PREVIOUSLY...

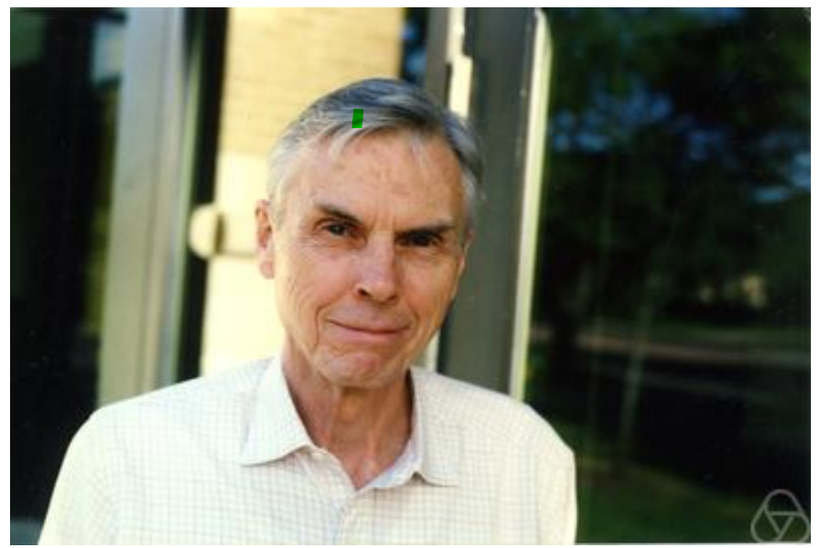
- Intro to Algebraic Geometry up to Riemann-Roch
  - ↳ Definition of elliptic curves and Weierstrass models
- The group law on an elliptic curve
- Isogenies between elliptic curves, and the dual isogeny.

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

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

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

$a_i \in \mathbb{Z}$

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

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

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 mult