① Formal Groups are a useful tool for studying E.C. They pop up all over

A formal group law (fgl) over R (comm ring) is power series $F(X,Y) \in R[[X,Y]]$

① $F(X,Y) = X + Y +$ (terms of deg ≥ 2)

② $F(X, F(Y,Z)) = F(F(X,Y), Z)$

③ $F(X,Y) = F(Y,X)$

④ $F(X,0) = X$ & $F(0,Y) = Y$

⑤ $\exists !\ i(T) \in R[[T]]$ s.t. $F(T, i(T)) = 0$

"Gp law w/o gp elts"

<u>Ex</u>: $\hat{G}_a$ = formal additive gp, given by $F(X,Y) = X+Y$

$\hat{G}_m$ = formal multiplicative gp, given by $F(X,Y) = X+Y+XY$

Why should we care?

after change of coords

We want to study E locally. Open sets are dense so not a topologists version of locally. You can try Euclidean top, but still ∞-many pts in U

Best way: move from geo side to alg side & look at $K[E]_O$

after change of coords $Z = -\frac{X}{Y}$, $W = -\frac{1}{Y}$ (so $X = \frac{Z}{W}$ & $Y = -\frac{1}{W}$)

Then Z = local uniformizer @ O, i.e. has zero of order 1 at O

$W = Z^3 + a_1 ZW + a_2 Z^2 W + a_3 W^2 + a_4 Z W^2 + a_6 W^3 = f(Z,W)$

Plug w into self over & over: get $W = Z^3(1 + A_1 Z + A_2 Z^2 + \dots) \in \overbrace{\mathbb{Z}[a_1, \dots, a_6]}^{R}[[Z]]$

(2) Proof that this procedure converges to a power series is Hensel's Lemma

b/c R is complete w.r.t. (z) & we can get $f(z,b)-b=0$ for $b\in R$, $b\equiv 0\,(z^n)$

from $w_0=0$, $w_{m+1}=w_m+f(z,w)-w$

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

$x(z)$ & $y(z)$ are sol'n to W.E.

Can we plug in $z\in K$ & find pts on E?? [K = complete local field, R, m, k]

$m \hookrightarrow E(K)$ by $z\mapsto (x(z),y(z))$

- [Is there a power series to add them? Yes! $(z_1,w(z_1))\oplus(z_2,w(z_2))=F(z_1,z_2)$

by finding eqn of line b/t them, intersecting w/ E, & flipping via i (T)

- Recall: w/ conditions on R, fgl over $R \Rightarrow \exists$ group $\mathcal{F}(m)=(m,\oplus_{\mathcal{F}})$ b/c $x\oplus_{\mathcal{F}}y=F(x,y)$ conv.

So we have just proven $\hat{E}(m)\hookrightarrow E(K)$ is a gp homo.

Indeed, $\hat{E}(m)\hookrightarrow E_1(K)$ by $z\mapsto\left(\frac{z}{w(z)},\frac{-1}{w(z)}\right)$ 1-1 b/c $w(z)=0$ only if $z=0$

Also $E_1(K)\hookrightarrow \hat{E}(m)$ by $(x,y)\mapsto -\frac{x}{y}$ & composition is id so $\boxed{\hat{E}(m)\cong E_1(K)}$

$\boxed{E_1(K)=\{P\in E(K)\mid \tilde{P}=\tilde{O}\}}$

- Thus, $0\to\hat{E}(m)\to E(K)\to\tilde{E}(k)\to 0$ & $0\to\hat{E}(m)\to E_0(K)\to\tilde{E}_{ns}(k)\to 0$

Reduce study of $E(K)$ to study of $\hat{E}(m)$ & $\tilde{E}(k)$.

- Analogy: $0\to\hat{G}_a(m)\to R\to \underset{}{k}^{=R/m}\to 0$ & $1\to\overbrace{\hat{G}_m(m)}^{\{u\in R \mid u\equiv 1\,(m)\}}\to R^*\to k^{*\,=R^*/(1+m)}\to 1$

③ Why *else* should I care?

$\left| E(K)/mE(K) \right| < \infty \ \forall m$

→ FGLs use ~~[illegible]~~ in proof of Weak Mordell Weil b/c $[m]$ is iso if $p \nmid m$ so $\hat{E}(\mathfrak{m})[m] = 0$

$[m] =$ apply F m times b/c F is $+$

→ Height of $f: \mathcal{F} \to \mathcal{G}$ is h s.t. 1st nonzero term in f's power series exp is ax^{p^h}

Height of $\mathcal{F}$ is $ht([p])$

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

→ Given $L(s) = \sum_{n=1}^{\infty} a_n n^{-s}$, set $f(x) = \sum_{n=1}^{\infty} a_n \frac{x^n}{n}$ "like Taylor Exp of log"

then $F(X,Y) = f^{-1}(f(X) + f(Y))$

More generally, use differential forms from GSS to define $\log_{\mathcal{F}}(T) = \int \omega(T)$ ← inv differential

$$= \int (1 + c_1 T + c_2 T^2 + \dots)\, dT = T + \frac{c_1}{2} T^2 + \frac{c_2}{3} T^3 + \dots \in K[[T]] \text{ for } K = R \otimes \mathbb{Q}$$

Then for torsion-free R, $\log_{\mathcal{F}} : \mathcal{F} \to \hat{G}_a$ is iso over K

i.e. much of $\mathcal{F}(\mathfrak{m})$ looks additive

i.e. $F(X,Y) = \log_{\mathcal{F}}^{-1}(\log_{\mathcal{F}}(X) + \log_{\mathcal{F}}(Y))$

For $\hat{E}(\mathfrak{m})$, ~~[illegible]~~ inv differential is $\frac{dx(z)}{2y(z) + a_1 x(z) + a_3}$ as in class

→ Formal Gps can be used to construct extensions of local fields with specified ramification