10/18/04.

Lemma. $[C(\mathbb{Q}) : 2C(\mathbb{Q})]$ is finite.

Proposition If we have $C, \bar{C}$ given by the following equations

$$C: y^2 = x^3 + ax^2 + b \qquad \bar{a} = -2a \quad \bar{b} = a^2 - 4b.$$
$$\bar{C}: y^2 = x^3 + \bar{a}x^2 + \bar{b}$$

and $T = (0,0)$

then we have the following homomorphism:

a) $$\phi(P) = \begin{cases} \left(y^2/x^2, \; y(x^2-b)/x^2 \right) & \text{if } P \neq \mathcal{O}, T \\ \bar{\mathcal{O}}, & \text{if } P = \mathcal{O}, T \end{cases}$$
$P = (x, y)$

and let $\phi = \{\mathcal{O}, T\}$.

b) There is a homomorphism $\psi : \bar{C} \longrightarrow C$ s.t.

$$\psi(\bar{P}) = \begin{cases} \left(\bar{y}^2/4\bar{x}^2, \; \bar{y}(\bar{x}^2-\bar{b})/8\bar{x}^2 \right) & \bar{P} \neq \bar{\mathcal{O}}, \bar{T} \\ \bar{\mathcal{O}} & \bar{P} = \bar{\mathcal{O}}, \bar{T} \end{cases}$$

and we have $\psi \circ \phi(P) = 2P$.

Proof. (a) 1. if $P \in C$, $\phi(P) \in \bar{C}$.

2. $\phi(P_1 + P_2) = \phi(P_1) + \phi(P_2) \quad \forall \; P_1, P_2 \in C$.

2.1. If $P_1 = \mathcal{O}$, then $\Rightarrow$ trivial case.

2.2 if $P_1 = T$ then $\phi(P_1 + T) = \phi(P)$ for all P.

$P = (x, y) \qquad T = (0,0) \qquad P+T = \left(\frac{b}{x}, \frac{-by}{x^2}\right)$

$\Big(\; x(P+T) = \left(\frac{y}{x}\right)^2 - a - x$ etc. . . .

$\bar{x}(P+T) =$ x coordinate of $\phi(P+T) =$

$$\left\{ \left(-\frac{by/x^2}{b/x} \right)^2 , \quad \cancel{\left(\frac{-by/x^2}{b/x}\right)^2} - b = \bar{x}(P) = \frac{y^2}{x^2} \right.$$

$$\cancel{\frac{-\frac{by}{x^2}\left(\left(-\frac{b}{x}\right)^2 - b\right)}{(b/x)^2}} = \cancel{\bar{x}(P)} \left(\left(\frac{y}{x}\right)^2, \frac{y(x^2-b)}{x^2} \right).$$

$\bar{y}(P+T) = \bar{y}(P).$

2.3. $P = T \qquad \phi(T+T) = \phi(0) = \bar{0} = \phi(T) + \phi(T).$

2.4. $P = (x,y) \qquad \phi(-P) = \phi(x,-y) = \left(\left(-\frac{y}{x}\right)^2, \frac{-y(x^2-b)}{x^2} \right) =$

$-\phi(P).$

2.5. If $P_1, P_2, P_3 \in C$ and $P_1 + P_2 + P_3 = 0 \Rightarrow$
$\phi(P_1) + \phi(P_2) + \phi(P_3) = \bar{0}$. (suppose $\{P_1, P_2, P_3\} \cap \{0, T\} = \emptyset$.)

$\phi(P_1 + P_2) = \phi(-P_3) = -\phi(P_3) = \phi(P_1) + \phi(P_2).$

if $P_1 + P_2 + P_3 = 0 \iff P_1, P_2, P_3$ are the intersection of a line $y = \lambda x + \nu$ with the curve C

if $P_1 + P_2 + P_3 = 0$

then we shall prove that $\phi(P_1), \phi(P_2), \phi(P_3)$ lie on the line $y = \bar{\lambda} x + \bar{\nu}$ where $\bar{\lambda} = \dfrac{\nu\lambda - b}{\nu}$,

$$\bar{\nu} = \nu^2 - a\nu\lambda + b\lambda^2$$

If $P_i = (x_i, y_i)$, then ~~$\bar{y}_i$~~ $\bar{\lambda}\bar{x_i} + \bar{\nu} = \bar{y_i}$ for each $i = \overline{1,3}$.

$(\phi(P_i) = (\bar{x_i}, \bar{y_i}) \in \bar{C})$.

$\bar{\lambda}\bar{x_i} + \bar{\nu}$ ~~$= \bar{y}_i$~~

$$= \left(\frac{\nu\lambda - b}{\nu}\right)\left(\frac{y_i}{x_i}\right)^2 + \frac{\nu^2 - a\nu\lambda + b\lambda^2}{\nu} = \frac{(\nu\lambda - b)y_i^2 + (\nu^2 - a\nu\lambda + b\lambda^2)x_i^2}{\nu x_i^2}$$

$$= \frac{\nu\lambda(y_i^2 - a x_i^2) - b(y_i^2 - \lambda^2 x_i^2) + \nu^2 x_i^2}{\nu x_i^2}$$

$$= \ldots\ldots\ldots = \bar{y_i}.$$

We proved that if P_i lies on the line $y = \lambda x + \nu$, then $\phi(P_i)$ lies on the line $y = \bar{\lambda} x + \bar{\nu}$

we still need to check that ~~$\phi(P_1), \phi(P_2), \phi(P_3)$~~ $\bar{x}(P_1), \bar{x}(P_2), \bar{x}(P_3)$ are the three points of intersection of $y = \bar{\lambda}x + \bar{\nu}$ with $\bar{C}$ i.e.

are the three solutions of $(\bar{\lambda}x + \bar{\nu})^2 = x^3 + \bar{a}x^2 + \bar{b}x$.

(b). We defined a homomorphism between C and $\bar{C}$
We can define a homomorphism between $\bar{C}$ and $\bar{\bar{C}}$
$\bar{a} = 4a$, $\bar{b} = 16b$.

$(x,y) \in \bar{\bar{C}}$, $\bar{\bar{C}} = y^2 = x^3 + 4ax^2 + 16bx \iff \left(\frac{y}{8}\right)^2 = \left(\frac{x}{4}\right)^3 + a\left(\frac{x}{4}\right)^2 + b\left(\frac{x}{4}\right)$

$\cancel{\left(\frac{x}{4}, \frac{y}{8}\right) \in \bar{\bar{C}}}$.

$\iff \left(\frac{x}{4}, \frac{y}{8}\right) \in C$.

isomorphism $\quad \bar{\bar{C}} \longrightarrow C$

$$(x,y) \xrightarrow{\tau} \left(\frac{x}{4}, \frac{y}{8}\right).$$

$$\begin{tikzcd} \bar{C} \arrow[r, "\varphi"] \arrow[rr, bend right, "\psi"'] & \bar{\bar{C}} \arrow[r, "\tau"] & C \end{tikzcd}$$

$$(\bar{x}, \bar{y}) \overset{\psi}{\longmapsto} \left(\bar{y}^2/\bar{x}^2, \frac{\bar{y}(\bar{x}^2 - b)}{8\bar{x}^2}\right)$$

$$\psi \circ \varphi(x,y) = 2(x,y).$$

Def. An affine "variety" is the locus of a set of polynomial equations over a field
ex. $\{y^2 - x^3 - ax^2 - bx = 0\}$ is an affine "variety".
Def. A projective "variety" in $\mathbb{P}^2_k$ is similarly the locus of a set of homogeneous polynomial equations over a field.
ex. $\{Y^2Z - X^3 - aX^2Z - bXZ^2 = 0\}$ is projective variety.

$G_m = \{$ set of points of order $\mid m$ $\Rightarrow \mathbb{Z}_m \oplus \mathbb{Z}_m$. $\quad G_m = A \oplus B$.

Given $\Gamma =$

Γ/A

$$\begin{tikzcd}
\Gamma \arrow[r] \arrow[rr, bend right, "\ker\ G_m"'] & \underset{\bar\Gamma}{\Gamma/A} \arrow[r] & \underset{\bar{\bar\Gamma}}{\bar\Gamma/B}
\end{tikzcd}$$

$$\Gamma \longrightarrow \Gamma$$
$$P \longrightarrow mP$$
$$P \longrightarrow 2P$$