PREVIOUSLY...

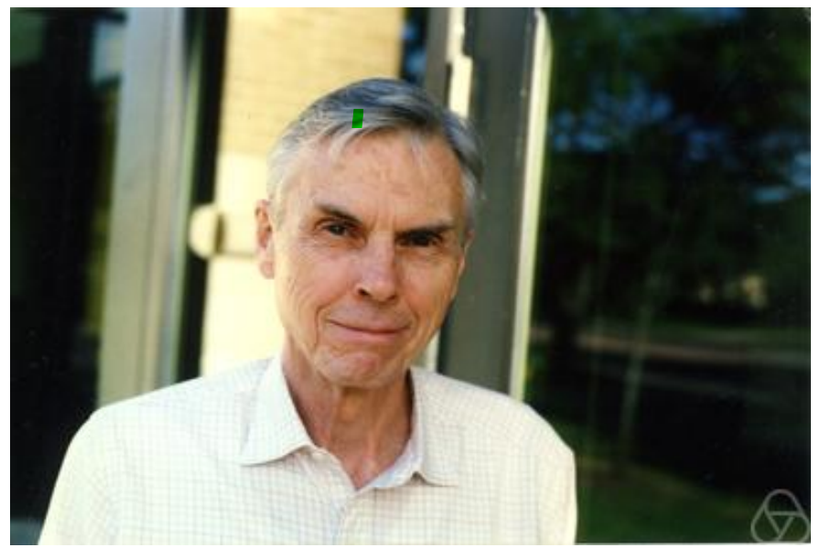
- Intro to Algebraic Geometry up to Riemann-Roch
  - ↳ Definition of elliptic curves and Weierstrass models
- The group law on an elliptic curve
- Isogenies between elliptic curves, and the dual isogeny.

TODAY:

The Tate Module

John Tate

1925 – 2019



LAST TIME:

Isogenies + dual isogenies $\Longrightarrow$ E/k w/ $\mathrm{char}\, k = 0$ then

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$$

for each $m \geq 2$,

$[m] : E \longrightarrow E$

$P \longmapsto \underbrace{P + \cdots + P}_{m}$

where $E[m] = E(\bar{k})[m] = \{P \in E(\bar{k}) : [m]P = \mathcal{O}\}$

$E[m]$: m-torsion subgp of E

ex (part of a hw problem)

Let $E/\mathbb{Q}$ be an elliptic curve given by $y^2 = f(x) = (x-a)(x-b)(x-c)$, $a, b, c \in \overline{\mathbb{Q}}$ (distinct!)

Then $E[2] = \{\mathcal{O}, \underbrace{(a,0)}_{P}, \underbrace{(b,0)}_{Q}, \underbrace{(c,0)}_{R}\}$. Moreover $P+Q=R$, $2P=\mathcal{O}$

$Q+R=P$, $2Q=\mathcal{O}$

$P+R=Q$, $2R=\mathcal{O}$

so $E[2] \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

ex $y^2 = x^3 - x = x(x-1)(x+1)$, $E[2] = \{\mathcal{O}, (0,0), (1,0), (-1,0)\} \subseteq E(\overline{\mathbb{Q}})$.

Inverse Limits

$\{G_n\}_{n=0}^{\infty}$ sequence of gps. $\{f_n : G_n \to G_{n-1}\}_{n=1}^{\infty}$

$$G_0 \xleftarrow{f_1} G_1 \xleftarrow{f_2} G_2 \xleftarrow{f_3} G_3 \leftarrow \cdots$$

$$\varprojlim (G_n, f_n) = \varprojlim G_n \subseteq \prod_{n=0}^{\infty} G_n$$

$$= \{(g_0, g_1, g_2, \ldots) : g_n \in G_n,\ f_n(g_n) = g_{n-1}\}$$

coherent sequences wrt $\{f_n\}$

ex 0 $\quad G_n = \dfrac{\mathbb{Z}[x]}{(x^n)}$, $n \geq 1$, $\quad f_n : \dfrac{\mathbb{Z}[x]}{(x^n)} \longrightarrow \dfrac{\mathbb{Z}[x]}{(x^{n-1})}$

$g(x) \bmod x^n \longmapsto g(x) \bmod x^{n-1}$

$$\varprojlim \frac{\mathbb{Z}[x]}{(x^n)} = \{(g_1(x), g_2(x), g_3(x), \ldots) : g_n(x) \in \mathbb{Z}[x],\ g_n(x) \equiv g_{n-1}(x) \bmod x^{n-1}\}$$

$g_1(x) \bmod x$: a; $g_2(x) \bmod x^2$: $a + bx$; $g_3(x) \bmod x^3$: $a + bx + cx^2$; $\sum a_i x^i$

$\sum a_i x^i$

ex 1 $G_0 = \{0\}$, $G_1 = \mathbb{Z}/p\mathbb{Z}$, $G_2 = \mathbb{Z}/p^2\mathbb{Z}$, $\dots$, $G_n = \mathbb{Z}/p^n\mathbb{Z}$

p prime

$$f_n : \mathbb{Z}/p^n\mathbb{Z} \longrightarrow \mathbb{Z}/p^{n-1}\mathbb{Z}$$
$$a \bmod p^n \longmapsto a \bmod p^{n-1}$$

$$\varprojlim G_n = \varprojlim \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p = \{(a_1, a_2, a_3, \dots) : a_n \equiv a_{n-1} \bmod p^{n-1}\}$$

$a_i \in \mathbb{Z}$

$a_1 \bmod p$, $a_2 \bmod p^2$, $a_3 \bmod p^3$

$\mathbb{Z}_p$: the p-adic integers

ex $p = 5$ $\quad u = (3, 8, 8, 133, 133, 3258, \dots)$

$3 \bmod 5$, $8 \bmod 25$, $133 \bmod 125$, $3258 \bmod 625$

$\mathbb{Z}_p$ is a ring under coord-wise addition and multiplication

ex 2 Let p be a prime, $\mu_{p^n} \subseteq \overline{\mathbb{Q}}$ the p^n-th roots of unity.

$$\{e^{\frac{2\pi i m}{p^n}} : 0 \le m < p^n\} \subseteq \overline{\mathbb{Q}} \subseteq \mathbb{C}$$

$$f_n : \mu_{p^n} \longrightarrow \mu_{p^{n-1}}, \quad \zeta \longmapsto \zeta^p$$

$e^{\frac{2\pi i(m+p^n)}{p^n}} = e^{\frac{2\pi i m}{p^n}} \cdot e^{2\pi i} = e^{\frac{2\pi i m}{p^n}}$ so $m \bmod p^n$

$$\varprojlim \mu_{p^n} = \left\{(\zeta_1, \zeta_2, \dots, \zeta_n, \zeta_{n+1}, \dots) : \zeta_n \in \mu_{p^n} \text{ and } \zeta_{n+1}^p = \zeta_n\right\}$$

$=$ $T_p(\mu)$, the Tate module of $\mathbb{Q}$. (gp under mult.)

- $T_p(\mu)$ is a $\mathbb{Z}_p$-module.

$T_p(\mu) = \varprojlim \mu_{p^n} \cong \varprojlim \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p$ a rank 1 $\mathbb{Z}_p$-module.

Let $u \in \mathbb{Z}_p$, $u = (u_1, u_2, \dots, u_n, \dots)$ $u_i \in \mathbb{Z}$, $u_n \equiv u_{n-1} \bmod p^{n-1}$

Let $t \in T_p(\mu)$, $t = (\zeta_1, \zeta_2, \dots, \zeta_n, \dots)$ $\zeta_i \in \mu_{p^i}$, $\zeta_n^p = \zeta_{n-1}$

$u \cdot t = (\zeta_1^{u_1}, \zeta_2^{u_2}, \dots, \zeta_n^{u_n}, \dots)$

$$(\zeta_n^{u_n})^p = (\zeta_n^p)^{u_n} = (\zeta_{n-1})^{u_n} = \zeta_{n-1}^{u_n \bmod p^{n-1}}$$

$\mu_{p^n} \cong \mathbb{Z}/p^n\mathbb{Z}$, $\zeta \in \mu_{p^n}$, $a \equiv b \bmod p^n$, $\zeta^a = \zeta^b$ $\cong \zeta_{n-1}^{u_{n-1}}$ ✓

ex 3

Let E/K be an elliptic curve ($\mathrm{char}\, K = 0$)

p prime, $G_n = E[p^n] = \ker [p^n]$

$$f_n : E[p^n] \longrightarrow E[p^{n-1}]$$
$$Q \longmapsto [p]Q$$

Remark: $[m] : \overline{K}^* \to \overline{K}^*$, $u \mapsto u^m$

$\mu_{p^n} = \ker [p^n]$

$\varprojlim E[p^n] = T_p(E)$ is the Tate module of E/K or the p-adic Tate module of E

Note: Recall ($\mathrm{char}\, K = 0$) $E[p^n] \cong \mathbb{Z}/p^n\mathbb{Z} \oplus \mathbb{Z}/p^n\mathbb{Z}$

$$T_p(E) = \varprojlim E[p^n] = \varprojlim \mathbb{Z}/p^n\mathbb{Z} \oplus \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p \oplus \mathbb{Z}_p$$

is a rank 2 $\mathbb{Z}_p$-module.

$u = (u_1, u_2, \ldots, u_n) \in \mathbb{Z}_p$

$t = (Q_1, Q_2, \ldots, Q_n, \ldots)$

$u \cdot t = ([u_1]\cdot Q_1, [u_2]\cdot Q_2, \ldots, [u_n]\cdot Q_n, \ldots)$

$[p]Q_n = Q_{n-1} \Rightarrow [p]([u_n]Q_n) = [u_{n-1}]Q_{n-1}$ ✓

Moreover, the Tate module enjoys a Galois action!

ex 2 $T_p(\mu)$, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on μ_{p^n} $\circlearrowright G_{\mathbb{Q}}$

$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = G_{\mathbb{Q}}$

and the action of Galois commutes with $f_n : \mu_{p^n} \longrightarrow \mu_{p^{n-1}}$, $\zeta \longmapsto \zeta^p$

If $\sigma \in G_{\mathbb{Q}}$, then $f_n(\sigma(\zeta)) = (\sigma(\zeta))^p = \sigma(\zeta^p) = \sigma(f_n(\zeta))$

This allows to extend the Gal. action to all of $T_p(\mu)$

by $\sigma \cdot ((\zeta_n)_{n\geq 1}) = (\sigma(\zeta_n))_{n\geq 1}$

Since $T_p(\mu) \cong \mathbb{Z}_p$, $\mathrm{Aut}(T_p(\mu)) \cong \mathbb{Z}_p^\times$, and induces a Gal. representation

$\chi_p : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(T_p(\mu)) \cong \mathbb{Z}_p^\times$ (the p-adic cyclotomic character)

$\sigma \longmapsto (u_n)_{n\geq 1}$ s.t. ζ is a p^n-th root of unity, then

$\sigma(\zeta) = \zeta^{u_n}$

$$\chi_p : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathbb{Z}_p^\times \xrightarrow{\bmod p} \left(\mathbb{Z}/p\mathbb{Z}\right)^\times$$

$$\sigma \longmapsto (u_n)_{n\geq 1} \longmapsto u_1 \bmod p$$

$$\overline{\chi}_p : G_{\mathbb{Q}} \longrightarrow \left(\mathbb{Z}/p\mathbb{Z}\right)^\times$$

mod-p cycl. character

$$\sigma \longmapsto u_1 \bmod p$$

ζ a non-trivial p-th root of unity

s.t. $\sigma(\zeta) = \zeta^{u_1}$.

(Fact: $\mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q}) \cong \left(\mathbb{Z}/p^n\mathbb{Z}\right)^\times$)

$$\left(\zeta \longmapsto \zeta^a\right) \longleftarrow a \bmod p^n$$

ex 3 E/K ell. curve, p prime (char $K = 0$)

$$\varprojlim E[p^n] = T_p(E) \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$$

$\mathrm{Gal}(\bar{K}/K)$ acts on $E[p^n]$:

$\sigma(Q) = \sigma((x_0, y_0)) = (\sigma(x_0), \sigma(y_0))$

$Q \in E[p^n]$: $[p^n](\sigma(Q)) = \sigma([p^n]Q) = \sigma(\mathcal{O}) = \mathcal{O}$

$\sigma \in G_K$ $\Rightarrow \sigma(Q) \in E[p^n]$.

Action extends to $T_p(E)$ $\circlearrowleft G_K$ ($[p^n]$ is an isogeny defined over K, $g(x,y)$ has K-coefficients then $g(\sigma(x), \sigma(y)) = \sigma(g(x,y))$)

Induces a Galois rep'n:

$$\rho_{E,p} : \mathrm{Gal}(\bar{K}/K) \longrightarrow \mathrm{Aut}(T_p(E)) \cong GL(2, \mathbb{Z}_p)$$

$$\sigma \longmapsto ((Q_n) \mapsto (\sigma(Q_n)))$$

CHOICE OF BASIS!!!

FACT!!

$$G_K \xrightarrow{\rho_{E,p}} GL(2, \mathbb{Z}_p) \xrightarrow{\det} \mathbb{Z}_p^\times$$

χ_p the cycl. character !!

- $T_p(E)$ can be used to study isogenies!

$E_1, E_2, \phi: E_1 \longrightarrow E_2 \rightsquigarrow \phi: E_1[p^n] \longrightarrow E_2[p^n]$, $Q \longmapsto \phi(Q)$

$\Rightarrow \mathbb{Z}_p$-linear map $\phi_p: T_p(E_1) \longrightarrow T_p(E_2)$, $(Q_n)_{n\geq 1} \longmapsto (\phi(Q_n))_{n\geq 1}$

$\Rightarrow \mathrm{Hom}(E_1, E_2) \longrightarrow \mathrm{Hom}(T_p(E_1), T_p(E_2))$

THM 7.4. The natural map $\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_p \longrightarrow \mathrm{Hom}(T_p(E_1), T_p(E_2))$

is injective. $\phi \longmapsto \phi_p$

COR. $\mathrm{Hom}(E_1, E_2)$ is a free $\mathbb{Z}$-module of rank at most 4.

Pf. We saw that $\mathrm{Hom}(E_1, E_2)$ is a torsion-free $\mathbb{Z}$-module so

$\mathrm{rank}_{\mathbb{Z}} \mathrm{Hom}(E_1, E_2) = \mathrm{rank}_{\mathbb{Z}_p} \mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_p$

and Thm 7.4 $\Rightarrow \mathrm{rank}_{\mathbb{Z}_p} \mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_p \leq \mathrm{rank}_{\mathbb{Z}_p} \underbrace{\mathrm{Hom}(T_p(E_1), T_p(E_2))}_{\cong M_2(\mathbb{Z}_p)}$

choosing bases

which is of rank 4

THM 7.7 $\mathrm{Hom}_K(E_1, E_2) \otimes \mathbb{Z}_p \longrightarrow \mathrm{Hom}_K(T_p(E_1), T_p(E_2))$

is an <u>isomorphism</u> if (a) K is a finite field (Tate)

(b) K is a number field (Faltings)

THM 7.9 (Serre's "open image" theorem)

Let K be a number field and E/K an ell. curve w/o CM ($\mathrm{End}(E) \cong \mathbb{Z}$)

$$\rho_{E,p} : G_K \longrightarrow GL(2, \mathbb{Z}_p)$$

(a) $\rho_{E,p}(G_K)$ is of finite index in $GL(2, \mathbb{Z}_p)$ for all primes p.

(b) $\rho_{E,p}(G_K) = GL(2, \mathbb{Z}_p)$ for all but fin. many p.

THM (Rouse, Zureick-Brown) Give a complete classification of the case $p=2$ over $K=\mathbb{Q}$.

There are (up to conjugation) exactly 1208 possibilies for $\rho_{E,2}(G_{\mathbb{Q}})$ when there is <u>no CM</u>.