CHARLES UNIVERSITY PRAGUE

faculty of mathematics and physics

Jan Butora

Department of algebra

British Elevator I

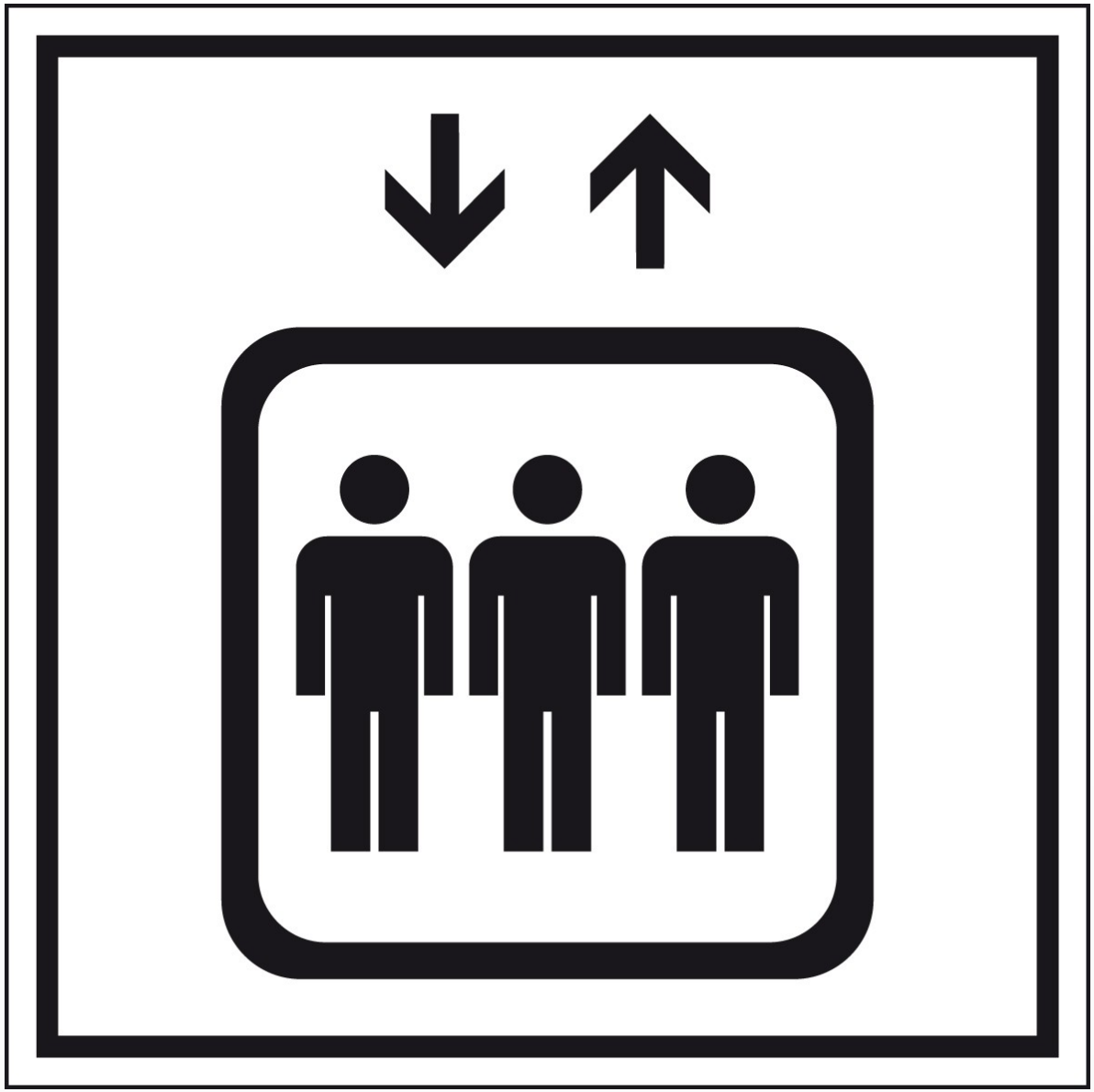
Theoretical background

Fall school of algebra 2016

Content

- p-adic numbers
- Formal groups and formal logarithm

Elevator



p-adic valuation

Definition

If $0 \neq x \in \mathbb{Z}$, the *p-adic valuation* of x is

$$v_p(x) = \max\{r : p^r | x\} \geq 0$$

For $a/b \in \mathbb{Q}$, the *p-adic valuation* of a/b

$$v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b)$$

We also introduce the convention that $v_p(0) = \infty$.

p-adic valuation

Definition

If $0 \neq x \in \mathbb{Z}$, the *p-adic valuation* of x is

$$v_p(x) = \max\{r : p^r | x\} \geq 0$$

For $a/b \in \mathbb{Q}$, the *p-adic valuation* of a/b

$$v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b)$$

We also introduce the convention that $v_p(0) = \infty$.

Lemma

If $x, y \in \mathbb{Q}$, the v_p has the following properties:

1. $v_p(x) = \infty$ *if and only if* $x = 0$;
2. $v_p(xy) = v_p(x) + v_p(y)$;
3. $v_p(x + y) \geq min\{v_p(x), v_p(y)\}$ *with equality if* $v_p(x) \neq v_p(y)$.

p-adic norm

Definition

For $x \in \mathbb{Q}$, let *the p-adic norm* of x be given by

$$|x|_p = \begin{cases} p^{-v_p(x)} & \text{if } x \neq 0, \\ p^{-\infty} = 0 & \text{if } x = 0. \end{cases}$$

p-adic norm

Definition

For $x \in \mathbb{Q}$, let *the p-adic norm* of x be given by

$$|x|_p = \begin{cases} p^{-v_p(x)} & \text{if } x \neq 0, \\ p^{-\infty} = 0 & \text{if } x = 0. \end{cases}$$

Lemma

The function $||_p : \mathbb{Q} \to \mathbb{R}^+$ has the properties:

1. $|x|_p = 0$ *if and only if* $x = 0$;
2. $|xy|_p = |x|_p |y|_p$;
3. $|x + y|_p \leq max\{|x|_p, |y|_p\}$, *with equality if* $|x|_p \neq |y|_p$.

Distance

Definition

The *distance* between $x, y \in R$ with respect to $||_p$ is

$$d_p(x, y) = |x - y|_p \in \mathbb{R}^+$$

Lemma (The Isosceles Triangle Principle)

Let $x, y, z \in R$ such that $d_p(x, z) \neq d_p(z, y)$. Then

$$d_p(x, y) = max\{d_p(x, z), d_p(z, y)\}.$$

The limit

Definition

The sequence (a_n) *tends to the limit* $a \in R$ *with respect to* $||_p$ if

$$\forall \epsilon > 0 \, \exists M \in \mathbb{N} \text{ such that } n > M \Longrightarrow |a - a_n|_p = d_p(a, a_n) < \epsilon$$

The limit

Definition

The sequence (a_n) *tends to the limit* $a \in R$ *with respect to* $||_p$ if

$$\forall \epsilon > 0 \, \exists M \in \mathbb{N} \text{ such that } n > M \Longrightarrow |a - a_n|_p = d_p(a, a_n) < \epsilon$$

Definition

The sequence (a_n) is *Cauchy with respect to* $||_p$ if

$$\forall \epsilon > 0 \, \exists M \in \mathbb{N} \text{ such that } m, n > M \Longrightarrow |a_m - a_n|_p = d_p(a_m, a_n) < \epsilon$$

The limit

Definition

The sequence (a_n) *tends to the limit* $a \in R$ *with respect to* $||_p$ if

$$\forall \epsilon > 0 \, \exists M \in \mathbb{N} \text{ such that } n > M \Longrightarrow |a - a_n|_p = d_p(a, a_n) < \epsilon$$

Definition

The sequence (a_n) is *Cauchy with respect to* $||_p$ if

$$\forall \epsilon > 0 \, \exists M \in \mathbb{N} \text{ such that } m, n > M \Longrightarrow |a_m - a_n|_p = d_p(a_m, a_n) < \epsilon$$

Example

Sequence (a_n), where $a_n = 1 + p + p^2 + \ldots + p^{n-1}$ is Cauchy and has a limit in $\mathbb{Q}$ with respect to $||_p$.

Cauchy sequences

Theorem

If $lim^{(p)} a_n$ exists, then (a_n) is Cauchy with respect to $||_p$.

Cauchy sequences

Theorem

If $\lim^{(p)} a_n$ exists, then (a_n) is Cauchy with respect to $||_p$.

Example

Consider $(a_n) \subseteq \mathbb{Q}$ whose n-th term is the decimal expansion of $\sqrt{2}$ up to the n-th decimal place, i.e., $a_1 = 1.4$, $a_2 = 1.41$, $a_3 = 1.414$, etc.

Cauchy sequences

Theorem

If $lim^{(p)} a_n$ exists, then (a_n) is Cauchy with respect to $||_p$.

Example

Consider $(a_n) \subseteq \mathbb{Q}$ whose n-th term is the decimal expansion of $\sqrt{2}$ up to the n-th decimal place, i.e., $a_1 = 1.4$, $a_2 = 1.41$, $a_3 = 1.414$, etc.

Definition

A sequence (a_n) is called a *null sequence* if $lim^{(p)} a_n = 0$.

Cauchy sequences

Theorem

If $lim^{(p)} a_n$ exists, then (a_n) is Cauchy with respect to $||_p$.

Example

Consider $(a_n) \subseteq \mathbb{Q}$ whose n-th term is the decimal expansion of $\sqrt{2}$ up to the n-th decimal place, i.e., $a_1 = 1.4$, $a_2 = 1.41$, $a_3 = 1.414$, etc.

Definition

A sequence (a_n) is called a *null sequence* if $lim^{(p)} a_n = 0$.

- $\mathrm{CS}(R) =$ the set of Cauchy sequences in R with respect to $||_p$,
- $\mathrm{Null}(R) =$ the set of null sequences in R with respect to $||_p$.

Cauchy sequences

Theorem

If $lim^{(p)} a_n$ exists, then (a_n) is Cauchy with respect to $||_p$.

Example

Consider $(a_n) \subseteq \mathbb{Q}$ whose n-th term is the decimal expansion of $\sqrt{2}$ up to the n-th decimal place, i.e., $a_1 = 1.4$, $a_2 = 1.41$, $a_3 = 1.414$, etc.

Definition

A sequence (a_n) is called a *null sequence* if $lim^{(p)} a_n = 0$.

- $\mathrm{CS}(R) =$ the set of Cauchy sequences in R with respect to $||_p$,
- $\mathrm{Null}(R) =$ the set of null sequences in R with respect to $||_p$.
- addition and multiplication in $\mathrm{CS}(R)$

$$(a_n) + (b_n) = (a_n + b_n), \quad (a_n) \times (b_n) = (a_n b_n)$$

Completion

Definition

A ring with the norm $||_p$ is *complete with respect to the norm* $||_p$ if every Cauchy sequence has a limit in R with respect to $||_p$.

Definition

Quotient ring $\mathrm{CS}(R)/\mathrm{Null}(R)$ is called the *completion of* R *with respect to the norm* $||_p$, and is denoted $\hat{R}$.

Completion

Definition

A ring with the norm $||_p$ is *complete with respect to the norm* $||_p$ if every Cauchy sequence has a limit in R with respect to $||_p$.

Definition

Quotient ring $\mathrm{CS}(R)/\mathrm{Null}(R)$ is called the *completion of* R *with respect to the norm* $||_p$, and is denoted $\hat{R}$.

Definition

The ring of *p-adic numbers* is the completion $\hat{\mathbb{Q}}$ of $\mathbb{Q}$ with respect to $||_p$; we will denote it $\mathbb{Q}_p$.

Completion

Definition

A ring with the norm $||_p$ is *complete with respect to the norm* $||_p$ if every Cauchy sequence has a limit in R with respect to $||_p$.

Definition

Quotient ring $\mathrm{CS}(R)/\mathrm{Null}(R)$ is called the *completion of* R *with respect to the norm* $||_p$, and is denoted $\hat{R}$.

Definition

The ring of *p-adic numbers* is the completion $\hat{\mathbb{Q}}$ of $\mathbb{Q}$ with respect to $||_p$; we will denote it $\mathbb{Q}_p$.

Definition

The unit ball about $0 \in \mathbb{Q}_p$ is the set of *p-adic integers*,

$$\mathbb{Z}_p = \{\alpha \in \mathbb{Q}_p : |\alpha|_p \leq 1\} = \{\alpha \in \mathbb{Q}_p : v_p(\alpha) \geq 0\}.$$

p-adic expansion

Theorem

The set of p-adic integers $\mathbb{Z}_p$ is a subring of $\mathbb{Q}_p$. Every element of $\mathbb{Z}_p$ is the limit of a sequence of (non-negative) integers and conversely, every Cauchy sequence in $\mathbb{Q}$ consisting of integers has a limit in $\mathbb{Z}_p$.

p-adic expansion

Theorem

The set of p-adic integers $\mathbb{Z}_p$ is a subring of $\mathbb{Q}_p$. Every element of $\mathbb{Z}_p$ is the limit of a sequence of (non-negative) integers and conversely, every Cauchy sequence in $\mathbb{Q}$ consisting of integers has a limit in $\mathbb{Z}_p$.

- p-adic expansion of $\alpha \in \mathbb{Z}_p$:

$$\alpha = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \ldots = \ldots \alpha_2 \alpha_1 \alpha_0$$

  - this expansion is *unique*

Theorem

The set of p-adic integers $\mathbb{Z}_p$ is a subring of $\mathbb{Q}_p$. Every element of $\mathbb{Z}_p$ is the limit of a sequence of (non-negative) integers and conversely, every Cauchy sequence in $\mathbb{Q}$ consisting of integers has a limit in $\mathbb{Z}_p$.

- p-adic expansion of $\alpha \in \mathbb{Z}_p$:

$$\alpha = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \ldots = \ldots \alpha_2 \alpha_1 \alpha_0$$

  - this expansion is *unique*
- p-adic expansion of $\alpha \in \mathbb{Q}_p$:
  - Suppose $|\alpha|_p = p^k$, with $k > 0$.
  - Consider $\beta = p^k \alpha$, which has $|\beta|_p = 1$.

$$\beta = \beta_0 + \beta_1 p + \beta_2 p^2 + \ldots$$

  - Then
    $\alpha = \beta_0 p^{-k} + \beta_1 p^{-k+1} + \ldots + \beta_{k-1} p^{-1} + \beta_k + \beta_{k+1} p + \ldots + \beta_{k+r} p^r + \ldots$
  - Can be written as

$$\alpha = \ldots \beta_{k+2} \beta_{k+1} \beta_k, \beta_{k-1} \ldots \beta_1 \beta_0$$

p-adic operations

Theorem

Every p-adic number $\alpha \in \mathbb{Q}_p$ has a unique p-adic expansion

$$\alpha = \alpha_{-r}p^{-r} + \alpha_{1-r}p^{1-r} + \dots \alpha_{-1}p^{-1} + \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \dots$$

with $a_n \in \mathbb{Z}$ and $0 \leq \alpha_n \leq (p-1)$. Furthermore, $\alpha \in \mathbb{Z}_p$ if and only if $\alpha_{-r} = 0$ whenever $r > 0$.

- Operations same as in p-adic representation of naturals.

Hensel's lemma

Theorem

Let $f(X) \in \mathbb{Z}_p[X]$ be a polynomial and let $\alpha \in \mathbb{Z}_p$ be a p-adic number for which

$$|f(\alpha)|_p < 1, |f'(\alpha)|_p = 1.$$

Define a sequence in $\mathbb{Q}_p$ by setting $\alpha_0 = \alpha$ and in general

$$\alpha_{n+1} = \alpha_n - \frac{f(\alpha_n)}{f'(\alpha_n)}.$$

Then each α_n is in $\mathbb{Z}_p$ and moreover

$$|f(\alpha_n)|_p < \frac{1}{p^n}.$$

Hence the sequence (α_n) is Cauchy with respect to $||_p$ and

$$f(\lim^{(p)}_{n\to\infty} \alpha_n) = 0.$$


2

Definition (Formal group)

A (one-dimensional) *formal group* $\mathscr{F}$ over a commutative ring R is a power series $F(X, Y) \in R[[X, Y]]$, such that

1. $F(X, Y) = X + Y +$ terms of higher degree
2. $F(X, F(Y, Z)) = F(F(X, Y), Z)$ (associativity)
3. $F(X, Y) = F(Y, X)$ (commutativity)
4. $\exists!$ power series $i(T) \in R[[T]]$, such that $F(T, i(T)) = 0$ (inverse)
5. $F(X, 0) = X$ and $F(0, Y) = Y$

We call $F(X, Y)$ the *formal group law*.

Definition (Formal group)

A (one-dimensional) *formal group* $\mathscr{F}$ over a commutative ring R is a power series $F(X, Y) \in R[[X, Y]]$, such that

1. $F(X, Y) = X + Y +$ terms of higher degree
2. $F(X, F(Y, Z)) = F(F(X, Y), Z)$ (associativity)
3. $F(X, Y) = F(Y, X)$ (commutativity)
4. $\exists!$ power series $i(T) \in R[[T]]$, such that $F(T, i(T)) = 0$ (inverse)
5. $F(X, 0) = X$ and $F(0, Y) = Y$

We call $F(X, Y)$ the *formal group law*.

Definition

The *formal additive group*, denoted by $\hat{\mathbb{G}}_a$, is defined by

$$F(X, Y) = X + Y.$$

The *formal multiplicative group*, denoted by $\hat{\mathbb{G}}_m$, is defined by

$$F(X, Y) = X + Y + XY.$$

Definition

Let $(\mathscr{F}, F)$ and $(\mathscr{G}, G)$ be formal groups defined over R. A *homomoprhism from $\mathscr{F}$ to $\mathscr{G}$ defined over R* is a power series $f \in R[[T]]$ that satisfies

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

The formal groups $\mathscr{F}$ and $\mathscr{G}$ are *isomorphic over R* if there are homomorphisms $f : \mathscr{F} \to \mathscr{G}$ and $g : \mathscr{G} \to \mathscr{F}$ defined over R such that

$$\mathrm{f(g(T)) = g(f(T)) = T.}$$

Definition

Let $(\mathscr{F}, F)$ and $(\mathscr{G}, G)$ be formal groups defined over R. A *homomoprhism from $\mathscr{F}$ to $\mathscr{G}$ defined over R* is a power series $f \in R[[T]]$ that satisfies

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

The formal groups $\mathscr{F}$ and $\mathscr{G}$ are *isomorphic over R* if there are homomorphisms $f : \mathscr{F} \to \mathscr{G}$ and $g : \mathscr{G} \to \mathscr{F}$ defined over R such that

$$\mathrm{f(g(T)) = g(f(T)) = T.}$$

Definition

Let R be a complete local ring with maximal ideal $\mathscr{M}$ and $\mathscr{F}$ a formal group defined over R, with formal group law $F(X, Y)$. The *group associated to $\mathscr{F}/R$*, denoted by $\mathscr{F}(\mathscr{M})$, is the set $\mathscr{M}$ endowed with the group operations.

$$x \oplus_{\mathscr{F}} y = F(x, y) \quad \text{(addition)} \quad \text{for } x, y \in \mathscr{M},$$
$$\ominus_{\mathscr{F}} x = i(x) \quad \text{(inversion)} \quad \text{for } x \in \mathscr{M}.$$

Associated groups vs. ideals

Lemma

Let $\mathscr{F}/R$ be a formal group defined over a complete local ring with maximal ideal $\mathscr{M}$. Then for each $n \geq 1$, the map

$$\frac{\mathscr{F}(\mathscr{M}^n)}{\mathscr{F}(\mathscr{M}^{n+1})} \to \frac{\mathscr{M}^n}{\mathscr{M}^{n+1}}$$

induced by identity map $x + \mathscr{M}^{n+1} \mapsto x + \mathscr{M}^{n+1}$ on sets is an isomorphism of groups.

Associated groups vs. ideals

Lemma

Let $\mathscr{F}/R$ be a formal group defined over a complete local ring with maximal ideal $\mathscr{M}$. Then for each $n \geq 1$, the map

$$\frac{\mathscr{F}(\mathscr{M}^n)}{\mathscr{F}(\mathscr{M}^{n+1})} \to \frac{\mathscr{M}^n}{\mathscr{M}^{n+1}}$$

induced by identity map $x + \mathscr{M}^{n+1} \mapsto x + \mathscr{M}^{n+1}$ on sets is an isomorphism of groups.

For any $x, y \in \mathscr{M}^n$ we have

$$\begin{aligned} x \oplus_{\mathscr{F}} y &= F(x, y) \\ &= x + y + (\text{higher-order terms}) \\ &= x + y (\text{mod } \mathscr{M}^{2n}). \quad \square \end{aligned}$$

The invariant differential

Definition

An *invariant differential* on a formal group $\mathscr{F}/R$ is a differential form

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

satisfying

$$\omega \circ F(T,S) = \omega(T).$$

Writing this out, $\omega(T) = P(T)dT$ is an invariant differential if it satisfies

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

where $F_X(T,S)$ is the partial derivative of F with respect to its first variable. An invariant differential is said to be *normalized* if $P(0) = 1$.

The invariant differential

Definition

An *invariant differential* on a formal group $\mathscr{F}/R$ is a differential form

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

satisfying

$$\omega \circ F(T,S) = \omega(T).$$

Writing this out, $\omega(T) = P(T)dT$ is an invariant differential if it satisfies

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

where $F_X(T,S)$ is the partial derivative of F with respect to its first variable. An invariant differential is said to be *normalized* if $P(0) = 1$.

- On the additive group $\hat{\mathbb{G}}_a$, the differential $\omega = dT$ is invariant.
- On the multiplicative group $\hat{\mathbb{G}}_m$, the differential $\omega = \frac{dT}{1+T}$ is invariant.

The normalized invariant differential

Theorem

Let $\mathscr{F}/R$ be a formal group. There exists a unique normalized invariant differential on $\mathscr{F}/R$. It is given by the formula

$$\omega = F_X(0, T)^{-1} dT.$$

The normalized invariant differential

Theorem

Let $\mathscr{F}/R$ be a formal group. There exists a unique normalized invariant differential on $\mathscr{F}/R$. It is given by the formula

$$\omega = F_X(0,T)^{-1}dT.$$

Suppose that $P(T)dT$ is an invariant differential on $\mathscr{F}/R$. Put $T = 0$. Then

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

From this we see that every invariant differential is of the form $a\omega$ with $a \in R$ and $\omega = F_X(0,T)^{-1}dT$.

Formal logarithm

Definition (Formal logarithm)

Let R be a torsion-free ring, let $K = R \otimes \mathbb{Q}$, let $\mathscr{F}/R$ be a formal group, and let

$$\omega(T) = (1 + c_1 T + c_2 T^2 + \ldots)dT$$

be the normalized invariant differential on $\mathscr{F}/R$. The *formal logarithm of* $\mathscr{F}/R$ is the power series

$$\log_{\mathscr{F}}(T) = \int \omega(T) = T + \frac{c_1}{2} T^2 + \frac{c_2}{3} T^3 + \ldots \in K[[T]].$$

Formal logarithm

Definition (Formal logarithm)

Let R be a torsion-free ring, let $K = R \otimes \mathbb{Q}$, let $\mathscr{F}/R$ be a formal group, and let

$$\omega(T) = (1 + c_1 T + c_2 T^2 + \ldots)dT$$

be the normalized invariant differential on $\mathscr{F}/R$. The *formal logarithm of* $\mathscr{F}/R$ is the power series

$$\log_{\mathscr{F}}(T) = \int \omega(T) = T + \frac{c_1}{2} T^2 + \frac{c_2}{3} T^3 + \ldots \in K[[T]].$$

The formal group law and invariant differential of the formal multiplicative group $\mathscr{F} = \hat{\mathbb{G}}_m$ are

$$F_{\mathscr{F}}(X, Y) = X + Y + XY \quad \text{and} \quad \omega_{\mathscr{F}}(T) = (1 + T)^{-1} dT.$$

Going additive

Theorem

Let R be a torsion-free ring and let $\mathscr{F}/R$ be a formal group. Then

$$\log_{\mathscr{F}} : \mathscr{F} \to \hat{\mathbb{G}}_a$$

is an isomorphism of formal groups over $K = R \otimes \mathbb{Q}$.

Going additive

Theorem

Let R be a torsion-free ring and let $\mathscr{F}/R$ be a formal group. Then

$$\log_{\mathscr{F}} : \mathscr{F} \to \hat{\mathbb{G}}_a$$

is an isomorphism of formal groups over $K = R \otimes \mathbb{Q}$.

Let $\omega(T)$ be the normalized invariant differential on $\mathscr{F}/R$, so

$$\omega(F(T,S)) = \omega(T).$$

Integrating both sides with respect to T gives

$$\log_{\mathscr{F}} F(T,S) = \log_{\mathscr{F}}(T) + C(S)$$

for some constant of integration $C(S) \in K[[S]]$. Taking $T = 0$ shows that $C(S) = \log_{\mathscr{F}}(S)$. □

Lemma

Let R be a ring of characteristic 0 that is complete with respect to a discrete valuation v, and let $p \in \mathbb{Z}$ be a prime with $v(p) > 0$. Let $f(T)$ be a power series of the form

$$f(T) = \sum_{n=1}^{\infty} \frac{a_n}{n} T^n \text{ with } a_n \in R.$$

If $x \in R$ satisfies $v(x) > 0$, then $f(x)$ converges in R.

Lemma

Let R be a ring of characteristic 0 that is complete with respect to a discrete valuation v, and let $p \in \mathbb{Z}$ be a prime with $v(p) > 0$. Let $f(T)$ be a power series of the form

$$f(T) = \sum_{n=1}^{\infty} \frac{a_n}{n} T^n \text{ with } a_n \in R.$$

If $x \in R$ satisfies $v(x) > 0$, then $f(x)$ converges in R.

For a general term of $f(x)$ we have

$$\begin{aligned} v(a_n x^n/n) &\geq nv(x) - v(n) \\ &\geq nv(x) - (\log_p n)v(p). \end{aligned}$$

That means sequence $(\frac{a_n}{n} x^n)$ is a null sequence, which means sequence (s_n) is Cauchy, where

$$s_n = \sum_{m=0}^{n} \frac{a_m}{m} x^m.$$

Therefore $f(x)$ converges. □

Main result

Theorem

Let K be a field of characteristic 0 that is complete with respect to a normalized discrete valuation v, i.e., $v(K^*) = \mathbb{Z}$, let R be the valuation ring of K, let $\mathscr{M}$ be the maximal ideal of R, and let p be a prime with $v(p) > 0$. Consider a formal group $\mathscr{F}/R$. Then the formal logarithm induces injective homomorphism

$$\log_{\mathscr{F}} : \mathscr{F}(\mathscr{M}) \to K,$$

where the group law on K is addition.

Main result

Theorem

Let K be a field of characteristic 0 that is complete with respect to a normalized discrete valuation v, i.e., $v(K^*) = \mathbb{Z}$, let R be the valuation ring of K, let $\mathscr{M}$ be the maximal ideal of R, and let p be a prime with $v(p) > 0$. Consider a formal group $\mathscr{F}/R$. Then the formal logarithm induces injective homomorphism

$$\log_{\mathscr{F}} : \mathscr{F}(\mathscr{M}) \to K,$$

where the group law on K is addition.

We already know that

$$\log_{\mathscr{F}}(F(X, Y)) = \log_{\mathscr{F}}(X) + \log_{\mathscr{F}}(Y)$$

Hence $\log_{\mathscr{F}}$ will be a homomorphism on $\mathscr{M}$ provided that $\log_{\mathscr{F}}(x)$ converges for $x \in \mathscr{M}$. But $\log_{\mathscr{F}}(m)$ converges for every $m \in \mathscr{M}$ from previous theorem. □

Main result for elliptic curves

Corollary

There is an injective homomorphism

$$\log_{\hat{E}} : \hat{E}(p\mathbb{Z}_p) \hookrightarrow \mathbb{Q}_p$$

where $\hat{E}(p\mathbb{Z}_p)$ is group associated to formal group $E/\mathbb{Q}_p$ given by formal group law for elliptic curves.

Main result for elliptic curves

Corollary

There is an injective homomorphism

$$\log_{\hat{E}} : \hat{E}(p\mathbb{Z}_p) \hookrightarrow \mathbb{Q}_p$$

where $\hat{E}(p\mathbb{Z}_p)$ is group associated to formal group $E/\mathbb{Q}_p$ given by formal group law for elliptic curves.

Corollary

$$\hat{E}(p\mathbb{Z}_p) \cong p\mathbb{Z}_p$$