Learning seminar for Mazur's paper

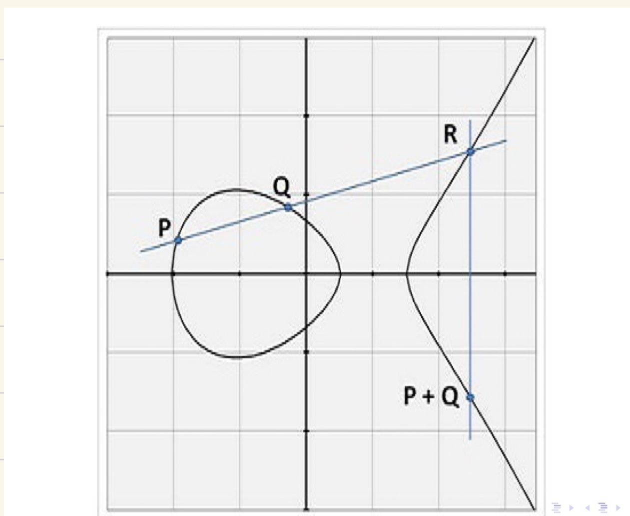
I: Overview.

Setup: k a field.

1: An elliptic curve (E.C.) $/k$ is a pair (E, o) where E is a (smooth, projective, connected) curve $/k$ with genus 1 & $o \in E(k)$.

2: An elliptic curve $/\mathbb{Q}$ is a curve which can be decribed by Weierstrass equation $y^2 = x^3 + ax + b$
so that the discriminant $\Delta = -16(4a^3 + 27b^2) \neq 0$.

3 There is a group low on $E(\mathbb{Q})$ which can be described in the following



Here $o = \infty$.

4. By Mordell-weil's Thm, $E(\mathbb{Q})$ is a finite generated $\mathbb{Z}$-module.
So $$E(\mathbb{Q}) = E(\mathbb{Q})_{tor} \oplus \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{r}$$

$r = \operatorname{rank} E(\mathbb{Q})$ which remains mysterious, BSD conjecture.

5. **Theorem (Mazur, 1977, MR488287).** $C(\mathbf{Q})_{\text{tors}}$ is isomorphic to one of the following 15 groups:

- $\mathbf{Z}/n\mathbf{Z}$ with $1 \leq n \leq 10$ or $n = 12$.
- $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ with $n = 2, 4, 6, 8$.

6: Basic idea: Try to show if $N > 13$ being prime

$$E[N] = E(\mathbb{Q})[N] = \{x \in E(\mathbb{Q}) \mid Nx = 0\} = \{0\}.$$

Let $Y_0(N)$ be modular curve which parameterize (E, G) where $G \subseteq E$ is a cyclic subgp of order N. Need to show $Y_0(N)(\mathbb{Q}) = \phi$. $Y_0(N) \subseteq X_0(N)$ its compactification. Let $J_0(N)$ be it Jacobian, we have $Y_0(N) \to X_0(N) \to J_0(N)$

Now we need construct $Y_0(N) \to X_0(N) \longrightarrow A$. a "good" abelian variety $Y_0(N)(\mathbb{Q}) = \phi$. Note Hecke algebra $\mathbb{T} \supseteq J_0(N)$

The key point is to select a Eisenstein ideal $I \subseteq \mathbb{T}$. to construct $J_0(N) \twoheadrightarrow A$. This involves modular form into the picture.

7: plan of seminar: Basically follows Snowden's course, but need to be condensed.

II Elliptic Curve.

I: Basic fact:

By Riemann-Roch thm $\ell(D) - \ell(K-D) = \deg D - g + 1$ & use $g=1$, we can prove (see silverman Chap II, III).

Group law: $E(k)$ is an abelian group via isomorphism $E(k) \to Cl^0(E)$ via $x \longmapsto [x] - [0]$.

Equation E satisfies cubic Equation.

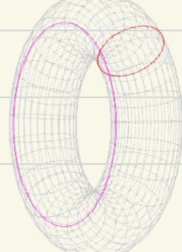
$$a_1y^2 + a_2x^3 + a_3xy + a_4x^2 + a_5y + a_6x + a_7 = 0$$

when $\mathrm{char}(k) \neq 2, 3$, the above equation can be simplified to

$$y^2 = x^3 + ax + b.$$

where $\Delta = -16(4a^3 + 27b^2) \neq 0$.

II Elliptic Curve / $\mathbb{C}$.

$E/\mathbb{C} \iff$ a torus $=$ 

$= \mathbb{C}/\Lambda$ where $\Lambda = \mathbb{Z}$-lattice $\subseteq \mathbb{C}$

i.e $\Lambda \otimes_{\mathbb{Z}} \mathbb{R} = \mathbb{C}$.

$\exists\ \phi: \mathbb{C}/\Lambda \longrightarrow E(\mathbb{C}) \subseteq \mathbb{P}^2(\mathbb{C})$ as isomorphism of complex

$z \longmapsto [\wp(z), \wp'(z), 1]$. Lie groups.

where $\wp(z)$ is Weierstrass $\wp$-function. (Silverman chap VI)

complex multiplication We can use $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$ $\tau \in a+bi$, $b>0$ to understand $\mathrm{End}(E)$, Since $\alpha\Lambda \subseteq \Lambda$, it is not hard to show $\mathrm{End}(E) = \mathbb{Z}$ or an order in $K/\mathbb{Q}$, where K is imaginary quadratic field $/\mathbb{Q}$. The latter case, we call E has complex multiplication.

III Isogenies:

Def An isogeny $f: E_1 \to E_2$ is a non-constant map & $f(0) = 0$.

An isogeny is a group homo. as $[x]-[O] \to [f(x)]-[0]$.

Example: ① $[n]: E \longrightarrow E$: via $x \longmapsto nx$

② If $\mathrm{char}(k) = p$ then $F_p: E \longrightarrow E^{(p)} = k \otimes_{\varphi} E$ via $(x, y) \longmapsto (x^p, y^p)$ is an isogeny.

Note f induces field extension of $k(E_1)/k(E_2)$ where $k(E_i)$ are function field of E_i. We have $k(E_2) \subseteq L \subseteq k(E_1)$ $L/k(E_2)$ is max. seperable extension. & $k(E_1)/L$ is purely inseperable.

Def ① $\deg(f) = [k(E_1) : k(E_2)]$

② If $L = k(E_1)$ then f is seperable

If $L = k(E_2)$ — — —— — inseperable

Example: ① $[n]$ is seperable $\iff$ $\mathrm{char}(k) \nmid n$. $\deg([n]) = n^2$.

② F_p is inseperable.

Dual Isogeny There exists a dual isogeny $f^\vee: E_2 \to E_1$ s.t

$$\begin{tikzcd} E_1 \arrow[r, "f"] \arrow[dr, "{[\deg f]}"'] & E_2 \arrow[d, "f^\vee"] \\ & E_1 \end{tikzcd}$$

see [Silverman, III, Thm 6.1]. Note $f^\vee$ is also defined via

$$\begin{array}{ccccccc} E_2 & \longrightarrow & Cl^0(E_2) & \xrightarrow{f^*} & Cl^0(E_1) & \xrightarrow{\text{sum}} & E_1 \\ Q & \longmapsto & [Q]-[0] & \underset{f^{-1}}{\longrightarrow} & \sum n_p[p] & \longrightarrow & \sum n_p P. \end{array}$$

Note: when $E/\mathbb{C} \simeq \mathbb{C}/\Lambda$. Then $E_1 \xrightarrow{f} E_2 \iff$ $\Lambda_1 \subseteq \Lambda_2$. Then $\deg f = [\Lambda_2 : \Lambda_1]$. & $f^\vee$ is induced by $\Lambda_2 \simeq \deg f\ \Lambda_2 \subseteq \Lambda_1$.

IV Tate module & Weil pairing.

Pick prime $\ell \neq \mathrm{char}(k)$, $E[\ell^n] := \{x \in E(\bar{k}) \mid \ell^n x = 0\}$

It turns out that

$$E[\ell^n] \simeq \mathbb{Z}/\ell^n\mathbb{Z} \oplus \mathbb{Z}/\ell^n\mathbb{Z}. \text{ with } G_k = \mathrm{Gal}(\bar{k}/k)-\text{action}$$

Consider the inverse system: $E[\ell^{n+1}] \xrightarrow{\ell} E[\ell^n]$.

Def The ℓ-adic Tate module $T_\ell(E) := \varprojlim_n E[\ell^n] \simeq \mathbb{Z}_\ell \oplus \mathbb{Z}_\ell$.

with G_k-action. This give arise the p-adic Galois rep.

$$\rho_E: G_k \longrightarrow GL_2(\mathbb{Z}_p).$$

Remark: $E[\ell^n] \simeq \mathbb{Z}/\ell^n\mathbb{Z} \oplus \mathbb{Z}/\ell^n\mathbb{Z}$ can be visually seen when $E \simeq \mathbb{C}/\Lambda$. Then $E[\ell^n] \simeq \frac{1}{\ell^n}\Lambda/\Lambda$.

Weil pairing: [Silverman, § III, 8.3].

Proposition. Let E/k be an elliptic curve and let n be prime to the characteristic. Then there exists a pairing $e_n: E[n] \times E[n] \to \mu_n$ satisfying the following:

- Bilinear: $e_n(x+y,z) = e_n(x,z)e_n(y,z)$. (Note: the group law on $E[n]$ is typically written additively, while that on μ_n is written multiplicatively.)
- Alternating: $e_n(x,x) = 1$. This implies $e_n(x,y) = -e_n(y,x)$, but is stronger if n is even.
- Non-degenerate: if $e_n(x,y) = 1$ for all $y \in E[n]$ then $x = 0$.
- Galois equivariant: $e_n(\sigma x, \sigma y) = \sigma e_n(x,y)$ for $\sigma \in G_k$.
- Compatibility: if $x \in E[nm]$ and $y \in E[n]$ then $e_{nm}(x,y) = e_n(mx,y)$.

Consequence: ① $\exists$ a bilinear, alternate, nondegenerate, Galois invariant pairing $e: T_\ell(E) \times T_\ell(E) \longrightarrow \mathbb{Z}_\ell(1)$.

Furthermore, $e(f(x), y) = e(x, f^\vee(y))$ for an isogeny $f: E_1 \to E_2$.

② For isogeny $f: E \to E$. $\deg(f) = \deg(f|_{T_\ell(E)})$.