Master Seminar – Elliptic Curves – Talk 6

The formal group of an elliptic curve

Marco Morosin

14.12.2020

The idea

E elliptic curve over a field K.

- local ring $K[E]_O$ is a discrete valuation ring
- its completion at M_O is isomorphic to $K[\![z]\!]$
- write x, y as $x(z), y(z) \in K[\![z]\!]$
- the group law is 'given by' a power series $F(z_1, z_2) \in K[\![z_1, z_2]\!]$:

$$(x(z_1), y(z_1)) + (x(z_2), y(z_2)) = (x(F(z_1, z_2)), y(F(z_1, z_2)))$$

$$\begin{cases} z := -\frac{x}{y} \\ w := -\frac{1}{y} \end{cases} \iff \begin{cases} x = \frac{z}{w} \\ y = -\frac{1}{w} \end{cases}$$

- O is $(z, w) = (0, 0)$, z is a local uniformizer at O
- $w = z^3 + (a_1 z + a_2 z^2)w + (a_3 + a_4 z)w^2 + a_6 w^3 = f(z, w)$

Substitute recursively $w = f(z, w)$ into itself:

$$\begin{aligned} w = z^3 &+ (a_1 z + a_2 z^2)[z^3 + (a_1 z + a_2 z^2)w + (a_3 + a_4 z)w^2 + a_6 w^3] + \\ &+ (a_3 + a_4 z)[z^3 + (a_1 z + a_2 z^2)w + (a_3 + a_4 z)w^2 + a_6 w^3]^2 + \\ &+ a_6 [z^3 + (a_1 z + a_2 z^2)w + (a_3 + a_4 z)w^2 + a_6 w^3]^3 = \\ &= \cdots \end{aligned}$$

i.e. we have a sequence $\begin{cases} f_1(z, w) = f(z, w) \\ f_{m+1}(z, w) = f_m(z, f(z, w)) \end{cases}$.

Claim

- $\exists \lim_{m\to\infty} f_m(z, 0) =: w(z) \in \mathbb{Z}[a_1, \ldots, a_6][[z]]$
- $w(z)$ is the unique element in $\mathbb{Z}[a_1, \ldots, a_6][[z]]$ such that $w(z) = f(z, w(z))$

Hensel's Lemma

Suppose: R complete in the I-adic topology, $F(X) \in R[X]$,
$\exists n \geqslant 1$, $a \in R$ such that $F(a) \in I^n$ and $F'(a) \in R^\times$.

Then: $\forall r \in R$ with $r \equiv F'(a) \mod I$, the sequence $\begin{cases} w_0 = a \\ w_{m+1} = w_m - \frac{F(w_m)}{r} \end{cases}$

converges to $b \in R$ satisfying $F(b) = 0$ and $b \equiv a \mod I^n$

If R is a domain, these conditions determine b uniquely.

In our case

$$R = \mathbb{Z}[a_1, \ldots, a_6][\![z]\!] \qquad I = (z) \qquad F(w) = f(z,w) - w$$
$$n = 1 \qquad a = 0 \qquad r = -1$$

Note: $w_m = f_m(z, 0)$:

$$w_0 = 0, \quad w_1 = F(0) = f(z,0), \quad w_2 = w_1 + F(w_1) = f(z, f(z,0)), \ldots$$

Moreover, the hypothesis are satisfied:

- $F(0) = f(z,0) = z^3 \in (z)$, $F'(0) = a_1 z + a_2 z^2 - 1 \in \mathbb{Z}[a_1, \ldots, a_6][\![z]\!]^\times$
- $-1 \equiv F'(0) \mod (z)$

$\implies \exists\, w(z) := \lim_m w_m$ and $f(z, w(z)) - w(z) = 0$

Proof of Hensel's lemma

By replacing $F(w)$ by $F(w+a)/r$, we suppose $a=0$ and $r=1$, i.e.

$$w_0 = 0 \qquad F(0) \in I^n \qquad F'(0) \equiv 1 \mod I \qquad w_{m+1} = w_m - F(w_m)$$

- $w_m \in I^n$ for all $m \geqslant 0$: $w_0 = 0$ and, by induction,
  $w_m \in I^n \implies$ (since $F(0) \in I^n$) $F(w_m) \in I^n \implies w_m - F(w_m) \in I^n$
- $w_m \equiv w_{m+1} \mod I^{m+n}$ for all $m \geqslant 0$: $w_0 = 0 \equiv -F(0) = w_1 \mod I^n$;

$$F(X) - F(Y) = (X-Y)(F'(0) + XG(X,Y) + YH(X,Y))$$

$$\implies w_{m+1} - w_m = w_m - w_{m-1} - (F(w_m) - F(w_{m-1})) =$$
$$= (w_m - w_{m-1})(1 - F'(0) - w_m G(w_m, w_{m-1}) - w_{m-1} H(w_m, w_{m-1}))$$
$$\in I^{m+n-1} I = I^{m+n}$$

- R complete $\implies \exists\, b := \lim w_m \in R$. Moreover, $w_m \in I^n \implies b \in I^n$:

$$\forall k\ \exists M_k : m \geqslant M_k \implies b \in w_m + I^k \subset I^n + I^k$$

so the limit exists and $b \equiv 0 \mod I^n$. $F(b) = 0$?

- $b \xleftarrow{m\to\infty} w_{m+1} = w_m - F(w_m) \xrightarrow{m\to\infty} b - F(b)$ hence $F(b) = 0$

Assume moreover that R is an integral domain.

Uniqueness of b

- let c also satisfy $F(c) = 0$ and $c \equiv 0 \mod I^n$, then

$$0 = F(b) - F(c) = (b - c)(F'(0) + bG(b, c) + cH(b, c))$$

- if $b \neq c$, we would have $F'(0) = -bG(b, c) - cH(b, c) \in I$
- this would contradict $F'(0) \equiv 1 \mod I$. Hence, $b = c$.

$\square$

Proposition

1. $w(z) = z^3(1 + A_1 z + A_2 z^2 + \cdots) \in \mathbb{Z}[a_1, \ldots, a_6][\![z]\!]$
2. *$w(z)$ is unique in $\mathbb{Z}[a_1, \ldots, a_6][\![z]\!]$ satisfying $w(z) = f(z, w(z))$*
3. *if $\mathbb{Z}[a_1, \ldots, a_6]$ is a graded ring by $wt(a_i) := i$, then A_n is a homogeneous polynomial of weight n*

Proof of 3.

- assign weights $\mathrm{wt}(z) := -1$, $\mathrm{wt}(w) := -3$.
- $f(z, w) = z^3 + (a_1 z + a_2 z^2)w + (a_3 + a_4 z)w^2 + a_6 w^3$ homogeneous of weight -3 in $\mathbb{Z}[a_1, \cdots, a_6, z, w]$
- by induction, the same holds for $f_m(z, w)$, hence

$$f_m(z, 0) = z^3(1 + B_1 z + B_2 z^2 + \cdots B_N z^N)$$

  homogeneous of weight -3
- $-3 = \mathrm{wt}(B_n z^{n+3}) = \mathrm{wt}(B_n) - n - 3 \implies B_n$ homogeneous of weight n $\implies$ the same for A_n because $f_m(0, z) \to w(z)$

$\square$

From $w(z)$ we get:

- $x(z) = \frac{z}{w(z)} = \frac{1}{z^2} - \frac{a_1}{z} - a_2 - a_3 z - (a_4 + a_1 a_3) z^2 - \cdots$
- $y(z) = -\frac{1}{w(z)} = -\frac{1}{z^3} + \frac{a_1}{z^2} + \frac{a_2}{z} + a_3 + (a_4 + a_1 a_3) z - \cdots$
- $\omega(z) = \frac{\mathrm{d}x(z)}{2y(z)+a_1 x(z)+a_3} = (1 + a_1 z + (a_1^2 + a_2) z^2 + \cdots)\mathrm{d}z$

with coefficients in $\mathbb{Z}[a_1, \ldots, a_6]$

Remark

- $(x(z), y(z))$ is a solution of

  $$E\colon y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

  in $\mathbb{Z}[a_1, \ldots, a_6]((z))$
- Idea: find points on E by evaluating $x(z), y(z)$ at $z \in K$
- Possible if K is a complete local field, $a_1, \ldots, a_6 \in \mathcal{O}_K$, $z \in \mathfrak{m}$. In this case we have an injective map

  $$\mathfrak{m} \to E(K) \qquad z \mapsto (x(z), y(z))$$

  with left-inverse $(x, y) \mapsto -x/y$ (remember $z := -x/y$)

The group law in terms of power series

Recall the formula for $(z_1, w(z_1)) + (z_2, w(z_2))$:

- the line through the two points is $w = \lambda(z_1, z_2)z + \nu(z_1, z_2)$ with

$$\lambda(z_1, z_2) := \frac{w_2(z) - w_1(z)}{z_2 - z_1} = \sum_{n=3}^{\infty} A_{n-3} \frac{z_2^n - z_1^n}{z_2 - z_1}$$

$$\nu(z_1, z_2) := w(z_1) - \lambda(z_1, z_2)z_1$$

- intersect $\begin{cases} w = f(z, w) \\ w = \lambda z + \nu \end{cases} \implies$ cubic in z with roots z_1, z_2
- the third root z_3 can be expressed as

$$z_3(z_1, z_2) = -z_1 - z_2 + \frac{a_1\lambda + a_3\lambda^2 - a_2 y - 2a_4\lambda\nu - 3a_6\lambda^2\nu}{1 + a_2\lambda + a_4\lambda^2 + a_6\lambda^3}$$

- $w_3 := \lambda z_3 + \nu = f(z_3, w_3)$. The only element with this property is $w(z_3)$, hence $w_3 = w(z_3)$
- The three points are collinear, so $(z_1, w(z_1)) + (z_2, w(z_2)) + (z_3, w(z_3)) = O$

$(z_1, w(z_1)) + (z_2, w(z_2)) = -(z_3, w(z_3))$. How to find this inverse?

- write (z, w) in xy coord.'s: $(x(z), y(z))$
- use the inversion formula: $-(x(z), y(z)) = (x(z), -y(z) - a_1x(z) - a_3)$
- switch back to zw coord.'s ($z = -x/y$): $(i(z), w(i(z)))$ where

$$i(z) = \frac{x(z)}{y(z) + a_1x(z) + a_3} = \frac{z^{-2} - a_1z^{-1} - \cdots}{-z^{-3} + 2a_1z^{-2} + \cdots} \in \mathbb{Z}[a_1, \ldots, a_6][\![z]\!]$$

Conclusion

The formal addition law is

$$F(z_1, z_2) = i(z_3(z_1, z_2)) = z_1 + z_2 + 2 - a_1z_1z_2 - a_2(z_1^2z_2 + z_1z_2^2) + \cdots \in \mathbb{Z}[a_1, \ldots, a_6][\![z_1, z_2]\!]$$

satisfying the usual properties

- $F(z_1, z_2) = F(z_2, z_1)$ (commutativity)
- $F(z_1, F(z_2, z)) = F(F(z_1, z_2), z)$ (associativity)
- $F(z, i(z)) = 0$ (inverse)

Formal Groups

Definition

A *(one-parameter commutative) formal group law* over a ring R is $F(X, Y) \in R[\![X, Y]\!]$ satisfying

- $F(X, Y) = X + Y +$ (terms of degree $\geqslant 2$)
- $F(X, F(Y, Z)) = F(F(X, Y), Z)$ (associativity)
- $F(X, Y) = F(Y, X)$ (commutativity)
- $\exists!\ i(T) \in R[\![T]\!]$ such that $F(T, i(T)) = 0$ (inverse)
- $F(X, 0) = X$ and $F(0, Y) = Y$

Definition

A *homomorphism* $f\colon F \to G$ is $f(T) \in R[\![T]\!]$ with no constant term, such that

$$f(F(X, Y)) = G(f(X), f(Y))$$

F and G are *isomorphic* if there are $f\colon F \to G$ and $g\colon G \to F$ such that

$$f(g(T)) = g(f(T)) = T$$

Notation

Denote by F/R a formal group law F over a ring R.

Examples

- formal additive group: $F(X, Y) = X + Y$
- formal multiplicative gr.: $F(X, Y) = X + Y + XY = (1 + X)(1 + Y) - 1$
- formal group associated to an elliptic curve E: $F(z_1, z_2) = i(z_3(z_1, z_2))$

Definition (multiplication by m)

F/R formal group; for $m \in \mathbb{Z}$, define homomorphisms $[m]\colon F \to F$ by

$$[0](T) = 0 \qquad [m+1](T) = F([m](T), T) \qquad [m-1](T) = F([m](T), i(T))$$

Proposition

1. $[m](T) = mT +$ *(higher order terms)*
2. *if* $m \in R^\times$*, then* $[m]$ *is an isomorphism*

Proof of 1.

Remember $F(X, Y) = X + Y + \cdots$. By induction: $[0](T) = 0$,

- for $m \geqslant 0$:
  $[m+1](T) = F([m](T), T) = F(mT + \cdots, T) = mT + T + \cdots$
- for $m \leqslant 0$:
  $0 = F(T, i(T)) = T + i(T) + \cdots \implies i(T) = -T + \cdots$
  downward induction: $[m-1](T) = F([m](T), i(T)) = mT + \cdots - T + \cdots$

Proof of 2.

More in general: if $a \in R^\times$ and $f(T) = aT +$ (higher order terms) $\in R[\![T]\!]$, then $\exists!\, g(T) \in R[\![T]\!]$ such that $f(g(T)) = T$. Moreover, $g(f(T)) = T$.

- We will define $g_n(T) \in R[T]$: $\begin{cases} f(g_n(T)) \equiv T \mod T^{n+1} \\ g_{n+1}(T) \equiv g_n(T) \mod T^{n+1} \end{cases}$
- $g_1(T) := a^{-1}T$. Suppose $g_{n-1}(T)$ has been constructed, then

  $$g_n(T) = g_{n-1}(T) + \lambda T^n \quad \text{for some } \lambda \in R$$

  We must find λ such that $f(g_n(T)) \equiv T \mod T^{n+1}$.

  $$\begin{aligned} f(g_n(T)) = f(g_{n-1}(T) + \lambda T^n) &\equiv f(g_{n-1}(T)) + a\lambda T^n \mod T^{n+1} \\ &\equiv T + bT^n + a\lambda T^n \mod T^{n+1} \quad \text{for some } b \in R \end{aligned}$$

  $\implies$ take $\lambda = -a^{-1}b$.
- $g(T) := \lim g_n(T) \in R[\![T]\!]$ exists and $f(g(T)) = T$

- Repeat the procedure using $f(T) := g(T)$:
  $h(T) := \lim h_n(T)$ satisfies $g(h(T)) = T$, so

$$g(f(T)) = g(f(g(h(T)))) = g(h(T)) = T$$

- Uniqueness: let $j(T) \in R[\![T]\!]$ such that $f(j(T)) = T$, then

$$g(T) = g(f(j(T))) = j(T)$$

$\square$

Groups associated to formal groups

Notation: R complete local ring, $\mathfrak{m}$ max ideal, $k = R/\mathfrak{m}$, F formal group over R

completeness $\implies$ $F(x, y) \in \mathfrak{m} \quad \forall x, y \in \mathfrak{m}$ $\implies$ group structure on $\mathfrak{m}$

Definition

The group associated to F, denoted by $F(\mathfrak{m})$, is the set $\mathfrak{m}$ with group structure

$$x \oplus_F y := F(x, y) \text{ (addition)} \qquad \ominus_F x := i(x) \text{ (inversion)}$$

- The additive group $\widehat{\mathbb{G}}_a(\mathfrak{m})$ is just $(\mathfrak{m}, +)$

$$0 \to \widehat{\mathbb{G}}_a(\mathfrak{m}) \to R \to k \to 0$$

- The multiplicative group $\widehat{\mathbb{G}}_m(\mathfrak{m})$ is isomorphic to $(1 + \mathfrak{m}, \cdot)$:

$$\widehat{\mathbb{G}}_m(\mathfrak{m}) \to 1 + \mathfrak{m} \qquad x \mapsto 1 + x$$

$$x \oplus_F y = x + y + xy \mapsto 1 + x + y + xy = (1 + x)(1 + y)$$

$$0 \to \widehat{\mathbb{G}}_m(\mathfrak{m}) \xrightarrow{x \mapsto 1+x} R^\times \to k^\times \to 1$$

Example

$\widehat{E}$ associated to an elliptic curve E/K, $K = \mathrm{Frac}(R)$.

$\mathfrak{m} \to E(K)$: $z \mapsto (x(z), y(z))$ gives a homomorphism $\widehat{E}(\mathfrak{m}) \to E(K)$:

- for $z_1 \neq z_2$: $z_1 \oplus_{\widehat{E}} z_2 = i(z_3(z_1, z_2)) \mapsto (x(z_1), y(z_1)) + (x(z_2), y(z_2))$
- for $z_1 = z_2$: continuity argument

There is often an exact sequence

$$0 \to \widehat{E}(\mathfrak{m}) \to E(K) \to \widetilde{E}(k) \to 0$$

where $\widetilde{E}$ is some elliptic curve over k.

Proposition

1. *The map* $\frac{F(\mathfrak{m}^n)}{F(\mathfrak{m}^{n+1})} \to \frac{\mathfrak{m}^n}{m^{n+1}}$ *induced by* $\mathrm{id}_{\mathfrak{m}^n/\mathfrak{m}^{n+1}}$ *is an isomorphism of groups*
2. *let* $p := \operatorname{char} k \geqslant 0$*; every torsion element in* $F(\mathfrak{m})$ *has order a power of* p

Proof of 1.

Enough to show it's a homomorphism: let $x, y \in \mathfrak{m}^n$, then
$x \oplus_F y = F(x, y) = x + y + (\text{higher order terms}) \equiv x + y \mod \mathfrak{m}^{2n}$

Proof of 2.

x of order $p^r m \implies p^r x$ of order m: enough to show that no element $\neq 0$ has order prime to p
Let $m \geqslant 1$ with $p \nmid m$; suppose $x \in F(\mathfrak{m})$ such that $[m](x) = 0$ Note that $(m, p) = 1 \implies m \notin \mathfrak{m}$:

- $p = 0$: $m \in \mathfrak{m}$ would imply $\operatorname{char}(k) = q$ for some q prime factor of m
- $p > 0$: write $1 = am + bp$, then $\overline{1} = \overline{am}$ hence $\overline{m} \neq \overline{0}$

So, $m \in R^\times \implies [m]$ is an automorphism of $F \implies [m]\colon F(\mathfrak{m}) \to F(\mathfrak{m})$ is an automorphism, so

$$\ker[m] = 0 \implies x = 0$$

□

The invariant differential

Definition

An *invariant differential* on a formal group F/R is a differential form

$$\omega(T) = P(T)dT \in R[\![T]\!]dT$$

such that $\omega \circ F(T,S) = \omega(T)$, i.e. $P(F(T,S))F_X(T,S) = P(T)$
We call it *normalized* if $P(0) = 1$

Examples

- $\omega = dT$ is invariant on $\widehat{\mathbb{G}}_a$:

$$P(F(T,S))F_X(T,S) = 1 = P(T)$$

- $\omega = \frac{dT}{1+T} = (1 - T + T^2 - T^3 + \cdots)dT$ is invariant on $\widehat{\mathbb{G}}_m$

$$F_X(T,S) = 1 + S$$

$$P(F(T,S))F_X(T,S) = \frac{1}{1+T+S+TS}(1+S) = \frac{1}{1+T} = P(T)$$

Proposition

On a formal group F/R, there exists a unique normalized invariant differential, namely $\omega(T) = F_X(0,T)^{-1}dT$. Any invariant differential is given by $a\omega$, $a \in R$

Proof

Let $P(T)dT$ be invariant, so $P(F(T,S))F_X(T,S) = P(T)$. Then

$$P(F(0,S))F_X(0,S) = P(S)F_X(0,S) = P(0)$$

hence

- $P(S)(1+\cdots) = P(0) \implies P(S) = P(0)F_X(0,S)^{-1}$
- $P(T)dT = P(0)F_X(0,T)^{-1}dT$ is of the form $a\omega$
- $F_X(0,0) = 1 \implies \omega$ is normalized

Is it invariant? $\iff F_X(0,F(T,S))^{-1}F_X(T,S) = F_X(0,T)^{-1}$?

$$F(U,F(T,S)) = F(F(U,T),S) \implies F_X(U,F(T,S)) = F_X(F(U,T),S)F_X(U,T)$$
$$\implies F_X(0,F(T,S)) = F_X(F(0,T),S)F_X(0,T) = F_X(T,S)F_X(0,T)$$

$\square$

For $f(T) \in R[\![T]\!]$, let $f'(T)$ be the formal derivative (term by term).

Corollary

Consider F, G with normalized invariant differentials ω_F, ω_G and a homomorphism $f\colon F \to G$. Then $\omega_G \circ f = f'(0)\omega_F$.

Proof

$\omega_G \circ f$ is an invariant differential on F:

$$\begin{aligned}(\omega_G \circ f)(F(T,S)) &= \omega_G(G(f(T), f(S))) = \\ &= \omega_G \circ G(f(T), f(S)) = (\omega_G \circ f)(T)\end{aligned}$$

hence $\omega_G \circ f = a\omega_F$ for some $a \in R$, i.e.

$$G_X(0, f(T))^{-1} f'(T) dT = aF_X(0, T)^{-1} dT$$

Evaluating at $T = 0$:

$$\begin{aligned}&G_X(0, f(0))^{-1} f'(0) = aF_X(0,0)^{-1} \\ \iff\ & G_X(0,0)^{-1} f'(0) = aF_X(0,0)^{-1} \\ \iff\ & f'(0) = a\end{aligned}$$

$\square$

Corollary

Let F/R formal group, $p \in \mathbb{Z}$ prime. Then there are $f(T), g(T) \in R[\![T]\!]$ with $f(0) = g(0) = 0$ such that

$$[p](T) = pf(T) + g(T^p)$$

Proof

- Remember $[p](T) = pT + (\text{higher order terms})$, hence $[p]'(0) = p$
- so, by the previous result:

$$\begin{aligned} p\omega(T) &= (\omega \circ [p])(T) \\ &= F_X(0, [p](T))^{-1}[p]'(T)dT = (1 + \cdots)[p]'(T)dT \end{aligned}$$

- $(1 + \cdots) \in R[\![T]\!]^\times \implies [p]'(T) = p(1 + \cdots)^{-1}\omega(T) \in pR[\![T]\!]$
- write $[p](T) = \sum_{n \geqslant 0} a_n T^n \implies [p]'(T) = \sum_{n \geqslant 1} a_n n T^{n-1}$, then:

$$\mathbb{N} = \{n \mid a_n = pa'_n \in pR\} \cup \{n \mid n = pn'\} =: A \cup B$$

- $f(T) := \sum_{n \in A} a'_n T^n \implies pf(T) = \sum_{n \in A} a_n T^n$
  $g(T) := \sum_{n \in B \setminus A} a_{n'} T^{n'} \implies g(T^p) = \sum_{n \in B \setminus A} a_{n'} T^n$

$\square$

The formal logarithm

Let R be a torsion-free ring, $K := R \otimes_{\mathbb{Z}} \mathbb{Q}$. We have an injection $R \hookrightarrow K$.

Definition

F/R formal group, $\omega(T) = (1 + c_1 T + c_2 T^2 + \cdots)dT$ its normalized invariant differential. The *formal logarithm* of F is

$$\log_F(T) := \int \omega(T) = T + \frac{c_1}{2}T^2 + \frac{c_2}{3}T^3 + \cdots \in K[\![T]\!]$$

The *formal exponential* of F is the unique element $\exp_F(T) \in K[\![T]\!]$ such that

$$\log_F \circ \exp_F(T) = \exp_F \circ \log_F(T) = T$$

Example

$$\log_{\widehat{\mathbb{G}}_m}(T) = \int \frac{dT}{(1+T)} = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}T^n}{n} \qquad \exp_{\widehat{\mathbb{G}}_m}(T) = \sum_{n=1}^{\infty} \frac{T^n}{n!}$$

are the usual Taylor expansions for $\log(1+T)$ and $e^T - 1$.

Proposition

F formal group over R torsion-free. Then $\log_F \colon F \to \widehat{\mathbb{G}}_a$ is an isomorphism of formal groups over $K = R \otimes \mathbb{Q}$.

Proof.

$\omega_F(F(T,S)) = \omega_F(T)$. Integrating in T gives:

$$\log_F F(T,S) = \log_F(T) + c(S) \qquad \text{for some } c(S) \in K[\![T]\!]$$

for $T = 0$ we get $c(S) = \log_F(S)$, so $\log_F$ is a homomorphism.
It is an isomorphism with inverse $\exp_F$. $\square$

Application

Note: to define ω_F, $\log_F$, $\exp_F$ we did not use commutativity of F.
If R torsion-free, the proposition implies

$$F(X,Y) = \exp_F(\log_F(X) + \log_F(Y)) = \exp_F(\log_F(Y) + \log_F(F)) = F(Y,X)$$

Conclusion: any one-parameter formal group over a torsion-free ring is commutative.

Lemma

Let $f(T) = \sum_{n=1}^{\infty} (a_n/n!) T^n \in K[\![T]\!]$ with $a_n \in R$, $a_1 \in R^\times$.
Then the unique $g(T) \in K[\![T]\!]$ with $f(g(T)) = T$ has the form
$g(T) = \sum_{n=1}^{\infty} (b_n/n!) T^n$ with $b_n \in R$.

Proof.

Write $g(T) = \sum_{n=1}^{\infty} (b_n/n!) T^n$ with $b_n \in K$.
$f(g(T)) = T \implies f'(g(T))g'(T) = 1 \implies f'(g(0))g'(0) = a_1 b_1 = 1$

$$\implies b_1 = a_1^{-1} \in R$$

Differentiate again: $f'(g(T))g''(T) + f''(g(T))g'(T)^2 = 0 \implies$

$$a_1 b_2 = -a_2 b_1^2 \implies b_2 = -a_2 b_1^2 / a_1 \in R$$

By induction $b_n \in R$ for all n. $\square$

Application

$\log_F(T)$ has the form $\sum_{n=1}^{\infty} (a_n/n) T^n = \sum_{n=1}^{\infty} (a'_n/n!) T^n$ with $a'_n \in R$, $a'_1 = 1$.
By the lemma: $\exp_F(T) = \sum_{n=1}^{\infty} (b_n/n!) T^n$ for some $b_n \in R$, $b_1 = 1$.

Formal groups over DVR's

Remember: F formal group over complete local ring $R \implies F(\mathfrak{m})$ has no torsion of order prime to $p := \mathrm{char}(R/\mathfrak{m})$.

Theorem

Let R be a complete DVR, v its valuation, $p := \mathrm{char}(R/\mathfrak{m}) \geqslant 0$, F/R formal group. If $x \in F(\mathfrak{m})$ has order p^n, then $v(x) \leqslant \frac{v(p)}{p^n - p^{n-1}}$

Proof

If $\mathrm{char}(R) > 0$ or $p = 0$, then $v(p) = \infty$, trivial. So, we assume $\mathrm{char}(R) = 0$ and $p > 0$.
Choose $f(T), g(T) \in R[\![T]\!]$ such that

$$[p](T) = pf(T) + g(T^p)$$

Remember $[p](T) = pT + \cdots$, hence $f(T) = T + \cdots$
By induction on n:

- let $x \neq 0$ such that $[p](x) = 0$:

$$0 = pf(x) + g(x^p) = px + g(x^p) + \cdots$$
$$\implies v(px) \geqslant v(x^p) \iff v(p) + v(x) \geqslant pv(x) \iff v(p) \geqslant (p-1)v(x)$$

- $n \mapsto n+1$; suppose x has order p^{n+1}
  then $[p](x)$ has order $p^n \implies$ induction hypothesis:

  $$\frac{v(p)}{p^n - p^{n-1}} \geqslant v([p](x))$$

  Moreover:

  $$\begin{aligned} v([p](x)) = v(pf(x) + g(x^p)) &\geqslant \min\{v(pf(x)), v(g(x^p))\} \\ &= \min\{v(px), v(x^p)\} \end{aligned}$$

  Hence

  $$\frac{v(p)}{p^n - p^{n-1}} \geqslant \min\{v(px), v(x^p)\}$$

  but we can't have $\frac{v(p)}{p^n - p^{n-1}} \geqslant v(px) = v(p) + v(x) > v(p)$,

  $$\implies \frac{v(p)}{p^n - p^{n-1}} \geqslant v(x^p) = pv(x)$$

  $$\implies \frac{v(p)}{p^{n+1} - p^n} \geqslant v(x)$$

$\square$

Example: formal groups over $\mathbb{Z}_p$

$v(p) = 1$. If $x \in F(p\mathbb{Z}_p)$ has order p^n, then

$$0 < v(x) \leqslant \frac{1}{p^n - p^{n-1}}$$

- for $p = 2$: if $n = 1$, $0 < v(x) \leqslant 1$ is possible: we may have elements x of order $p = 2$; no torsion elements of higher order
- for $p > 2$: impossible $\implies$ no torsion elements

Analogously for O_K with K finite unramified extension of $\mathbb{Q}_p$.

Lemma

Let R be a DVR, $p \in \mathbb{Z}$ a prime with $0 < v(p) < \infty$. Then, for all $n \geqslant 1$, $v(n!) \leqslant \frac{(n-1)v(p)}{p-1}$.

Proof

$$v(n!) = \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right] v(p) \leqslant \sum_{i=1}^{[\log_p n]} \frac{nv(p)}{p^i} = nv(p)\frac{1 - p^{-[\log_p n]}}{p-1} \leqslant \frac{(n-1)v(p)}{p-1}$$

Lemma

Let R be a complete DVR, $\mathrm{char}(R) = 0$, *$p \in \mathbb{Z}$ a prime with $v(p) > 0$.*

1. *let $f(T) = \sum_{n=1}^{\infty}(a_n/n)T^n$ with $a_n \in R$. If $x \in R$ has $v(x) > 0$, then $f(x) \in R$*
2. *let $g(T) = \sum_{n=1}^{\infty}(b_n/n!)T^n$ with $b_n \in R$. If $x \in R$ has $v(x) > v(p)/(p-1)$, then $g(x) \in R$. If moreover $b_1 \in R^\times$, then $v(g(x)) = v(x)$*

Proof of 1.

We must check that $f(x) = \sum_{n=1}^{\infty}(a_n/n)x^n \in R$:

$$v(a_n x^n/n) = v(a_n) + nv(x) - v(n) \geqslant nv(x) - v(n)$$
$$\geqslant nv(x) - v(p)\log_p n \to \infty$$

Proof of 2.

We must check that $g(x) = \sum_{n=1}^{\infty}(b_n/n!)x^n \in R$:

$$v(b_n x^n/n!) = v(b_n) + nv(x) - v(n!) \geqslant nv(x) - v(n!) \geqslant$$
$$\geqslant nv(x) - (n-1)\frac{v(p)}{p-1} = v(x) + (n-1)\left(v(x) - \frac{v(p)}{p-1}\right) \to \infty$$

This also shows: $n \geqslant 2 \implies v(b_n x^n/n!) > v(x)$.
If $b_1 \in R^\times$ then $v(b_1 x) = v(x)$, so $v(g(x)) = v(b_1 x) = v(x)$.

$\square$

Theorem

Assume: K *complete DVF,* $\mathrm{char}(K) = 0$, $v(K^\times) = \mathbb{Z}$, $R := \mathcal{O}_K$, $p \in \mathbb{Z}$ *prime with* $v(p) > 0$, F/R *formal group.*

1. *The formal logarithm induces a homomorphism* $\log_F \colon F(\mathfrak{m}) \to (K, +)$
2. *If* $r > v(p)/(p-1)$*, it induces an isomorphism* $\log_F \colon F(\mathfrak{m}^r) \to \widehat{\mathbb{G}}_a(\mathfrak{m}^r)$

Proof

1. $\log_F(F(X,Y)) = \log_F(X) + \log_F(Y)$ as power series. Convergence?
   We just proved:
   $$\sum_{n=1}^{\infty} \frac{a_n}{n} T^n \qquad (a_n \in R)$$
   converges if $v(x) > 0$.
   We proved previously: $\log_F$ is of such form.
2. Do $\log_F(x)$, $\exp_F(x)$ converge to values in $\mathfrak{m}^r$? Write $\log_F$, $\exp_F$ as
   $$\sum_{n=1}^{\infty} \frac{b_n}{n!} T^n \qquad (b_n \in R)$$
   $x \in \mathfrak{m}^r \iff v(x) \geqslant r > v(p)/(p-1)$, hence convergence in R
   $b_1 = 1 \in R^\times \implies v(g(x)) = v(x)$, hence $g(x) \in \mathfrak{m}^r$

$\square$

Formal groups in characteristic p

From now on, R is a ring of characteristic p.

Definition

For $f\colon F \to G$ homomorphism of formal groups over R, the *height of f* $\mathrm{ht}(f)$ is the largest $h \in \mathbb{Z}$ such that $f(T) = g(T^{p^h})$ for some $g(T) \in R[\![T]\!]$.
$\mathrm{ht}(0) \coloneqq \infty$.
Define the height of a formal group by $\mathrm{ht}(F) \coloneqq \mathrm{ht}([p])$, $[p]\colon F \to F$.

Remark

- $m \geqslant 1$ prime to $p \implies \mathrm{ht}([m]) = 0$ because $[m](T) = mT + \cdots$
- $\mathrm{ht}([p]) \geqslant 1$ because $[p](T) = pf(T) + g(T^p) = g(T^p)$ (char p)

Proposition

$f : F \to G$ homomorphism of formal groups over R.

1. *if $f'(0) = 0$, then $f(T) = f_1(T^p)$ for some $f_1 \in R[\![T]\!]$*
2. *write $f(T) = g(T^{p^h})$ with $h = ht(f)$. Then $g'(0) \neq 0$*

Proof

1. $0 = f'(0)\omega_F(T) = (\omega_G \circ f)(T) = (1 + \cdots)f'(T)dT \implies f'(T) = 0$ $\implies f(T) = f_1(T^p)$
2. $q := p^h$, $F(X, Y) = \sum_{i,j} a_{ij} X^i Y^j$. Since $\mathrm{char}(R) = p$, one can check that $F^{(q)}(X, Y) := \sum_{i,j} a_{ij}^q X^i Y^j$ is still a formal group.
   We show that g is a homomorphism $F^{(q)} \to G$: if $S^q = X$, $T^q = Y$, then
   $$\begin{aligned} g(F^{(q)}(X, Y)) &= g(F(S, T)^q) = f(F(S, T)) = \\ &= G(f(S), f(T)) = G(g(S^q), g(T^q)) = G(g(X), g(Y)) \end{aligned}$$
   Suppose $g'(0) = 0$: by 1. $g(T) = g_1(T^p)$
   $\implies f(T) = g(T^{p^h}) = g_1(T^{p^{h+1}})$ would contradict $h = \mathrm{ht}(f)$.

Proposition

$F \xrightarrow{f} G \xrightarrow{g} H$ homomorphisms; then $ht(g \circ f) = ht(f) + ht(g)$.

Proof

$f(T) = f_1(T^{p^{\mathrm{ht}(f)}})$, $g(T) = g_1(T^{p^{\mathrm{ht}(g)}})$

$$g(f(T)) = g_1(f_1(T^{p^{\mathrm{ht}(f)}})^{\mathrm{ht}(g)}) = g_1(\widetilde{f_1}(T^{p^{\mathrm{ht}(f)+\mathrm{ht}(g)}}))$$

$\widetilde{f_1}$ obtained from f_1 raising coefficients to $p^{\mathrm{ht}(g)}$.
We have seen that $f_1'(0) \neq 0 \neq g_1'(0)$, i.e. f_1, g_1 have $\neq 0$ linear terms

E_1/K, E_2/K elliptic curves over K of char p.

Recall

An *isogeny* $E_1 \to E_2$ is a morphism $\varphi\colon E_1 \to E_2$ such that $\varphi(O) = O$
$\deg \varphi := [K(E_1) : \varphi^* K(E_2)] = (\deg_i \varphi)(\deg_s \varphi)$

Theorem

Let $\varphi\colon E_1 \to E_2$ *be a nonzero isogeny over* K, $f : \widehat{E}_1 \to \widehat{E}_2$ *the induced homomorphism of formal groups. Then*

$$\deg_i(\varphi) = p^{ht(f)}$$

Special case: $\varphi = (-)^{p^r}$

$\deg_i \varphi = p^r$ (talk 2) and $f(T) = T^{p^r}$, hence $\mathrm{ht}(f) = r \implies \deg_i(\varphi) = p^{\mathrm{ht}(f)}$.

Special case: φ is separable

Fact: $\varphi\colon E_1 \to E_2$ separable $\iff \varphi^* : \Omega_{E_2} \to \Omega_{E_1}$ injective

$$0 \neq \omega \circ f = f'(0)\omega \implies f'(0) \neq 0 \implies \mathrm{ht}(f) = 0$$

General case

Let φ be any isogeny.
Fact: $\varphi = \lambda \circ \varphi'$ with $\varphi' =$ (($\deg_i \varphi$)-th power Frobenius) and λ separable.

$$\mathrm{ht}(\varphi) = \mathrm{ht}(\lambda \circ \varphi') = \mathrm{ht}(\lambda) + \mathrm{ht}(\varphi') = \mathrm{ht}(\varphi')$$

$$\deg_i(\varphi) = \deg_i(\lambda)\deg_i(\varphi') = p^{\mathrm{ht}(\lambda)} p^{\mathrm{ht}(\varphi')} = p^{\mathrm{ht}(\varphi)}$$

Corollary

For E/K with $\mathrm{char}(K) = p > 0$ we have $ht(\widehat{E}) \in \{1, 2\}$

Proof

- By the theorem with $\varphi = [p]$: $\deg_i([p]) = p^{\mathrm{ht}([p])}$
- Fact (talk 2): $\deg([p]) = p^2$
- Hence, $\deg_i([p]) \in \{1, p, p^2\}$
- but $\deg_i([p]) \neq 1$ because $[p]$ is not separable
- therefore, $\deg_i([p]) = p^{\mathrm{ht}([p])} \in \{p, p^2\}$, so $\mathrm{ht}([p]) \in \{1, 2\}$

$\square$