5/10 – Formal Gps

- Defn
- $\hat{G}_a$ example : $F(X,Y) = X+Y$
- $\hat{G}_m$ example: $F(X,Y) = X+Y+XY$
- E given by $w = z^3 + a_1zw + a_2z^2w + a_3w^2 + a_4zw^2 + a_6w^3 = f(z,w)$

We want to <u>work locally</u>, but Zariski Top has open sets dense

So look at algebra side: <u>$K[E]_{(P)}$</u> -- localized at max. ideal (P)

This is easier w/ $P = \mathcal{O}$ = identity

$z = -\frac{x}{y}$, $w = -\frac{1}{y}$ change of coords $\Rightarrow$ z has a zero of order 1 at $\mathcal{O}$ $\Rightarrow$ z is a <u>local uniformizer at $\mathcal{O}$</u>

Plug into W.E. to get $w = z^3 + (a_1z + a_2z^2)w + (a_3 + a_4z)w^2 + a_6w^3$

Sub in recursively for w to get $w(z) \in \mathbb{Z}[a_1,\dots,a_6][[z]]$

Pf is Hensel's Lemma: R complete w.r.t. (z), find soln to $f(z,w) - w$

- We now have Laurent series for x & y: $x(z) = \frac{z}{w(z)}$, $y(z) = -\frac{1}{w(z)}$

Also for the Invariant Differential $\omega(z) = \frac{dx(z)}{2y(z) + a_1x(z) + a_3}$

- $x(z)$ & $y(z)$ are a soln to W.E. Can we plug in values $z \in K$ and get pts on E? Well, we need K = complete local field

$R = \mathcal{O}_K$, $\mathfrak{M}$ = max. in R

Then $\mathfrak{M} \hookrightarrow E(K)$ by eval of $x(z), y(z)$

- Messy linear algebra $\Rightarrow$ $(z_1, w(z_1)) \oplus (z_2, w(z_2))$ can be expressed as $F(z_1, z_2)$ by finding line b/t them, intersecting w/ E, then flipping via $i(z)$

$\hat{E}$ = formal gp assoc to E/K with this $F(z_1,z_2)$

So $\hat{E}(\mathfrak{M}) \hookrightarrow E(K)$ is a gp homomorphism.

still local field condition, so R complete & local.

- Recall: $\hat{F}(\mathfrak{m}) =$ gp assoc to $F = (\mathfrak{m}, \oplus)$ where $x \oplus y = F(x,y)$ & $\ominus x = i(x)$

- Ex: $\hat{G}_a(\mathfrak{m})$ is $\mathfrak{m}$ with usual addition law. $0 \to \hat{G}_a(\mathfrak{m}) \to R \to k \to 0$ ($R \to k$ is $R/\mathfrak{m}$)

- Ex: $\hat{G}_m(\mathfrak{m}) = (1\text{-units}, \text{gp law mult})$. $1 \to \hat{G}_m(\mathfrak{m}) \xrightarrow{z \mapsto 1+z} R^* \to k^* \to 1$ ($k^* = R^*/(1+\mathfrak{m})$)

- Recall: $0 \to \underbrace{E_1(K)}_{\{P \in E(K) \mid \tilde{P} = \tilde{0}\}} \to E_0(K) \xrightarrow[\text{mod } \pi]{} \tilde{E}_{ns}(k) \to 0$

$$0 \to E_1(K) \to E(K) \xrightarrow{\text{red}^n} \tilde{E}(k) \to 0$$

Fact: $\hat{E}(\mathfrak{m}) \hookrightarrow E_1(K)$ by $z \mapsto \left(\frac{z}{w(z)}, -\frac{1}{w(z)}\right)$ is an iso

well-def b/c $\mathfrak{m}$ maximal so $w(z)$ converges

$\hat{E}(\mathfrak{m}) \cong E_1(K)$

Homo b/c the power series for $\oplus$ on $\hat{E}$ just uses $\oplus$ from E & $w \mapsto w(z)$

1-1 b/c $w(z) = 0$ only when $z = 0$

Onto b/c $E_1(K) \to \hat{E}(\mathfrak{m})$ by $(x,y) \mapsto -\frac{x}{y}$ well-def $\left(\frac{x}{y} \in \mathfrak{m}\right)$

& homo & 1-1 so $\hat{E}(\mathfrak{m}) \hookrightarrow E_1(K) \hookrightarrow \hat{E}(\mathfrak{m})$ (id)

- Note: $[m]$ is iso on $\hat{E}(\mathfrak{m})$ if $p \nmid m$. $\hat{E}(\mathfrak{m})[m] = 0$

$\forall a \in \hat{E}(\mathfrak{m})$, $\text{ord}(a) = p^\ell$ some ℓ (b/c $\hat{E}(\mathfrak{m}^n)/\hat{E}(\mathfrak{m}^{n+1}) \cong \mathfrak{m}^n/\mathfrak{m}^{n+1} \in k\text{-vect}$)

$\therefore E_1(K)$ has no non-triv pts of order m

$\therefore$ If $\tilde{E}$ is non-sing $E(K)[m] \to \tilde{E}(k)$ reduction map is 1-1 b/c $E_1(K) = pt$.

This is used to prove weak Mordell-Weil $\left|E(K)/mE(K)\right| < \infty$ $\forall m$

- To prove $[m]$ is sj need $\forall a \in R^*$ $\forall f(T) \in R[[T]]$ s.t. $f(T) = aT + \cdots$ $\exists g(T)$ s.t. $f(g(T)) = T$

~~Height 0 E.C. ⇔ Supersingular~~

Height 1 E.C. ⇔ Ordinary

Height 2 E.C. ⇔ Supersingular

Elliptic Cohomology is a functor: {E.C.'s} → Cohomology theories

Tate curve captures info of height 2 curves. W.E. for many E.C.s

Tate curves are like a cusp of {E.C.'s}

- Often we can reduce to studying $\hat{G}_a$:

  A differential form is $P(T)dT$

  The invariant differential $w(T)$ has $P(F(T,S))F_X(T,S) = P(T)$

  ↳ $P(T) = F_X(0,T)^{-1}$ works

$$\log_F(T) = \int w(T) = \int 1 + c_1 T + c_2 T^2 + c_3 T^3 + \cdots \; dT = T + \frac{c_1}{2}T^2 + \frac{c_2}{3}T^3 + \cdots \in K[[T]]$$

- Fact: R torsion-free $\Rightarrow \log_F : F \to \hat{G}_a$ is iso over $K = R \otimes \mathbb{Q}$

  ↳ Cor: $\log_F(F(X,Y)) = \log_F(X) + \log_F(Y)$ so $\log_F^{-1}(\log_F(X) + \log_F(Y)) = F(X,Y)$ ∴ [log defn]

- Now, If $R = \mathbb{Z}_p$ & $p \neq 2$ then $F(p\mathbb{Z}_p)$ has no torsion (Varg)

  $p = 2$ then at most elts of order 2

  Same for $\mathcal{O}_K$ of any unramified K over $\mathbb{Q}_p$

  (A large part of $F(M)$ looks like the additive gp)

Char 0 (complete local field)

- If $v(K^*) = \mathbb{Z}$, p prime, $v(p) > 0$, & F/R then $\log_F : F(m) \to (K, +)$ is homo

  Also, if $r > v(p)/(p-1)$ in $\mathbb{Z}$ then $\log_F : F(m^r) \to \hat{G}_a(m^r)$ is iso

---

Char p

- $f : F \to G$ ... height is max h s.t. $f(T) = g(T^{p^h})$ some $g(T) \in R[[T]]$

  OR: 1st nonzero term in f's power series exp is ax^{p^h}

- Height$(F) := ht([p])$

- $K = \bar{K} \Rightarrow ht(F) = ht(G)$ iff $F \cong G$

- $$ht(\hat{E}) = \begin{cases} 1 & \text{if } E \text{ ordinary} \\ 2 & \text{if } E \text{ supersingular i.e. } E[p^r](\bar{K}) \cong 0 \ \forall r \end{cases}$$

Connection b/t FGL & L-Series

- Let E be E.C. & $\omega = dx/(2y + a_1x + a_3)$ be inv. differential

If E is modular & corresponds to cusp form $g(q)$ then $\omega = c \cdot \frac{g(q)}{q} dq$
$= c\sum a_n q^{n-1}$

$\therefore \int \omega = f$ & $f(q) = c\sum a_n \frac{q^n}{n}$ ... elliptic logarithm

FGL on E is $F(x,y) = f^{-1}(f(x) + f(y))$

Eichler-Shimura $\Rightarrow$ coeffs of $g(q)$ are coeffs of $L(s) = \sum a_n n^{-s}$

- Given $L(s) = \sum a_n n^{-s}$, set $f(x) = \sum a_n \frac{x^n}{n}$ & fact: $F(x,y) = f^{-1}(f(x) + f(y))$

$E(\mathbb{C}) \cong \mathbb{C}/\Lambda \cong \mathbb{C}^*/q^{\mathbb{Z}}$ for $q = e^{2\pi i z}$

more gen: K complete w.r.t. nonarch abs value

$K/\mathbb{Q}_p$ finite

Tate p-Uniformization Thm: Let K be a p-adic field & E/K with $|j(E)| > 1$, $\gamma(E/K) = -c_4/c_6 \in K^*/K^{*2}$

a) $\exists!\ q \in K^*$ with $|q|<1$ & $E \cong E_q$ over $\bar{K}$

Tate Curve

Here $E_q : y^2 + xy = x^3 + a_4(q)x + a_6(q)$ for $s_k(q) = \sum_{n\geq 1} \frac{n^k q^n}{1-q^n}$, $a_4(q) = -5s_3(q)$

$$a_6(q) = -\frac{5s_3(q) + 7s_5(q)}{12}$$

b) TFAE:
(i) $E \cong E_q$ over K
(ii) $\gamma(E/K) = 1$
(iii) E has split multiplicative reduction

- For (a) you just need $\exists!\ q$ with $j(E_q) = j(E)$
For (b) need "$E \cong E_q$ over K iff $j(E) = j(E_q)$ & $\gamma(E/K) = \gamma(E_q/K)$"
Use formulas in 3.1 for c_4 & c_6 to get (i)$\Leftrightarrow$(ii), i.e. $\gamma(E_q) = 1$
(i)$\Rightarrow$(iii): $|a_4(q)| = |a_6(q)| = |q| < 1 \Rightarrow \tilde{E}_q$ is $y^2 + xy = x^3$, which has split mult red.
(iii)$\Rightarrow$(ii): $(0,0)$ singular mod $\mathfrak{m} \Rightarrow a_3 \equiv a_4 \equiv a_6 \equiv 0 \pmod{\mathfrak{m}}$ & $\gamma \equiv \frac{1}{b_2} \equiv b_2 \pmod{K^{*2}}$ for b_2 unit
split red $\Rightarrow b_2$ is a square in K^* b/c $\tilde{E}$ has a node $(y-\tilde{\alpha}x)(y-\tilde{\beta}x)$
and Hensel $\Rightarrow \tilde{\alpha}$ & $\tilde{\beta}$ lift uniquely s.t. $b_2 = (-\alpha-\beta)^2 + 4(-\alpha\beta) \equiv 1 \pmod{K^{*2}}$

- **Thm 3.1:** If $|\cdot|$ is the absolute value of K & $|q|<1$ w/ $q \in K^*$
a) $a_4(q)$ & $a_6(q)$ converge in K
b) $\Delta(E_q) = q\prod_n (1-q^n)^{24}$ & $j(E_q) = \frac{1}{q} + \sum_n c(n)q^n$ for $c(n) \in \mathbb{Z}$
c) $X(u,q) = \sum_n \frac{q^n u}{(1-q^n u)^2} - 2s_1(q)$, $Y(u,q) = \sum_n \frac{(q^n u)^2}{(1-q^n u)^3} + s_1(q)$

Tate Map

converge $\forall u \in \bar{K}, u \notin q^{\mathbb{Z}}$, so $\phi : \bar{K}^* \to E_q(\bar{K})$ by $u \mapsto \begin{cases} (X(u,q), Y(u,q)) & \text{if } u \notin q^{\mathbb{Z}} \\ \mathcal{O} & \text{if } u \in q^{\mathbb{Z}} \end{cases}$

d) $\forall \sigma \in G_{\bar{K}/K}$, $\Phi(u^\sigma) = \Phi(u)^\sigma$. $\ker \Phi = q^{\mathbb{Z}}$ so $L^*/q^{\mathbb{Z}} \cong E_q(L)$ by Φ for L/K algebraic.

Pf(a): $|q|<1$ & $a_4(q) \in \mathbb{Z}[[q]] \Rightarrow$ conv in K. Same for $a_6(q)$.

Pf(b): $\Delta(q) \equiv q \pmod{q^2}$ by subbing in $a_j(q)$ to usual Δ formula
$\therefore |\Delta(q)| = |q| \neq 0$. Result is now Jacobi's formula for $q \in \mathbb{C}$ but
now lifted to be an identity of formal power series.
$j(q)$ similar, need a formal quotient of power series

Pf(c): $u \in \bar{K}^* \setminus q^{\mathbb{Z}}$ to have $|X|, |Y| < 1$. Terms of series are in $K(u) = \mathbb{Q}_p(u,q)$
which is complete b/c finite ext of $\mathbb{Q}_p$.
Rewrite $X(u,q)$ & $Y(u,q)$ as elts of $\mathbb{Q}(u)[[q]]$
Show E_q holds even when these are subbed in for x, y. It will hold $\forall u$.
Restrict to $|q| < |u| \leq 1$ & $u \neq 1$. Show $Y(u,q)^2 + X(u,q)\,Y(u,q) \overset{?}{=} X(u,q)^3 + a_4(q) X(u,q) + a_6(q)$
in $\mathbb{Q}(u)[[q]]$

$|q|_\omega < |u|_\omega < |q|_\omega \Rightarrow$ True for #s. Let u fixed w/ $|q|_\omega < |u|_\omega < 1$ & let q vary. So power series are $=$.
Now let u vary & coeffs are $=$. "Lift the # equalities"

Φ homo: Use "periodicity" $\Phi(qu) = \Phi(u)$ & set $u_3 = u_1 \cdot u_2$ then prove $P_3 = P_1 + P_2 \in E_q$
Cases: $u_i = 1$, $u_1 u_2 = 1$, $P_i = O$
$x_i = X(u_i, q)$ $x_1 \neq x_2 \Rightarrow$ get 2 identities from $P_1 + P_2 = P_3$ relation & "lift equality" to $\mathbb{Q}(u)[[q]]$
$x_1 = x_2 \Rightarrow P_1 = \pm P_2 \Rightarrow$ Φ algebra & canceling $\Phi(u)$ from eqn.
$\ker \Phi = q^{\mathbb{Z}} = \{1, q, q^{-1}, q^2, q^{-2}, \ldots\}$ is clear from defn of Φ.

Surj: Show $\Phi: L^* \to E_q(L)$ surj $\forall$ L/K finite (notation: $L = K$, $K = \mathbb{Q}_p$ so $K/\mathbb{Q}_p$ finite)
$E_{q,0} = \{P \mid \tilde{P} \in \tilde{E}_{q,ns}(k)\}$ & $E_{q,1} = \{P \mid \tilde{P} = \tilde{O}\}$ reduction mod $\mathcal{M}$
$E_q(K) \supseteq E_{q,0}(K) \supseteq E_{q,1}(K)$ with $E_{q,1} \cong \hat{E}_q$ & $E_{q,0}/E_{q,1} = \tilde{E}_{q,ns}$
$K^*/q^{\mathbb{Z}} \supseteq R^* \supseteq R_1^* = \{u \in R \mid u \equiv 1 \pmod{\mathcal{M}}\} = 1\text{-units} = \hat{G}_m(\mathcal{M})$ & $R^*/R_1^* \cong k^*$

① φ on R_1^*

φ surj: $u \equiv 1 \pmod{\mathfrak{m}} \Rightarrow \operatorname{ord}_v(X(u,q)) < 0$ so $\varphi(R_1^*) \subseteq E_{q,1}(K)$

Iso b/c $\hat{G}_m(\mathfrak{m}) \xrightarrow{\cong} R_1^* \xrightarrow{\varphi} E_{q,1}(K) \xrightarrow{\cong} \hat{E}_q(\mathfrak{m})$

$\mathfrak{m}$ — Laurent Series in $t = q-1$

Map is $\psi: \mathfrak{m} \to \mathfrak{m}$ & ψ has an inverse power series
$t \mapsto t\left(1 + \sum_m \gamma_m t^m\right)$

② φ on R^*/R_1^*... $\varphi(R^*) \subseteq E_{q,0}(K)$ b/c $X(u,q) \not\equiv 0 \pmod{\mathfrak{m}}$ $\forall u$

$k^* \cong R^*/R_1^* \xrightarrow{\varphi} E_{q,0}(K)/E_{q,1}(K) \cong \tilde{E}_{q,ns}(k)$

surj w/ inverse $(x,y) \mapsto \frac{x^2}{x^3}$ so it's iso.

③ φ on R^*:

$$\begin{array}{ccccccc} 1 & \to & R_1^* & \to & R^* & \to & k^* \to 1 \\ & & \downarrow\cong & & \downarrow\varphi & & \downarrow\cong \\ 0 & \to & E_{q,1}(K) & \to & E_{q,0} & \to & \tilde{E}_{q,ns}(k) \to 0 \end{array}$$

$\therefore \varphi$ is iso

④ $\varphi: K^*/R^* q^{\mathbb{Z}} \to E_q(K)/E_{q,0}(K)$ is surj ... LHS $\cong \mathbb{Z}/\operatorname{ord}_v(q)\mathbb{Z}$ via $u \mapsto \operatorname{ord}_v(u)$

Prop: $\#\, E_q(K)/E_{q,0}(K) \leq \operatorname{ord}_v(q)$ via geometry & cosets (counting)

Lemma: $E_q(K)$ is $E_{q,0}(K) = \{(x,y) \mid |x| \geq 1 \text{ or } |y| \geq 1\}$

$U_n = \{(x,y) \mid |\pi|^n = |y| > |x+y|\}$
$V_n = \{(x,y) \mid |\pi|^n = |x+y| > |y|\}$
$W_n = \{(x,y) \mid |y| = |x+y| = |q|^{1/2}\}$

components of fiber of Neron model of E_q over $\operatorname{Spec}(R)$

Cases w/ $\operatorname{ord}_v(q)$ & where P_1 & P_2 lie.

• Exponentiating $\mathbb{C}/\Lambda_\tau$ picture gives $\frac{\mathbb{C}^*}{q^{\mathbb{Z}}} \xrightarrow{\cong} E_q(\mathbb{C})$

for $q = e^{2\pi i \tau}$ $\quad u \longmapsto \begin{cases} (x,y) & u \notin q^{\mathbb{Z}} \\ O & \text{o/w} \end{cases}$

• Let $q \in \mathbb{Q}_p^*$ with $|q| < 1$. Then $\mathbb{Q}_p^* \cong q^{\mathbb{Z}}$ as a discrete subgp

• Let $K/\mathbb{Q}_p$ finite, $q \in K^*$, $|q| < 1$. Then $E_q(K) : y^2 + xy = x^3 + a_4(q) + a_6(q)$ & $a_4(q)$ converge

---

• Cor of Tate: K = # field, $j(E) \notin \mathcal{O}_K$ then for a.a. ℓ in $\mathbb{Z}$ $\exists \sigma \in G_{K(E)/K}$

s.t. $\rho_\ell(\sigma) \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{\ell}$ by $\rho_\ell : G_{K(E)/K} \to \mathrm{Aut}(T_\ell E)$

• Cor: Hypotheses above $\Rightarrow \mathrm{End}(E) \cong \mathbb{Z}$