§1. Elliptic curve over $\mathbb{Q}$ and their reduction.

Recall general Weierstrass equation

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad a_i \in \mathbb{Q}$$

- E is integral if $a_i \in \mathbb{Z}$
- $E \sim E'$ if $\exists u' \in \mathbb{Q}^\times$, $r,s,t \in \mathbb{Q}$ s.t. $(x,y) = (u^2x' + r, u^3y' + su^2x' + t)$.
- $v_p(E) := \min\{ v_p(\Delta(E')) : E \sim E' : \text{integral} \} \geq 0 \quad \forall p \in \operatorname{Spec}\mathbb{Z}$.

  $\Delta_{\min}(E) := \prod_p p^{v_p(E)}$ (global minimal discriminant)

  By Ex. 8.3.2, $\exists$ global minimal Weierstrass equation $E' \sim E$ s.t. $\Delta(E') = \Delta_{\min}(E)$.
- For $p \in \operatorname{Spec}\mathbb{Z}$, define reduction of E at p by modulo the equation of g.m.W.e.

$$\bar{E}: y^2 + \bar{a}_1xy + \bar{a}_3y = x^3 + \bar{a}_2x^2 + \bar{a}_4x + \bar{a}_6 \quad \bar{a}_i \in \mathbb{F}_p.$$

  - good if $\bar{E}$ is nonsingular i.e. $p \nmid \Delta_{\min}(E)$
    - ordinary if $\bar{E}[p] \simeq \mathbb{Z}/p\mathbb{Z}$, i.e. $\hat{\sigma}_p$ is sep. (σ_p: p-th Frobenius)
    - supersingular if $\bar{E}[p] \simeq \{0\}$, i.e. $\hat{\sigma}_p$ is insep.
  - bad if $\bar{E}$ is singular i.e. $p \mid \Delta_{\min}(E)$. Locally at unique singular point,

$$\bar{E}: (y - m_1x)(y - m_2x) = x^3$$

(Recall singular point is $\mathbb{F}_p$-point)

    - multiplicative if $m_1 \neq m_2$ (node)
      - split if $m_1, m_2 \in \mathbb{F}_p$
      - non-split if $m_1, m_2 \notin \mathbb{F}_p$
    - additive if $m_1 = m_2$ (cusp)
- Define algebraic conductor $N_E = \prod p^{f_p}$, $f_p = \begin{cases} 0 & \text{good at } p \\ 1 & \text{mult. at } p \\ 2 & \text{add. at } p \geq 5 \\ 2 + \delta_p & \text{add. at } p = 2 \text{ or } 3 \end{cases}$

  $(\delta_2 \leq 6, \delta_3 \leq 3)$

Then $p \mid \Delta_{\min} \iff p \mid N_E$.

$a_p(E) = p + 1 - |\bar{E}(\mathbb{F}_p)|$

Def. If $E/\mathbb{Q}$ is elliptic curve, define $t_{p^e}(E) = p^e + 1 - |\bar{E}(\mathbb{F}_{p^e})|$

Prop. $t_{p^e}(E) = t_p(E)\,t_{p^{e-1}}(E) - 1_E(p)\,p\,t_{p^{e-2}}(E) \quad \forall p \; \forall e \geq 2$,

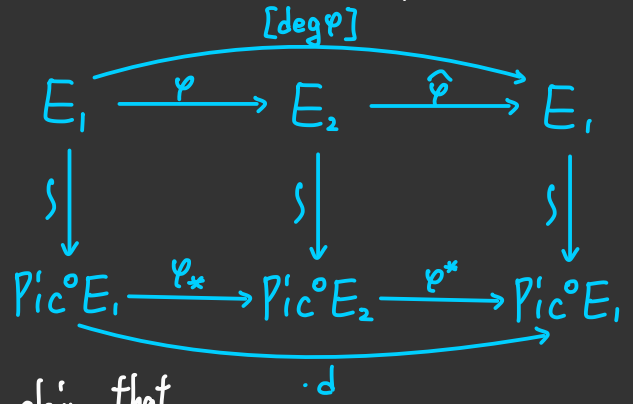
where 1_E is trivial char. mod. N_E.

(pf.) ($\sigma_p : \overline{E} \to \overline{E}$ ∵ E define over $\mathbb{F}_p$)

- E is good at p : Note that $E(\overline{\mathbb{F}}_{p^e}) = \ker(\sigma_p^e - 1)$ and $\sigma_p^e - 1$ is separable.
(Recall : $\phi \in \mathrm{Hom}(E_1, E_2)$ is insep. $\Leftrightarrow \phi^* \omega_2 = 0$, where ω_2 is invariant 1-form on E_2)

So $|E(\mathbb{F}_{p^e})| = \deg_{sep}(\sigma_p^e - 1) = \deg(\sigma_p^e - 1) = \widehat{(\sigma_p^e - 1)} \circ (\sigma_p^e - 1) = p + 1 - \hat{\sigma}_p^e - \sigma_p^e$

$\Rightarrow t_{p^e}(E) = \hat{\sigma}_p^e + \sigma_p^e \Rightarrow t_{p^e}(E) - t_p(E)\, t_{p^{e-1}}(E) = -(\sigma_p \hat{\sigma}_p^{e-1} + \hat{\sigma}_p \sigma_p^{e-1}) = -p\, t_{p^{e-2}}(E)$.



- E is bad at p : We claim that

$$t_{p^e}(E) = \begin{cases} 1 & \text{split at } p \\ (-1)^e & \text{nonsplit at } p \\ 0 & \text{add. at } p \end{cases}$$

($q = p^e$)

Consider $f : \mathbb{P}^1(\mathbb{F}_q) \longrightarrow \overline{E}(\mathbb{F}_q)$

$t \longmapsto \left((t-m_1)(t-m_2),\ t(t-m_1)(t-m_2)\right)$

$\frac{y}{x} \longleftarrow (x,y) \neq (0,0)$ give a bijection

$\Rightarrow t_q(E) = q + 1 - \underbrace{|\overline{E}(\mathbb{F}_q) \setminus (0,0)|}_{= |\mathbb{P}^1(\mathbb{F}_q) \setminus f^{-1}(0,0)|} - 1 = |f^{-1}(0,0)| - 1$ as desired. □

Prop. $E/\mathbb{Q}$ good at p, then $\begin{cases} \text{ordinary} & \text{if } p \nmid a_p(E) \\ \text{supersingular} & \text{if } p \mid a_p(E) \end{cases}$

(pf.) supersingular $\Leftrightarrow \hat{\sigma}_p^* \omega = 0 \Leftrightarrow a_p \omega = [a_p]^* \omega = 0 \Leftrightarrow p \mid a_p$.

Lemma. $\deg : \mathrm{Hom}(E_1, E_2) \longrightarrow \mathbb{Z}$ positive definite quadratic form. Moreover,

$$\underbrace{|\deg(\varphi + \psi) - \deg(\varphi) - \deg(\psi)|}_{:= B(\varphi,\psi)} \leq 2\sqrt{(\deg\varphi)(\deg\psi)}.$$

(pf.) We need to prove $B(\varphi,\psi)$ is bilinear form. Recall that $[\ ] : \mathbb{Z} \hookrightarrow \mathrm{End}$.

$$[B(\varphi,\psi)] = \widehat{\varphi+\psi} \circ (\varphi+\psi) - \hat{\varphi}\circ\varphi - \hat{\psi}\circ\psi = \hat{\varphi}\circ\psi + \psi\circ\hat{\varphi}$$

is bilinear form $\Rightarrow B(\varphi,\psi)$ is. Then $\forall m,n \in \mathbb{Z}$

$$0 \leq \deg(m\varphi + n\psi) = m^2 \deg\varphi + mn B(\varphi,\psi) + n^2 \deg\psi \Rightarrow |B(\varphi,\psi)| \leq 2\sqrt{(\deg\varphi)(\deg\psi)}.$$

Cor. (Hasse) $t_p(E) \le 2p^{1/2}$ (Apply $(\varphi,\psi)=(\sigma_p^r-1, 1)$ in above lemma)

Cor. $t_p(E)=0$ if E is supersingular at $p \ge 5$. ($|a_p| \le 2\sqrt{p} < p$ and $p \mid a_p$)

§2. Elliptic curve over $\bar{\mathbb{Q}}$ and their reduction.

(1) Reduction on curve

Let $E/\bar{\mathbb{Q}}$ be a elliptic curve, $\mathfrak{p} \in \operatorname{Spec} \bar{\mathbb{Z}}$, $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. We may define reduction at $\mathfrak{p}$ via

$$\bar{\mathbb{Z}}_{(\mathfrak{p})}/\mathfrak{p}\bar{\mathbb{Z}}_{(\mathfrak{p})} \cong \bar{\mathbb{Z}}/\mathfrak{p} \cong \bar{\mathbb{F}}_p.$$

Lemma. $\forall \alpha \in \bar{\mathbb{Q}}^\times$, α or α in $\bar{\mathbb{Z}}_{(\mathfrak{p})}$

(pf.) Let $K=\mathbb{Q}(\alpha)$ and $\mathfrak{p}_K = \mathcal{O}_K \cap \mathfrak{p}$. Then α or α^{-1} in $\mathcal{O}_{K,(\mathfrak{p}_K)} \subseteq \bar{\mathbb{Z}}_{(\mathfrak{p})}$. (DVR)

Prop. Every $E/\bar{\mathbb{Q}}$ has $\mathfrak{p}$-integral W.e. with good or mult. reduction at $\mathfrak{p}$.

- If $p \neq 2$: Consider Legendre form $E_\lambda: y^2 = x(x-1)(x-\lambda)$ $\lambda \in \bar{\mathbb{Q}} \setminus \{0,1\}$.

  Note that E_λ & $E_{\lambda^{-1}}$ define same elliptic curve, by lemma we may assume $\lambda \in \bar{\mathbb{Z}}_{(\mathfrak{p})} \setminus \{0,1\}$.

  Then $\Delta(E_\lambda) = 16\lambda^2(1-\lambda)^2$ & $c_4 = 16(1-\lambda(1-\lambda))$.

  $$\Delta \in \mathfrak{p}\bar{\mathbb{Z}}_{(\mathfrak{p})} \Rightarrow \lambda(1-\lambda) \in \mathfrak{p}\bar{\mathbb{Z}}_{(\mathfrak{p})} \Rightarrow c_4 \notin \mathfrak{p}\bar{\mathbb{Z}}_{(\mathfrak{p})}$$

  Hence E_λ is good or mult. reduction at $\mathfrak{p}$. (existence by solve j)

- If $p=2$. Consider Deuring normal form $E_\alpha: y^2+\alpha xy+y = x^3$, $\alpha \in \bar{\mathbb{Q}}$. $\alpha^3 \neq 27$

  $$\Delta(E_\alpha) = \alpha^3 - 27, \quad c_4(E_\alpha) = \alpha(\alpha^3-24)$$

  ∵ If $\alpha \in \bar{\mathbb{Z}}_{(\mathfrak{p})}$: $\Delta, c_4 \in \mathfrak{p}\bar{\mathbb{Z}}_{(\mathfrak{p})} \Rightarrow 3\alpha \in \mathfrak{p}\bar{\mathbb{Z}}_{(\mathfrak{p})} \Rightarrow \alpha \in \mathfrak{p}\bar{\mathbb{Z}}_{(\mathfrak{p})} \Rightarrow 27 \in \mathfrak{p}\bar{\mathbb{Z}}_{(\mathfrak{p})} \Rightarrow 3 \in \mathfrak{p}\bar{\mathbb{Z}}_{(\mathfrak{p})}$ →←.

  ∵ If $\alpha \notin \bar{\mathbb{Z}}_{(\mathfrak{p})}$: Let $K=\mathbb{Q}(\alpha)$, $\mathfrak{p}_K = \mathfrak{p} \cap \mathcal{O}_K$. Let π: uniformizer of $\mathcal{O}_{K,\mathfrak{p}_K}$ and $r \ge 1$ s.t. $\beta = \pi^r \alpha \in \mathcal{O}_{K,(\mathfrak{p}_K)}^\times \subseteq \bar{\mathbb{Z}}_{(\mathfrak{p})}$. Consider $(x,y) = (\pi^{2r}x', \pi^{3r}y')$ gives W.e.

  $$E': y'^2 + \beta x'y' + \pi^{3r}y' = x'^3 \quad \text{with} \quad \begin{aligned} \Delta(E') &= \pi^{9r}(\beta^3 - 27\pi^{3r}) \equiv 0 \pmod{\mathfrak{p}} \\ c_4(E') &= \beta(\beta^3 - 24\pi^{3r}) \equiv \beta^4 \not\equiv 0 \pmod{\mathfrak{p}}. \end{aligned}$$

Def. A $\mathfrak{p}$-integral W.e. with good or mult. reduction is called $\mathfrak{p}$-minimal.

Prop. Ordinary, supersingular, and multiplicative are well-defined on equiv. class of $\mathfrak{p}$-minimal.

If $E \sim E'$ are $\mathfrak{p}$-minimal W.e. with good at $\mathfrak{p}$, then $\bar{E} \cong \bar{E}'$ over $\bar{\mathbb{F}}_p$.

(pf.) - If $E \sim E'$, then $u^{12}\Delta = \Delta'$ & $u^4 c_4 = c_4'$ for some $u \in \bar{\mathbb{Q}}$ (may assume in $\bar{\mathbb{Z}}_{(\mathfrak{p})}$).

If $\Delta \in \mathfrak{p}\bar{\mathbb{Z}}_{(\mathfrak{p})}$, then both E, E' are mult.. If $\Delta \in \bar{\mathbb{Z}}_{(\mathfrak{p})}^\times$ and $\Delta' \in \mathfrak{p}\bar{\mathbb{Z}}_{(\mathfrak{p})}$, then $u \in \mathfrak{p}\bar{\mathbb{Z}}_{(\mathfrak{p})}$ and thus $c_4' \in \mathfrak{p}\bar{\mathbb{Z}}_{(\mathfrak{p})}$ →←.

- Given change of variables between two equation of good reduction, we may assume $u \in \bar{\mathbb{Z}}_{(\mathfrak{p})}$.

Then $u^{12}\Delta = \Delta' \Rightarrow u \in \bar{\mathbb{Z}}_{(p)}^{\times}$. By Ex 8.4.3, $r,s,t \in \bar{\mathbb{Z}}_{(p)}$. Hence $E \cong E'$ by change of variables $\bar{u} \in \bar{\mathbb{F}}_p^{\times}, \bar{r},\bar{s},\bar{t} \in \bar{\mathbb{F}}_p$. Hence $\bar{E}[p] \cong \bar{E}'[p] \Rightarrow$ same reduction type.

Prop. $E/\bar{\mathbb{Q}}$ has good reduction at $p \Leftrightarrow j(E) \in \bar{\mathbb{Z}}_{(p)}$.

(pf.) • ($\Rightarrow$) Take p-minimal W.e. $\Rightarrow \Delta \in \bar{\mathbb{Z}}_{(p)}^{\times}$, $c_4 \in \bar{\mathbb{Z}}_{(p)} \Rightarrow j(E) \in \bar{\mathbb{Z}}_{(p)}$.

• ($\Leftarrow$) •• If $p \nmid 2$, take p-integral Legendre form. If $\Delta \in p\bar{\mathbb{Z}}_{(p)}$, then

$$p\bar{\mathbb{Z}}_{(p)} \ni j\lambda^2(1-\lambda)^2 = 2^8(1-\lambda(1-\lambda))^3 \notin p\bar{\mathbb{Z}}_{(p)} \quad \not\rightarrow\leftarrow.$$

•• If $p=2$, take Deuring normal E_α given in above.

··· $\alpha \in \bar{\mathbb{Z}}_{(p)}$: If $\Delta \in p\bar{\mathbb{Z}}_{(p)}$, then α or $\alpha^3 - 24 \in p\bar{\mathbb{Z}}_{(p)} \Rightarrow 3 \in p\bar{\mathbb{Z}}_{(p)} \not\rightarrow\leftarrow$.

··· $\alpha \notin \bar{\mathbb{Z}}_{(p)}$: Then E' is p-integral with $v_{P_K}(\Delta) = 9r$, $v_{P_K}(c_4) = 0 \Rightarrow j(E) \in \bar{\mathbb{Z}}_{(p)} \not\rightarrow\leftarrow$.

(2) Reduction on points

Define the reduction map at p $\bar{\ }: \mathbb{P}^n(\bar{\mathbb{Q}}) \longrightarrow \mathbb{P}^n(\bar{\mathbb{F}}_p)$ as follows:

For $P = [x_0 : \cdots : x_n]$ with $x_i \in \bar{\mathbb{Q}}$. Then P has representative with all $x_i \in \bar{\mathbb{Z}}_{(p)}$ and at least one of them is equal to 1 by using the valuation v_{P_K} on $K = \mathbb{Q}(x_1, \cdots, x_n)$. Define

$$\bar{P} = [\bar{x}_0 : \cdots : \bar{x}_n] \in \mathbb{P}^n(\bar{\mathbb{F}}_p)$$

The scaler quotient of two such representatives must in $\bar{\mathbb{Z}}_{(p)}^{\times}$ and thus reduce to $\bar{\mathbb{F}}_p^{\times}$.

The affine point $[1 : x_1 : \cdots : x_n] \in \mathbb{P}^n(\bar{\mathbb{Q}})$ reduce to affine points of $\mathbb{P}^n(\bar{\mathbb{F}}_p)$ if $x_i \in \bar{\mathbb{Z}}_{(p)}$.

For $E \subseteq \mathbb{P}^2$ defined by W.e., $\ker(E \to \bar{E}) = E \setminus \bar{\mathbb{Z}}_{(p)}^2$.

Prop. Let $E/\bar{\mathbb{Q}}$ good at p, then

(1) $E[N] \hookrightarrow \bar{E}[N]$ $\forall p \nmid N$

(2) $E[N] \twoheadrightarrow \bar{E}[N]$ $\forall N$

(3) If C is subgp. of E of order p, then E/C is good at p. Moreover, E & E/C have same reduction type.

(pf) (1) For $p \nmid 6N$, take a p-minimal Weierstrass equation of the form $y^2 = x^3 + Ax + B$. Recall that (Silverman Ex 3.7) the division polynomial $\psi_N \in \mathbb{Z}[A,B,x]\, y^{N\%2}$ s.t.

$$[N]P = O_E \Leftrightarrow \psi_N(P) = 0 \qquad \& \qquad \psi_N^2 = N^2 x^{N^2-1} + \cdots \in \mathbb{Z}[A,B][x] \subseteq \bar{\mathbb{Z}}_{(p)}[x].$$

Since $p \nmid N$, ψ_N^2/N^2 is monic poly. in $\bar{\mathbb{Z}}_{(p)}[x] \Rightarrow x(P) \in \bar{\mathbb{Z}}_{(p)}$ $\forall P \in E[N] \Rightarrow y(P) \in \bar{\mathbb{Z}}_{(p)}$.

Hence $E[N] \hookrightarrow \bar{E}[N]$. For general case, see Silverman VII Prop. 3.1. (or 3.4)

(2) For $p \nmid N$, $|E[N]| = N^2 = |\bar{E}[N]|$. By (a), $E[N] \xrightarrow{\sim} \bar{E}[N]$ $\forall p \nmid 6N$.

For general case, see Silverman VII Prop. 3.4.

(3) • In fact, if $\exists \varphi \in \mathrm{Hom}_{\bar{\mathbb{Q}}}(E_1, E_2)$. then E_1 and E_2 has the same place of good reduction:

• Let $E' = E/C$, $\varphi: E \to E'$ with dual isogeny $\psi: E' \to E$. We using the Thm. will prove later that $\exists\, \bar{\varphi}: \bar{E} \to \bar{E'}$, $\bar{\psi}: \bar{E'} \to \bar{E}$ s.t. $\bar{\psi} \circ \bar{\varphi} = [P]_{\bar{E}}$, $\bar{\varphi} \circ \bar{\psi} = [P]_{\bar{E'}}$. Then

$[P]_{\bar{E}'} \circ \bar{\varphi} = \bar{\varphi} \circ \bar{\psi} \circ \bar{\varphi} = \bar{\varphi} \circ [P]_{\bar{E}} \Rightarrow \deg_{sep} [P]_{\bar{E}} = \deg_{sep} [P]_{\bar{E}'}$.

§3. Reduction of alg. curves and maps

(1) Reduction on curve

Def. C: nonsingular affine alg. curve / $\bar{\mathbb{Q}}$ defined by $I \subseteq \mathbb{Z}_{(p)}[x]$.

Then C has good reduction at p if $I \in \mathrm{Spec}\, \mathbb{Z}_{(p)}[x]$ and $\bar{I} \in \mathrm{Spec}\, \mathbb{F}_p[x]$.

Rmk. $I \in \mathrm{Spec}\, \mathbb{Z}_{(p)}[x]$ is necessary, otherwise for $I = \langle p(px-1), (y^2-x)(px-1) \rangle$.

$I_{\bar{\mathbb{Q}}}$ defined a line $x = \frac{1}{p}$ but $\bar{I}$ define hyperbolic $y^2 = x$.

Notation: $x = (x_1, \cdots, x_n)$, $x_{(i)} = (x_1, \cdots, x_{i-1}, 1, x_{i+1}, \cdots, x_n)$,

$\varphi_{(i)} = \varphi(x_{(i)})$ $\forall\, \varphi \in k[x]$, $\varphi_{(i),hom} \in k[x]$ s.t. $x_i \nmid \varphi_{(i),hom}$ & $x_i^{e_i} \varphi_{(i),hom} = \varphi$ for some $e \geq 0$.

Lemma. Let $I \subset k[x]$ be homogenization of a prime ideal $I_{(0)}$ that defines an affine alg. curve.

Then I is a prime. For each i that $I_{(i)} \neq k[x_{(i)}]$, $I_{(i)}$ is a prime, $I_{(i),hom} = I$. and $I_{(i)}$ defines an affine alg. curve.

Def. Let C_{hom} be a nonsingular proj. curve / $\bar{\mathbb{Q}}$ defined by homogenization $I \subset \mathbb{Z}_{(p)}[x]$ of $I_{(0)} \in \mathrm{Spec}\, \mathbb{Z}_{(p)}[x_{(0)}]$. Then C_{hom} has good reduction at p if $\forall i$ either C_i defined by $I_{(i)}$ has good reduction at p, or empty reduction at p. The curve $\bar{C}_{hom}$ defined by homogenization $(\overline{I_{(0)}})_{hom}$ is reduction of C at p.

Prop. If C good at p, then $\bar{C}_{hom}$ is defined by any nonempty reduction $\bar{C}_i$ of an affine piece of C_{hom}.

(pf.) • Let $J = \bar{I}_{(0),hom}$. Then $\bar{I} \subseteq J \Rightarrow \bar{I}_{(i)} \subseteq J_{(i)}$ with $J_{(0)} = \bar{I}_{(0)} = \overline{I_{(0)}}$. Then $\bar{C}_{hom}$ is defined by any $J_{(i)} \neq \mathbb{F}_p[x_{(i)}]$

• If $J_{(i)} \neq \mathbb{F}_p[x_{(i)}]$, then $J_{(i)} = \bar{I}_{(i)}$ (since both are prime and define curve)

• If $J_{(i)} = \mathbb{F}_p[x_{(i)}]$, then $x_i^m \in J$ for some $m \geq 0$. Then $x_i^m \in J_{(0)} = \bar{I}_{(0)} \Rightarrow x_i \in \bar{I}_{(0)}$. Say $x_i = f + pg$ for $f \in I_{(0)} \Rightarrow \forall\, Q = [1 : a_1 : \cdots : a_n] \in C_0$, $a_i \in p\bar{\mathbb{Z}}_{(p)}$. Then $Q \notin C_{i,1}$, where $C_{i,1}$ denoted the points of C whose i-th coordinate can be normalize to 1 and others are p-integral. Then $C_{i,1} \subseteq C \setminus C_0$ is finite. By next theorem, $C_{i,1} \twoheadrightarrow \bar{C}_i$.

Hence $\bar{C}_i$ is finite $\Rightarrow$ empty $\Rightarrow I_{(i)} = \mathbb{F}_p[x_{(i)}]$.

(2) Reduction on points (may replace by number field K)

Main theorem: C: nonsingular alg. proj. curve / $\mathbb{Q}$ good at p. Then $C \twoheadrightarrow \bar{C}$.

(pf.)

- The problem is local, we may assume C is affine. For $Q' \in \bar{C}$,

$$\begin{array}{ccccccccc} & & p\mathbb{Z}_{(p)}[C] & & \mathbb{Z}_{(p)}[C] & & \mathbb{F}_p[\bar{C}] & & \\ & & \| & & \| & & \| & & \\ 0 & \to & \langle p \rangle & \longrightarrow & \mathbb{Z}_{(p)}[x]/I & \longrightarrow & \mathbb{F}_p[x]/\bar{I} & \to & 0 \\ & & p \in m & \longleftarrow & m_{Q'} & & & & \\ & & \downarrow & & \downarrow & & & & \\ & & f & & \bar{f} \neq 0 & & & & \end{array}$$

$\bar{f}$ is nonzero divisor in $\mathbb{Z}_{(p)}[C]/\langle p \rangle \Rightarrow \bar{p}$ is nonzero divisor of $\mathbb{Z}_{(p)}[C]/\langle f \rangle$

Take minimal prime P over f containing $m \Rightarrow p \notin P$.

- Consider $\mathbb{Q}[C] = \mathbb{Q}[x]/I_{\mathbb{Q}}$. then $P\mathbb{Q}[C]$ is nonzero prime of $\mathbb{Q}[C]$ (proper by $p \notin P$). Say $P\mathbb{Q}[C] = m_Q$ for some $Q \in C$. We can identify $\mathbb{Q}[C]/m_Q$ by evaluate at Q, which is a subfield of the Galois extension $K/\mathbb{Q}$ generated by coordinates of Q.

  Claim. $P = m_Q \cap \mathbb{Z}_{(p)}[C]$.

  subpf. ($\subseteq$) Clear. ($\supseteq$) $\forall h \in m_Q$, $\exists n$ s.t. $p^n h \in P \Rightarrow h \in P$ if $h \in \mathbb{Z}_{(p)}[C]$. □

  By Claim, we have

$$e_Q : \mathbb{Z}_{(p)}[C]/P \hookrightarrow \mathbb{Q}[C]/m_Q \subseteq K \quad \text{via evaluate at } Q.$$

- **Lemma.** If S is $\mathbb{Z}_{(p)}$-subalg. of number field K, and $p \in m \in \operatorname{Max} S$.

  Then $\exists q \in \operatorname{Max} \mathcal{O}_K$ lying over p s.t. $S \subseteq \mathcal{O}_{K,(q)}$ and $m \subseteq q\mathcal{O}_{K,(q)}$.

  By Lemma, $\exists q \in \mathcal{O}_K$ lying over p s.t.

$$e_Q\left(\mathbb{Z}_{(p)}[C]/P\right) \subseteq \mathcal{O}_{K,(q)} \quad \text{and} \quad e_Q\left(m_Q/P\right) \subseteq q\mathcal{O}_{K,(q)}$$

$$\Rightarrow e_Q : \mathbb{Z}_{(p)}[C]/m_Q \hookrightarrow \mathcal{O}_{K,(q)}/q\mathcal{O}_{K,(q)}$$

- The reduction map $C \to \bar{C}$ depends on initial choice of maximal prime of $\bar{\mathbb{Z}}$ lying over p, denote $\mathfrak{p}$ be the intersection of that prime with $\mathcal{O}_K$.

  Claim. $\exists \sigma \in \operatorname{Gal}(K/\mathbb{Q})$ takes q to $\mathfrak{p}$.

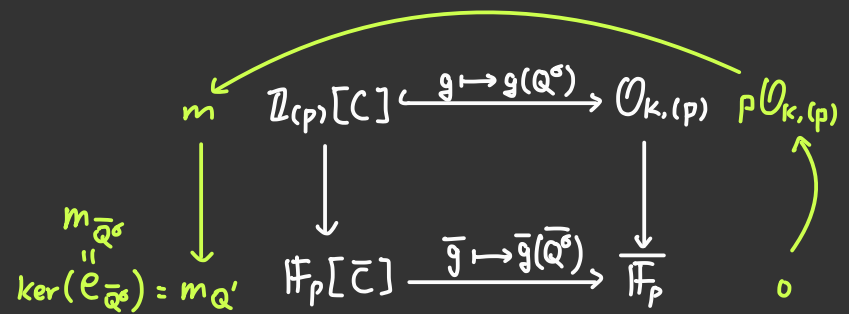
  subproof. Assume $\mathfrak{p} \notin \{q^\sigma : \sigma \in \operatorname{Gal}(K/\mathbb{Q})\}$. By CRT, $\exists \alpha \in \mathcal{O}_K$ s.t. $\alpha \equiv 0 \pmod{\mathfrak{p}}$, $\alpha \equiv 1 \pmod{q^\sigma}$.

  Then $N(\alpha) = \prod_\sigma \alpha^\sigma \in \mathbb{Z} \cap \mathfrak{p} = p\mathbb{Z} \subseteq q \rightsquigarrow \alpha \in q^{\sigma^{-1}}$ for some $\sigma \in \operatorname{Gal}(K/\mathbb{Q})$ $\to\!\leftarrow$.

  Now $\sigma \circ e_Q : \mathbb{Z}_{(p)}[C]/m \hookrightarrow \mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{K,(\mathfrak{p})}$ is evaluate at Q^σ, so all denoted $e_{Q^\sigma} = \sigma \circ e_Q$.

  In particular, takes $x_i \in \mathbb{Z}_{(p)}[C]/m \Rightarrow Q^\sigma$ has $\mathfrak{p}$-integral coordinates.

- Now



Claim: Let V be the affine variety $/k$. If P, P' be the closed point of V and $m_Q = m_{Q'}$ in $k[V]$. Then $\exists \tau \in \mathrm{Aut}(\bar{k}/k)$ s.t. $P' = P^\tau$.

subpf. Say $P = (P_1, \cdots, P_n) \in \mathbb{A}^n_{\bar{k}}$, let $K = \mathbb{Q}(P_1, \cdots, P_n)$ alg. $/k$. Define $\tau: K \longrightarrow \bar{k}$ which is $P_i \longmapsto P_i'$
$P' = (P_1', \cdots, P_n') \in \mathbb{A}^n_{\bar{k}}$

well-defined by $m_P = m_{P'}$. Extend τ to $\bar{k} \longrightarrow \bar{k}$ as required. □

By Claim, $Q' = \bar{Q}^{\sigma^z}$ for some $z \in \mathrm{Aut}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$, which restrict to auto. of finite field $\mathcal{O}_{K,(p)}/p\mathcal{O}_{K,(p)}$. Recall that

$$D_p \twoheadrightarrow D_p/I_p \xrightarrow{\sim} \mathrm{Gal}\left(\mathcal{O}_K/\mathbb{F}_p\right).$$

We may lift τ to D_p, then $Q' = \overline{Q^{\tau\sigma}}$.

Proof of Lemma

Since $S_m\mathcal{O}_K$ is f.g. S_m-module, $S_m\mathcal{O}_K \neq mS_m\mathcal{O}_K$ by Nakayama. Take $M \in \mathrm{Max}\, S_m\mathcal{O}_K$ contains $mS_m\mathcal{O}_K$. It suffices to prove for $(S_m\mathcal{O}_K, M)$. By CRT, $\forall q$ lying over p $\exists \pi_q \in \mathcal{O}_K$ s.t. $v_q(\pi_q) = 1$
$v_{q'}(\pi_q) = 0 \ \forall q' \neq q$.

For $\mathcal{Q} \subseteq \{q \in \mathrm{Spec}\,\mathcal{O}_K : q \mid p\}$, define $R(\mathcal{Q}) = \{x \in K \mid v_q(x) \geq 0 \ \forall q \in \mathcal{Q}\}$. Then

$$R(\emptyset) = K \supset S_m\mathcal{O}_K \supset (\mathbb{Z}\setminus p)^{-1}\mathcal{O}_K = R(\{q \mid p\})$$

($\supseteq$): By uniformizer choose above, may assume $\frac{a}{b}$ $b \notin q$ $\forall p \mid q$. Then $a/b = \frac{a \cdot N(b)/b}{N(b)} \in (\mathbb{Z}\setminus p)^{-1}\mathcal{O}_K$.

Claim. If $R(\mathcal{Q}) \subsetneq S_m\mathcal{O}_K$, $s \in S_m\mathcal{O}_K$, $q \in \mathcal{Q}$ s.t. $v_q(s) < 0$. Then $R(\mathcal{Q}\setminus\{q\}) \subseteq S_m\mathcal{O}_K$.
($\Rightarrow \exists \mathcal{Q} \subseteq \{q \mid p\}$ s.t. $S_m\mathcal{O}_K = R(\mathcal{Q})$.)

subpf. By multiply suitable uniformizer for each prime, may assume $v_q(s) = -1$, $v_{q'}(s) > 0 \ \forall q' \neq q$
By adding π_q, may assume $v_q(s) = -1$, $v_{q'}(s) = 0 \ \forall q' \neq q$. If $t \in R(\mathcal{Q}\setminus\{q\}) \setminus S_m\mathcal{O}_K$, then $v := v_q(t) < 0$, $v_{q'}(t) \geq 0 \ \forall q' \in \mathcal{Q}\setminus\{q\}$. Then $ts^v \in R(\mathcal{Q}) \subseteq S_m\mathcal{O}_K \Rightarrow t \in s^v S_m\mathcal{O}_K \subseteq S_m\mathcal{O}_K$ ↯ □

Claim. Every ideal of $S_m\mathcal{O}_K$ is of the form $\{x : v_q(x) \geq a_q \ \forall q \in \mathcal{Q}\}$ for some $a_q \geq 0$.

subpf. For $x \in I$ and $y \in S_m\mathcal{O}_K$, if $v_q(y) \geq v_q(x) \ \forall q \in \mathcal{Q}$. Then $\frac{y}{x} \in S_m\mathcal{O}_K \Rightarrow y \in xS_m\mathcal{O}_K$ □

By Claim, $\exists q \in \mathcal{Q}$ s.t. $M = S_m\mathcal{O}_K \cap \{v_q \geq 1\}$. Hence $q \in \mathrm{Spec}\,\mathcal{O}_K$ as desired.

(3) Reduction on morphism

$h: C \to C'$ be morphism $/\mathbb{Q}$, say $h = [h_0 : \cdots : h_r]$. May assume $h_i \in R = \mathbb{Z}_{(p)}[C_0] \subseteq \mathbb{Q}[C_0]$ on affine piece. Define $v_p(h_i) = \sup\{e : h_i \in p^e R\} \in \mathbb{N} \cup \{\infty\}$ and $v_p(h) = \min v_p(h_i) < \infty$ (by $\bigcap p^n R = \{0\}$)

Rewrite $h_i' = p^{-v_p(h)} h_i$ and define rational map $\bar{h} = [\bar{h_0'} : \bar{h_1'} : \cdots : \bar{h_r'}] : \bar{C_0} \dashrightarrow \mathbb{P}^r(\mathbb{F}_p)$ since at least one $h_i' \in R \setminus pR$. For each point in $\bar{C_0}$ has the form $\bar{P}$ for some $P \in C_0$. If $\bar{h}(\bar{P}) \neq 0$, then $\bar{g}(\bar{h}(\bar{P})) = \overline{g(h(P))} = 0 \ \forall g \in I'_{(i)} \Rightarrow \bar{h}(\bar{P}) \in \bar{C_i'}$.

$\Rightarrow \bar{h}(\bar{P}) = \overline{h(P)}$ for $\bar{P}$ outside a finite set. Now $\bar{h}$ define a rational map between smooth curve, which can extend uniquely to a morphism $\bar{h}: \bar{C} \to \bar{C'}$

Thm. C, C': nonsingular proj. alg. curve $/\mathbb{Q}$ with good reduction at p, $g(C') > 1$. The diagram

$$\begin{array}{ccc} C & \xrightarrow{h} & C' \\ \downarrow & & \downarrow \\ \bar{C} & \xrightarrow{\bar{h}} & \bar{C'} \end{array}$$

commute for all morphism $h: C \xrightarrow{h} C'$. Moreover, $\deg h = \deg \bar{h}$.

Rmk.
- The diagram may not commute if $g(C') = 0$. For example, $h: \mathbb{P}^1 \to \mathbb{P}^1$ defined by $[x:y] \mapsto [px:y]$.
- The proof is out of scope in this case, which need some knowledge about Néron-model. See more in [BLR 90] Theorem 9.5.1.

Cor. If $g(C'), g(C'') > 0$, then
- $h: C \twoheadrightarrow C' \Rightarrow \bar{h}: \bar{C} \twoheadrightarrow \bar{C'}$ (by reduction map is surj.)
- If $k: C' \to C''$, then $\overline{k \circ h} = \bar{k} \circ \bar{h}$ (by reduction map is surj. $\Rightarrow$ uniqueness)
- If h is isom. then so is $\bar{h}$.

Thm. C, C': nonsingular proj. alg. curve $/\mathbb{Q}$ with good reduction at p. Then

$$\mathrm{Pic}^0(C) \longrightarrow \mathrm{Pic}^0(\bar{C}), \quad [\textstyle\sum n_P(P)] \longmapsto [\sum n_P(\bar{P})]$$

is well-defined. Hence

$$\begin{array}{ccc} \mathrm{Pic}^0(C) & \xrightarrow{h_*} & \mathrm{Pic}^0(C') \\ \downarrow & & \downarrow \\ \mathrm{Pic}^0(\bar{C}) & \xrightarrow{\bar{h}_*} & \mathrm{Pic}^0(\bar{C'}) \end{array}$$

commute for all morphism $h: C \to C'$.

Thm. Let $\varphi: E_1 \to E_2$ be an isogeny over $\overline{\mathbb{Q}}$ of elliptic / $\overline{\mathbb{Q}}$. Then there is a reduction $\overline{\varphi}: \overline{E_1} \longrightarrow \overline{E_2}$ s.t.

(a) $\overline{\varphi}$ is an isogeny.

(b) If ψ is also an isogeny, then $\overline{\psi \circ \varphi} = \overline{\psi} \circ \overline{\varphi}$

(c)
$$\begin{array}{ccc} E_1 & \xrightarrow{\varphi} & E_2 \\ \downarrow & \circlearrowright & \downarrow \\ \overline{E_1} & \xrightarrow{\overline{\varphi}} & \overline{E_2} \end{array}$$

(d) $\deg \varphi = \deg \overline{\varphi}$.