

UNIVERSITÀ DEGLI STUDI DI PADOVA

Università degli Studi di Padova
Dipartimento di Matematica "Tullio Levi-Civita"
Corso di Laurea Magistrale in Matematica

p-adic periods of one-dimensional commutative formal groups

Supervisor : Prof. Marco Andrea Garuti
Ngandjia Mbembe Chamir : 1188575

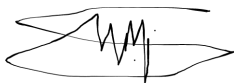
15 luglio 2020

Abstract

A n -dimension commutative formal group over a commutative ring R can be described in a general context, with very restrictive results. However if we restrict ourselves to the one-dimensional case over a p -adic integer ring, we get much more precised and accurate results, from their construction to their classification. The classification gives us a very important invariant of the class, which is the height. In addition to that there is a second invariant for a class, that is the Tate module attached to it. The latter invariant is a key tool for constructing algebraic and arithmetic structures attached to a formal group (the class). In this project we will discuss the p -adic period which at some extend is an invariant for the class of a commutative one-dimensional formal group over a p -adic ring.

Declaration

I, the undersigned, hereby declare that the work contained in this essay is my original work, and that any work done by others or by myself previously has been acknowledged and referenced accordingly.



Ngandjia Chamir, 12 June 2020.

Contents

Abstract	i
1 Introduction	1
2 Commutative formal groups of dimension 1 over a p-adic ring	3
2.1 Generalities on commutative formal groups	3
2.2 The p-adic case	10
2.3 Classification in the case of complete and non-ramified rings	26
3 p-adic periods : The one-dimensional case	34
3.1 The Tate module for a one-dimensional formal group	34
3.2 General facts on the rings B_{dR} , B_{cris} and the ring of Witt vectors over a DVR	36
3.3 Construction of the period map	38
4 Conclusion	43
Acknowledgements	44
References	45

1. Introduction

Formal groups over a commutative ring R are basically finite tuples of power series with coefficients in R , subject to conditions closed enough to the axioms defining a structure of a group. But to define an abstract group from it, we need to construct a landscape, and make clear what the law is. The theory of formal groups has many applications in number theory, algebraic geometry and the theory of Lie groups. They have been developed and used in the theory of Lie groups by Salomon Bochner [1] in 1946, and also by M. Lazard [11]. As for the number theory part, Jean A. Dieudonné studied formal groups over fields of positive characteristic; the special case of interest in the one-dimensional one, over a p -adic integer ring and was carried by Lubin. Together with J. Tate he was able to find interesting results yet in the one-dimensional case. When the landscape attached to a formal group is set, we can consider a bunch of additional algebraic constructions, such as p -adic periods. In 1970, the Japanese mathematician Taira Honda wrote an article in which he gave a construction for a certain general family of commutative formal groups of arbitrary dimension over a p -adic integer ring. In this project, the aim is to adapt the work of Honda to the one-dimensional case over a p -adic ring integer of a local field which is unramified over \mathbb{Q}_p (where p is a prime number), and then to use this machinery to understand p -adic periods of one-dimensional formal groups [7]. The general plan is as follow :

1. In chapter 2 we study the special case of one-dimensional commutative formal groups.

We will first of all give a general method in full details for their construction : Take an element u of the form $p + \sum_{\nu \geq 0} c_\nu T^\nu$ called a special element, where c_ν are integer over our local field, and put $pu^{-1} = \sum_{\nu \geq 0} b_\nu T^\nu$, write $f(x) = \sum_{\nu \geq 0} b_\nu x^{p^\nu}$, finally put $F(x, y) = f^{-1}(f(x) + f(y))$. Then F has integer coefficients, and it is a formal group (over the integers), and any formal group over the integers is isomorphic to one obtained in this fashion. Now let v be another special element $v = p + \sum_{\nu \geq 0} c'_\nu T^\nu$ and G be the formal group defined by $G(x, y) = g^{-1}(g(x) + g(y))$ where $g(x) = \sum_{\nu \geq 0} b'_\nu x^{p^\nu}$ for $pv^{-1} = \sum_{\nu \geq 0} b'_\nu T^\nu$, then an homomorphism from F to G over the integers is of the form $g^{-1}(cf)$ where c is an integer.

Then after, we bijectively identify the strong isomorphism classes of formal groups with the left associate classes of special elements. And this leads to an invariant for the strong isomorphism class of a formal group, the height.

Last of all we end by the classification for one-dimensional commutative formal groups over the integers.

2. In chapter 3 we construct p -adic periods for one-dimensional commutative formal groups.

First of all we start by considering our very first landscape, the Tate module $T_p(F)$ attached to a formal group F . We can exploit the definition of F to build an abelian group law in the set of none invertible integers of an algebraic closure of our local field. If we denote by $F[p^n]$ the subgroup of p^n -torsion elements, then the multiplication by p map raises an inverse system $(F[p^n])_n$ of abelian groups, as for elliptic curves, $T_p(F)$ is simply the projective limit of the system $(F[p^n])_n$. This is a free \mathbb{Z}_p -module of rank h , where h denotes the height of the formal group F . Since the height is an invariant of the strong isomorphism class, then if two formal groups F and G are strongly isomorphic, their respective Tate module are isomorphic. Thanks to the finiteness of the subgroups $F[p^n]$, $T_p(F)$ is a profinite group; we have even more, $T_p(F)$ is a pro- p -group. If ψ

is a morphism of formal groups from F to G over the integers, then for all $n \geq 0$, it induces a morphism

$$\psi_n : F[p^n] \longrightarrow G[p^n],$$

Then by the universal property of projective limit, this induces a canonical morphism

$$T_p(\psi) : T_p(F) \longrightarrow T_p(G).$$

$T_p(-)$ defines a functor from the category of commutative one-dimensional formal groups to the restrictive category of profinite groups.

And then we briefly recall general results on the ring of Witt vectors over a perfect DVR, in order to mention facts about the rings B_{dR} and B_{cris} (see [8]).

Last of all we try to understand p -adic periods of one-dimensional formal groups [7].

2. Commutative formal groups of dimension 1 over a p-adic ring

In this chapter, we investigate the theory of commutative formal groups. We firstly deal with the general context, and later on we restrict to the 1-dimensional case, that is of interest for this project. The main references used for this part are [3], [10] and [13].

2.1 Generalities on commutative formal groups

If not otherwise specified, R will denote a commutative ring with a unit. x is a single indeterminate. We begin by looking at single-variable formal power series with coefficients in R , and after we study multi-variate formal power series, and we focus on those that are invertible with respect to formal composition operation.

2.1.1 Definition. A formal power series with coefficients in R is a formal symbol of the form $\sum_{n=0}^{\infty} a_n x^n$. $R[[x]]$ stands for the set of formal power series with coefficients in R .

We define addition and R -scalar multiplication in $R[[x]]$ to be degree-wise. We define multiplication in $R[[x]]$ by the following rule:

$$\left(\sum_{n=0}^{\infty} a_n x^n \right) \cdot \left(\sum_{n=0}^{\infty} b_n x^n \right) = \sum_{n=0}^{\infty} c_n x^n \text{ with } c_n = \sum_{k=0}^n a_k b_{n-k}$$

Endowed with these operations, $R[[x]]$ becomes a commutative R -algebra.

We recall that if $f(x) \in R[[x]]$ the order $\omega(f(x))$ of $f(x)$ is the index of the first nonzero coefficient of $f(x)$ if $f(x)$ is not zero, and is defined to be infinity otherwise.

Let $f(x) = \sum_{n=0}^{\infty} a_n x^n$, $g(x) = \sum_{n=0}^{\infty} b_n x^n$ be elements of $R[[x]]$ such that $\omega(g(x)) \geq 1$ (which means that the constant term of $g(x)$ vanishes), we define the composition $f \circ g$ to be the power series :

$$\begin{aligned} (f \circ g)(x) &= f(g(x)) \\ &= \sum_{n=0}^{\infty} a_n g(x)^n \\ &= \sum_{n=0}^{\infty} c_n x^n \end{aligned}$$

Where

$$c_n = \sum_{k \in \mathbb{N}, i_1 + \dots + i_k = n, i_1, \dots, i_k \geq 0} a_k b_{i_1} \dots b_{i_k}.$$

The composition $f \circ g$ is well defined due to the condition $\omega(g(x)) \geq 1$, and it is associative, with identity the power series defined by $i(x) = x$. In few lines bellow, we are going to show a more general result that will in particular say that any power series with order equals to 1, and such that the degree 1 coefficient

is invertible in R , should be invertible in $R[[x]]$ with respect to the formal power series composition. Therefore the set of formal power series with order 1 and with degree 1 coefficient invertible in R is a (noncommutative)group with respect to the formal power series composition.

2.1.2 Definition. Let $x = (x_1, \dots, x_n)$ be n indeterminates, $R[[x_1, \dots, x_n]]$ is the set of formal power series with coefficients in R on the indeterminates x_1, \dots, x_n , that is any formal symbol of the form

$$f(x_1, \dots, x_n) = \sum_{(i_1, \dots, i_n) \in \mathbb{N}^n} a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n},$$

where each of the $a_{i_1 \dots i_n}$ belongs to R .

We want to generalize the composition of formal power series from the case of a single indeterminate to the case of n indeterminates. For the sake of convenience, we write $f(x)$ in the place of $f(x_1, \dots, x_n)$, we also state that from now on, if not otherwise specified, formal power series have zero constant term.

If we consider two formal power series in n indeterminates, it is unclear how one might go about composing them. Instead we look, not at individual formal power series, but at n -tuples of formal power series in n indeterminates

2.1.3 Definition. Let $f(x) = (f_1(x), \dots, f_n(x))$ and $g(x) = (g_1(x), \dots, g_n(x)) \in R[[x_1, \dots, x_n]]^n$, we define the composition $f \circ g$ to be the n -tuples of formal power series

$$(f \circ g)(x) = (f_1(g_1(x), \dots, g_n(x)), \dots, f_n(g_1(x), \dots, g_n(x)))$$

It is just a consequence of the single indeterminate case that it still holds here that the composition is associative with identity the formal power series $i(x) = (x_1, \dots, x_n)$

2.1.4 Definition. Let $f(x) = (f_1(x), \dots, f_n(x)) \in R[[x_1, \dots, x_n]]^n$, for any $i = 1, \dots, n$, write

$$f_i = a_{i1}x_1 + \dots + a_{in}x_n + (\text{terms of total degree at least } 2).$$

Then the matrix $M_f = (a_{ij})_{1 \leq i, j \leq n}$ is called the degree 1 matrix of f

2.1.5 Proposition. An element $f(x) = (f_1(x), \dots, f_n(x)) \in R[[x_1, \dots, x_n]]^n$ is invertible with respect to the composition of formal power series if and only if the degree 1 matrix M_f is invertible in the usual ring of square matrices with coefficients in R .

The proof which is pretty much a bit of R -linear algebra can be found in [4].

A particular case of interest will be when $n = 1$, in this case thanks to proposition 2.1.5 we see that a formal power series in a single indeterminate with zero constant term is invertible with respect to the composition of formal power series if and only if the coefficient of the degree 1 monomial is invertible in R . $x = (x_1, \dots, x_n)$ and $y = (y_1, \dots, y_n)$ are n -tuples of indeterminates. From now on, we will write $R[[x]]_0$ for power series with zero constant term. For $f(x), g(x) \in R[[x]]$, we write $f(x) \equiv g(x) \pmod{\text{degr } r}$ if $\omega(f(x) - g(x)) \geq r$

2.1.6 Definition. An n -dimensional formal group over R is an element $F(x, y) \in R[[x, y]]^n$ satisfying :

- i) $F(x, y) = x + y \pmod{\text{deg} 2}$
- ii) $F(F(x, y), z) = F(x, F(y, z))$

If in addition $F(x, y) = F(y, x)$, we say that the formal group F is commutative.

Thanks to proposition 2.1.5, and from the point (i), we can see that any formal group is invertible. Now from (ii), and the fact that $F(0, 0) = 0$ we have $F(F(x, 0), 0) = F(x, F(0, 0)) = F(x, 0)$, therefore $F(x, 0) = F(0, x) = x$.

2.1.7 Definition. Let F and G be formal groups over R of dimensions n and m respectively, a morphism from F to G is any element $\varphi \in R[[x]]_0^m$ satisfying $\varphi(F(x, y)) = G(\varphi(x), \varphi(y))$.

We point out that in the case $n = m$, if φ is invertible, then its inverse φ^{-1} is a morphism from G to F , we say in this case that F and G are weakly isomorphic over R . If in addition $\varphi(x) \equiv x \pmod{\deg 2}$, then we say that F and G are strongly isomorphic over R .

2.1.8 Example. $n = 1$, $R = \mathbb{Q}$ then $F(x, y) = x + y$ and $G(x, y) = x + y + xy$ are 1-dimensional commutative formal groups over the rationals, and $\varphi(x) = -1 + \exp(x) = \sum_{n \geq 1} \frac{1}{n!} x^n$ is a morphism from F to G over the rationals, which is a strong isomorphism.

From now on, all the formal groups considered are assumed to be commutative. Let F be a n -dimensional formal group over R . Put $[0]_F x = 0$ and $[m+1]_F x = F(x, [m]_F x)$ for all $m \geq 0$. When there is no risk of confusion we just write $[m]$ in the place of $[m]_F$.

2.1.9 Remark. We then have the following facts:

1. For all m, m' in \mathbb{N} , $[m+m']x = F([m]x, [m']x)$. To show this, we fix m' and we show the result by induction on m , the result then follows thanks to the associativity property of F .
2. For all m, m' in \mathbb{N} , $[mm']x = [m]([m']x)$. Once again to show this, we fix m' and we show the result by induction on m . By what follows

$$[(m+1)m']x = [mm' + m']x = F([mm']x, [m']x),$$

now by induction hypothesis

$$F([mm']x, [m']x) = F([m][m']x, [m']x) = F([m']x, [m][m']x),$$

the latter equality is the commutativity of F . By definition, $F([m']x, [m][m']x) = [m+1]([m']x)$, and this ends the proof.

3. Since $F(x, y) \equiv x + y \pmod{\deg 2}$, then;

$$\begin{aligned} [m]x &= F(x, [m-1]x) \\ &\equiv x + [m-1]x \pmod{\deg 2} \\ &\equiv x + x + [m-2]x \pmod{\deg 2}, \text{ using the same argument} \end{aligned}$$

Then we keep applying this argument and we arrive at $[m]x \equiv mx \pmod{\deg 2}$

4. For all $n \in \mathbb{N}$, we have $F([m]x, [m]y) = [m]F(x, y)$. We show it by induction on m .

$$\begin{aligned}
F([m+1]x, [m+1]y) &= F(F(x, [m]x), F(y, [m]y)), \text{ by definition} \\
&= F(x, F([m]x, F(y, [m]y))), \text{ by associativity of } F \\
&= F(x, F(F([m]x, y), [m]y)), \text{ by associativity of } F \\
&= F(x, F(F(y, [m]x), [m]y)), \text{ by commutativity of } F \\
&= F(x, F(y, F([m]x, [m]y))), \text{ by associativity of } F \\
&= F(F(x, y), F([m]x, [m]y)), \text{ by associativity of } F \\
&= F(F(x, y), [m]F(x, y)), \text{ by induction hypothesis} \\
&= [m+1]F(x, y)
\end{aligned}$$

Let F be a one-dimensional formal group over R , assume now that R is a field of characteristic $p > 0$, assume that $[p]x$ is not zero. Then set q to be the greatest integer such that $[p]x \equiv 0 \pmod{\deg q}$. Since $\text{char}(R) = p$ then from the third point of the previous remark we see that q must be at least 2. By the maximality of q , there is $r \in R$ nonzero such that $[p]x \equiv rx^q \pmod{\deg(q+1)}$. The fact that $F(x, y) \equiv x + y \pmod{\deg 2}$, implies the following two congruences :

$$[p](F(x, y)) \equiv r(x + y)^q \pmod{\deg(q+1)}$$

and

$$F([p]x, [p]y) \equiv r(x^q + y^q) \pmod{\deg(q+1)}.$$

Therefore by the fourth point of the previous remark we have

$$r(x^q + y^q - (x + y)^q) \equiv 0 \pmod{\deg(q+1)}.$$

But for the sake of degrees, the polynomial $r(x^q + y^q - (x + y)^q)$ must be zero, and since r is nonzero then $x^q + y^q - (x + y)^q = 0$, but this implies that $p|q$, then $q = pq'$, and the equation becomes $(x^p)^{q'} + (y^p)^{q'} - (x^p + y^p)^{q'} = 0$. Then with the same argument $p|q'$. We iterate this, and conclude that q is a power of p . Put $q = p^h$. This justifies the following definition from [11].

2.1.10 Definition. Let F be a one-dimensional formal group over a field of characteristic $p > 0$.

1. If $[p]x$ is not zero, we say that the height of F is h
2. If $[p]x = 0$, we say that the height of F is infinite.

Intuitively, the second point of the definition actually makes perfect sense, because the integer q can get as big as it wants, the congruence is still satisfied.

2.1.11 Example. We try to compute the height in the following two cases, where $R = \mathbb{F}_p$.

1. $F(x, y) = x + y$, let $m \geq 1$ then $[m]x = F(x, [m-1]x) = x + [m-1]x$, then by keeping iterating we find $[m]x = mx$. In particular $[p]x = 0$, then $\text{height}(F) = \infty$.
2. $F(x, y) = x + y + xy$, let $m \geq 1$ then

$$[m]x = F(x, [m-1]x) = x + [m-1]x + x([m-1]x) = (1+x)([m-1]x) + x,$$

by successive iteration downwards we find that for all $k \leq m$,

$$[m]x = (1+x)^k([m-k]x) + x \left(1 + (1+x) + (1+x)^2 + \dots + (1+x)^{k-1} \right).$$

After computation,

$$x \left(1 + (1+x) + (1+x)^2 + \dots + (1+x)^{k-1} \right) = (1+x)^k - 1.$$

Then for all $k \leq m$, $[m]x = (1+x)^k([m-k]x) + (1+x)^k - 1$. In particular for $k = m$ we have

$$[m]x = (1+x)^m([0]x) + (1+x)^m - 1 = (1+x)^m - 1.$$

In particular for $m = p$ we have $[p]x = 1 + x^p - 1 = x^p$, then $\text{height}(F) = 1$.

Put $A = R[[x]]$, we recall that the space of derivations of A over R is a free left A -module that we denote by $\mathcal{D}(A, R)$ with basis $(\frac{\partial}{\partial x_i})_{1 \leq i \leq n}$, actually for any $D \in \mathcal{D}(A, R)$, $D = \sum_{i=1}^n D(x_i) \frac{\partial}{\partial x_i}$. We will denote by $\mathcal{D}^*(A, R)$ the dual A -module of $\mathcal{D}(A, R)$, which is the space of differentials of A over R . For a fixed element $f \in A$, we can define a particular differential df , by

$$df(D) = \sum_{i=1}^n D(x_i) \frac{\partial f}{\partial x_i}(x).$$

Therefore we see that $(dx_i)_{1 \leq i \leq n}$ is an A -basis of $\mathcal{D}^*(A, R)$, and for all $f \in A$,

$$df = \sum_{i=1}^n \frac{\partial f}{\partial x_i}(x) dx_i.$$

Now consider $x' = (x'_1, \dots, x'_m)$ another set of indeterminates, and put $B = R[[x']]$, for any $\varphi(x) \in R[[x]]_0^m$, we define the R -homomorphism φ^* from $\mathcal{D}^*(B, R)$ to $\mathcal{D}^*(A, R)$ by

$$\varphi^* \left(\sum_{j=1}^m \psi_j(x') dx'_j \right) = \sum_{j=1}^m \psi_j(\varphi(x)) d(\varphi_j(x)).$$

2.1.12 Definition. Let F be a n -dimensional formal group over R . Consider another set of indeterminates $t = (t_1, \dots, t_n)$

- The element $T_t \in R_t[[x]]^n$ defined by $T_t(x) = F(x, t)$ is called the right translation on F , where $R_t = R[[t]]$.
- A differential $\omega \in \mathcal{D}^*(A, R)$ is said to be right invariant on F if $T_t^*(\omega) = \omega$

We will denote by $\mathcal{D}^*(F, R)$ the space consisting of all right invariant differentials on F .

2.1.13 Proposition. [10] F is an n -dimensional formal group over R , denote by $(\psi_{ij}(x))_{1 \leq i, j \leq n}$ the inverse matrix of $\left(\frac{\partial F_i}{\partial x_j}(0, x) \right)_{1 \leq i, j \leq n}$, then $\psi_{ij}(0) = \delta_{ij}$ for all i, j , and a R -basis of $\mathcal{D}^*(F, R)$ is given by the ω_i 's, where

$$\omega_i = \sum_{j=1}^n \psi_{ij}(x) dx_j,$$

we call it the canonical basis. In particular, $\mathcal{D}^*(F, R)$ is a free R -module of rank n .

The following theorem is of a crucial importance for this project, as it will be the main bridge for us to get to the algebraic study and classification of formal groups in a p -adic ring.

2.1.14 Theorem. [10] Let F be a formal group over a ring R of characteristic zero, and let $\omega = (\omega_1, \dots, \omega_n)$, where the ω_i 's are elements of the canonical basis of $\mathcal{D}^*(F, R)$, then there exists a unique element $f(x) \in R[[x]]_0^n$ such that $\omega = df$. Moreover we have

$$f(x) \equiv x \pmod{\text{deg}2} \text{ and } F(x, y) = f^{-1}(f(x) + f(y)).$$

For the rest of this paragraph we assume that R is an integral domain of characteristic zero, and K its fraction field.

2.1.15 Lemma. If $\psi(x) \in K[[x]]_0^m$ satisfies $\psi(x + y) = \psi(x) + \psi(y)$, then ψ must be K -linear.

Proof. Assume by contradiction that $\psi(x)$ has a nonzero term with total degree at least 2, then consider the smallest integer greater than 2 such that $\psi(x)$ has a nonzero term of total degree r , we can then write

$$\psi(x) = \sum_{i=1}^n a_i x_i + a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n} + (\text{terms of total degree at least } r),$$

where $a_{i_1 \dots i_n} \neq 0$ and $i_1 + \dots + i_n = r$, then

$$\psi(x + y) = \sum_{i=1}^n a_i (x_i + y_i) + a_{i_1 \dots i_n} (x_1 + y_1)^{i_1} \dots (x_n + y_n)^{i_n} + (\text{terms of total degree at least } r),$$

put $u = a_{i_1 \dots i_n} (x_1 + y_1)^{i_1} \dots (x_n + y_n)^{i_n}$. We have two cases :

- there is $j \in \{1, \dots, n\}$ such that $i_j = r$, say $i_1 = r$, then $i_2 = \dots = i_n = 0$, but then by splitting u we find $a_{i_1 \dots i_n} (x_1^r + y_1^r + T)$ where T is made of terms that do not appear in $\psi(x) + \psi(y)$, we must then have $a_{i_1 \dots i_n} = 0$.
- Without lost of generality we can assume here that i_1 and i_2 are not zero, then $a_{i_1 \dots i_n} y_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$ does not appear in $\psi(x) + \psi(y)$, and therefore we must have $a_{i_1 \dots i_n} = 0$.

We have shown that in any case $a_{i_1 \dots i_n} = 0$, but this is a contradiction by definition of $a_{i_1 \dots i_n}$. \square

Let F be a n -dimensional formal group over R , by theorem 2.1.14, there is $f(x) \in K[[x]]_0^n$ such that

$$f(x) \equiv x \pmod{\text{deg}2} \text{ and } F(x, y) = f^{-1}(f(x) + f(y)),$$

we can say more about $f(x)$ in the following proposition.

2.1.16 Proposition. The element $f(x) \in K[[x]]_0^n$ satisfying

$$f(x) \equiv x \pmod{\text{deg}2} \text{ and } F(x, y) = f^{-1}(f(x) + f(y)),$$

is unique having this property.

Proof. Let $h(x) \in K[[x]]_0^n$ such that $h(x) \equiv x \pmod{\deg 2}$ and $F(x, y) = h^{-1}(h(x) + h(y))$, then $(f \circ h^{-1})(x) \in K[[x]]_0^n$. Because h is invertible, write $x = h(x')$ and $y = h(y')$.

$$\begin{aligned} (f \circ h^{-1})(x + y) &= f(h^{-1}(h(x') + h(y'))) \\ &= f \circ F(x', y') \\ &= f(x') + f(y') \\ &= f \circ h^{-1}(x) + f \circ h^{-1}(y). \end{aligned}$$

We can then apply lemma 2.1 to $f \circ h^{-1}$ to deduce that it is K -linear, but we also have that

$$(f \circ h^{-1})(x) \equiv x \pmod{\deg 2},$$

therefore $f \circ h^{-1} = i$, which means that $f = h$ □

Proposition 2.1.16 leads us to consider the element f , and we call it the transformer of F .

2.1.17 Proposition. Let F be a n -dimensional formal group over R with transformer $f(x) \in K[[x]]_0^n$, and let G be a m -dimensional formal group over R with transformer $g(x) \in K[[x]]_0^m$, then :

- Every morphism $\varphi(x)$ from F to G over R has the form $g^{-1} \circ (Cf)$, where C is an $n \times m$ matrix with coefficients in R .
- If C is an $n \times m$ matrix with coefficients in R , then $g^{-1} \circ (Cf)$ is a morphism from F to G over R if and only if it has coefficients in R

Proof. Let $\varphi(x)$ be a morphism from F to G over R , then by definition we have

$$\varphi(f^{-1}(f(x) + f(y))) = g^{-1}(g(\varphi(x)) + g(\varphi(y))).$$

Substituting x, y by $f^{-1}(x), f^{-1}(y)$ respectively and composing by g we get

$$(g \circ \varphi \circ f^{-1})(x + y) = (g \circ \varphi \circ f^{-1})(x) + (g \circ \varphi \circ f^{-1})(y).$$

Hence by the previous lemma we deduce that $(g \circ \varphi \circ f^{-1})$ is K -linear, therefore there is a $n \times m$ matrix C with coefficients in K such that $(g \circ \varphi \circ f^{-1})(x) = Cx$. Replacing x by $f(x)$ and composing by g^{-1} we get

$$\varphi(x) = g^{-1} \circ (Cf)(x).$$

Since

$$f(x) \equiv x \pmod{\deg 2} \text{ and } g(x) \equiv x \pmod{\deg 2},$$

then $\varphi(x) \equiv Cx \pmod{\deg 2}$, but by definition $\varphi(x)$ has coefficients in R , then so has C .

Conversely assume that C is an $n \times m$ matrix with coefficients in R . If $g^{-1} \circ (Cf)(x)$ is a morphism from F to G over R , then by definition it has coefficients in R . Now if $g^{-1} \circ (Cf)(x)$ has coefficient in R , it amounts just to show that it verify the other condition of being a morphism from F to G over R , which is

$$g^{-1} \circ (Cf)(F(x, y)) = G(g^{-1} \circ (Cf)(x), g^{-1} \circ (Cf)(y)).$$

□

2.2 The p-adic case

In this paragraph we restrict to the case where the ring R is the ring of integers of a p -adic field. Our main reference for this is [10], and we try to adapt his work in the p -adic context. From now on to the rest of this chapter, if without further notice, we fix the following notations :

(K, v) is a complete discrete valuation field which is unramified and such that its residue class field $\kappa = \mathcal{O}_K/\mathfrak{m}_K$ is perfect of characteristic p , we can therefore fix p as a uniformizer, then $\mathfrak{m}_K = p\mathcal{O}_K$. $\sigma : K \rightarrow K$ is an endomorphism such that:

$$\sigma(\alpha) - \alpha^p \in p\mathcal{O}_K \text{ for any } \alpha \in \mathcal{O}_K.$$

Let $\alpha \in \mathcal{O}_K$, there is $x \in p\mathcal{O}_K$ such that $\sigma(\alpha) = \alpha^p + x$, therefore $\sigma(\alpha) \in \mathcal{O}_K$, which means that $\sigma(\mathcal{O}_K) \subset \mathcal{O}_K$, hence σ induces a ring homomorphism $\sigma : \mathcal{O}_K \rightarrow \mathcal{O}_K$. If in addition α is invertible, then σ being a homomorphism, $\sigma(\alpha)$ is invertible as well, this then means that $\sigma(\mathcal{O}_K^*) \subset \mathcal{O}_K^*$.

Take again $\alpha \in \mathcal{O}_K$, there are $n \in \mathbb{N}$ and $u \in \mathcal{O}_K^*$ such that $\alpha = up^n$, since $\sigma(\mathcal{O}_K^*) \subset \mathcal{O}_K^*$, then,

$$v(\sigma(\alpha)) = v(p^n) = n = v(\alpha).$$

Then $v(\sigma(\alpha)) = v(\alpha)$ for all $\alpha \in \mathcal{O}_K$.

In particular for all $x \in \mathfrak{m}_K$, $v(\sigma(x)) = v(x) \geq 1$, this means that $\sigma(\mathfrak{m}_K) \subset \mathfrak{m}_K$. Therefore σ induces a morphism of fields

$$\tilde{\sigma} : \mathcal{O}_K/\mathfrak{m}_K \rightarrow \mathcal{O}_K/\mathfrak{m}_K \text{ defined by } \tilde{\sigma}(\alpha + \mathfrak{m}_K) = \sigma(\alpha) + \mathfrak{m}_K$$

Since $\sigma(\alpha) - \alpha^p \in \mathfrak{m}_K$, then $\tilde{\sigma}(\alpha + \mathfrak{m}_K) = \alpha^p + \mathfrak{m}_K = (\alpha + \mathfrak{m}_K)^p$. Therefore $\tilde{\sigma}$ is just the Frobenius endomorphism of the residue class field $\mathcal{O}_K/\mathfrak{m}_K$, which is perfect, then $\tilde{\sigma}$ is an isomorphism. Thus for all $\alpha \in \mathcal{O}_K$ there is $\beta \in \mathcal{O}_K$ such that $\alpha - \sigma(\beta) \in \mathfrak{m}_K$.

T denotes an undeterminate, for all $k \in \mathbb{N}$, σ^k denotes the endomorphism obtained by repeatedly composing k times with σ , and starting with the identity map. In particular $\sigma^0 = id$. We put

$$K_\sigma[[T]] = (K[[T]], +, \cdot)$$

Here the addition is the usual addition of formal power series, whereas the multiplication is given by the following rule : $T\alpha = \sigma(\alpha)T$ for all $\alpha \in K$. More explicitly :

$$\text{For all } f = \sum_{i \geq 0} \alpha_i T^i \text{ and } g = \sum_{i \geq 0} \beta_i T^i \in K_\sigma[[T]],$$

the coefficient of T^i in the expression of fg is

$$(fg)_i = \sum_{k=0}^i \alpha_k \sigma^k(\beta_{i-k}).$$

$K_\sigma[[T]]$ satisfies all the axioms to be a (noncommutative) ring, we are going to check the associativity of the product which is the less straight forward.

$$\text{Let } f = \sum_{i \geq 0} \alpha_i T^i, g = \sum_{i \geq 0} \beta_i T^i \text{ and } h = \sum_{i \geq 0} \gamma_i T^i \in K_\sigma[[T]]$$

We need to check that $(fg)h = f(gh)$, which amounts to check that they have the same coefficients for every T^i .

$$\begin{aligned} (f(gh))_i &= \sum_{k=0}^i f_k \sigma^k((gh)_{i-k}) \\ &= \sum_{k=0}^i \alpha_k \sigma^k \left(\sum_{j=0}^{i-k} \beta_j \sigma^j(\gamma_{i-k-j}) \right) \\ &= \sum_{k=0}^i \sum_{j=0}^{i-k} \alpha_k \sigma^k(\beta_j) \sigma^{k+j}(\gamma_{i-k-j}) \end{aligned}$$

$$\begin{aligned} ((fg)h)_i &= \sum_{k=0}^i (fg)_k \sigma^k(h_{i-k}) \\ &= \sum_{k=0}^i \sum_{l=0}^k \alpha_l \sigma^l(\beta_{k-l}) \sigma^k(\gamma_{i-k}) \\ &= \sum_{l=0}^i \sum_{k=l}^i \alpha_l \sigma^l(\beta_{k-l}) \sigma^k(\gamma_{i-k}) \\ &= \sum_{k=0}^i \sum_{l=k}^i \alpha_k \sigma^k(\beta_{k-l}) \sigma^l(\gamma_{i-k}) \text{ we have switched the variables } k, l \\ &= \sum_{k=0}^i \sum_{j=0}^{i-k} \alpha_k \sigma^k(\beta_j) \sigma^{k+j}(\gamma_{i-k-j}) \text{ we have set } j = l - k \end{aligned}$$

Then $(f(gh))_i = ((fg)h)_i$ for all $i \in \mathbb{N}$.

An important notice is that the multiplication on $K_\sigma[[T]]$ is an extension of the usual multiplication on K , therefore K is a subring of $K_\sigma[[T]]$. We denote by $\mathfrak{B}_{m,n}$ the K -vector space consisting of elements of the form $\sum_{\nu=0}^{\infty} C_\nu T^\nu$, where the C_ν are $m \times n$ matrices with coefficients in K . In the same way we denote by $\mathfrak{A}_{m,n}$ the \mathcal{O}_K -module consisting of elements of the form $\sum_{\nu=0}^{\infty} C_\nu T^\nu$, where the C_ν are $m \times n$ matrices with coefficients in \mathcal{O}_K .

If $u = \sum_{\nu=0}^{\infty} C_\nu T^\nu \in \mathfrak{B}_{l,m}$ and $v = \sum_{\nu=0}^{\infty} D_\nu T^\nu \in \mathfrak{B}_{k,l}$, then we define the product vu by

$$vu = \sum_{\nu=0}^{\infty} E_\nu T^\nu \in \mathfrak{B}_{k,m} \text{ where } E_\nu = \sum_{i=0}^{\nu} D_i \sigma^i(C_{\nu-i})$$

We recall that $x = (x_1, \dots, x_n)$ is a n -tuples of indeterminates, take $f(x) \in K[[x]]_0^n$, and $u = \sum_{\nu=0}^{\infty} C_\nu T^\nu \in \mathfrak{B}_{l,m}$, we define the element $u * f \in K[[x]]_0^n$ by

$$(u * f)(x) = \sum_{\nu=0}^{\infty} C_\nu f^{\sigma^\nu}(x^{p^\nu})$$

Where f^{σ^ν} stands for the power series obtained from f by applying the endomorphism σ^ν to all its coefficients; and x^{p^ν} stands for the n -tuples $(x_1^{p^\nu}, \dots, x_n^{p^\nu})$. We mention that $u * f$ is actually a well-defined power series as f has zero constant term.

Consider again u, v as above, then

$$\begin{aligned}
(v * (u * f))(x) &= \sum_{\nu=0}^{\infty} D_\nu (u * f)^{\sigma^\nu} (x^{p^\nu}) \\
&= \sum_{\nu=0}^{\infty} D_\nu \left(\sum_{\mu=0}^{\infty} C_\mu f^{\sigma^\mu} \left((x^{p^\nu})^{p^\mu} \right) \right)^{\sigma^\nu} \\
&= \sum_{\nu=0}^{\infty} D_\nu \left(\sum_{\mu=0}^{\infty} C_\mu f^{\sigma^\mu} \left(x^{p^{\nu+\mu}} \right) \right)^{\sigma^\nu} \\
&= \sum_{\nu=0}^{\infty} D_\nu \sum_{\mu=0}^{\infty} C_\mu^{\sigma^\nu} f^{\sigma^{\nu+\mu}} \left(x^{p^{\nu+\mu}} \right) \\
&= \sum_{\lambda=0}^{\infty} \left(\sum_{\nu+\mu=\lambda} D_\nu C_\mu^{\sigma^\nu} \right) f^{\sigma^\lambda} \left(x^{p^\lambda} \right) \\
&= \sum_{\lambda=0}^{\infty} E_\lambda f^{\sigma^\lambda} \left(x^{p^\lambda} \right) \\
&= ((vu) * f)(x)
\end{aligned}$$

Let I be any ideal of \mathcal{O}_K , for $f(x), g(x) \in K[[x]]^n$, we write $f(x) \equiv g(x) \pmod{I}$, to say that $f_i(x) - g_i(x)$ has coefficients in I , for all $i \in \{1, \dots, n\}$. The same notation can therefore be restricted to polynomials with coefficients in \mathcal{O}_K .

2.2.1 Lemma. Let $f(x), g(x) \in \mathcal{O}_K[x]$, such that $f(x) \equiv g(x) \pmod{\mathfrak{m}_K}$, then for all $i \in \mathbb{N}$,

$$f(x)^{p^i} \equiv g(x)^{p^i} \pmod{\mathfrak{m}_K^{i+1}}$$

Proof. We prove the result by induction on i . For $i = 0$ the result is just the hypothesis. Now assume that $i \geq 0$ and that the result is true for i , then there is $h(x) \in \mathcal{O}_K[x]$ such that

$$f(x)^{p^i} = g(x)^{p^i} + p^{i+1}h(x).$$

Now raising this to p , applying the binomial formula and using the fact that for all $k \in \{1, \dots, p-1\}$, p divides the binomial coefficient $\binom{p}{k}$, we deduce that there is $h'(x) \in \mathcal{O}_K[x]$ such that

$$f(x)^{p^{i+1}} = g(x)^{p^{i+1}} + p^{i+2}h'(x).$$

Which just means that $f(x)^{p^{i+1}} \equiv g(x)^{p^{i+1}} \pmod{\mathfrak{m}_K^{i+2}}$ □

2.2.2 Corollary. For any rational integers $\nu \geq 0$, $a \geq 1$ and $m \geq 1$ we have the following congruence

$$p^{-1}(x + py)^{mp^{a\nu}} \equiv p^{-1}x^{mp^{a\nu}} \pmod{\mathfrak{m}_K}$$

Proof. As a variable here we have $z = (x_1, \dots, x_n, y_1, \dots, y_n)$, set $f(z) = x + py$ and $g(z) = x$. Then $f(x), g(x) \in \mathcal{O}_K[z]$, are such that $f(z) \equiv g(z) \pmod{\mathfrak{m}_K}$. Therefore $f(z)^m \equiv g(z)^m \pmod{\mathfrak{m}_K}$, we apply lemma 2.2.1 in the latter congruence and deduce that

$$(x + py)^{mp^{a\nu}} \equiv x^{mp^{a\nu}} \pmod{\mathfrak{m}_K^{a\nu+1}}.$$

But $a\nu + 1 \geq \nu + 1$, therefore $(x + py)^{mp^{a\nu}} \equiv x^{mp^{a\nu}} \pmod{\mathfrak{m}_K^{\nu+1}}$. Which finally means that

$$p^{-1}(x + py)^{mp^{a\nu}} \equiv p^{-1}x^{mp^{a\nu}} \pmod{\mathfrak{m}_K}.$$

□

In the sequel we write \mathfrak{B}_n for $\mathfrak{B}_{n,n}$, same for \mathfrak{A}_n .

2.2.3 Remark. Let $u = \sum_{\nu \geq 0} C_\nu T^\nu \in \mathfrak{A}_n$ such that the matrix C_0 is invertible in the ring of matrices with coefficients in \mathcal{O}_K , we wonder if we can construct an element $v = \sum_{\nu \geq 0} D_\nu T^\nu \in \mathfrak{A}_n$ such that $uv = I_n$, the identity matrix. This means that we have to find a family of matrices $(D_\nu)_{\nu \geq 0}$ with coefficients in \mathcal{O}_K such that

$$\sum_{k=0}^{\nu} C_k \sigma^k(D_{\nu-k}) = \delta_{0,\nu} \text{ for all } \nu \geq 0 \text{ (*).}$$

We set $D_0 = C_0^{-1}$. Let $\nu \geq 1$, assume by induction that $D_0, \dots, D_{\nu-1}$ have been constructed and with coefficients in \mathcal{O}_K , then from relation (*) applied to ν , we have that $C_0 D_\nu = -\sum_{k=1}^{\nu} C_k \sigma^k(D_{\nu-k})$,

therefore $D_\nu = -C_0^{-1} \sum_{k=1}^{\nu} C_k \sigma^k(D_{\nu-k})$ has coefficient in \mathcal{O}_K .

Now since D_0 is invertible, the same argument applied to v shows that there is $v' \in \mathfrak{A}_n$ such that $vv' = I_n$. Then $vu = vuI_n = vuvv' = v(uv)v' = vI_nv' = vv' = I_n$. Hence $uv = vu = I_n$ which means that $v = u^{-1}$. Conversely, if u is invertible in \mathfrak{A}_n , then obviously C_0 is invertible in the ring of matrices with coefficients in \mathcal{O}_K . We notice that the same result holds replacing \mathcal{O}_K by K , and \mathfrak{A}_n by \mathfrak{B}_n .

2.2.4 Definition. We call an element $u \in \mathfrak{A}_n$ special if $u \equiv pI_n \pmod{\text{deg } 1}$. If P is an invertible matrix in $M_n(\mathcal{O}_K)$ and $u \in \mathfrak{A}_n$ a special element, then we say that an element $f(x) \in K[[x]]_0^n$ is of type (P, u) if the following are satisfied :

- $f(x) \equiv Px \pmod{\text{deg } 2}$
- $(u * f)(x) \equiv 0 \pmod{\mathfrak{m}_K}$

In the sequel, if $f(x)$ is of type (I_n, u) we just say that $f(x)$ is of type u .

If $u \in \mathfrak{A}_n$ is a special element, then by definition, $u = pI_n + \sum_{\nu \geq 1} C_\nu T^\nu$, then from the previous remark, since $C_0 = pI_n$ is invertible in $K_{n,n}$, then u is invertible in \mathfrak{B}_n . Set $w = u^{-1}p$, then $w = pu^{-1}$ because $\sigma(p) = p$, then $uw = pI_n$. We recall that $i(x) \in K[[x]]_0^n$ is defined by $i(x) = x$.

$$\text{Set } w = \sum_{\nu \geq 0} B_\nu T^\nu,$$

necessarily $B_0 = I_n$, then :

$$\begin{aligned}
 (w * i)(x) &= \sum_{\nu \geq 0} B_\nu i^{\sigma^\nu}(x^{p^\nu}) \\
 &= \sum_{\nu \geq 0} B_\nu x^{p^\nu} \\
 &= I_n x + \sum_{\nu \geq 1} B_\nu x^{p^\nu} \\
 &\equiv I_n x \pmod{\text{deg } 2}
 \end{aligned}$$

combined with

$$(u * (w * i))(x) = ((uw) * i)(x) = ((pI_n) * i)(x) = px \equiv 0 \pmod{\mathfrak{m}_K},$$

enable us to say that $w * i$ is of type u .

2.2.5 Lemma. Let $u \in \mathfrak{A}_n$ be a special element and put $w = pu^{-1} = \sum_{\nu \geq 0} B_\nu T^\nu$, then :

$$p^\nu B_\nu \text{ has coefficients in } \mathcal{O}_K \text{ for all } \nu \geq 0$$

Proof. Write $u = pI_n + \sum_{\nu \geq 1} C_\nu T^\nu$, set $C_0 = pI_n$ and $uw = \sum_{\nu \geq 0} D_\nu T^\nu$ then since $uw = pI_n$, we deduce that

$$D_\nu = \sum_{i=0}^{\nu} C_i \sigma^i(B_{\nu-i}) \text{ for all } \nu \geq 0 (*).$$

But $u \in \mathfrak{A}_n$, then C_ν has coefficients in \mathcal{O}_K for all $\nu \geq 0$. We are going to show our result by induction. $B_0 = I_n$ has coefficients in \mathcal{O}_K . Let $\nu \geq 1$, assume $p^j B_j$ has coefficients in \mathcal{O}_K for all $0 \leq j \leq \nu - 1$. Then from (*) we have

$$C_0 B_\nu = -\sum_{i=1}^{\nu} C_i \sigma^i(B_{\nu-i}).$$

Multiplying both sides of the equality by $p^{\nu-1}$ we get

$$p^\nu B_\nu = -\sum_{i=1}^{\nu} C_i \sigma^i(p^{\nu-1} B_{\nu-i}).$$

But each of the $p^{\nu-1} B_{\nu-i}$ has coefficients in \mathcal{O}_K by induction hypothesis. □

If $f(x)$ and $g(x)$ are elements of $K[[x]]^n$, then we write

$$f(x) \equiv g(x) \pmod{\text{deg } r, \pmod{\mathfrak{m}_K}}$$

if there are $\varphi(x)$ and $\psi(x) \in K[[x]]^n$ such that

$$f(x) - g(x) = \varphi(x) + \psi(x)$$

where

$$\varphi(x) \equiv 0 \pmod{\text{deg } r}, \text{ and } \psi(x) \equiv 0 \pmod{\mathfrak{m}_K}.$$

From now on, except otherwise specified, $u \in \mathfrak{A}_n$ is a special element, we write $w = pu^{-1}$ and $h(x) = (w * i)(x)$ which has been shown to be of type u .

2.2.6 Lemma. Let $v \in \mathfrak{A}_{m,n}$ and $\psi(x') \in K[[x']]_0^n$ where x' is a finite tuple of indeterminates, if the coefficients of components of ψ , of terms of total degree $\leq r-1$ belong to \mathcal{O}_K for some $r \geq 2$, then :

$$v * (h \circ \psi) \equiv (v * h) \circ \psi \pmod{\deg(r+1), \text{ mod } \mathfrak{m}_K}$$

Proof. Write $w = \sum_{\nu \geq 0} B_\nu T^\nu$, of course $B_0 = I_n$, write $v = \sum_{\nu \geq 0} A_\nu T^\nu$, then

$$vw = \sum_{\lambda \geq 0} C_\lambda T^\lambda \text{ where } C_\lambda = \sum_{0 \leq \nu, \mu, \nu+\mu=\lambda} A_\nu \sigma^\nu(B_\mu).$$

therefore

$$\begin{aligned} ((v * h) \circ \psi)(x') &= (((vw) * i)((\psi)(x'))) \\ &= \sum_{\lambda \geq 0} C_\lambda i^{\sigma^\lambda} (\psi(x'))^{p^\lambda} \\ &= \sum_{\lambda \geq 0} \left(\sum_{0 \leq \nu, \mu, \nu+\mu=\lambda} A_\nu \sigma^\nu(B_\mu) (\psi(x'))^{p^\lambda} \right) \\ &= \sum_{0 \leq \nu, \mu} A_\nu \sigma^\nu(B_\mu) (\psi(x'))^{p^{\nu+\mu}} \quad (1) \end{aligned}$$

$$h \circ \psi(x') = (w * i)(\psi(x')) = \sum_{\mu \geq 0} B_\mu i^{\sigma^\mu} ((\psi(x'))^{p^\mu}) = \sum_{\mu \geq 0} B_\mu (\psi(x'))^{p^\mu},$$

then :

$$(v * (h \circ \psi))(x') = \sum_{\nu \geq 0} A_\nu (h \circ \psi)^{\sigma^\nu} (\psi(x'))^{p^\nu} = \sum_{\nu, \mu \geq 0} A_\nu \sigma^\nu(B_\mu) (\psi^{\sigma^\nu}(x'^{p^\nu}))^{p^\mu} \quad (2)$$

From (1) and (2) it is enough to just show that for all $\nu, \mu \geq 0$,

$$A_\nu \sigma^\nu(B_\mu) (\psi(x'))^{p^{\nu+\mu}} \equiv A_\nu \sigma^\nu(B_\mu) (\psi^{\sigma^\nu}(x'^{p^\nu}))^{p^\mu} \pmod{\deg(r+1), \text{ mod } \mathfrak{m}_K} \quad (3)$$

Combining the fact that for all $\nu \geq 0$, A_ν has coefficients in \mathcal{O}_K , and the fact that from lemma 2.2.5 $p^\mu B_\mu$ has coefficients in \mathcal{O}_K for all $\mu \geq 0$, we deduce that to prove (3) it is enough to prove that :

$$p^{-\mu} (\psi(x'))^{p^{\nu+\mu}} \equiv p^{-\mu} (\psi^{\sigma^\nu}(x'^{p^\nu}))^{p^\mu} \pmod{\deg(r+1), \text{ mod } \mathfrak{m}_K} \quad (4).$$

(4) is obviously true if $\nu = \mu = 0$. As terms of degree $\geq r$ do not affect the congruence, we may behave like $\psi(x')$ is an element of $\mathcal{O}_K[x']$ of degree $\leq r-1$, in this case we just show the congruence mod \mathfrak{m}_K . Since σ acts on $\mathcal{O}_K/\mathfrak{m}_K$ as the Frobenius endomorphism, then

$$\psi(x')^p \equiv \psi^p(x'^p) \equiv \psi^\sigma(x'^p) \pmod{\mathfrak{m}_K}$$

where ψ^p stands for the polynomial obtained by taking all the coefficients of ψ to power p . And by induction on ν one deduces that

$$\psi(x')^{p^\nu} \equiv \psi^{\sigma^\nu}(x'^{p^\nu}) \pmod{\mathfrak{m}_K}.$$

Then from lemma 2.2.1 we have,

$$(\psi(x'))^{p^{\nu+\mu}} \equiv (\psi^{\sigma^\nu}(x'^{p^\nu}))^{p^\mu} \pmod{\mathfrak{m}_K^{\mu+1}}.$$

Therefore

$$p^{-\mu} (\psi(x'))^{p^{\nu+\mu}} \equiv p^{-\mu} (\psi^{\sigma^\nu}(x'^{p^\nu}))^{p^\mu} \pmod{\mathfrak{m}_K}.$$

Which ends our proof. □

2.2.7 Corollary. Let $f(x)$ and $g(x) \in K[[x]]_0^n$, P, Q be invertible matrices in $M_n(\mathcal{O}_K)$ and $u \in \mathfrak{A}_n$ such that $f(x)$ is of type (P, u) , while $g(x)$ is of type (Q, u) , then $g^{-1} \circ f \in \mathcal{O}_K[[x]]_0^n$.

Proof. Since $g(x)$ is of type (Q, u) and Q is invertible, then from proposition 2.1.5, $g(x)$ is invertible, then same argument holds for $h(x)$ and $f(x)$. Define $\varphi = h^{-1} \circ f$, we need to show by induction that all the coefficients of $\varphi(x)$ belong to \mathcal{O}_K . The constant term of $\varphi(x)$ is zero, then it belongs to \mathcal{O}_K . we recall that h is of type u , then $h^{-1} \circ f(x) \equiv Px \pmod{\deg 2}$, this combined with the fact that $P \in M_n(\mathcal{O}_K)$ means that the first-degree coefficients of $\varphi(x)$ are in \mathcal{O}_K . Let $r \geq 2$, assume that the coefficients of $\varphi(x)$ of total degree $\leq r - 1$ are in \mathcal{O}_K , then we have

$$\begin{aligned} p\varphi &= (u * h) \circ \varphi, \text{ by definition} \\ &\equiv u * (h \circ \varphi) \pmod{\deg(r+1)}, \pmod{\mathfrak{m}_K}, \text{ from lemma 2.2.6} \\ &= u * f \equiv 0 \pmod{\mathfrak{m}_K} \end{aligned}$$

This precisely means that the r -th degree coefficients of $\varphi(x)$ belong to \mathcal{O}_K . Using a similar reasoning we show that $h^{-1} \circ g$ also belongs to $\mathcal{O}_K[[x]]_0^n$. Therefore, from the formula

$$g^{-1} \circ f = (g^{-1} \circ h) \circ (h^{-1} \circ f) = (h^{-1} \circ g)^{-1} \circ (h^{-1} \circ f)$$

we deduce the result. □

In the next corollary we generalize the result of lemma 2.2.6

2.2.8 Corollary. Let $v \in \mathfrak{A}_{m,n}$ and $\psi(x') \in K[[x']]_0^n$ where x' is a finite tuple of indeterminates, if all the coefficients of components of ψ , of terms of total degree $\leq r - 1$ belong to \mathcal{O}_K for some $r \geq 2$, and if $f(x) \in K[[x]]_0^n$ is of type (P, u) then :

$$v * (f \circ \psi) \equiv (v * f) \circ \psi \pmod{\deg(r+1)}, \pmod{\mathfrak{m}_K}.$$

We first note that since h is of type u , then corollary 2.2.8 is a generalization of lemma 2.2.6.

Proof. Again we keep $\varphi = h^{-1} \circ f$, put $v = \sum_{\nu \geq 0} A_\nu T^\nu$, since $\varphi(x) \equiv Px \pmod{\deg 2}$, then by definition we have

$$((v * h) \circ \varphi)(x) \equiv A_0 Px \equiv (v * (h \circ \varphi))(x) \pmod{\deg 2}.$$

Then define

$$s_1(x) = ((v * h) \circ \varphi)(x) - A_0 Px \text{ and } s_2(x) = (v * (h \circ \varphi))(x) - A_0 Px.$$

From corollary 2.2.7 $\varphi(x)$ has all coefficients in \mathcal{O}_K , then from lemma 2.2.6 we have

$$s_1(x) \equiv s_2(x) \pmod{\deg(r+1)}, \pmod{\mathfrak{m}_K}.$$

Now since all the coefficients of ψ , of terms of total degree $\leq r - 1$ belong to \mathcal{O}_K , and combined to the fact that the constant term of $\psi(x)$ is zero, we deduce that

$$s_1 \circ \psi(x) \equiv s_2 \circ \psi(x) \pmod{\deg(r+1)}, \pmod{\mathfrak{m}_K}. \quad (*)$$

we then have

$$\begin{aligned}
v * (f \circ \psi) &= v * (h \circ (\varphi \circ \psi)) \\
&\equiv ((v * h) \circ \varphi \circ \psi) \bmod \deg(r+1), \bmod \mathfrak{m}_K, \text{ by lemma 2.2.6} \\
&= A_0 P \psi + s_1 \circ \psi \bmod \deg(r+1), \bmod \mathfrak{m}_K, \text{ by definition of } s_1 \\
&\equiv A_0 P \psi + s_2 \circ \psi \bmod \deg(r+1), \bmod \mathfrak{m}_K, \text{ from the congruence } (*) \\
&= (v * (h \circ \varphi)) \circ \psi \bmod \deg(r+1), \bmod \mathfrak{m}_K, \text{ by definition of } s_2 \\
&= (v * f) \circ \psi \bmod \deg(r+1), \bmod \mathfrak{m}_K.
\end{aligned}$$

□

Corollary 2.2.8 will be mostly used in the following particular case of interest.

2.2.9 Corollary. Under notations and hypothesis of corollary 2.2.8, if we ask in addition that $\psi(x')$ has all coefficients in \mathcal{O}_K , then

$$v * (f \circ \psi) \equiv (v * f) \circ \psi \bmod \mathfrak{m}_K.$$

Proof. Assume that the congruence does not hold. From lemma 2.2.8 there are

$$r \geq 2, \psi_{r+1} \text{ and } \varphi \in K[[x']]_0^n$$

such that

$$w(\psi_{r+1}) \geq r+1, \varphi \equiv 0 \bmod \mathfrak{m}_K$$

and

$$v * (f \circ \psi) - (v * f) \circ \psi = \psi_{r+1} + \varphi.$$

Then necessarily, ψ_{r+1} has a coefficient of total degree say $s \geq r+1$ that does not belong to \mathfrak{m}_K . We apply lemma 2.2.8 again, then there are

$$\psi_{s+1} \text{ and } \varphi' \in K[[x']]_0^n$$

such that

$$w(\psi_{s+1}) \geq s+1, \varphi' \equiv 0 \bmod \mathfrak{m}_K$$

and

$$v * (f \circ \psi) - (v * f) \circ \psi = \psi_{s+1} + \varphi'.$$

But then $\psi_{r+1} - \psi_{s+1} = \varphi' - \varphi \equiv 0 \bmod \mathfrak{m}_K$, and since $w(\psi_{s+1}) \geq s+1 \geq r+1$, then $\psi_{r+1} - \psi_{s+1}$ has a coefficient of total degree s that does not belong to \mathfrak{m}_K , but this contradicts the latter congruence. □

We now use the above constructed machinery to construct some formal groups over \mathcal{O}_K .

2.2.10 Theorem. Let P, Q and u be defined as usual, $f(x)$ be of type (P, u) , and $g(x)$ be of type (Q, u) , then :

1. $F(x, y) = f^{-1}(f(x) + f(y))$ is a (commutative) formal group over \mathcal{O}_K .
2. Let $G(x, y) = g^{-1}(g(x) + g(y))$, then the formal groups F and G are isomorphic over \mathcal{O}_K .
3. If in addition $P = Q$, then the formal groups F and G are strongly isomorphic over \mathcal{O}_K .

Proof. Define $H(x, y) = h^{-1}(h(x) + h(y))$, We first show that $H(x, y)$ is a formal group over \mathcal{O}_K , for this we first show that it has coefficients in \mathcal{O}_K , which we do by induction. The constant term of $H(x, y)$ is zero, then it belongs to \mathcal{O}_K . We recall that $h(x)$ is of type u , then from proposition 2.1.5 we have

$$\begin{aligned} H(x, y) &= h^{-1}(h(x) + h(y)) \\ &\equiv I_n(h(x) + h(y)) \bmod \deg 2 \\ &\equiv x + y \bmod \deg 2 \end{aligned}$$

Then the first-degree coefficients of $H(x, y)$ belong to \mathcal{O}_K . Now let $r \geq 2$ and assume that the coefficients of $H(x, y)$ of terms of degree $\leq r - 1$ belong to \mathcal{O}_K , then

$$\begin{aligned} pH(x, y) &= ((u * h) \circ H)(x, y), \text{ by definition} \\ &\equiv (u * (h \circ H))(x, y) \bmod \deg (r + 1), \bmod \mathfrak{m}_K, \text{ by corollary 2.2.8} \\ &= (u * h)(x) + (u * h)(y) \bmod \deg (r + 1), \bmod \mathfrak{m}_K \\ &= px + py \bmod \deg (r + 1), \bmod \mathfrak{m}_K \\ &\equiv 0 \bmod \mathfrak{m}_K. \end{aligned}$$

Therefore the r -th degree coefficients of $H(x, y)$ belong to \mathcal{O}_K . Thus $H(x, y)$ has coefficients in \mathcal{O}_K . Moreover

$$\begin{aligned} H(H(x, y), z) &= h^{-1}(h(H(x, y)) + h(z)) \\ &= h^{-1}(h(x) + h(y) + h(z)) \\ &= h^{-1}(h(x) + h \circ h^{-1}(h(y) + h(z))) \\ &= h^{-1}(h(x) + h(H(y, z))) \\ &= H(x, H(y, z)). \end{aligned}$$

Then $H(x, y)$ is a formal group over \mathcal{O}_K . we are now ready to prove the points of our theorem.

1. From proposition 2.1.5 we have

$$F(x, y) = f^{-1}(f(x) + f(y)) \equiv P^{-1}(Px + Py) \bmod \deg 2 = x + y \bmod \deg 2.$$

In the same way than we did for $H(x, y)$, we can also show that $F(F(x, y), z) = F(x, F(y, z))$. Therefore it is only left to prove that $F(x, y)$ has coefficients in \mathcal{O}_K . for this we just remark that $F(x, y) = (\varphi^{-1} \circ H \circ \varphi)(x, y)$, where as usual $\varphi = h^{-1} \circ f$. But as we have shown above H has coefficients in \mathcal{O}_K , so have φ and φ^{-1} , thus F has coefficients in \mathcal{O}_K .

2. From the first point we deduce that $G(x, y)$ is also a formal group over \mathcal{O}_K . Put $\psi = h^{-1} \circ g$. Then as for F , $G = \psi^{-1} \circ H \circ \psi$. Define

$$\phi = \psi^{-1} \circ \varphi \in \mathcal{O}_K[[x]]_0^g \text{ because of corollary 2.2.7.}$$

Moreover we have

$$\phi \circ F = \phi \circ \varphi^{-1} \circ H \circ \varphi = \psi^{-1} \circ \varphi \circ \varphi^{-1} \circ H \circ \psi \circ \phi = \psi^{-1} \circ H \circ \psi \circ \phi = G \circ \phi$$

Then ϕ is a morphism of formal groups from F to G over \mathcal{O}_K , but ϕ is invertible by definition, then F and G are isomorphic.

3. We have the following congruences : $\psi(x) \equiv Qx \pmod{\deg 2}$, and $\varphi(x) \equiv Px \pmod{\deg 2}$, therefore

$$\phi(x) \equiv Q^{-1}Px \pmod{\deg 2}.$$

Whence if $P = Q$ we deduce that $\phi(x) \equiv x \pmod{\deg 2}$, which means that F and G are strongly isomorphic.

□

2.2.11 Remark. Take P and u as above, take any element $f \in K[[x]]_0^n$, and put $\varphi = h^{-1} \circ f$.

- i) If we assume that f is of type (P, u) , then as we already know $\varphi(x)$ has coefficients in \mathcal{O}_K and $\varphi(x) \equiv Px \pmod{\deg 2}$.
- ii) Conversely if we assume that $\varphi(x)$ has coefficients in \mathcal{O}_K and that $\varphi(x) \equiv Px \pmod{\deg 2}$, then :

$$\begin{aligned} f(x) &= h \circ \varphi(x) \\ &\equiv I_n \varphi(x) \pmod{\deg 2}, \text{ because } h \text{ is of type } u \\ &\equiv I_n P x \pmod{\deg 2} \\ &\equiv P x \pmod{\deg 2} \end{aligned}$$

We also have;

$$\begin{aligned} u * f &= u * (h \circ \varphi) \\ &\equiv (u * h) \circ \varphi \pmod{\mathfrak{m}_K}, \text{ because of corollary 2.2.9} \\ &= p\varphi \pmod{\mathfrak{m}_K} \\ &= 0 \pmod{\mathfrak{m}_K}. \end{aligned}$$

Then f is of type (P, u) .

The following proposition will enable us to consider a very important coset of equivalence class of special elements over \mathcal{O}_K .

2.2.12 Proposition. Take P and u as usual, and assume $f \in K[[x]]_0^n$ is of type (P, u) , and $v \in \mathfrak{A}_{m,n}$, then :

$$v * f \equiv 0 \pmod{\mathfrak{m}_K} \text{ if and only if there exists } t \in \mathfrak{A}_{m,n} \text{ such that } v = tu.$$

Proof. First assume that $v = tu$, with $t \in \mathfrak{A}_{m,n}$, then simple calculation give

$$v * f = t * (u * f) \equiv 0 \pmod{\mathfrak{m}_K}.$$

Conversely assume $v * f \equiv 0 \pmod{\mathfrak{m}_K}$. Since $v = (vu^{-1})u$ it is enough to show that $vu^{-1} \in \mathfrak{A}_{m,n}$, which means that pvu^{-1} must have coefficients in \mathfrak{m}_K . Then write

$$pvu^{-1} = \sum_{\nu \geq 0} A_\nu T^\nu,$$

we are going to show that each of the A_ν belongs to \mathfrak{m}_K . We set $\varphi = h^{-1} \circ f$, recall that φ is invertible and has coefficients in \mathcal{O}_K . From one hand we have

$$v * h = v * ((pu^{-1}) * i) = (pvu^{-1}) * i = \sum_{\nu \geq 0} A_\nu x^{p^\nu} \quad (*)$$

On the other hand we have

$$\begin{aligned}
(v * h) \circ \varphi &\equiv v * (h \circ \varphi) \pmod{\mathfrak{m}_K}, \text{ because of corollary 2.2.9} \\
&\equiv v * f \pmod{\mathfrak{m}_K} \\
&\equiv 0 \pmod{\mathfrak{m}_K} \quad (**).
\end{aligned}$$

Then :

$$\begin{aligned}
\sum_{\nu \geq 0} A_\nu x^{p^\nu} &= v * h, \text{ because of } (*) \\
&= ((v * h) \circ \varphi) \circ \varphi^{-1} \\
&\equiv 0 \pmod{\mathfrak{m}_K}, \text{ because of } (**).
\end{aligned}$$

Then every A_ν belongs to \mathfrak{m}_K □

The following theorem enables us to study homomorphisms of formal groups built in theorem 2.2.10.

2.2.13 Theorem. *Let $u \in \mathfrak{A}_n$ and $v \in \mathfrak{A}_m$ be special elements; $f \in K[[x]]_0^n$ and $g \in K[[x]]_0^m$ be of type u and v respectively. Take C a matrix of type (m, n) with coefficients in \mathcal{O}_K , consider the formal groups*

$$F(x, y) = f^{-1}(f(x) + f(y)) \text{ and } G(x, y) = g^{-1}(g(x) + g(y)).$$

Then $g^{-1} \circ (Cf)$ is a morphism from F to G over \mathcal{O}_K if and only if there exists $t \in \mathfrak{A}_{m,n}$ such that $vC = tu$

Proof. From proposition 2.1.17, $g^{-1} \circ (Cf)$ is a morphism from F to G over \mathcal{O}_K if and only if it has coefficients in \mathcal{O}_K . Therefore we will show that $g^{-1} \circ (Cf)$ has coefficients in \mathcal{O}_K if and only if there exists $t \in \mathfrak{A}_{m,n}$ such that $vC = tu$.

1. Assume that $g^{-1} \circ (Cf)$ has coefficients in \mathcal{O}_K . Write $h_2 = (pv^{-1}) * i$ and put $\varphi_2 = h_2^{-1} \circ g$, then $v * h = (pI_n) * i = px$, we also recall that from corollary 2.2.7, φ_2 has coefficients in \mathcal{O}_K , then

$$\begin{aligned}
(vC) * f &= v * (Cf) \\
&= v * (g \circ g^{-1} \circ (Cf)) \\
&\equiv (v * g) \circ g^{-1} \circ (Cf) \pmod{\mathfrak{m}_K}, \text{ from corollary 2.2.9} \\
&\equiv (v * (h_2 \circ \varphi_2)) \circ g^{-1} \circ (Cf) \pmod{\mathfrak{m}_K} \\
&\equiv (v * h_2) \circ \varphi_2 \circ g^{-1} \circ (Cf) \pmod{\mathfrak{m}_K}, \text{ from corollary 2.2.9} \\
&\equiv p\varphi_2 \circ g^{-1} \circ (Cf) \pmod{\mathfrak{m}_K} \\
&= 0 \pmod{\mathfrak{m}_K}, \text{ because } \varphi_2 \circ g^{-1} \circ (Cf) \text{ has coefficients in } \mathcal{O}_K.
\end{aligned}$$

Therefore from proposition 2.2.12 there exists $t \in \mathfrak{A}_{m,n}$ such that $vC = tu$.

2. Conversely assume that there exists $t \in \mathfrak{A}_{m,n}$ such that $vC = tu$. We need to show by induction on the degree of terms of $g^{-1} \circ (Cf)$ that it has coefficients in \mathcal{O}_K . We have

$$g^{-1} \circ (Cf)(x) \equiv Cx \pmod{\text{deg } 2},$$

and since C has coefficients in \mathcal{O}_K , then the constant term and the first-degree of $g^{-1} \circ (Cf)$ belong to \mathcal{O}_K . Let $r \geq 2$, assume all coefficients of $g^{-1} \circ (Cf)$ of terms of degree $\leq r-1$ belong to \mathcal{O}_K , then

$$\begin{aligned}
p \varphi_2 \circ g^{-1} \circ (Cf) &= (v * g) \circ g^{-1} \circ (Cf) \\
&\equiv v * (g \circ g^{-1} \circ (Cf)) \pmod{\deg(r+1), \pmod{\mathfrak{m}_K}, \text{ because of corollary 2.2.8}} \\
&= v * (Cf) \pmod{\mathfrak{m}_K} \\
&= (vC) * f \pmod{\mathfrak{m}_K} \\
&= (tu) * f \pmod{\mathfrak{m}_K} \\
&= t * (u * f) \pmod{\mathfrak{m}_K} \\
&= 0 \pmod{\mathfrak{m}_K}, \text{ because } f \text{ is of type } u
\end{aligned}$$

This just means that the r -th degree coefficients of $\varphi_2 \circ g^{-1} \circ (Cf)$ belong to \mathcal{O}_K , but φ_2 also has coefficients in \mathcal{O}_K , therefore we deduce that $g^{-1} \circ (Cf)$ has coefficients in \mathcal{O}_K .

□

Since K is of characteristic 0, so is \mathcal{O}_K , therefore p is not zero in \mathcal{O}_K , therefore we can divide by p if we consider the expression to belong to $\text{Frac}(\mathcal{O}_K) = K$. This being said, let $r \geq 2$ define $\Lambda_r(x, y) \in \mathcal{O}_K[x, y]$ as follow :

- If r is not a power of p , set $\Lambda_r(x, y) = (x + y)^r - x^r - y^r$
- If r is a power of p , set $\Lambda_r(x, y) = p^{-1}[(x + y)^r - x^r - y^r]$

The following lemma gives the most important property of r that is going to be of interest in the sequel of this chapter.

2.2.14 Lemma. $\Lambda_r(x, y)$ is a primitive polynomial in $\mathcal{O}_K[x, y]$ for all r

Proof. The proof is divided into the two parts that correspond each to the definition of $\Lambda_r(x, y)$.

1. r is not a power of p , then $r = p^n s$, where $(p, s) = 1$ and $s \neq 1$.

$$\begin{aligned}
(x + y)^r &= ((x + y)^{p^n})^s \\
&\equiv (x^{p^n} + y^{p^n})^s \pmod{\mathfrak{m}_K} \\
&= x^r + y^r + sX^{(s-1)p^n} y^{p^n} + \dots \pmod{\mathfrak{m}_K}.
\end{aligned}$$

Then

$$\Lambda_r(x, y) \equiv sX^{(s-1)p^n} y^{p^n} + \dots \pmod{\mathfrak{m}_K}.$$

But $(p, s) = 1$, then $\Lambda_r(x, y) \not\equiv 0 \pmod{\mathfrak{m}_K}$, which means that $\Lambda_r(x, y)$ has a coefficient not belonging to \mathfrak{m}_K , this coefficient must then be invertible, whence $\Lambda_r(x, y)$ is primitive.

2. $r = p^n$ for some $n \geq 1$. Then $(x + y)^{p^{n-1}} \equiv x^{p^{n-1}} + y^{p^{n-1}} \pmod{\mathfrak{m}_K}$, then from lemma 2.2.1 we have

$$\begin{aligned} (x + y)^{p^n} &\equiv (x^{p^{n-1}} + y^{p^{n-1}})^p \pmod{\mathfrak{m}_K^2} \\ &= x^{p^n} + y^{p^n} + pP(x, y) \pmod{\mathfrak{m}_K^2} \end{aligned}$$

Where $x^{p^{n-1}(p-1)}y^{p^{n-1}}$ is a monomial of $P(x, y) \in \mathcal{O}_K[x, y]$ with coefficient 1. Then

$$\Lambda_r(x, y) \equiv P(x, y) \pmod{\mathfrak{m}_K}$$

and

$$P(x, y) \not\equiv 0 \pmod{\mathfrak{m}_K}$$

Therefore $\Lambda_r(x, y) \not\equiv 0 \pmod{\mathfrak{m}_K}$, which means again that $\Lambda_r(x, y)$ is primitive.

□

In the sequel $x = (x_1, \dots, x_n)$ is as usual a n -tuples of indeterminates, and for $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$, x^α stands for $x_1^{\alpha_1} \dots x_n^{\alpha_n}$, we also write $|\alpha|$ for $\alpha_1 + \dots + \alpha_n$.

2.2.15 Lemma. Let $r \in \mathbb{N}$, consider $\lambda(x) = \sum_{|\alpha|=r} a_\alpha x^\alpha$ a homogeneous polynomial of degree r , where $a_\alpha \in K$. Assume in addition that

$$\lambda(x + y) \equiv \lambda(x) + \lambda(y) \pmod{\mathfrak{m}_K}.$$

Then $a_\alpha \in \mathfrak{m}_K$. In addition we have what follows :

1. $a_\alpha \in \mathfrak{m}_K$ whenever α is not one of the $r\epsilon_i$, where ϵ_i is the vector of \mathbb{N}^n with zeroes everywhere but 1 at the i -th component.
2. $a_\alpha \in \mathfrak{m}_K$ whenever r is not a power of p .

Proof. We start by proving the first statement.

1. Let $\alpha = (\alpha_1, \dots, \alpha_n)$ be such that $|\alpha| = r$ and such that it is not one of the $r\epsilon_i$, which means that α has at least two nonzero components, say α_1 and α_2 for the sake of convenience. Then writing $\lambda(x + y)$ we have

$$\lambda(x + y) = \sum_{|\alpha|=r} a_\alpha (x + y)^\alpha = \sum_{|\alpha|=r} a_\alpha (x_1 + y_1)^{\alpha_1} \dots (x_n + y_n)^{\alpha_n}.$$

Therefore the coefficient of $x_1^{\alpha_1} y_2^{\alpha_2} \dots y_n^{\alpha_n}$ in $\lambda(x + y)$ is a_α , but as α_1 and α_2 are nonzero the term $x_1^{\alpha_1} y_2^{\alpha_2} \dots y_n^{\alpha_n}$ does not appear in $\lambda(x) + \lambda(y)$. Whence the congruence

$$\lambda(x + y) \equiv \lambda(x) + \lambda(y) \pmod{\mathfrak{m}_K}$$

implies that $a_\alpha \in \mathfrak{m}_K$

2. Assume r is not a power of p , and let α be such that $|\alpha| = r$, we need to show that $a_\alpha \in \mathfrak{m}_K$. From the previous point we may assume that $\alpha = r\epsilon_i$ for some fixed i . Then a_α is the coefficient of the monomial x_i^r in $\lambda(x)$, it is also the coefficient of the monomial y_i^r in $\lambda(y)$. But the monomial $(x_i + y_i)^r$ is free with any other monomial of $\lambda(x + y)$ coming from another α , therefore the congruence

$$\lambda(x + y) \equiv \lambda(x) + \lambda(y) \pmod{\mathfrak{m}_K}$$

implies the congruence

$$a_\alpha[(x_i + y_i)^r - x_i^r - y_i^r] \equiv 0 \pmod{\mathfrak{m}_K}.$$

But since r is not a power of p , then the latter congruence is just

$$a_\alpha \Lambda_r(x, y) \equiv 0 \pmod{\mathfrak{m}_K}.$$

Consider $(b_j)_j$ the coefficients of $\Lambda_r(x, y)$, we recall that each of the b_j belongs to \mathcal{O}_K . Our latter congruence says that $a_\alpha b_j \in \mathfrak{m}_K$ for all j . From lemma 2.2.14 the b_j 's are coprime, then there exists $(u_j)_j$ elements of \mathcal{O}_K such that $\sum_j u_j b_j = 1$. Then $a_\alpha = \sum_j u_j (a_\alpha b_j) \in \mathfrak{m}_K$.

To complete our proof we have to prove that without any condition $a_\alpha \in \mathcal{O}_K$. Then Let α be such that $|\alpha| = r$. From the first two points we can assume without lost of generality that r is a power of p , and that $\alpha = r\epsilon_i$ for some fixed i , because otherwise we will have $a_\alpha \in \mathfrak{m}_K$ which a fortiori implies that $a_\alpha \in \mathcal{O}_K$. As above we then have

$$pa_\alpha \Lambda_r(x, y) \equiv 0 \pmod{\mathfrak{m}_K}.$$

Since $\Lambda_r(x, y)$ is primitive, then again we deduce that $pa_\alpha \in \mathfrak{m}_K$, hence $a_\alpha \in \mathcal{O}_K$. □

Lemma 3.3.1 is crucial in the proof of the following proposition which is the starting point of our classification theory of formal groups of dimension 1 over \mathcal{O}_K .

2.2.16 Proposition. F is an n -dimensional formal group over \mathcal{O}_K and f its transformer. There is $u \in \mathfrak{A}_n$ a special element such that f is of type u .

Proof. We first prove by induction that we can construct a family of matrices $C_\mu \in M_n(\mathcal{O}_K)$ such that for all $\mu \geq 0$,

$$pf(x) + \sum_{\nu=1}^{\mu} C_\nu f^{\sigma^\nu}(x^{p^\nu}) \equiv 0 \pmod{\deg(p^\mu + 1)}, \pmod{\mathfrak{m}_K}.$$

Since f has zero constant term, set $C_0 = pI_n$. By definition of f , $f(x) \equiv x \pmod{\deg 2}$ therefore we have $pf(x) \equiv 0 \pmod{\deg 2}, \pmod{\mathfrak{m}_K}$. Hence the result holds for $\mu = 0$. Now let $\mu \geq 0$, assume C_0, \dots, C_μ have been constructed and that

$$pf(x) + \sum_{\nu=1}^{\mu} C_\nu f^{\sigma^\nu}(x^{p^\nu}) \equiv 0 \pmod{\deg(p^\mu + 1)}, \pmod{\mathfrak{m}_K} \quad (1).$$

We write $f(x) = (f_1(x), \dots, f_n(x))$, and for all i , we put

$$f_i(x) = \sum_{\alpha \in \mathbb{N}^n} a_{\alpha,i} x^\alpha, \text{ with } a_{\alpha,i} \in K.$$

From proposition 2.1.13, the \mathcal{O}_K -basis $\{\omega_1, \dots, \omega_n\}$ of $\mathcal{D}^*(F, \mathcal{O}_K)$ is such that any ω_i has coefficients in \mathcal{O}_K . As $df_i(x) \in \mathcal{D}^*(F, \mathcal{O}_K)$ it then has coefficients in \mathcal{O}_K , hence $\frac{\partial f_i}{\partial x_j}(x)$ has coefficients in \mathcal{O}_K for all i and for all j . Wich says in particular that $\alpha_j a_{\alpha,i} \in \mathcal{O}_K$ for all i and for all j . Let α be an index of $f_i(x)$, then

$$\begin{aligned} a_{\alpha,i}(x+py)^\alpha &= a_{\alpha,i}(x_1+py_1)^{\alpha_1} \prod_{j=2}^n (x_j+py_j)^{\alpha_j} \\ &\equiv a_{\alpha,i} x_1^{\alpha_1} \prod_{j=2}^n (x_j+py_j)^{\alpha_j} \pmod{\mathfrak{m}_K}, \text{ because of lemma 2.2.1} \end{aligned}$$

Repeating the same argument leads us to

$$a_{\alpha,i}(x+py)^\alpha \equiv a_{\alpha,i} x^\alpha \pmod{\mathfrak{m}_K} \quad (2)$$

The congruence in (1) says that modulo \mathfrak{m}_K we can assume that $pf(x) + \sum_{\nu=1}^{\mu} C_\nu f^{\sigma^\nu}(x^{p^\nu})$ has only terms with total degree at least $p^\mu + 1$. Then write

$$pf(x) + \sum_{\nu=1}^{\mu} C_\nu f^{\sigma^\nu}(x^{p^\nu}) = \sum_{|\beta| \geq p^\mu + 1} b_\beta x^\beta \pmod{\mathfrak{m}_K} \quad (3),$$

b_β being n -tuples of K^n . Now if in (3) we substitute x by $F(x, y)$ we get

$$pf(F(x, y)) + \sum_{\nu=1}^{\mu} C_\nu f^{\sigma^\nu}(F(x, y)^{p^\nu}) = \sum_{|\beta| \geq p^\mu + 1} b_\beta F(x, y)^\beta \pmod{\mathfrak{m}_K} \quad (4).$$

From (2) we deduce that $f_i(x+py) \equiv f_i(x) \pmod{\mathfrak{m}_K}$, this implies that

$$f_i^{\sigma^\nu}(x+py) \equiv f_i^{\sigma^\nu}(x) \pmod{\mathfrak{m}_K}.$$

Then

$$f^{\sigma^\nu}(x+py) \equiv f^{\sigma^\nu}(x) \pmod{\mathfrak{m}_K}.$$

With this we can therefore conclude that if two arguments of f^{σ^ν} are congruent modulo \mathfrak{m}_K , then so are their images under f^{σ^ν} . We know that $F(x, y)^{p^\nu} \equiv F^{\sigma^\nu}(x^{p^\nu}, y^{p^\nu}) \pmod{\mathfrak{m}_K}$. Now using the latter congruence as arguments of f^{σ^ν} we deduce that

$$f^{\sigma^\nu}(F(x, y)^{p^\nu}) \equiv f^{\sigma^\nu}(F^{\sigma^\nu}(x^{p^\nu}, y^{p^\nu})) \pmod{\mathfrak{m}_K}.$$

It is also a straight remark that $(g \circ f)^\sigma = g^\sigma \circ f^\sigma$, as well as $(f^\sigma)^{-1} = (f^{-1})^\sigma$ and $F^\sigma(x, y) = (f^{-1})^\sigma(f^\sigma(x) + f^\sigma(y))$. We then have

$$\begin{aligned} pf(F(x, y)) + \sum_{\nu=1}^{\mu} C_\nu f^{\sigma^\nu}(F(x, y)^{p^\nu}) &\equiv pf(F(x, y)) + \sum_{\nu=1}^{\mu} C_\nu f^{\sigma^\nu}(F^{\sigma^\nu}(x^{p^\nu}, y^{p^\nu})) \pmod{\mathfrak{m}_K} \\ &= pf(f^{-1}(f(x) + f(y))) + \sum_{\nu=1}^{\mu} C_\nu f^{\sigma^\nu}((f^{-1})^{\sigma^\nu}(f^{\sigma^\nu}(x^{p^\nu}) + f^{\sigma^\nu}(y^{p^\nu}))) \\ &= pf(x) + pf(y) + \sum_{\nu=1}^{\mu} C_\nu f^{\sigma^\nu}(x^{p^\nu}) + \sum_{\nu=1}^{\mu} C_\nu f^{\sigma^\nu}(y^{p^\nu}) \\ &\equiv \sum_{|\beta| \geq p^\mu + 1} b_\beta (x^\beta + y^\beta) \pmod{\mathfrak{m}_K}, \text{ from (3)} \end{aligned}$$

Therefore equation (4) implies that

$$\sum_{|\beta| \geq p^{\mu+1}} b_{\beta} F(x, y)^{\beta} \equiv \sum_{|\beta| \geq p^{\mu+1}} b_{\beta} (x^{\beta} + y^{\beta}) \pmod{\mathfrak{m}_K}.$$

For all $i \leq n$ we denote by $b_{\beta, i}$ the i -th component of b_{β} , then

$$\sum_{|\beta| \geq p^{\mu+1}} b_{\beta, i} [F(x, y)^{\beta} - x^{\beta} - y^{\beta}] \equiv 0 \pmod{\mathfrak{m}_K} \quad (5).$$

If $b_{\beta, i} \in \mathfrak{m}_K$ for all β and for all i , then from (3) we deduce a construction of a special element such that $u * f \equiv 0 \pmod{\mathfrak{m}_K}$. We can therefore assume for the rest of the proof that there is some β such that there is some i for which $b_{\beta, i} \notin \mathfrak{m}_K$. We put r to be the minimum of $|\beta|$ for all such β . Since $F(x, y) \equiv x + y \pmod{\deg 2}$, then in (5) the only terms of $F(x, y)^{\beta}$ that might add to $-x^{\beta} - y^{\beta}$ are exclusively terms coming from the monomial $(x + y)^{\beta}$ of $F(x, y)^{\beta}$, therefore from (5) we deduce that

$$\sum_{|\beta| \geq p^{\mu+1}} b_{\beta, i} [(x + y)^{\beta} - x^{\beta} - y^{\beta}] \equiv 0 \pmod{\mathfrak{m}_K}.$$

For the sake of degrees we deduce from this that

$$\sum_{|\beta|=r} b_{\beta, i} [(x + y)^{\beta} - x^{\beta} - y^{\beta}] \equiv 0 \pmod{\mathfrak{m}_K} \quad (6).$$

In (6) if we replace r by any degree level, we obtain the same congruence.

Define $\lambda(x) = \sum_{|\beta|=r} b_{\beta, i} x^{\beta}$, (6) shows that $\lambda(x)$ satisfies the congruence

$$\lambda(x + y) \equiv \lambda(x) + \lambda(y) \pmod{\mathfrak{m}_K},$$

then by lemma 3.3.1 r should be a power of p , because otherwise we would have $b_{\beta, i} \in \mathfrak{m}_K$ for all i and for all β such that $|\beta| = r$, but this would contradict the above made assumption on such $b_{\beta, i}$. Since $r \geq p^{\mu} + 1$, hence $r \geq p^{\mu+1}$. Therefore by the minimality of r , for all β such that $|\beta| \in \{p^{\mu} + 1, p^{\mu} + 2, \dots, p^{\mu+1} - 1\}$, we have $b_{\beta, i} \in \mathfrak{m}_K$ for all i . We can then deduce from (3) that

$$\begin{aligned} pf(x) + \sum_{\nu=1}^{\mu} C_{\nu} f^{\sigma^{\nu}}(x^{p^{\nu}}) &\equiv \sum_{|\beta| \geq p^{\mu+1}} b_{\beta} x^{\beta} \pmod{\mathfrak{m}_K} \\ &\equiv \sum_{|\beta|=p^{\mu+1}} b_{\beta} x^{\beta} \pmod{\deg(p^{\mu+1} + 1), \pmod{\mathfrak{m}_K}} \quad (7). \end{aligned}$$

Put $\beta_j = p^{\mu+1} \epsilon_j$, then from lemma 3.3.1 again we have

$$\begin{aligned} \sum_{|\beta|=p^{\mu+1}} b_{\beta} x^{\beta} &\equiv \sum_{j=1}^n b_{\beta_j} x^{\beta_j} \pmod{\mathfrak{m}_K} \\ &= \sum_{j=1}^n b_{\beta_j} x_j^{p^{\mu+1}} \quad (8). \end{aligned}$$

Now from the observation we made just after establishing (6) replacing r by $p^{\mu+1}$ and in accordance with lemma 3.3.1 we deduce that $b_{\beta_j, i} \in \mathcal{O}_K$ for all j , for all i .

$$\begin{aligned} \sum_{j=1}^n b_{\beta_j} x_j^{p^{\mu+1}} &= \sum_{j=1}^n \left(b_{\beta_j, 1} x_j^{p^{\mu+1}}, \dots, b_{\beta_j, n} x_j^{p^{\mu+1}} \right) \\ &= \left(\sum_{j=1}^n b_{\beta_j, 1} x_j^{p^{\mu+1}}, \dots, \sum_{j=1}^n b_{\beta_j, n} x_j^{p^{\mu+1}} \right) \\ &= M x^{p^{\mu+1}} \quad (9), \end{aligned}$$

where $M = (b_{\beta_j, i})_{1 \leq i, j \leq n}^T$ has coefficients in \mathcal{O}_K . Therefore (7), (8) and (9) imply that

$$p f(x) + \sum_{\nu=1}^{\mu} C_{\nu} f^{\sigma^{\nu}}(x^{p^{\nu}}) \equiv M x^{p^{\mu+1}} \pmod{\deg(p^{\mu+1} + 1), \text{ mod } \mathfrak{m}_K} \quad (10).$$

Since $f(x) \equiv x \pmod{\deg 2}$, then $f^{\sigma^{\mu+1}}(x^{\mu+1}) \equiv x^{\mu+1} \pmod{\deg 2}$, therefore

$$M f^{\sigma^{\mu+1}}(x^{\mu+1}) \equiv M x^{\mu+1} \pmod{\deg 2},$$

hence the congruence (10) becomes

$$p f(x) + \sum_{\nu=1}^{\mu} C_{\nu} f^{\sigma^{\nu}}(x^{p^{\nu}}) - M f^{\sigma^{\mu+1}}(x^{\mu+1}) \equiv 0 \pmod{\deg(p^{\mu+1} + 1), \text{ mod } \mathfrak{m}_K}.$$

We take $C_{\mu+1} = -M$.

This leads us to $u * f \equiv 0 \pmod{\mathfrak{m}_K}$, where $u = \sum_{\mu \geq 0} C_{\mu} T^{\mu}$, and this ends the proof. \square

Results established in this section are going to be applied in the sake of classification of commutative formal groups in dimension 1. We can already say that thanks to proposition 2.2.16 every formal group over \mathcal{O}_K is obtained from a special element of \mathfrak{A}_n .

2.3 Classification in the case of complete and non-ramified rings

We start this section by the following observations:

2.3.1 Remark. Let F and G be n -dimensional formal groups over \mathcal{O}_K , with transformers f and g respectively, then from proposition 2.2.16 there are special elements u and v in \mathfrak{A}_n such that f and g are respectively of type u and v .

1. Assume that F and G are strongly isomorphic, and call φ the strong isomorphism. From proposition 2.1.17 there is $C \in M_n(\mathcal{O}_K)$ such that $\varphi(x) = g^{-1} \circ (Cf)(x) \in \mathcal{O}_K[[x]]_0^n$. Since $\varphi(x) \equiv x \pmod{\deg 2}$ we deduce that $C = I_n$, therefore $g^{-1} \circ f(x) \in \mathcal{O}_K[[x]]_0^n$.
2. Conversely assume that $\varphi(x) := g^{-1} \circ f(x) \in \mathcal{O}_K[[x]]_0^n$, then $\varphi(x) \equiv x \pmod{\deg 2}$ and

$$\varphi \circ F(x, y) = g^{-1}(f(x) + f(y)) = g^{-1}(g(\varphi(x)) + g(\varphi(y))) = G(\varphi(x), \varphi(y)).$$

Therefore φ is a strong isomorphism between F and G .

It is important to note that in the above remark we could not just use lemma 2.2.7 to conclude that $g^{-1} \circ (f)(x) \in \mathcal{O}_K[[x]]_0^n$ as u and v might be different, which does not then fit with the assumption of lemma 2.2.7.

In definition 2.1.7 we have talked about strong isomorphism of formal groups, which actually defines an equivalence relation on formal groups. Put $Cl_{n, \mathcal{O}_K}(\mathfrak{F})$ the set of strong isomorphism classes of n -dimensional formal groups over \mathcal{O}_K . We now give a definition that will later appear to be his correspondant at some extend.

2.3.2 Definition. Let u and v in \mathfrak{A}_n , we say that v is left associated with u if there exists a unit $t \in \mathfrak{A}_n$ such that $v = tu$.

Left association obviously defines an equivalence relation on \mathfrak{A}_n . Put $Cl(S\mathfrak{A}_n)$ the subset of the quotient set made of left associate classes of special elements of \mathfrak{A}_n .

2.3.3 Theorem. *The strong isomorphism classes of n -dimensional formal groups over \mathcal{O}_K correspond bijectively to the left associate classes of special elements of \mathfrak{A}_n . More precisely the map $\Phi : Cl_{n, \mathcal{O}_K}(\mathfrak{F}) \rightarrow Cl(S\mathfrak{A}_n)$ is bijective, where $\Phi([F]) = [u]$, u being a special element of \mathfrak{A}_n such that the transformer of F is of type u .*

Proof. We split the proof into three steps.

1. We first of all show that Φ is a well defined map, by first showing that the image of a class $[F]$ does not depend on the chosen special element u attached to the transformer of F , and then by showing that the image of a class $[F]$ again does not depend on the representative F .
 - i) Assume the transformer f of F is of type u , and of type v , where u and v are special elements of \mathfrak{A}_n . Then $v * f \equiv 0 \pmod{\mathfrak{m}_K}$, then from proposition 2.2.12 there is $t \in \mathfrak{A}_n$ such that $v = tu$, since u and v are invertible, so is t , therefore u and v are left associate, hence $[u] = [v]$.
Whence, the image of a class $[F]$ does not depend on the chosen special element u attached to the transformer of F .
 - ii) Assume $[F] = [G]$ where F, G are n -dimensional formal groups over \mathcal{O}_K . Let u respectively v be a special element of \mathfrak{A}_n such that the transformer of F respectively G is of type u respectively v . By the equality $[F] = [G]$ we deduce that F and G are strongly isomorphic over \mathcal{O}_K , then by remark 2.3.1 we have $g^{-1} \circ f(x) \in \mathcal{O}_K[[x]]_0^n$, then from proposition 2.1.17 $g^{-1} \circ f(x)$ is a morphisme from F to G over \mathcal{O}_K , and from theorem 2.2.13 there exists $t \in \mathfrak{A}_n$ such that $v = tu$, then t must be invertible, hence $[u] = [v]$. Thus the image of a class $[F]$ does not depend on the representative F .
2. We now show that Φ is injective. Assume $\Phi([F]) = \Phi([G])$. Set as above u respectively v a special element of \mathfrak{A}_n such that the transformer of F respectively G is of type u respectively v . Then $[u] = [v]$, which means that there exists $t \in \mathfrak{A}_n$ such that $v = tu$, then from theorem 2.2.13 $g^{-1} \circ f$ is a morphism from F to G over \mathcal{O}_K , we also see that $g^{-1} \circ f$ is obviously a strong isomorphism. Then F and G are strongly isomorphic over \mathcal{O}_K , which then means $[F] = [G]$. Hence Φ is injective.

3. We conclude the proof by the surjectivity of Φ . Let u be a special element of \mathfrak{A}_n , then we have seen that $f := (pu^{-1}) * i$ is of type u . Then the formal group F defined by

$$F(x, y) = f^{-1}(f(x) + f(y))$$

as in theorem 2.2.10 is the preimage of $[u]$.

□

Theorem 2.3.3 can be further refined in the following way.

2.3.4 Corollary. Set M to be a complete system of representatives of $\mathcal{O}_K/\mathfrak{m}_K$ containing p as representative for the zero class. Then the strong isomorphism classes of n -dimensional formal groups over \mathcal{O}_K correspond bijectively to the special elements of \mathfrak{A}_n whose coefficients matrices have elements in M .

Proof. Thanks to theorem 2.3.3 we just have to show that the left associate classes of special elements of \mathfrak{A}_n correspond bijectively to the special elements of \mathfrak{A}_n whose coefficients matrices have elements in M . Clearly speaking, it means that if u is a special element of \mathfrak{A}_n , then we can find one and only one special element left associated to u and such that its matrices coefficients have elements in M . Let then $u = \sum_{\nu \geq 0} C_\nu T^\nu$ be a special element, meaning that $C_0 = pI_n$, we need to show that there is only one unit $t \in \mathfrak{A}_n$ such that tu has matrices with coefficients in M . We then need to construct matrices $A_\nu \in M_n(\mathcal{O}_K)$ uniquely such that $t = \sum_{\nu \geq 0} A_\nu T^\nu$ is a unit in \mathfrak{A}_n and tu is a special element of \mathfrak{A}_n such that its matrices coefficients have elements in M . We are going to construct the sequence $(A_\nu)_\nu$ by induction on ν . tu must be equal to $\sum_{\nu \geq 0} B_\nu T^\nu$, where

$$B_\nu = \sum_{\mu=0}^{\nu} A_\mu \sigma^\mu(C_{\nu-\mu}),$$

we must also have $A_0 = I_n$ in order to comply with the fact that tu is a special element in \mathfrak{A}_n . This means that we have just constructed A_0 uniquely such that $B_0 = A_0 C_0 = pI_n$ has matrices coefficients in M . Now let $\nu \geq 0$, assume we have constructed matrices $A_0, \dots, A_{\nu-1}$ uniquely such that $B_0, \dots, B_{\nu-1}$ have coefficients in M . The above equality is also equivalent to

$$B_\nu = A_\nu \sigma^\nu(C_0) + \sum_{\mu=0}^{\nu-1} A_\mu \sigma^\mu(C_{\nu-\mu}) = pA_\nu + \sum_{\mu=0}^{\nu-1} A_\mu \sigma^\mu(C_{\nu-\mu}).$$

In the latter equality, we need to uniquely construct the matrix A_ν such that B_ν has coefficients in M . Write

$$\sum_{\mu=0}^{\nu-1} A_\mu \sigma^\mu(C_{\nu-\mu}) = (b_{ij}^{(\nu)})_{1 \leq i, j \leq n}.$$

By definition of M , we have that for all $i, j \in \{1, \dots, n\}$ there is a unique $x_{ij} \in M$ such that

$$b_{ij}^{(\nu)} \equiv x_{ij} \pmod{\mathfrak{m}_K},$$

then by definition of the congruence, there is again a unique $a_{ij}^{(\nu)} \in \mathcal{O}_K$ such that

$$b_{ij}^{(\nu)} - x_{ij} = pa_{ij}^{(\nu)}.$$

We have just shown that for all $i, j \in \{1, \dots, n\}$ there is a unique $a_{ij}^{(\nu)} \in \mathcal{O}_K$ such that $pa_{ij}^{(\nu)} + b_{ij}^{(\nu)} \in M$. Define

$$A_\nu = (a_{ij}^{(\nu)})_{1 \leq i, j \leq n},$$

then A_ν is unique such that B_ν has coefficients in M . \square

The following lemma sets the fundamental basis for the proof of the main result of this section, a result for which we restrict from now on to the case $n = 1$.

2.3.5 Lemma. Let $u = p + \sum_{\nu \geq 1} c_\nu T^\nu$ be a special element of \mathfrak{A}_1 .

1. If all the coefficients c_ν belong to \mathfrak{m}_K , then there is a unit $t \in \mathfrak{A}_1$ such that $tu = p$.
2. If c_1, \dots, c_{h-1} all belong to \mathfrak{m}_K but $c_h \notin \mathfrak{m}_K$, then there is a unit $t \in \mathfrak{A}_1$ such that

$$tu = p + \sum_{\nu=1}^h b_\nu T^\nu,$$

where b_1, \dots, b_{h-1} all belong to \mathfrak{m}_K but $b_h \notin \mathfrak{m}_K$.

Proof. Assume all the coefficients c_ν belong to \mathfrak{m}_K , and write $c_\nu = pc'_\nu$, where $c'_\nu \in \mathcal{O}_K$ for all $\nu \geq 1$, then $u = ps$, where $s = 1 + \sum_{\nu \geq 1} c'_\nu T^\nu$ is a unit in \mathfrak{A}_1 , finally $tu = p$ with $t = s^{-1}$. Now we assume that c_1, \dots, c_{h-1} all belong to \mathfrak{m}_K but $c_h \notin \mathfrak{m}_K$. We are firstly going to show by induction that for all $i \geq 1$, there are $b_1^{(i)}, \dots, b_h^{(i)} \in \mathcal{O}_K$ and a unit $t_i \in \mathfrak{A}_1$ subject to the following three conditions

$$b_\nu^{(i+1)} \equiv b_\nu^{(i)} \pmod{\mathfrak{m}_K^i}, \quad b_\nu^{(1)} \equiv c_\nu \pmod{\mathfrak{m}_K} \quad (1)$$

$$t_i \equiv 1 \pmod{\text{deg } 1}, \quad t_{i+1} \equiv t_i \pmod{\mathfrak{m}_K} \quad (2)$$

$$t_i u \equiv p + \sum_{\nu=1}^h b_\nu^{(i)} T^\nu \pmod{\mathfrak{m}_K^i} \quad (3).$$

For $i = 1$, put $b_1^{(1)} = \dots = b_{h-1}^{(1)} = 0$, $b_h^{(1)} = c_h$ and $t_1 = c_h \left(\sum_{\nu \geq h} c_\nu T^{\nu-h} \right)^{-1}$, (1) is then obviously satisfied, $t_1 \equiv 1 \pmod{\text{deg } 1}$ is also true, then (2) is satisfied; now since c_h is a unit we deduce in addition that t_1 as coefficients in \mathcal{O}_K .

$$\begin{aligned} t_1 u &= c_h \left(\sum_{\nu \geq h} c_\nu T^{\nu-h} \right)^{-1} u \\ &= c_h T^h \left(\sum_{\nu \geq h} c_\nu T^\nu \right)^{-1} \left(\sum_{\nu=0}^{h-1} c_\nu T^\nu + \sum_{\nu \geq h} c_\nu T^\nu \right) \\ &\equiv c_h T^h \left(\sum_{\nu \geq h} c_\nu T^\nu \right)^{-1} \sum_{\nu \geq h} c_\nu T^\nu \pmod{\mathfrak{m}_K}, \text{ because } c_1, \dots, c_{h-1} \text{ all belong to } \mathfrak{m}_K \\ &= c_h T^h \pmod{\mathfrak{m}_K} \end{aligned}$$

Then (3) is also satisfied. Now let $i \geq 1$, suppose that for all $j \leq i$ we have constructed $b_1^{(j)}, \dots, b_h^{(j)} \in \mathcal{O}_K$ and a unit $t_j \in \mathfrak{A}_1$ subject to (1), (2) and (3). We are then constructing $b_\nu^{(i+1)} = b_\nu^{(i)} + p^i d_\nu^{(i)}$ and $t_{i+1} = t_i + p^i v_i$ for all $\nu \in \{1, \dots, h\}$ where $d_\nu^{(i)} \in \mathcal{O}_K$ and $v_i \in \mathfrak{A}_1$ are such that

$$(t_i + p^i v_i)u \equiv p + \sum_{\nu=1}^h (b_\nu^{(i)} + p^i d_\nu^{(i)})T^\nu \pmod{\mathfrak{m}_K^{i+1}} \quad (4).$$

Since c_1, \dots, c_{h-1} all belong to \mathfrak{m}_K , then $u \equiv \sum_{\nu \geq h} c_\nu T^\nu \pmod{\mathfrak{m}_K}$, therefore

$$p^i u \equiv p^i \sum_{\nu \geq h} c_\nu T^\nu \pmod{\mathfrak{m}_K^{i+1}}.$$

From (3) we have $w_i := p^{-i}[t_i u - (p + \sum_{\nu=1}^h b_\nu^{(i)} T^\nu)] \in \mathfrak{A}_1$, also since $t_i u \equiv p \pmod{\deg 1}$, then w_i has zero constant term. Hence (4) is equivalent to

$$v_i \sum_{\nu \geq h} c_\nu T^\nu \equiv \sum_{\nu=1}^h d_\nu^{(i)} T^\nu - w_i \pmod{\mathfrak{m}_K} \quad (5).$$

By definition, w_i is known, so the only unknowns of the congruence (5) are v_i and the $d_\nu^{(i)}$'s. Let us take the unique choice of the $d_\nu^{(i)}$'s such that the right hand side of (5) has all its terms of degree $\leq h$ cancelled. Now we just remains to give a solution for the congruence (5), with v_i as the only unknown, for this we write $v_i = \sum_{\nu \geq 0} V_\nu T^\nu$, we need to construct the V_ν 's by induction. By construction of the $d_\nu^{(i)}$'s, we must have $V_0 = 0$. Let $\nu \geq 0$, assume $V_0, \dots, V_{\nu-1}$ have been constructed. Write $\sum_{\nu \geq h} X_\nu T^\nu$ the term on the right hand side of the congruence (5). Then (5) becomes

$$\sum_{\nu \geq h} \left(\sum_{\mu=1}^{\nu} V_\mu \sigma^\mu(c_{\nu-\mu}) \right) T^\nu \equiv \sum_{\nu \geq h} X_\nu T^\nu \pmod{\mathfrak{m}_K}.$$

At the level of coefficients of T^ν we conclude that $pV_\nu + \sum_{\mu=1}^{\nu-1} V_\mu \sigma^\mu(c_{\nu-\mu}) = X_\nu + px_\nu$, where $x_\nu \in \mathcal{O}_K$.

Which means that $X_\nu - \sum_{\mu=1}^{\nu-1} V_\mu \sigma^\mu(c_{\nu-\mu}) \in \mathfrak{m}_K$, therefore $V_\nu = x_\nu + p^{-1} \left(X_\nu - \sum_{\mu=1}^{\nu-1} V_\mu \sigma^\mu(c_{\nu-\mu}) \right)$ is well defined. This ends the construction of v_i , and hence ends the proof of the fact that for all $i \geq 1$, there are $b_1^{(i)}, \dots, b_h^{(i)} \in \mathcal{O}_K$ and a unit $t_i \in \mathfrak{A}_1$ subject to (1), (2) and (3). We remark that since v_i does not have a constant term, then we must have $t_{i+1} \equiv 1 \pmod{\deg 1}$. The second congruence in (2) shows that at any degree the sequence made of coefficients of the $(t_i)_i$ is a Cauchy sequence, then by the completeness hypothesis it converges. We then write $t = \lim_{i \rightarrow \infty} t_i$ where at each degree the coefficient of t is just the limit of the sequence made of coefficients of the $(t_i)_i$ at that degree. In the same spirit, the first congruence in (1) enables us to define $b_\nu = \lim_{i \rightarrow \infty} b_\nu^{(i)}$ for all ν .

In addition, let $\nu \leq h-1$, since $c_\nu \in \mathfrak{m}_K$, then from (1), $b_\nu^{(i)} \in \mathfrak{m}_K$ for all i , hence $b_\nu \in \mathfrak{m}_K$, because \mathfrak{m}_K is a closed subset of \mathcal{O}_K . Now for $\nu = h$, $c_h \notin \mathfrak{m}_K$, then again from (1) we deduce that $b_h^{(i)} \notin \mathfrak{m}_K$

for all i . But since \mathfrak{m}_K is a neighbourhood of 0, there exists $i_0 \in \mathbb{N}$ such that for all $i \in \mathbb{N}$, $i \geq i_0$ implies $b_h^{(i)} - b_h \in \mathfrak{m}_K$. Now if $b_h \in \mathfrak{m}_K$, then $b_h^{(i_0)} \in \mathfrak{m}_K$, which is a contradiction. Therefore $b_h \notin \mathfrak{m}_K$.

The congruence in (3) implies that $\lim_{i \rightarrow \infty} [t_i u - (p + \sum_{\nu=1}^h b_\nu^{(i)} T^\nu)] = 0$, thus $tu = p + \sum_{\nu=1}^h b_\nu T^\nu$. The last equality says that the constant term of t must be 1, which means that t is a unit in \mathfrak{A}_1 . \square

2.3.6 Definition. Let F be a one-dimensional formal group over \mathcal{O}_K , we define the height of F to be the height of F modulo \mathfrak{m}_K .

The following lemma insures the compatibility of this definition with the strong isomorphism relation.

2.3.7 Lemma. Let F, G be strong isomorphic one-dimensional formal groups over \mathcal{O}_K , we have

$$\text{height}(F) = \text{height}(G).$$

Proof. Put φ to be the strong isomorphism between F and G , and let $m \geq 0$.

$$\varphi([m+1]_F x) = \varphi(F(x, [m]_F x)) = G(\varphi(x), \varphi([m]_F x)),$$

replacing x by $\varphi^{-1}(x)$ we get

$$\varphi([m+1]_F \varphi^{-1}(x)) = G(x, \varphi([m]_F \varphi^{-1}(x))),$$

We also have $\varphi([0]_F \varphi^{-1}(x)) = \varphi(0) = 0$. Therefore we must have $\varphi([m]_F \varphi^{-1}(x)) = [m]_G x$. For the rest of the proof, the computations are done modulo \mathfrak{m}_K . Assume $[p]_F x \equiv 0 \pmod{\deg p^h}$ for some $h \geq 0$. Then using the two congruences

$$\varphi(x) \equiv x \pmod{\deg 2}, \text{ and } \varphi^{-1}(x) \equiv x \pmod{\deg 2}$$

we deduce that

$$[p]_F(\varphi^{-1}(x)) \equiv 0 \pmod{\deg p^h}, \text{ and } \varphi([p]_F(\varphi^{-1}(x))) \equiv 0 \pmod{\deg p^h}.$$

Which just means that $[p]_G x \equiv 0 \pmod{\deg p^h}$. We can use the same argument to show that if $[p]_G x \equiv 0 \pmod{\deg p^h}$ for some $h \geq 0$, then $[p]_F x \equiv 0 \pmod{\deg p^h}$. We deduce that F and G have the same height. \square

Lemma 2.3 allows us to define height on $Cl_{n, \mathcal{O}_K}(\mathfrak{F})$.

From example 2.1.11, we see that $\text{height}(F) = \infty$ where $F(x, y) = x + y$.

The following proposition gives the expected classification of 1-dimensional commutative formal groups we aimed for.

2.3.8 Proposition. The strong isomorphism classes of 1-dimensional formal groups over \mathcal{O}_K , of height h (where $1 \leq h < \infty$) correspond bijectively to the special elements of the form $u = p + \sum_{\nu=1}^h b_\nu T^\nu$ where b_1, \dots, b_{h-1} all belong to \mathfrak{m}_K but $b_h \notin \mathfrak{m}_K$.

Proof. We first point out that lemma 2.3 makes it legal to define height as stated in the proposition. Here is the plan of the proof; We first of all show that any strong isomorphism class can indeed be represented by such a special element u as stated in the proposition, and only by one such u , and lastly we show that the degree of u is actually the height of the isomorphism class.

1. Let F be a representative of a class $[F]$, where F is a one-dimensional formal group over \mathcal{O}_K with height as in the proposition, let f be the transformer of F , by proposition 2.2.16 there is a special element $u \in \mathfrak{A}_1$ such that f is of type u . Thanks to theorem 2.3.3, $[F]$ is identified with $[u]$. If all the coefficients of u are in \mathfrak{m}_K , then from lemma 2.3.5 there is a unit $t \in \mathfrak{A}_1$ such that $v := tu = p$.

$$v * i = p * i \equiv 0 \pmod{\mathfrak{m}_K},$$

then i is of type v , but u and v are associate, therefore from theorem 2.3.3 the formal groups built from f and i are strongly isomorphic, this means F is isomorphic to the formal group

$$G(x, y) = x + y,$$

now from lemma 2.3, $\text{height}(F) = \text{height}(G)$, but we have seen that $\text{height}(G) = \infty$; therefore $\text{height}(F) = \infty$, but this contradicts the hypothesis of the proposition. Hence we can assume that

u is of the form $u = p + \sum_{\nu=1}^h b_\nu T^\nu$ where b_1, \dots, b_{h-1} all belong to \mathfrak{m}_K but $b_h \notin \mathfrak{m}_K$. Now assume

$[F]$ is also represented by another special element of the form $u' = p + \sum_{\nu=1}^h b'_\nu T^\nu$ where b'_1, \dots, b'_{h-1} all belong to \mathfrak{m}_K but $b'_h \notin \mathfrak{m}_K$, then u, u' are associate, hence there is a unit $t \in \mathfrak{A}_1$ such that $u = tu'$, for the sake of degrees and from the fact that u and u' have the same constant term, we deduce that $t = 1$, then $u = u'$, and this ends the first part of the proof.

2. Now take F a representative of a class $[F]$, where F is a one-dimensional formal group over \mathcal{O}_K with height as in the proposition, let u be the unique special element as constructed above, $u = p + \sum_{\nu=1}^h b_\nu T^\nu$ where b_1, \dots, b_{h-1} all belong to \mathfrak{m}_K but $b_h \notin \mathfrak{m}_K$. We need to show that

$\text{height}(F) = h$. $u = p \left(1 + \sum_{\nu \geq 1}^{h-1} b_\nu T^\nu \right) + b_h T^h$, put $t := 1 + \sum_{\nu \geq 1}^{h-1} b_\nu T^\nu$ a unit in \mathfrak{A}_1 , then

$$t^{-1}u = p + b_h T^h t = p + b_h T^h + (\text{terms of degree } > h).$$

We write it by $u' := p + b_h T^h + \dots$. Set $l = (pu'^{-1}) * i$, we know that l is of type u' , then by theorem 2.2.10, $L(x, y) = l^{-1}(l(x) + l(y))$ is a formal group over \mathcal{O}_K with transformer u' ; we also know that u and u' are associate, then from theorem 2.3.3, the formal groups F and L are strongly isomorphic. Hence $\text{height}(F) = \text{height}(L)$. To complete our proof, we are left to show that $\text{height}(L) = h$. For $m \in \mathbb{N}$,

$$\begin{aligned} [m]_L x &= L(x, [m-1]_L x) \\ &= l^{-1}(l(x) + l([m-1]_L x)) \\ &= l^{-1}(l(x) + l \circ l^{-1}(l(x) + l([m-2]_L x))), \text{ we have applied the second equality} \\ &= l^{-1}(2l(x) + l([m-2]_L x)) \end{aligned}$$

We keep applying the same argument repeatedly, and we reach to

$$[m]_L x = l^{-1}(ml(x) + l([0]_L x)) = l^{-1}(ml(x)).$$

In particular for $m = p$, $[p]_L x = l^{-1}(pl(x))$. Then to complete the proof we just show that the order of $l^{-1}(pl(x))$ modulo \mathfrak{m}_K is p^h . Write $u'^{-1} = \sum_{\nu \geq 0} a_\nu T^\nu$, from the equation $u'u'^{-1} = 1$ we deduce that

$$a_0 = p^{-1}, \quad a_\nu = 0 \text{ for all } \nu \text{ between } 1 \text{ and } h-1, \quad pa_h + b_h \sigma(a_0) = 0.$$

The last equation gives $a_h = -p^{-2}b_h$. Hence $pu'^{-1} = 1 - p^{-1}b_h T^h + \dots$

Then $l(x) = ((pu'^{-1}) * i)(x) = x - p^{-1}b_h i^{\sigma^h}(x^{p^h}) + \dots = x - p^{-1}b_h x^{p^h} + \dots$

Now write $l^{-1}(x) = \sum_{\nu \geq 0} a_\nu x^\nu$, then from the equation $l(l^{-1}(x)) = x$, which is equivalent to $l^{-1}(x) - p^{-1}b_h(l^{-1}(x))^{p^h} + \dots = x$ we deduce that :

$$a_0 = 0, \quad a_1 = 1, \quad a_2 = \dots = a_{p^h-1} = 0, \quad a_{p^h} - p^{-1}b_h a_1 = 0,$$

the last equality gives $a_{p^h} = p^{-1}b_h$. Therefore $l^{-1}(x) = x + p^{-1}b_h x^{p^h} + \dots$, Then

$$l^{-1}(pl(x)) = pl(x) + p^{-1}b_h(pl(x))^{p^h} + \dots = (px - b_h x^{p^h} + \dots) + p^{-1}b_h (px - b_h x^{p^h} + \dots)^{p^h} + \dots$$

Therefore modulo \mathfrak{m}_K , $-b_h x^{p^h}$ is the term with the least degree, this just means that the order of $l^{-1}(pl(x))$ modulo \mathfrak{m}_K is p^h .

□

3. p -adic periods : The one-dimensional case

In the previous chapter, we have given a classification for one-dimensional commutative formal groups, in the present chapter we give a construction of the p -adic period map. We start by giving a construction for the Tate module attached to a one-dimensional formal group, for this part the main references used are [9], [10] and [13]. Then we briefly review general results about the rings B_{dR} and B_{cris} for which we have used [12] and [2] for results about Witt vectors, and [8], [5], [6] for notions on the rings B_{dR} and B_{cris} . We conclude this chapter by giving a construction for the p -adic period map due to Colmez, and for this we mainly use [7]. Unless otherwise specified, F is a commutative one-dimensional formal group over \mathcal{O}_K of finite height h ; K is a local field unramified over \mathbb{Q}_p , \mathcal{O}_K and \mathfrak{m}_K are respectively its ring of integers and its maximal ideal, we normalize the valuation on K , so that $v(p) = 1$. \mathbb{C}_p is the p -adic completion of $\overline{\mathbb{Q}_p}$. Finally, σ is an endomorphism of K such that $\sigma(x) \equiv x^p \pmod{\mathfrak{m}_K}$ for all $x \in \mathcal{O}_K$.

3.1 The Tate module for a one-dimensional formal group

Let \bar{K} be an algebraic closure of K , write $\bar{\mathcal{O}}_K$ for the integral closure of \mathcal{O}_K over \bar{K} . Put $\mathfrak{m} = \{x \in \bar{\mathcal{O}}_K, x \text{ is not invertible in } \bar{\mathcal{O}}_K\}$. $0 \in \mathfrak{m}$. Let $x, y \in \mathfrak{m}$ and $a \in \bar{\mathcal{O}}_K$

- Then $ax \in \bar{\mathcal{O}}_K$. Now if $ax \in \bar{\mathcal{O}}_K^\times$, then there is $u \in \bar{\mathcal{O}}_K$ such that $uax = 1$, therefore $x \in \bar{\mathcal{O}}_K$, but this is a contradiction, then $ax \in \mathfrak{m}$
- Assume $x + y \notin \mathfrak{m}$, there is $u \in \bar{\mathcal{O}}_K$ such that $u(x + y) = 1$. Let L be a finite extension of K containing x, y and u , they are then integers in L . Since $\mathcal{O}_L^\times \subset \bar{\mathcal{O}}_K^\times$, then x and y do not belong to \mathcal{O}_L^\times , hence they belong to \mathfrak{m}_L . We still write v for the unique extension of v in L . We have

$$0 = v(1) = v(u(x + y)) \geq v(x + y) \geq 1$$

This is a contradiction, then $x + y \in \mathfrak{m}$. Therefore $\bar{\mathcal{O}}_K$ is a local ring with maximal ideal \mathfrak{m} .

Let x, y in \mathfrak{m} , and L be a finite extension of K containing x and y , from the above we know that x and y belong to \mathfrak{m}_L , therefore if F is a formal group over \mathcal{O}_K , the series $F(x, y)$ converges in \mathcal{O}_L . Since the constant term of F is zero, then $F(x, y) \in \mathfrak{m}_L \subset \mathfrak{m}$. This raises an internal operation on \mathfrak{m} , defined by $x +_F y = F(x, y)$. The following proposition makes this internal operation into an group law.

3.1.1 Proposition. (Corollary 1.5 of [13]) Let F be a formal group over \mathcal{O}_K , there is a unique formal power series $i_F(x)$ over \mathcal{O}_K such that $F(x, i_F(x)) = 0$

The associativity and commutativity of $+_F$ come from that of F . By definition of F , 0 is the neutral element. By proposition 3.1.1, the inverse of an element $x \in \mathfrak{m}$ is just $i_F(x)$. Be aware that $i_F(x)$ actually belongs to \mathfrak{m} , indeed from the fact that $F(x, y) \equiv x + y \pmod{\text{deg } 2}$, we deduce that $i_F(x)$ has a zero constant term. We write $[n]x$ for $x +_F x +_F \dots +_F x$; x appearing exactly n times. And we will denote this group structure by $F(\mathfrak{m}) = (\mathfrak{m}, +_F, 0)$.

3.1.2 Example. For $F(x, y) = x + y$, we have $[n]x \equiv nx \pmod{\text{deg } 2}$, then the torsion subgroup is null, and $F(\mathfrak{m})$ is just the usual addition on \mathfrak{m} .

It is a result from the book of Froehlich ([9]) that for all $a \in \mathfrak{m}$ the equation $[p]x = a$ has p^h solutions in \mathfrak{m} .

3.1.3 Remark. For all $n \in \mathbb{N}$ we put $F[n]$ to be the set of n -torsion elements of $F(\mathfrak{m})$. by commutativity of $F(\mathfrak{m})$, we deduce that $F[n]$ is a subgroup of $F(\mathfrak{m})$. The equation $[p]x = 0$ has p^h solutions, which means that $|F[p]| = p^h$, hence from the structure theorem for finitely generated abelian groups we have that $F[p]$ is isomorphic to $\frac{\mathbb{Z}}{p^{i_1}\mathbb{Z}} \oplus \dots \oplus \frac{\mathbb{Z}}{p^{i_r}\mathbb{Z}}$, where $i_1 + \dots + i_r = h$ and $i_j \geq 1$ for all j . Since every element of $F[p]$ is a p -torsion element, then $i_1 = \dots = i_r = 1$, hence $F[p]$ is isomorphic to $\bigoplus_{i=1}^h \frac{\mathbb{Z}}{p\mathbb{Z}}$.

3.1.4 Remark. We need to see by induction that $F[p^n]$ is isomorphic to $\bigoplus_{i=1}^h \frac{\mathbb{Z}}{p^n\mathbb{Z}}$. For $n = 1$, it just corresponds to the previous remark. Now let $n \geq 1$, assume that $F[p^n]$ is isomorphic to $\bigoplus_{i=1}^h \frac{\mathbb{Z}}{p^n\mathbb{Z}}$. Since $F[p^{n+1}]$ is a finitely generated abelian group, we apply the structure theorem. Then $F[p^{n+1}]$ is isomorphic to $\frac{\mathbb{Z}}{p^{i_1}\mathbb{Z}} \oplus \dots \oplus \frac{\mathbb{Z}}{p^{i_r}\mathbb{Z}}$, where $i_1 + \dots + i_r = h$ and $i_j \geq 1$ for all j , we also have that $i_j \leq n+1$ because elements of $F[p^{n+1}]$ are p^{n+1} -torsion.

$$0 \longrightarrow \text{Ker}\varphi_n \longrightarrow F[p^{n+1}] \xrightarrow{\varphi_n} F[p^n] \longrightarrow 0$$

is an exact sequence, where φ_n is the multiplication by p map. $\text{Ker}\varphi_n = F[p]$, then from

$$\frac{F[p^{n+1}]}{\bigoplus_{i=1}^h \frac{\mathbb{Z}}{p\mathbb{Z}}} \simeq \bigoplus_{i=1}^h \frac{\mathbb{Z}}{p^n\mathbb{Z}}$$

we deduce that $i_j \geq n+1$ for all j , then $F[p^{n+1}]$ is isomorphic to $\bigoplus_{i=1}^h \frac{\mathbb{Z}}{p^{n+1}\mathbb{Z}}$

3.1.5 Remark. Consider the absolute Galois group $G = \text{Gal}(\bar{K}/K)$ of K , take $g \in G$, then for all $x, y \in \mathfrak{m}$, $g(x +_F y) = g(F(x, y)) = F(g(x), g(y)) = g(x) +_F g(y)$, the second equality holds due to the fact that F has coefficients in K , which is the fixed field of G . Hence the restriction of g in \mathfrak{m} is an endomorphism of $F(\mathfrak{m})$, also for all $n \in \mathbb{N}$, $g([n]x) = [n]g(x)$. In particular for all $x \in F[p^n]$, $g(x) \in F[p^n]$. This therefore defines an action of the absolute Galois group of K on each of the $F[p^n]$.

We have now gathered enough tools to give the construction of the Tate module of F .

For all $n \geq 1$, the maps $F[p^{n+1}] \xrightarrow{\varphi_n} F[p^n]$ as defined above give us an inverse system of abelian groups $(F[p^n], \varphi_n)_{n \geq 1}$.

3.1.6 Definition. The Tate module $T_p(F)$ of F is defined to be the projective limit of the inverse system $(F[p^n], \varphi_n)_{n \geq 1}$

Set theoretically, $T_p(F) = \{u = (u_n)_{n \geq 1}, \text{ for all } n \geq 1, [p^n]u_n = 0, \text{ and } [p]u_{n+1} = u_n\}$. Since $F[p^0] = \{0\}$, then we can still view $T_p(F)$ as

$$T_p(F) = \{u = (u_n)_{n \geq 0}, \text{ for all } n \geq 0, [p^n]u_n = 0, \text{ and } [p]u_{n+1} = u_n\}$$

of course we see that $u_0 = 0$. From the universal property of the projective limit, we have canonical maps $\pi_n : T_p(F) \longrightarrow F[p^n]$ defined by $\pi_n(u) = u_n$, the n -th projection.

For all n , the equality $[p]u_{n+1} = u_n$ translates the fact that $\pi_n = \varphi_n \circ \pi_{n+1}$. The projective limit functor is left exact and commutes with finite direct sums, then

$$T_p(F) = \lim_{\leftarrow} F[p^n] = \lim_{\leftarrow} \bigoplus_{i=1}^h \frac{\mathbb{Z}}{p^n \mathbb{Z}} = \bigoplus_{i=1}^h \lim_{\leftarrow} \frac{\mathbb{Z}}{p^n \mathbb{Z}} = \bigoplus_{i=1}^h \mathbb{Z}_p$$

Then $T_p(F)$ is a free \mathbb{Z}_p -module of rank h . We have seen in the previous remark that $Gal(\bar{K}/K)$ naturally acts on each $F[p^n]$, we can then extend this action to $T_p(F)$ by continuity. More precisely for all $g \in Gal(\bar{K}/K)$, for all $u \in T_p(F)$, $g(u) := (g(u_n))_n$. Therefore $T_p(F)$ is equipped with a continuous Galois action.

3.2 General facts on the rings B_{dR} , B_{cris} and the ring of Witt vectors over a DVR

Before we can get to the construction of p -adic periods, we first have a quick glance on the ring $W(R)$ of Witt vectors over a DVR, by recalling general facts about it, a detailed exposition about this topic can be found in [2]. We assume R is a DVR of characteristic p and perfect. Most of what we will say here remains true for a non DVR ring. Set $x = (x_0, x_1, \dots)$ be an indeterminate, also consider the polynomial $\Phi_n(x) = \sum_{i=0}^n p^i x_i^{p^{n-i}}$ for all $n \geq 0$. Finally we consider the map

$$\Phi : R^{\mathbb{N}} \longrightarrow R^{\mathbb{N}}$$

taking $a = (a_0, a_1, \dots)$ to $(\Phi_0(a), \Phi_1(a), \dots)$.

By induction we see that

$$\Phi_{n+1}(x) = \Phi_n(x^p) + p^{n+1}x_{n+1}, \text{ for all } n \geq 0,$$

where x^p stands for (x_0^p, x_1^p, \dots) . We also note that $\Phi_n(x)$ only depends on the $n+1$ first coordinates of x , therefore we can write $\Phi_n(x_0, x_1, \dots, x_n)$ instead of $\Phi_n(x)$. The main result is the following proposition.

3.2.1 Proposition. [12] There are sequences of polynomials,

$$(S_n(x, y))_{n \geq 0}, (P_n(x, y))_{n \geq 0} \in \mathbb{Z}[x, y]^{\mathbb{N}}, \text{ and } (I_n(x))_{n \geq 0} \in \mathbb{Z}[x]^{\mathbb{N}},$$

unique such that :

$$S_n(x, y) \in \mathbb{Z}[x_0, \dots, x_n, y_0, \dots, y_n], \text{ and } \Phi_n(S_0(x, y), \dots, S_n(x, y)) = \Phi_n(x) + \Phi_n(y) \quad (1)$$

$$P_n(x, y) \in \mathbb{Z}[x_0, \dots, x_n, y_0, \dots, y_n], \text{ and } \Phi_n(P_0(x, y), \dots, P_n(x, y)) = \Phi_n(x)\Phi_n(y) \quad (2)$$

$$I_n(x) \in \mathbb{Z}[x_0, \dots, x_n], \text{ and } \Phi_n(I_0(x), \dots, I_n(x)) = -\Phi_n(x) \quad (3)$$

3.2.2 Example. Replacing n by 0 in (1), (2) and (3), we get

$$S_0(x, y) = x_0 + y_0, \quad P_0(x, y) = x_0 y_0, \quad I_0(x) = -x_0 \quad (4)$$

Then by induction we compute the polynomials for all n .

In the previous example, relation (4) inspires definitions of laws in $R^{\mathbb{N}}$ by means of the polynomials S_n, P_n and I_n . Then let $a, b \in R^{\mathbb{N}}$, put :

$$a + b = (S_n(a, b))_{n \geq 0}, \quad ab = (P_n(a, b))_{n \geq 0}, \quad -a = (I_n(a))_{n \geq 0}.$$

We have the following proposition from [12].

3.2.3 Proposition. $R^{\mathbb{N}}$ endowed with the three operations previously defined is a commutative ring with zero element $(0, 0, \dots)$ and unity as $(1, 0, 0, \dots)$, it is called the ring of Witt vectors over R and denoted $W(R)$. Furthermore the map Φ is a ring homomorphism from $W(R)$ to $R^{\mathbb{N}}$, where $R^{\mathbb{N}}$ is equipped with his natural structure of ring.

We also recall that for all $a \in R$, $[a] := (a, 0, 0, \dots) \in W(R)$ denotes the Teichmueller representative of a . and for all $b \in R$, $[ab] = [a][b]$.

For all $n \geq 0$, put $\text{Fil}^n W(R) = \{a \in W(R), a_0 = a_1 = \dots = a_{n-1} = 0\} \subset W(R)$. This defines a filtration on $W(R)$, with $\text{Fil}^0 W(R) = W(R)$.

$W_n(R) = W(R)/\text{Fil}^n W(R)$ is the ring of Witt vectors of length n .

3.2.4 Remark. Consider the map $f : R \rightarrow W_1(R)$ defined by $f(a) = [a] + \text{Fil}^1 W(R)$. f is multiplicative due to the multiplicativity of the Teichmueller. Let $a_0, b_0 \in R$,

$$\begin{aligned} f(a_0 + b_0) &= [a_0 + b_0] + \text{Fil}^1 W(R) \\ &= (S_n([a_0], [b_0]))_{n \geq 0} + \text{Fil}^1 W(R), \text{ because } (S_n([a_0], [b_0]))_{n \geq 0} - [a_0 + b_0] \in \text{Fil}^1 W(R) \\ &= ([a_0] + [b_0]) + \text{Fil}^1 W(R) \\ &= f(a_0) + f(b_0) \end{aligned}$$

Therefore f is a ring homomorphism which is obviously surjective. Moreover, if $f(a_0) = 0$, then $[a_0] \in \text{Fil}^1 W(R)$, which just means that $a_0 = 0$. Hence f is a injective. We conclude that $W_1(R) \simeq R$.

We end this subsection on Witt vectors by recalling that any $a = (a_0, a_1, \dots) \in W(R)$ can be written as

$$a = \sum_{n \geq 0} p^n [a_n^{p^{-n}}].$$

We point out that since R is perfect then the element $a_n^{p^{-n}}$ exists.

For the rest of this chapter R will be the ring

$$R = \{(x^{(n)})_{n \geq 0}, \text{ for all } n \geq 0, x^{(n)} \in \mathcal{O}_{\mathbb{C}_p}, \text{ and } (x^{(n+1)})^p = x^{(n)}\}$$

where addition and multiplication are defined as follow : for all $x = (x^{(n)})_{n \geq 0}$ and $y = (y^{(n)})_{n \geq 0}$ in R ,

$$(x + y)^{(n)} = \lim_{m \rightarrow \infty} (x^{(n+m)} + y^{(n+m)})^{p^m}, \text{ and } (xy)^{(n)} = x^{(n)} y^{(n)}.$$

We recall that R is perfect and that the map $v_R(x) = v(x^{(0)})$ endows R with a structure of a complete valuation ring of characteristic p . Therefore R satisfies the hypothesis under which we have stated the above results about Witt vectors.

In the sequel we use the ring of Witt vectors $W(R)$ with R stated as above, and we recall the construction (due to Fontaine [8]), of the rings B_{dR} and B_{cris} . Set $\theta : W(R) \rightarrow \mathcal{O}_{\mathbb{C}_p}$ the surjective homomorphism defined by

$$\theta(x) = \sum_{n \geq 0} p^n x_n^{(n)}, \text{ where } x = (x^{(n)})_{n \geq 0},$$

for which the kernel is a principal ideal. We put $\text{Ker}\theta = \xi$. We can extend θ to $W(R)[p^{-1}]$, by setting $\theta(p^{-n}x) = p^{-n}\theta(x)$ for all $x \in W(R)$, for all $n \in \mathbb{N}$. We still denote it by θ . This makes θ into a surjective homomorphism from $W(R)[p^{-1}]$ to \mathbb{C}_p , with a kernel the principal ideal of $W(R)[p^{-1}]$ generated by ξ . Let I be a proper ideal of $W(R)[p^{-1}]$ such that $(\xi) \subset I$, then by surjectivity of θ we have that $\theta(I)$ is an ideal of \mathbb{C}_p . Hence $\theta(I) = 0$ or \mathbb{C}_p . But if $\theta(I) = \mathbb{C}_p$, then

$$W(R)[p^{-1}] = \theta^{-1}(\theta(I)) = I + (\xi) = I,$$

which is a contradiction, whence $\theta(I) = 0$, this just means that $I \subset (\xi)$. We conclude that (ξ) is a maximal ideal of $W(R)[p^{-1}]$. In addition, assume that $\xi^n = 0$, then $\text{Ker}\theta \subset \sqrt{(0)}$. Since \mathbb{C}_p is a field, then $\sqrt{(0)} \subset \text{Ker}\theta$. Then $(\xi) = \sqrt{(0)} = \bigcap_{P \text{ prime}} P$. This means that (ξ) is the unique maximal

ideal. This is a contradiction because $(0, 1, 0, 0, \dots)$ is not invertible, but it does not belong to $\text{Ker}\theta$. The conclusion is that ξ is not a nilpotent element. Put $B_{dR}^+ = \varprojlim W(R)[p^{-1}]/(\xi^n)$ the completion of $W(R)[p^{-1}]$ with respect to the (ξ) -adic topology. We extend θ by continuity to B_{dR}^+ , which we still denote by θ . Then B_{dR}^+ is a complete valuation ring, with maximal ideal $\text{Ker}\theta$ and whose residue field is \mathbb{C}_p . This gives a filtration $\text{Fil}^n B_{dR}^+ = (\text{Ker}\theta)^n$ of B_{dR}^+ .

B_{dR} is the fraction field of B_{dR}^+ . Since $\xi \in \text{Fil}^1 B_{dR}^+$, then in particular $B_{dR} = B_{dR}^+[\xi^{-1}]$.

Since $\bigcap (\xi)^n = 0$, then the canonical map from $W(R)[p^{-1}]$ to B_{dR}^+ is injective. Therefore $W(R)$ and $W(R)[p^{-1}]$ can be identified to subrings of B_{dR}^+ .

It therefore makes sense to consider the subring $A_{\text{inf},K}$ of B_{dR}^+ generated by $W(R)$ and \mathcal{O}_K .

We also recall the subring A_{cris} of B_{dR}^+ whose elements are the series $\sum_{n \geq 0} x_n \frac{\xi^n}{n!}$ where $(x_n)_n$ converges to 0 for the p -adic topology of $W(R)$. We put $B_{cris}^+ = A_{cris}[p^{-1}]$, so that $B_{cris}^+ \subset B_{dR}^+$.

Following the same idea, we put $A_{cris,K}$ to be the subring of B_{dR}^+ generated by A_{cris} and \mathcal{O}_K . Since K is unramified over \mathbb{Q}_p , then $B_{cris}^+ = A_{cris,K}[p^{-1}]$.

3.3 Construction of the period map

In this section, we try to give a detailed exposition of the proof of ([7], proposition 3.1) due to Colmez. We then split it into many steps.

We use $\omega = \alpha(x)dx$ to denote a (closed) differential form over K , where x is an indeterminate and $\alpha(x) \in K[[x]]$. Since K is of characteristic 0, then from lemma 1.4 ([10]), there is a unique $F_\omega \in K[[x]]$ such that $dF_\omega = \omega$ and $F_\omega(0) = 0$. Put F_ω^2 for the formal power series defined by

$$F_\omega^2(x, y) = F_\omega(F(x, y)) - F_\omega(x) - F_\omega(y) \in K[[x, y]].$$

For the rest of our exposition, we will need to consider the following sets :

$$\Omega_F = \{\omega \text{ differential forms over } K \text{ such that } F_\omega^2 = 0\}$$

$\Omega_F^{\text{ex}} = \{\omega \text{ differential forms over } K \text{ such that there exists } r \in \mathbb{N}, p^r F_\omega \text{ has coefficients in } \mathcal{O}_K\}$

$\Omega_F^2 = \{\omega \text{ differential forms over } K \text{ such that there exists } r \in \mathbb{N}, p^r F_\omega^2 \text{ has coefficients in } \mathcal{O}_K\}.$

By the linearity of the differential and the unicity of F_ω , we deduce that if ω' is another differential form over K , and $\lambda \in K$, then $F_{\lambda\omega + \omega'} = \lambda F_\omega + F_{\omega'}$. In particular the sets Ω_F , Ω_F^{ex} and Ω_F^2 are K -vector spaces. It is also straight that both Ω_F and Ω_F^{ex} are subspaces of Ω_F^2 . It then makes sense to consider the quotient K -vector space $D(F) = \Omega_F^2 / \Omega_F^{\text{ex}}$.

$D(F)$ is equipped with the action $\phi(\omega) = \omega^\sigma(x^p)$, where ω^σ stands for the differential form over K obtained from ω by applying σ at any of the coefficients of ω . $\phi(\lambda\omega + \omega') = \sigma(\lambda)\phi(\omega) + \phi(\omega')$. Then the action is σ -linear.

There is a canonical Frobenius action on $W(R)$ taking $(x_n)_n$ to $(x_n^p)_n$. Extending this by continuity we have a Frobenius endomorphism φ of B_{cris}^+ .

If $\omega \in \Omega_F^2$, then there exists $r \in \mathbb{N}$ such that $p^r F_\omega^2$ has coefficients in \mathcal{O}_K , therefore by definition of F_ω^2 there is an interger $s \geq r$ such that $p^s \omega$ has coefficients in \mathcal{O}_K . Moreover we have the following lemma.

3.3.1 Lemma. [7]

1. Let $x \in A_{\text{inf},K}$ such that the p -adic norm of $\theta(x)$ is less than 1, then $F_\omega([p]x) - pF_\omega(x) \in p^{-s} A_{\text{inf},K}$. Where $[p]x$ stands for the multiplication by p with respect to the formal group F .
2. There is a fixed interger r_0 such that for all y :

$$y - x \in A_{\text{inf},K} \cap \text{Ker}\theta \text{ implies } F_\omega(y) - F_\omega(x) \in p^{-s-r_0} A_{\text{cris},K}$$

3.3.2 Lemma. For all $\omega \in \Omega_F^2$, for all $a \in W(R)$, $\varphi(F_\omega(a)) = F_{\phi(\omega)}(a)$

Proof. Since $\omega \in \Omega_F^2$, then by linearity we can assume without loss of generality that ω has coefficients in \mathcal{O}_K .

$$d(F_{\phi(\omega)}(x)) = \phi(\omega)(x) = \omega^\sigma(x^p) = d(F_\omega^\sigma(x^p)),$$

we also have

$$d(\varphi(F_\omega(x))) = d(F_\omega^\varphi(\varphi(x))) = d(F_\omega^p(x^p)),$$

the first equality comes from the fact that φ is an endomorphism, and the second equality comes from the fact that F_ω has coefficients in K . Finally $\varphi(F_\omega(0)) - F_{\phi(\omega)}(0) = 0$ \square

We recall that since $W(R)$ can be identified with a subring of A_{cris} , then $A_{\text{inf},K}$ is viewed as a subring of $A_{\text{cris},K}$.

3.3.3 Proposition. Let $\omega \in \Omega_F^2$, $u = (u_n)_n \in T_p(F)$ with $u_0 = 0$, by the surjectivity of θ , for all $n \geq 0$, write $u_n = \theta(\widehat{u}_n)$ where $\widehat{u}_n \in A_{\text{inf},K}$. Then the sequence $(-p^n F_\omega(\widehat{u}_n))_n$ converges in B_{cris}^+ . And the limit depends only on u and on the class of ω in $D(F)$.

Proof.

$$-p^{n+1} F_\omega(\widehat{u}_{n+1}) - (-p^n F_\omega(\widehat{u}_n)) = -[p^n (-p F_\omega(\widehat{u}_{n+1}) - F_\omega([p]\widehat{u}_{n+1})) + p^n (F_\omega([p]\widehat{u}_{n+1}) - F_\omega(\widehat{u}_n))]$$

from lemma 3.3.1 :

$$-p F_\omega(\widehat{u}_{n+1}) - F_\omega([p]\widehat{u}_{n+1}) \in p^{n-s} A_{\text{inf},K}.$$

Again from lemma 3.3.1 :

$$F_\omega([p]\widehat{u}_{n+1}) - F_\omega(\widehat{u}_n) \in p^{n-s-r_0} A_{cris,K},$$

because $\theta([p]\widehat{u}_{n+1}) = [p]u_{n+1} = u_n = \theta(\widehat{u}_n)$. Then since $A_{inf,K} \subset A_{cris,K}$ we have that :

$$-p^{n+1}F_\omega(\widehat{u}_{n+1}) - (-p^n F_\omega(\widehat{u}_n)) \in p^{n-s-r_0} A_{cris,K} \subset p^n B_{cris}^+$$

therefore $(-p^n F_\omega(\widehat{u}_n))_n$ is a cauchy sequence in B_{cris}^+ for the p -adic topology.

- we show that the limit of $(-p^n F_\omega(\widehat{u}_n))_n$ does not depend on the chosen sequence $(\widehat{u}_n)_n$. For all $n \geq 0$, let $\widehat{v}_n \in A_{inf,K}$ such that $u_n = \theta(\widehat{v}_n)$. Then $\theta(\widehat{u}_n - \widehat{v}_n) = 0$, hence $\widehat{u}_n - \widehat{v}_n \in A_{inf,K} \cap Ker\theta$, then from lemma 3.3.1, $F_\omega(\widehat{u}_n) - F_\omega(\widehat{v}_n) \in p^{-s-r_0} A_{cris,K} \subset B_{cris}^+$, hence $p^n F_\omega(\widehat{u}_n) - p^n F_\omega(\widehat{v}_n)$ converges to 0 in B_{cris}^+ .
- Now we show that the limit of $(-p^n F_\omega(\widehat{u}_n))_n$ only depends on the class of ω in $D(F)$. This amounts to showing that if $\omega \in \Omega_F^{ex}$, then $(-p^n F_\omega(\widehat{u}_n))_n$ converges to 0. Since $\omega \in \Omega_F^{ex}$, there exists r integer such that $p^r F_\omega$ has coefficients in \mathcal{O}_K , then

$$-p^n F_\omega(\widehat{u}_n) = -p^{n-r} p^r F_\omega(\widehat{u}_n) \in p^{n-r} A_{inf,K} \subset p^{n-r} A_{cris,K} \subset p^n B_{cris}^+,$$

which shows that $(-p^n F_\omega(\widehat{u}_n))_n$ converges to 0.

□

Thanks to proposition 3.3.3, the limit of the sequence $(-p^n F_\omega(\widehat{u}_n))_n$ depends only on u and the class of ω in $D(F)$, if we write $\int_u \omega$ this limit, then this defines a map

$$P : D(F) \times T_p(F) \longrightarrow B_{cris}^+, \text{ by } P(\omega, u) = \int_u \omega$$

P is called the period map.

3.3.4 Proposition. Let $\omega \in \Omega_F^2$ and $u \in T_p(F)$

1. The map P is bilinear
2. If $\omega \in \Omega_F$ then $\int_u \omega \in \text{Fil}^1 B_{dR}^+$
3. For all $g \in \text{Gal}(\bar{K}/K)$, $g(\int_u \omega) = \int_{g(u)} \omega$.

Where $g(u)$ is the result of the action of g on u . This says the map P commutes with the action of the absolute Galois group.

Proof. We split the proof into three parts.

1. Since $F_{\omega+\omega'} = F_\omega + F_{\omega'}$, then we get the linearity with respect to ω .

$$-p^n F_\omega(F(\widehat{u}_n, \widehat{u}_n')) - (-p^n F_\omega(\widehat{u}_n)) - (-p^n F_\omega(\widehat{u}_n')) = -p^n F_\omega^2(\widehat{u}_n, \widehat{u}_n') \in p^{n-r} A_{cris,K},$$

then this sequence tends to 0, the belonging relation is due to the fact that $\omega \in \Omega_F^2$. Furthermore, $\theta(F(\widehat{u}_n, \widehat{u}_n')) = F(u, u')$. Therefore we deduce that $\int_{F(u, u')} \omega = \int_u \omega + \int_{u'} \omega$.

2. If $\omega \in \Omega_F$ then for all n , we have by induction on m that $F_\omega([m]u_n) = mF_\omega(u_n)$. Hence

$$0 = F_\omega(0) = F_\omega([p^n]u_n) = p^n F_\omega(u_n)$$

This says that $F_\omega(u_n) = 0$, then

$$\theta(F_\omega(\widehat{u}_n)) = F_\omega(\theta(\widehat{u}_n)) = 0.$$

This means that $F_\omega(\widehat{u}_n) \in \text{Ker}\theta$. We deduce that $-p^n F_\omega(\widehat{u}_n) \in \text{Fil}^1 B_{dR}^+$, which is closed, then $\int_u \omega \in \text{Fil}^1 B_{dR}^+$.

3. Since $g \in \text{Gal}(\bar{K}/K)$, then by definition of $A_{\text{inf},K}$ we have $g(\widehat{u}_n) \in A_{\text{inf},K}$ also

$$\theta(g(\widehat{u}_n)) = g(\theta(\widehat{u}_n)) = g(u_n);$$

which according to the action is the n -th component of $g(u)$, then

$$\lim_n -p^n F_\omega(g(\widehat{u}_n)) = \int_{g(u)} \omega.$$

$g(F_\omega(\widehat{u}_n)) = F_\omega(g(\widehat{u}_n))$, because F_ω has coefficients in K which is the fixed field of $\text{Gal}(\bar{K}/K)$. Since the action is continuous, then

$$g(\lim_n -p^n F_\omega(\widehat{u}_n)) = \lim_n -p^n F_\omega(g(\widehat{u}_n)).$$

This just means that $g(\int_u \omega) = \int_{g(u)} \omega$.

□

The next proposition shows that the period map is compatible with the Frobenius action.

3.3.5 Proposition. Let $\omega \in \Omega_F^2$ and $u \in T_p(F)$, then $\varphi(\int_u \omega) = \int_u \phi(\omega)$.

Proof. Take any $y_n \in R$ such that $y_n^{(0)} = u_n$, set :

$$\widehat{u}_n = [y_n] \in W(R) \subset A_{\text{inf},K}$$

which is the Teichmueller representative of y_n . Since only the first component of \widehat{u}_n is possibly nonzero, then algebraic operations carried on \widehat{u}_n apply exactly as when they are carried on y_n , whence $F_\omega(\widehat{u}_n) \in A_{\text{inf},K}$, because $\omega \in \Omega_F^2$. Now from lemma 3.3.2 $\varphi(F_\omega(\widehat{u}_n)) = F_{\phi(\omega)}(\widehat{u}_n)$, hence

$$\varphi(-p^n F_\omega(\widehat{u}_n)) = -p^n F_{\phi(\omega)}(\widehat{u}_n).$$

Taking the limit, and considering the continuity of φ , we deduce that $\varphi(\int_u \omega) = \int_u \phi(\omega)$. □

We recall that $T_p(F)$ is a free \mathbb{Z}_p -module of rank h , where h denotes the height of the formal group F . Thanks to the finiteness of the subgroups $F[p^n]$, $T_p(F)$ is a profinite group; we have even more, $T_p(F)$ is a pro- p -group.

Since the height is an invariant of the strong isomorphism class, then if two formal groups F and G are strongly isomorphic, their respective Tate module are isomorphic.

More precisely : If ψ is a strong isomorphism of formal groups from F to G over the integers, then for all $n \geq 0$, it induces an isomorphism

$$\psi_n : F[p^n] \longrightarrow G[p^n],$$

Then by the universal property of projective limit, this induces a canonical isomorphism

$$T_p(\psi) : T_p(F) \longrightarrow T_p(G).$$

$T_p(-)$ defines a functor from the category of commutative one-dimensional formal groups to the restrictive category of profinite groups.

4. Conclusion

The main purpose of this project was to study commutative one-dimensional formal groups over a p -adic integer ring in order to understand p -adic periods attached to it. We have started by studying n -dimensional commutative formal groups for a complete unramified field equipped with the Frobenius action, we obtained exposed a technique for explicitly computing formal groups by the means of special element and transformers, we have also characterized homomorphisms of formal groups, and deduce a classification of commutative one-dimensional formal groups over a p -adic integer ring via the height, which is an invariant of the strong isomorphism class for a formal group.

We recall that the construction of a formal group was as follow : if we consider a special element u , that is $u = p + \sum_{\nu \geq 0} c_\nu T^\nu$, where c_ν are integer over our local field, and put

$$pu^{-1} = \sum_{\nu \geq 0} b_\nu T^\nu,$$

then write

$$f(x) := ((pu^{-1}) * i)(x) = \sum_{\nu \geq 0} b_\nu x^{p^\nu},$$

finally put

$$F(x, y) = f^{-1}(f(x) + f(y)).$$

Then F has integer coefficients, and it is a formal group over the integers.

as for the classification, we have seen that for a strong isomorphism class of a given height equal to h (nonzero and finite), this isomorphism class can be identify with a unique special element of the form

$u = p + \sum_{\nu=1}^h b_\nu T^\nu$ where b_1, \dots, b_{h-1} belong to the maximal ideal \mathfrak{m}_K and b_h is an invertible integer.

We have also recalled a precise method of constructing the Tate module attached to a one-dimensional formal group, and noticed that this Tate module is actually attached to the strong isomorphism class of the formal group.

Then the Tate module is another invariant for the strong isomorphism class of the formal group. Therefore at some extend, the p -adic periods map computed for a given one-dimensional group is the same as when computer for any other one-dimensional formal group in the same strong isomorphism class.

Acknowledgements

I hereby express my thankfulness to my supervisor Prof. Denis Benois for his highly valuable support in the realization of this project whether academically or emotionally, but above all for accepting and allowing me to have my project in the field of my interest, thank you. My gratefulness goes towards the ALGANT Consortium for the opportunity given to us in order to attend an international program in pure mathematics; in the same current I thank the universities of Padova and Bordeaux for hosting us in all regards during the mobility period. I thank Prof. Marco Garuti without whom I wouldn't probably have gotten the opportunity of accessing this program. Special thanks go to Professors Adrian Iovita, Andrea D'Agnolo and Olivier Brinon for the very tough but extremely useful notes they put at our disposal. I also thank my professors at the university of Yaounde 1 who assisted me during my very first steps in Mathematics, I especially think of Prof. Nkuimi Celestin, Prof. Ayissi and Dr. Takam Patrice. A very special thank to my "second mother" Karimatou Djenabou who always take care of me in special times. I can not end this without thanking all my classmates from Padova and Bordeaux with whom we have shared beautiful times, especially Njaka Andria, Lian Kelvin and Sainhery Phrador with whom I had interesting exchanges that made me learn a lot in Mathematics.

References

- [1] Salomon Bochner. Formal lie groups. *Annals of Mathematics*, pages 192–201, 1946.
- [2] N Bourbaki. Elements de mathematique (chapitres 8-9), algebre commutative, 1985.
- [3] Nicolas Bourbaki. *Algèbre: Chapitre 4 à 7*. Springer Science & Business Media, 2007.
- [4] Thomas S Brewer. Algebraic properties of formal power series composition. 2014.
- [5] Olivier Brinon. *Représentations p -adiques cristallines et de de Rham dans le cas relatif*. Société Mathématique de France, 2008.
- [6] Olivier Brinon and Brian Conrad. Cmi summer school notes on p -adic hodge theory (preliminary version). *course notes*, 2009.
- [7] Pierre Colmez. Périodes p -adiques des variétés abéliennes. *Mathematische Annalen*, 292(1):629–644, 1992.
- [8] Jean-Marc Fontaine and Yi Ouyang. Theory of p -adic galois representations. *preprint*, 2008.
- [9] Albrecht Fröhlich. *Formal groups*, volume 74. Springer, 2006.
- [10] Taira Honda. On the theory of commutative formal groups. *Journal of the Mathematical Society of Japan*, 22(2):213–246, 1970.
- [11] Michel Lazard. Sur les groupes de lie formels à un paramètre. *Bulletin de la Société Mathématique de France*, 83:251–274, 1955.
- [12] Jean-Pierre Serre. *Local fields*, volume 67. Springer Science & Business Media, 2013.
- [13] Thomas Zink and Cartiertheorie kommutativer formaler Gruppen. Cartier theory of commutative formal groups. *With English, French and Russian summaries. Teubner-Texte zur Mathematik [Teubner Texts in Mathematics]*, 68.