<u>Last time</u> We finished discussing $\mathbb{Q}_\ell$-representations of G_K for $K/\mathbb{Q}_p$ finite extension.

<u>Main consequence:</u> Described by a representation w/ finite image on inertia & a nilpotent matrix.

Examples of p-adic representations:

Cyclotomic character, Kummer representations, abelian representations.

<u>Today:</u> Elliptic curves, Tate modules & examples from this (baby case of étale cohomology).

Elliptic curve over a field K is a smooth proper genus 1 dimension 1 geometrically connected scheme $/K$.

(char $K \neq 2,3$) $\quad E: y^2 = x^3 + ax + b \quad$ $a, b \in K$. no multiple roots

(take Zariski closure in $\mathbb{P}^2$).

<u>E.g.</u> $\mathbb{C}/\Lambda \qquad \Lambda = \mathbb{Z}e + \mathbb{Z}f$ lattice.

(use $\wp \qquad y = \wp' \quad x = \wp$).

If E/K is an elliptic curve then E is a group <u>scheme</u>. (i.e. $\underset{\text{addition}}{E \times E \to E}$ w/ expected properties)

identity element is $\infty = [0:1:0]$.

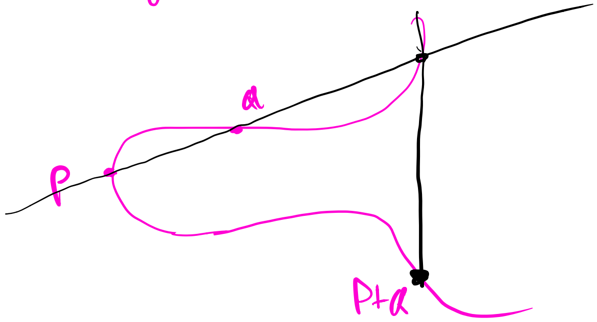
($E \subseteq \mathbb{P}^2$ via Weierstrass equation).

Group structure is obvious

In general: $E \xrightarrow{\sim} \mathrm{Jac}\, E$ ← Group structure.

$P \mapsto (P) - (\infty)$

Can also give a geometric construction:



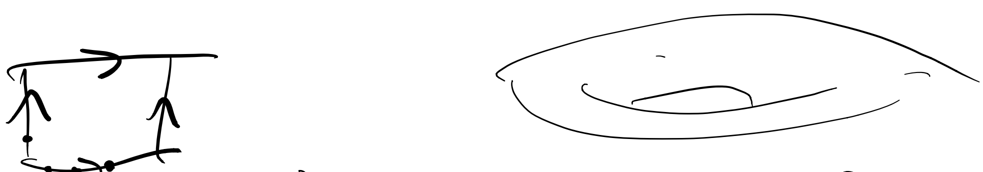
If $\overline{K}$ is an algebraic closure of K

$E(\overline{K})[n]$ ← n-torsion points

($E[n](\overline{K})$ $E[n]$ = n-torsion sub-scheme)

<u>Example</u> $\mathbb{C}/\mathbb{Z}+\mathbb{Z}i \cong E(\mathbb{C})$ $E: y^2 = x^3 + x$

n-torsion



$$\left(\tfrac{1}{n}\mathbb{Z} + \tfrac{1}{n}\mathbb{Z}i\right)/\mathbb{Z}+\mathbb{Z}i \cong (\mathbb{Z}/n\mathbb{Z})^2$$

with basis $\frac{1}{n}$, $\frac{i}{n}$.

In general if $(n, \mathrm{char}\, K)$ then $E(\overline{K})[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$.

$$G_K = \mathrm{Gal}(\overline{K}/K) \circlearrowright E(\overline{K})[n].$$

Because E, multiplication, identity element
are all defined using polynomials over K.

(e.g. $y^2 = x^3 + x$ $\quad K = \mathbb{R}$

$y = i$ $\quad x = a =$ real root of $x^3 + x = 1$.

(i, a) $\quad i^2 = a^3 + a$

$(\bar{i}, \bar{a})$

$(-i, a)$ $\quad (-i)^2 = a^3 + a$

$\quad\quad\quad\quad\quad\quad i^2$.

fix compatible bases for $E[\ell^n]$.

If ℓ is a prime number

$$T_\ell E := \varprojlim_n E(\bar{K})[\ell^n] \leftarrow \mathbb{Z}_\ell\text{-module.}$$

free of rank 2 if $(\mathrm{char}\, K, \ell) = 1$.

$$V_\ell E = T_\ell E[\tfrac{1}{\ell}]$$

$V_\ell E$ 2-dim'l $\mathbb{Q}_\ell$-vector space.

$$G_K \circlearrowright T_\ell E \qquad G_K \circlearrowright V_\ell E.$$

2-dim'l representation of G_K.

Back to $K =$ finite extension of $\mathbb{Q}_p$.

<u>Claim</u> For any $\pi \in K$ with $|\pi| < 1$
there is an elliptic curve
E_π s.t. $E_\pi(\mathbb{C}_p) \cong \mathbb{C}_p^\times / \pi^{\mathbb{Z}}$

compatible with G_K-actions.

(Tate curve)

(Like if $\tau \in \mathbb{H}$ $(\tau = a+bi \quad b>0)$

$$\mathbb{C}/\mathbb{Z}+\mathbb{Z}\tau \xrightarrow{\sim} \mathbb{C}^*/(e^{2\pi i \tau})^{\mathbb{Z}}$$

$$z \longmapsto e^{2\pi i z}.$$

$|\pi| < 1.$)

<u>Exercise</u> Find a basis for $E_\pi(\mathbb{C}_p)[n]$ and describe the Galois action on it.

(take $n = \ell$ prime if it's easier to think about.)

ζ_n = primitive nth root of unity.

$\pi^{1/n}$ = nth root of π

$\zeta_n^n = 1$ = identity in $\mathbb{C}_p^\times/\pi^{\mathbb{Z}}$

$(\pi^{1/n})^n = \pi$ = identity in $\mathbb{C}_p^\times/\pi^{\mathbb{Z}}$.

Give a basis.

Subspace generated is preserved by Galois

χ_n = nth cyclotomic.

$$G_K \to GL_2(\mathbb{Z}/n\mathbb{Z}).$$

$$\sigma \mapsto \begin{pmatrix} \chi_n & \tau_\pi \\ 0 & 1 \end{pmatrix}$$

Extension of trivial representation by cyclotomic.

$\tau_\pi : G_K \to \mu_n(\mathbb{C}_p)$

(a cocycle; homomorphism if $\mu_n(\mathbb{C}_p) \subseteq K$.)

If I look at ℓ-adic Tate-module.

$$G_K \to \begin{pmatrix} \chi_{\ell\text{-adic}} & \tau_\pi \\ 0 & 1 \end{pmatrix}$$

in basis (ζ_{ℓ^n}) (π^{1/ℓ^n})

Kummer representations.

$\ell \neq p$ tamely ramified. $\ell = p$ very wildly ramified.

WARNING: Unlike over $\mathbb{C}$, not every elliptic curve over K (over $\mathbb{C}_p$) admits such a uniformization.

__Bonus exercise:__ Do same exercise for $K = \mathbb{R}$.

__Example__ $E: y^2 = x^3 + x$

(Caveat: no matter what p is this will not be a Tate curve).

$K = \mathbb{Q}_p$ if $p \equiv 1 \bmod 4$

$\mathbb{Q}_{p^2}$ if $p \equiv 3 \bmod 4$

Ignore $p = 2$.

$i \in K$ s.t. $i^2 = -1$.

$$(x, y) \overset{F_i}{\longmapsto} (-x, iy)$$

$$(iy)^2 \overset{?}{=} (-x)^3 + (-x)$$

$(F_i)^2(x, y) = (x, -y)$ which is -1 in the group law

$-y^2 = -x^3 + -x$ ✓ if $y^2 = x^3 + x$.

so F_i is an automorphism of E.

(as curve + group structure).

$\mathbb{Q}_\ell \subseteq \mathrm{End}(V_\ell E)$ $(\cong M_2(\mathbb{Q}_\ell))$.

$F_i \in$

$$\underline{\underline{\mathbb{Q}_\ell[x]/x^2+1}} \subseteq \mathrm{End}(V_\ell E).$$

$\cong$

unramified ext'n of degree 2 of $\mathbb{Q}_\ell$ $=$ $\mathbb{Q}_{\ell^2}$ if $\ell \equiv 3 \bmod 4$ $\mathbb{Q}_\ell \times \mathbb{Q}_\ell$ if $\ell \equiv 1 \bmod 4$. $\leftarrow$ as $\mathbb{Q}_\ell$-algebra.

Because F_i is defined with coefficients in K, the action of G_K commutes with this.

If $\ell \equiv 3 \bmod 4$

$V_\ell E$ 1-dim'l $\mathbb{Q}_{\ell^2}$-vector space

with G_K-action.

$\uparrow$ so it must be abelian.

$\Downarrow$

Looks like the abelian action I wrote down last time if $\ell = p$.