Even More on Formal Groups...

Previously...

- Formal groups $(\mathcal{F}, F)$ — R complete local ring, $\mathfrak{m} \subseteq R$:
  → Groups assoc. to formal gps $\mathcal{F}(\mathfrak{m})$.
  $x \oplus y = F(x,y)$.
- **Prop.** Let $p = \mathrm{char}(k) = \mathrm{char}(R/\mathfrak{m})$.
  Then, every torsion elt. of $\mathcal{F}(\mathfrak{m})$ has order a power of p.
- The invariant differential $\omega(T) = P(T)dT$ s.t. $\omega(F(T,S)) = \omega(T)$.
  → **Cor.** $[p](T) = p \cdot f(T) + g(T^p)$ where $f, g \in R[\![T]\!]$, $f(0) = g(0) = 0$.
- Formal log: $\log_{\mathcal{F}}(T) = \int \omega(T)$
  → Unique inverse: $\exp_{\mathcal{F}}(T)$

Prop $\mathcal{F}/R$, $\mathrm{char}(R)=0$.

Then, $\log_{\mathcal{F}} : \mathcal{F} \longrightarrow \hat{\mathbb{G}}_a$ is an isom. of formal gps over $K = R\otimes\mathbb{Q}$.

Pf. Let $\omega_{\mathcal{F}}(T)$ the formal inv. diff., so $\int \omega(F(T,S)) = \int \omega(T)$

$$\Rightarrow \log_{\mathcal{F}} F(T,S) = \log_{\mathcal{F}}(T) + G(S), \quad (*)$$

for some constant of integration $G(S) \in K[\![S]\!]$.

Evaluate $T=0$, get $\log_{\mathcal{F}}(F(0,S)) = \log_{\mathcal{F}}(0) + G(S)$

$\log_{\mathcal{F}}(S)$ $\Longrightarrow$ $G(S) = \log_{\mathcal{F}}(S)$

$(*) \Rightarrow \log_{\mathcal{F}}(F(T,S)) = \log_{\mathcal{F}}(T) + \log_{\mathcal{F}}(S)$, so it's a hom.

and $\exp_{\mathcal{F}}$ is inverse! $\Rightarrow \log_{\mathcal{F}}$ is an iso. ▨

Prop (5.5) Let R be of $\mathrm{char}(R)=0$. $\mathcal{F}/R$ formal gp.

Then, $\log_{\mathcal{F}}(T) = \sum_{n=1}^{\infty} \frac{a_n}{n} T^n$, $\exp_{\mathcal{F}}(T) = \sum_{n=1}^{\infty} \frac{b_n}{n!} T^n$

for some $a_n, b_n \in R$, $a_1 = b_1 = 1$.

F. GPS OVER DVR'S

Def (DVR) A discrete valuation ring is a ring R (w/ fract. field K) w/ a valuation $\nu : K \longrightarrow \mathbb{Z} \cup \{\infty\}$

s.t. • $\nu(x) = \infty \iff x = 0$

• $\nu(xy) = \nu(x) + \nu(y)$

• $\nu(x+y) \geq \min\{\nu(x), \nu(y)\}$ (w/ eq. if $\nu(x) \neq \nu(y)$)

R complete (local) wrt $\mathfrak{M}$, max'l idel, $x \in R$, $\nu(x) =$ largest $d \in \mathbb{Z}$ s.t. $x \in \mathfrak{M}^d$

$\mathcal{F}/R$ — a DVR, $\mathcal{F}(m)$ has no torsion of order prime to p.
"char(R/m)"

GOAL Study the p-primary torsion of $\mathcal{F}(m)$.

Lemma R, $\mathrm{char}(R)=0$, complete wrt ν (val), p prime, $\nu(p)>0$.

(a) $f(T)=\sum_{n=1}^{\infty}\frac{a_n}{n}T^n$, $a_n\in R$ and $\nu(x)>0$, then $f(x)$ converges in R.

(b) $g(T)=\sum_{n=1}^{\infty}\frac{b_n}{n!}T^n$, $b_n\in R$, $b_1\in R^*$

if $\nu(x)>\frac{\nu(p)}{p-1}$ then $g(x)$ converges in R and $\nu(g(x))=\nu(x)$.

ex $R=\mathbb{Q}_p$, $m=p\mathbb{Z}_p$, $\nu(p)=1$, $\exp_{\mathcal{F}}$ will converge in m

when $\nu(x)>\frac{1}{p-1}\geq\begin{cases}1/2 & p>2 \\ 1 & p=2\end{cases}$ in m^2

Thm Let K be a fld of char $=0$ complete wrt. a normalized discrete valuation v (i.e., $v(K^*) = \mathbb{Z}$). Let R be the val. ring, $\mathfrak{m}$ max'l ideal, p prime, $v(p) > 0$, $\mathcal{F}/R$ a formal gp. Then: ($\hat{\mathbb{G}}_a(\mathfrak{m}) \cong \mathfrak{m} \subseteq K$)

(a) $\log_{\mathcal{F}}$ induces a hom.: $\log_{\mathcal{F}} : \mathcal{F}(\mathfrak{m}) \to K$ (additive)

(b) Let $r > \frac{v(p)}{p-1}$ an integer. Then $\log_{\mathcal{F}}$ induces an iso:

$$\log_{\mathcal{F}} : \mathcal{F}(\mathfrak{m}^r) \xrightarrow{\cong} \hat{\mathbb{G}}_a(\mathfrak{m}^r)$$

Pf. (a) $\log_{\mathcal{F}} : \mathcal{F} \to \hat{\mathbb{G}}_a$ iso $/K = R \otimes \mathbb{Q}$

for (a) it suffices to show that $\log_{\mathcal{F}}$ converges for $x \in \mathfrak{m}$ (Lemma ✓)

(b) $\exp_{\mathcal{F}}$ also converges as long as $v(x) > \frac{v(p)}{p-1}$ $\Rightarrow$ iso ▨

Remark If $r > \frac{v(p)}{p-1} \longrightarrow \mathcal{F}(\mathfrak{m}^r) \cong \underbrace{\hat{G}_a(\mathfrak{m}^r)}_{\cong \mathfrak{m}^r \text{ torsion free}}$

$\longrightarrow \mathcal{F}(\mathfrak{m}^r)$ is torsion free!

Theorem (6.1)

Let R be a DVR, $\mathfrak{M}$, $p = \mathrm{char}(R/\mathfrak{m})$.

Let $\mathcal{F}/R$, $\mathcal{F}(\mathfrak{m})$, $x \in \mathcal{F}(\mathfrak{m})$ of exact order p^n, $n \geq 1$.

(i.e., $[p^n](x) = 0$, $[p^{n-1}](x) \neq 0$). Then $v(x) \leq \frac{v(p)}{p^n - p^{n-1}}$.

ex $R = \mathbb{Z}_p$, $p \geq 3$, then $v(x) \leq \frac{v(p)}{p^n - p^{n-1}} \leq \frac{1}{2}$

but if $x \in \underbrace{\mathfrak{M}}_{p\mathbb{Z}_p}$, $v(x) \geq 1$. $\Longrightarrow$ No torsion!

Pf. (x of exact order p^n, then $v(x) \leq \frac{v(p)}{p^n - p^{n-1}}$)

R, $\mathrm{char} = 0$, $p = \mathrm{char}(R/m)$. Induction on n:

n=1 $[p](T) = p \cdot f(T) + g(T^p)$ and $f(0) = g(0) = 0$

$f(T) = T + \text{HOT}$ (Recall $[p](T) = pT + \cdots$)

Suppose $[p](x) = 0$, $x \neq 0$. Then:

val's need to match

$$0 = p \cdot f(x) + g(x^p) = \underbrace{p(x + \text{HOT})}_{} + \underbrace{g(x^p)}_{}$$

Recall $v(x+y) \geq \min\{v(x), v(y)\}$

$v(px) = v(\text{first term of } g(x^p))$

$$\Rightarrow \underbrace{v(px)}_{v(p) + v(x)} \geq \underbrace{v(x^p)}_{p\,v(x)} \quad \Rightarrow v(p) \geq (p-1)\, v(x) \Rightarrow v(x) \leq \frac{v(p)}{p-1}$$

□

$[n \Rightarrow n+1]$ Let x be of order p^{n+1}. Then

$$\frac{v(p)}{p^n - p^{n-1}} \geq v([p]x) = v(pf(x) + g(x^p)) \geq \min\left(v(px), v(x^p)\right)$$

Ind. hyp.

- If min is $v(px) \Rightarrow \dfrac{v(p)}{p^n - p^{n-1}} \geq v(px) = v(p) + v(x)$, with $v(x) > 0$

$v(p) > v(p) + v(x)$ ⚡

- Thus: $\dfrac{v(p)}{p^n - p^{n-1}} \geq v(x^p) = p\,v(x) \Rightarrow v(x) \leq \dfrac{v(p)}{p^{n+1} - p^n}$ □

Thus by ind, result follows! ▨

Elliptic Curves over Local Fields

K local field, complete wrt a disc. val. v

R ring of integers $(v(x) \geq 0)$, $R^\times$ unit gp. $(v(x) = 0)$

$\mathfrak{m}$ max'l ideal $(v(x) > 0)$

π a uniformizer for R (i.e., $\mathfrak{m} = \pi R$)

$k = R/\mathfrak{m}$ the res. field, $p = \mathrm{char}(k)$

(or $x = u^2 x' + r$, $y = u^3 y' + u^2 s x' + t$, then $\Delta \mapsto u^{-12}\Delta = \Delta'$, $c_4 \mapsto u^{-4} c_4 = c_4'$)

Minimal Weierstrass Eqn's.

$$E/K : \quad y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \qquad a_i \in K$$

Recall: $(x, y) \longmapsto (u^{-2}x, u^{-3}y)$ then $a_i \mapsto u^i a_i = a_i'$

$$\Delta \mapsto u^{-12}\Delta = \Delta'$$

$$c_4 \longmapsto u^{-4}\Delta = c_4'$$

Def Let E/K be an ell. curve. A Weiers. eq'n as above is called a minimal Weiers. eq'n for E at v if $v(\Delta)$ is minimal subject to the condition $a_i \in R$. Such Δ is called the minimal discriminant.

Rk $a_i \in R$, $\Delta \in R$, $c_4 \in R$

If Δ is not minimal, then there is a change of vars $(x,y) \mapsto (u^2x, u^3y)$ with $\Delta' = \frac{\Delta}{u^{12}}$ minimal (so u only changes by mult. of 12)
the val

If $a_i \in R$ and $v(\Delta) < 12$, then eq. is minimal!
$\Delta \in R$

Similarly, val. of c_4 changes by mult. of 4, so if $a_i \in R$, $v(c_4) < 4$ then eq. is minimal.

(If $\mathrm{char}\, K \neq 2,3$, the converse also holds!)

ex

$$y^2 = x^3 + 5^6 \quad / \mathbb{Q} \qquad \xrightarrow{\text{mod } 5} \qquad \underbrace{y^2 = x^3}_{\text{singular!}} \text{ over } \mathbb{F}_5$$

$$\| \wr$$

$$y'^2 = x'^3 + 1 \quad / \mathbb{Q} \qquad \xrightarrow{\text{mod } 5} \qquad y'^2 = x'^3 + 1 \text{ over } \mathbb{F}_5 \text{ is non-singular!}$$

ex

$$E: \; y^2 + xy + y = x^3 + x^2 + 22x - 9$$

$$\Delta_E = -2^{15} \cdot 5^2, \quad c_4 = -5 \cdot 211$$

- minimal for $p \geq 2$ b/c $v_p(c_4) = \begin{cases} 0 & \text{if } p \neq 5, 211 \\ 1 & \text{if } p = 5, 211 \end{cases}$

< 4 in all cases.