibers are smooth. $\square$

Cor Let $E \to S$ be EC. Then $[n] : E \to E$

is finite loc free of rank n^2.

If $n \in \mathcal{O}_S^\times$, then $[n]$ is étale.

<u>Proof</u> $[n]$ is automatically proper

Its fibers are 0-dim'l, so also finite.

(finite = proper + q. finite)

$E \to S$ flat and fibers $[n](s)$ flat

$\xRightarrow{\text{fiber crit.}}$ $[n]$ also flat as claimed,

hence finite loc free as claimed.

If $n \in \mathcal{O}_S^\times$, then $[n](s)$ étale $\forall s \in S$

$\xRightarrow{\text{fib. crit.}}$ $[n]$ is étale. $\square$