Algebra, Geometry and Number Theory
ALGANT Master Program

MASTER'S THESIS

Formal Groups and p-adic Periods

Institut de Mathématiques de Bordeaux

Università degli Studi di Padova

Adrien
Chassaing-Monjou

Advisor: Pr. Denis Benois

July 2019

Abstract

The aim of this Master's thesis is to understand formal groups, in particular commutative formal groups of dimension 1 over a ring of integers of a local field, to study the construction of the period map of formal groups. Below is a brief discussion on the content of each section.

1) Formal Groups. In this section we start by giving the definitions and basic properties about formal groups of dimension n. Then we study commutative formal groups of dimension 1 over different kind of rings. The aim is to understand their structure and the construction of the Tate module for formal groups.

2) The Period rings B_{dR} and B_{cris}. This second section explains the construction of Fontaine of different p-adic period rings as B_{dR} and B_{cris}. We give also properties of these objects. We talk at some point about the p-adic analogous of $2i\pi$ which is an interesting object living in B_{dR}^{+}.

3) p-adic Periods of Formal Groups. In this last section, we discuss about the construction of the period map of formal groups which is a special case of the period map for abelian varietes, and give an example after, showing the link between the complex case and the p-adic one.

A good reference for the first section in which it is based on is [Fro68] and if the reader look at it, he will see how rich is the theory of formal groups. For the construction of the ring of periods, [BC], [FO] or [Col07] are really good introductions and I can only stress how useful they were to understand these objects. Normally, any references required are specified where needed.
In this work, no originality is claimed as it is based on [Ber01] and [Col92]. Any mistake found is mine.

Remerciment

J'aimerais remercier mon directeur de mémoire, Monsieur Denis Benois, pour avoir accepté de me superviser pour ce travail et m'avoir introduit à une théorie surprenante et très riche, ainsi que Madame Christine Bachoc sans qui je n'aurais sûrement jamais intégré le master ALGANT.
Je tiens également à remercier ma famille, en espérant qu'ils voient l'accomplissement de mes efforts et des heures passées à étudier dans ma chambre. Je ne pourrais pas citer tous mes amis qui m'ont soutenu, mais je tiens à citer ceux qui ont toujours été là pour moi dans les moments compliqués : Xavier, Anthony, je ne sais pas comment vous remercier. Il y a aussi ceux qui ont toujours su me rendre le sourire grâce à leur bonne humeur : Aloïs, Sergio, Pierre, Naomi, Roxane et tant d'autres !

Contents

1 Formal Groups

1.1 Formal Groups of dimension n

In this section, we take R to be a fixed commutative unitary ring, and all power series are over R.

Definition 1.1. A formal group $F(X, Y)$ of dimension n is a system $F_i(X, Y)$ of n power series in $2n$ indeterminates $X = (X_1, ..., X_n)$, $Y = (Y_1, ..., Y_n)$ satisfying :

$$\begin{aligned} &i)\ F(X, 0) = X, F(0, Y) = Y \\ &ii)\ F(F(X, Y), Z) = F(X, F(Y, Z)) \end{aligned}$$

Remark 1.2. i) tells us that $F(0, 0) = 0$ and so we have $F_i(X, Y) = X_i + Y_i$ mod degree 2. Moreover, terms of degree greater than 1 are "mixed", i.e., X's and Y's only occur together.
We say that F is commutative if $F(X, Y) = F(Y, X)$.

Proposition 1.3. *Given F, there exists a unique $i(X)$ (n power series in n inderterminates) so that $F(X, i(X)) = F(i(X), X) = 0$.*

Proof. Put $g_i(X, Y) = X_i - F_i(X, Y)$, for $i = 1, ..., n$. Note that g_i has no constant term when viewed as a power series in Y.
$(\partial g_i/\partial Y_k)_{X=Y=0} = -(\partial F_i/\partial Y_k)_{X=Y=0} = -\delta_{ik}$. The determinant of $(\partial g_i/\partial Y_k)_{Y=0}$ is a unit of $R[[X_1, ...X_n]]$.
Therefore there exist $h_i(X, Y)$, (for $i = 1, ..., n$) such that $g_i(X, h_i(X, Y)) = Y_i$, or $F_i(X, h(X, Y)) = X_i - Y_i$ (for $i = 1, ..., n$). Put $Y = X$, then $F_i(X, h(X, X)) = 0$. Take $i(X) = h(X, X)$. The proof of the uniqueness is a translation of the one of group theory. □

Remark 1.4. This proposition tells us that to any element $x \in R$, there exists a unique inverse $i(x)$ with respect to F. With property i) and ii), we start to see that F looks like to a group law. We will see later in the section about the group of points of a formal group that it is possible, thanks to F, to put a structure of a group on maximal ideal.

For $i = (i_1, .., i_n) \in \mathbb{N}^n$, define $|i| = \sum_{k=1}^{n} i_k$. For $f \in R_n = R[[X_1, ..., X_n]]$, we define the order of f to be $ord(f) = \inf_{f_i \neq 0} |i|$.
For $m \in \mathbb{N}$, define $A_m = \{f \in R_n \mid ord(f) \geq m\}$. A_m is a subgroup of R_n and $A_m \supseteq A_{m+1}$. Defining $A_\infty = \bigcap_{m \in \mathbb{N}} A_m$, we have in fact $A_\infty = \{f \in R_n \mid ord(f) = \infty\}$.

If $(f_k)_{k\in\mathbb{N}}$ is a sequence of elements of R_n, and $\lim\limits_{k\to\infty} ord(f_k - f) = \infty$ then we write $\lim_{ord} f_k = f$ when $k \to \infty$. One can replace (R_n, ord) by any (A, v) where A is a commutative unitary ring and v a filtration defined on A.
Suppose now that F and G are formal groups of dimension n and m respectively.

Definition 1.5. A homomorphism $f : F \to G$ is a "vector" $f = f_1, ..., f_m$ of m power series in $X_1, ..., X_n$ with no constant terms, so that $f(F(X,Y)) = G(f(X), f(Y))$.

The homomorphism f determines a homomorphism $\theta_f : R[[Z_1, ..., Z_m]] \to R[[X_1, ..., X_n]]$ given by $\theta_f(Z_i) = f_i(X)$. If $f : F \to G$, $g : G \to H$ are homomorphisms of formal groups then $g \circ f : F \to H$ is a homomorphism of formal groups. Also $1_i(X) = X_i$ gives the identity homomorphism of F. Hence :

Theorem 1.6. *The formal groups and their homomorphism form a category $\mathcal{F}_R(= \mathcal{F})$ and $f \mapsto \theta_f$ defines a functor $\mathcal{F}_R \to \mathcal{P}_R$, where $\mathcal{P}_R$ is the category whose objects are (R_n, ord) and the morphisms are the continuous ring homomorphisms.*

Remark 1.7. A homomorphism $f : F \to G$ of formal groups is an isomorphism (in $\mathcal{F}_R$) if and only if θ_f is an isomorphism (in $\mathcal{P}_R$). Moreover, if f is any "vector" of n power series with θ_f an isomorphism, and if F is a formal group of dimension n, then there is a unique formal group $G(= f \circ F \circ f^{-1})$ so that f is an isomorphism $F \to G$.

In $R_n = R[[X_1, ..., X_n]]$, consider the ideal $I = Ker(R_n \to R)$ and denote by $\overline{f}$ the image of f under the natural epimorphism $I \to I/I^2 =: D(R_n)$.

For a given prime number p, denote $\pi : R_n \to R_n$ the homomorphism which fixes R_n and takes X_i into X_i^p. Then $\pi^{(m)} : X_i \mapsto X_i^{p^m}$ for any $m \geq 1$.
Let R^+ denote the additive group of R.

Theorem 1.8. *Let $f : F \to G$ be a homomorphism of formal groups (of dimension n and m respectively) and let $\theta_f : R_m \to R_n$ the corresponding homomorphism of rings.*
i) suppose R^+ is torsion free. Then $D(\theta_f) = 0$ if and only if $f = 0$
ii) suppose R^+ is of exponent p (prime),that means that there exists $g : F \to G$ a homomorphism of formal groups such that $f(X) = g(X^p)$. Then $D(\theta_f) = 0$ if and only if either $f = 0$, or $\theta_f = \phi_f \circ \pi^{(q)}$, where $D(\phi_f) \neq 0$ and $q > 0$.

Proof. See [Fro68] Chapter I, section 2, Theorem 2. □

Definition 1.9. Assume that R^+ is of exponent p. If $\theta = \phi \circ \pi^{(h)}$ and $D(\phi) \neq 0$, then $h = ht(\theta)$ is called the height of θ. We define $ht(0) = \infty$.
For f a homomorphism of formal groups, $ht(\theta_f) = ht(f)$ is called the height of f.
If $f \neq 0$, then $ht(f) = h$ is the greatest integer so that f is a power series in X^{p^h}.

Proposition 1.10. *i) If f, g are homomorphisms of formal groups and $f \circ g$ is defined, then $ht(f \circ g) \geq ht(f) + ht(g)$.*
ii) If G is a commutative formal group and $f, g \in Hom_{\mathcal{F}}(F, G)$, then

$$ht(G(f,g)) \geq \inf\{ht(f), ht(g)\}$$

.

Proof. See [Fro68] Chapter I, section 3, Proposition 5. □

Remark 1.11. If our formal groups are of dimension 1, R is an integral domain and $f \circ g$ is defined, then $ht(f) + ht(g) = ht(f \circ g)$ and the height function from $R_n \to \mathbb{Z} \cup \{\infty\}$ is a valuation.

1.2 Commutative formal Groups of dimension one

Throughout this section, all formal groups are now commutative of dimension one. We repeat the definitions in this case and state a few pertinent facts.
Let R be a ring.

Definition 1.12. A formal group $F(X, Y)$ is a power series (over R) in two variables X,Y satisfying :

$$\begin{aligned} &i)\ F(0, X) = X = F(X, 0) \text{ (Identity element)} \\ &ii)\ F(F(X, Y), Z) = F(X, F(Y, Z)) \text{ (Associativity)} \\ &iii)\ F(X, Y) = F(Y, X) \text{ (Commutativity)} \end{aligned}$$

Remark 1.13. As before, we necessarily have $F(X, Y) \equiv X + Y$ (mod degree 2).

Proposition 1.14. *Given F, there exists a unique $i(X)$ (a power series in one indeterminate) so that $F(X, i(X)) = F(i(X), X) = 0$*

Proof. We already proved this for dimension n in Proposition 1.3. □

Definition 1.15. A homomorphism $f : F \to G$ of formal groups is a power series (with zero constant term) in one variable satisfying the relation

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

We denote by $Hom_R(F, G)$ the set of homomorphisms $F \to G$ of formal groups. If $f, g \in Hom_R(F, G)$, $(f + g)(X) = G(f(X), g(X))$. With respect to this addition, $Hom_R(F, G)$ is an abelian group, and the composition $\circ$ for homomorphisms is bilinear. We denote the category of commutative formal groups of dimension 1 over R by $\mathcal{G}_R$. $Hom_R(F, F) = End_R(F)$ is a ring with identity.

Definition 1.16. We define the multiplication-by-m map $[\ .\ ]_F : \mathbb{Z} \to End_R(F)$ with $[n + 1]_F(X) = F([n]_F(X), X)$ to be the unique homomorphism which preserves identities.
We have $[1]_F(X) = X$ and $[-1]_F(X)$ is the power series $i(X)$ of Proposition 1.14, i.e., $F(X, i(X)) = 0$.

For $n \in \mathbb{Z}$ and $f \in Hom_R(F, G)$ we have

$$f \circ [n]_F = [n]_G \circ f$$

Now we recall the definition of the map D. For dimension 1, we simply have $D(f) = f_1$ =coefficient of X in $f(X)$ and :

$$D(f \circ g) = D(f).D(g)$$
$$D(f+g) = D(f) + D(g)$$

Moreover f is an isomorphism if and only if $D(f) \in U(R)$(= the units of R).

Proposition 1.17. *If R is an integral domain, then $End_R(F)$ is a (non-commutative integral) domain and $Hom_R(F,G)$ is a torsion free $End_R(F)$ (and $End_R(G)$)-module.*

Proof. If $f = f_r X^r + f_{r+1}X^{r+1} + \ldots$ and $g = g_s X^s + g_{s+1}X^{s+1} + \ldots$ with $f_r, g_s \neq 0$ then $f \circ g = f_r g_s^r X^{r+s} + \ldots$ and $f_r g_s^r \neq 0$. Therefore $f \circ g = 0$ implies either $f = 0$ or $g = 0$. From this we deduce that $End_R(F)$ is an integral domain, and that $Hom_R(F,G)$ is a torsion-free $End_R(F)$ (and $End_R(G)$)-module. □

The image of $[\ .\ ] : \mathbb{Z} \to End_R(F)$ is thus also an integral domain and its kernel must therefore either be 0 or $p\mathbb{Z}$ for some prime p. If the characteristic of the quotient field of R is 0 then $D : End_R(F) \to R$ is an embedding. Therefore $End_R(F)$ is a commutative integral domain and $Ker(\mathbb{Z} \to End_R(F)) = 0$

Theorem 1.18. *A formal group F is isomorphic over R to the additive group G_a if and only if, for all primes p, $[p]_F$ has coefficient in pR. (We have $G_a(X,Y) = X + Y$).*

Proof. See [Fro68] Chapter III, section 1, Theorem 2. □

1.2.1 The invariant Differential

In this section we study a formal group F of dimension 1 defined over an arbitrary integral ring R. In a formal setting of this sort, a differential form is simply an expression $Q(X)dX$ with $Q(X) \in R[[X]]$. Of particular interest are those differential forms that respect the group structure of F.

Definition 1.19. An invariant differential on a formal group F is a differential form $\omega(X) = Q(X)dX \in R[[X]]dX$ satisfying $\omega \circ F(X,Y) = \omega(X)$.
Writing this out, $\omega(X) = Q(X)dX$ is an invariant differential if it satisfies

$$Q(F(X,Y))F_1(X,Y) = Q(X)$$

where $F_1(X,Y)$ is the partial derivative of F with respect to its first variable.
An invariant differential is said to be normalized if $Q(0) = 1$.

Example 1.20. On the additive group G_a, the differential $\omega = dX$ is invariant.

Example 1.21. On the multiplicative group G_m, the following is an invariant differential :

$$\omega = \frac{dX}{1+X} = (1 - X + X^2 - X^3 + ...)dX$$

Proposition 1.22. *Let F be a formal group defined over R. There exists a unique normalized invariant differential on F. It is given by the formula $\omega = F_1(0,X)^{-1}dX$. Every differential on F is of the form $a\omega$ for some $a \in R$.*

Proof. Suppose that $Q(X)dX$ is an invariant differential on F, so it satisfies

$$Q(F(X,Y))F_1(X,Y) = Q(X)$$

Putting $X = 0$ and since $F(0,Y) = Y$, we have $Q(Y)F_1(0,Y) = Q(0)$.
Since $F_1(0,Y) = 1 + ...$ we see that that $Q(X)$ is completely determined by the value $Q(0)$, and further that every invariant differential is of the form $a\omega$ with $a \in R$ and $\omega = F_1(0,X)^{-1}dX$.
Since this differential ω is normalized, it remains only to show that it is invariant. We need to prove that $F_1(0,F(X,Y))^{-1}F_1(X,Y) = F_1(0,X)^{-1}$.
To do this, we differentiate the associative law : $F(Z,F(X,Y)) = F(Z,X),Y)$ with respect to Z to obtain $F_1(Z,F(X,Y)) = F_1(F(Z,X)Y)F_X(Z,X)$. Putting $Z = 0$ and using the fact that $F(0,X) = X$ yields $F_1(0,F(X,Y)) = F_1(X,Y)F_1(0,X)$, which is the desired result. □

Before starting the first corollary, we set the notation $f'(X)$ for the formal derivative of a power series $f(X) \in R[[X]]$ i.e., $f'(X)$ is obtained by formally differentiating $f(X)$ term by term.

Corollary 1.23. *Let F and G be formal groups with normalized differentials ω_F and ω_G. Let $f : F \to G$ be a homomorphism of formal groups. Then $\omega_G \circ f = f'(0)\omega_F$.*

Proof. We compute $(\omega_G \circ f)(F(X,Y)) = \omega_G(G(f(X),f(Y))) = (\omega_G \circ f)(X)$. Hence it is an invariant differential to F. By last proposition, we know that $\omega_G \circ f$ is equal to $a\omega_F$ for some $a \in R$. Comparing coefficients on X on each side gives $a = f'(0)$. □

Corollary 1.24. *Let F be a formal group and let $p \in \mathbb{Z}$ be a prime. Then there are power series $f(X), g(X) \in R[[X]]$ with $f(0) = g(0) = 0$ such that*

$$[p]_F(X) = pf(X) + g(X^p).$$

Proof. Let $\omega(X)$ be the normalized invariant differential on F.
We know that $D([p]_F) = p$, so last corollary implies that

$$p\omega(X) = (\omega \circ [p]_F)(X) = (1 + ...)D([p]_F)(X)dX.$$

The series $(1+...)$ is invertible in $R[[X]]$, from which it follows that $D([p]_F) \in pR[[X]]$. Therefore every term aX^n in the series $[p]_F(X)$ satisfies either $a \in pR$ or $p|n$. □

1.2.2 Commutative formal groups of dimension one over a separably closed field of characteristic $p \neq 0$

Let k denote our base field, separably closed of characteristic p. For formal group F and G (over k) and $f \in Hom_k(F, G)$, f is a power series in X^{p^h}, where $h = ht(f)$. More precisely, we have: $f(X) = a_1 X^{p^h} + a_2 X^{2p^h} + ...$ with $a_1 \neq 0$.

Proposition 1.25. *Let f and g be homomorphisms of formal groups, then :*
i) $ht(f+g) \geq \inf(ht(f), ht(g))$
ii) $ht(f \circ g) = ht(f) + ht(g)$

Proof. i) already done in 1.10
ii) Put $n = ht(f)$, $m = ht(g)$. Then $f(X) = aX^{p^n} + ...$ and $g(X) = bX^{p^m} + ...$ with $a \neq 0$ and $b \neq 0$. Therefore $f(g(X)) = ab^{p^n} X^{p^{n+m}} + ...$ with $ab^{p^n} \neq 0$ and clearly we get $ht(f \circ g) = n + m = ht(f) + ht(g)$. □

Corollary 1.26. $ht(u) = 0$ *if and only if u is an invertible power series, in which case* $ht(u \circ f \circ u^{-1}) = ht(f)$

Proof. $ht(u) = 0 \Leftrightarrow u(X) = a_1 X + a_2 X^2 + ...$ with $a_1 \neq 0$. But we have that
$\varepsilon(u) = a_1 \in U(k) \Leftrightarrow u$ is invertible.
By the previous proposition we get $ht(u \circ u^{-1}) = ht(1) = 0 \Rightarrow ht(u) = -ht(u^{-1})$. Hence $ht(u \circ f \circ u^{-1}) = ht(u) + ht(f) + ht(u^{-1}) = ht(f)$. □

Corollary 1.27. *If we consider $\mathbb{Z}$ with the p-adic filtration, and $End_k(F)$ with the height filtration, then $\mathbb{Z} \to End_k(F)$ is continuous.*

Proof. $\mathbb{Z} \to End_k(F)$ is continuous if for $(a_n)_n \in \mathbb{Z}^{\mathbb{Z}_{\geq 0}}$, $v_p(a_n) \to \infty \Rightarrow ht([a_n]_F) \to \infty$ which is clear since the height function of $[a_n]$ depends on the greatest power of p which divides a_n. □

Definition 1.28. We define the height $Ht(F)$ of the formal group F to be $ht([p]_F)$.

Remark 1.29. By Corollary 1.26, $Ht(F)$ only depends on the isomorphism class of F.

Corollary 1.30. *If $Ht(F) \neq Ht(G)$, then $Hom_k(F,G) = 0$.*

Proof. If $f \in Hom_k(F,G)$, then $f \circ [p]_F = [p]_G \circ f$. Hence, $ht(f) + Ht(F) = ht(f) + Ht(G)$. Since $Ht(F) \neq Ht(G)$, then $ht(f) = \infty$ and we get $f = 0$. □

Proposition 1.31. *$Hom_k(F,G)$ is complete under the height filtration.*

Proof. Let $\{f_n\}$ be a Cauchy sequence under the height filtration. Then it is a Cauchy sequence with respect to the order filtration, and $ord(g) = p^{ht(g)}$. Put $f = \lim_{ord}(f_n)$. Then, working modulo degree n we have

$$f(F(X,Y)) \equiv f_n(F(X,Y)) = G(f_n(X), f_n(Y)) \equiv G(f(X), f(Y))$$

Hence $f \in Hom_k(F,G)$ and f is the limit of $\{f_n\}$ under the height filtration. □

Corollary 1.32. *The homomorphism $\mathbb{Z} \to End_k(F)$ extends to a homomorphism $\mathbb{Z}_p \to End_k(F)$.*

Proof. Use Corollary 1.27 and Proposition 1.31 □

1.3 Commutative Formal Groups of Dimension One over a Discrete Valuation Ring

Suppose from now on that R is a discrete valuation ring with quotient field K of characteristic 0, maximal ideal $\mathfrak{M}$ and residue field k of characteristic $p \neq 0$. Let v denote the valuation on K given by $\mathfrak{M}$ (we take v normalized so that $v(p) = 1$). We denote by $\overline{k}$ the separable closure of k. The homomorphism $R \to \overline{k}$ induces a functor $\mathcal{G}_R \to \mathcal{G}_{\overline{k}}$ under which $F \mapsto \overline{F}$.

Proposition 1.33. *If $\overline{F}$ is not isomorphic to $\overline{G_a}$ then $Hom_R(F, G) \to Hom_{\overline{k}}(\overline{F}, \overline{G})$ is injective.*

Proof. Suppose $f : F \to G$ is a non-zero homomorphism such that $\overline{f} = 0$. Let $(\pi) = \mathfrak{M}$. Then $f(X) = \pi^r g(X)$ where $r > 0$ and $\overline{g} \neq 0$. We have

$$\begin{aligned}\pi^r g(F(X, Y)) &= G(\pi^r g(X), \pi^r g(Y))\\ &\equiv \pi^r g(X) + \pi^r g(Y) \pmod{\mathfrak{M}^{r+1} R[[X]]}\end{aligned}$$

Hence $g(F(X, Y)) \equiv g(X) + g(Y) \pmod{\mathfrak{M} R[[X]]}$ and $\overline{g}(\overline{F}(X, Y)) = \overline{g}(X) + \overline{g}(Y)$. Therefore $\overline{g} \circ [p]_{\overline{F}} = [p]_{\overline{G_a}} \circ \overline{g} = 0$. Since $\overline{g} \neq 0$, then $[p]_{\overline{F}} = 0$, i.e., $\overline{F} = \overline{G_a}$ (by Theorem 1.18. □

Corollary 1.34. *If $Ht(\overline{F}) \neq \infty$, $Ht(\overline{F}) \neq Ht(\overline{G})$, then $Hom_R(F, G) = 0$.*

Proof. $Ht(\overline{F}) \neq \infty$ implies that $\overline{F}$ is not isomorphic to $\overline{G_a}$ and so $Hom_R(F, G) \to Hom_{\overline{k}}(\overline{F}, \overline{G})$ is injective. But $Ht(\overline{F}) \neq Ht(\overline{G})$ implies that $Hom_{\overline{k}}(\overline{F}, \overline{G}) = 0$. And so, by the injectivity we deduce that $Hom_R(F, G) = 0$. □

1.3.1 The Group of Points of a Formal Group

In this section R is a complete discrete valuation ring with quotient field K of characteristic 0, maximal ideal $\mathfrak{M}$ and residue field k of characteristic $p \neq 0$. We assume that the $\mathfrak{M}$-valuation v on K is normalized so that $v(p) = 1$. All formal groups, unless otherwise mentioned, are defined over R, and are assumed to be commutative of dimension 1. $\overline{K}$ is the algebraic closure of K. The integers in $\overline{K}$ (i.e. the elements of the integral closure in $\overline{K}$ of R) form a local ring $\overline{R}$ (it is not Noetherian). The unique extension to $\overline{K}$ of the valuation v of K will again be denoted by v. Note that $\overline{K}$ is not complete.

Suppose L is a finite field extension of K and let S denote the integers in L. Take $f \in S[[X_1, ..., X_n]]$. Then for $\alpha_1, ..., \alpha_n \in \overline{\mathfrak{M}}$, $f(\alpha_1, ..., \alpha_n)$ makes sense and converges in $\overline{R}$ (and if the constant term in f is 0, $f(\alpha_1, ..., \alpha_n)$ lies in $\overline{\mathfrak{M}}$).

Note that $\alpha_1, ..., \alpha_n$ and all the coefficients of f are integers in $L_1 := L(\alpha_1, ..., \alpha_n)$, and L_1 being a finite extension of a complete field K, is complete.

Proposition 1.35. *i) The elements of $\overline{\mathfrak{M}}$ form an abelian group $F(\overline{R})$ that we denote $P(F)$ under the operation $\alpha *_F \beta = F(\alpha, \beta)$ and $v(\alpha *_F \beta) \geq \inf(v(\alpha), v(\beta))$.*
The elements of $P(F)$ of finite order form a subgroup $\Lambda(F)$, the torsion subgroup of $P(F)$.
ii) $P(F)$ and $\Lambda(F)$ are modules over $\Gamma = Gal(\overline{K}/K)$.
iii) If $f : F \to G$ is a homomorphism of formal groups defined over R then the map $\alpha \mapsto f(\alpha)$ is a homomorphism $P(f) : P(F) \to P(G)$.
P and Λ are covariant functors from the category $\mathcal{G}_R$ to the category of Γ-modules. In particular, $P(F)$ ad $\Lambda(F)$ are modules over $End_R(F)$ and these endomorphisms commute with Γ.

Proof. i) see [Fro68] Chapter IV, section 2, Proposition 1.
ii) If $\gamma \in \Gamma$, then $F(\alpha, \beta)^\gamma = F(\alpha^\gamma, \beta^\gamma)$ since F is defined over R and its coefficients are therefore fixed by γ. It is thus easy to verify that $P(F)$ and $\Lambda(F)$ are indeed Γ-modules.
iii) If $f : F \to G$ is a homomorphism defined over R, then f maps $\overline{\mathfrak{M}}$ into itself (since f has no constant term). Since $f(F(X, Y)) = G(f(X), f(Y))$ we have $f(\alpha *_F \beta) = f(F(\alpha, \beta)) = G(f(\alpha), f(\beta)) = f(\alpha) *_G f(\beta)$. As $f(\alpha)^\gamma = f(\alpha^\gamma)$, f commutes with γ. □

Remark 1.36. i) If F is the additive group G_a, then $P(F)$ is just $\overline{\mathfrak{M}}$ with the ordinary addition and $\Lambda(F) = 0$.
ii) If F is the multiplicative group G_m, with

$$G_m(X, Y) = X + Y + XY = (X + 1)(Y + 1) - 1$$

then $P(F)$ is isomorphic to the group U of principal units u of $\overline{R}$ for which $u \equiv 1 \pmod{\overline{\mathfrak{M}}}$.
The isomorphism $P(F) \to U$ is given by $\alpha \mapsto 1 + \alpha$.

Definition 1.37. An isogeny $f : F \to G$ is defined to be a non-zero homomorphism defined over $\overline{R}$.

From now on, all formal groups to be considered are assumed to be of finite height, unless otherwise mentioned.

Theorem 1.38. *(Lubin, Serre)*
Let $f : F \to G$ be an isogeny. Then :
i) The map $P(f) : P(F) \to P(G)$ is surjective
ii) The kernel of $P(f)$ is a finite group of order $p^{ht(f)}$

To prove this theorem we will need the Weierstrass preparation theorem that we will admit.
For $f \in R_n$, $\overline{f}$ denotes its image in k_n under the epimorphism $R_n \to k_n$ induced by $R \to k$.

Definition 1.39. The Weierstrass-order of f, denoted $W\text{-}ord(f)$ is defined by $W\text{-}ord(f) = ord_k(\overline{f})$.

Definition 1.40. A distinguished polynomial f of R is a polynomial of the form $f_0 + f_1X + ... + f_{m-1}X^{m-1}$ where all the f_i are in $\mathfrak{M}$.

Remark 1.41. Note then that for a distinguished polynomial $W\text{-}ord(f) = deg(f)$.

Theorem 1.42. *(Weierstrass preparation theorem)*
If $f \in R[[X]]$ and $W\text{-}ord(f) = m < \infty$, then there exist a unique $u \in U(R[[X]])$ and a unique distinguished polynomial g such that $f = u.g$. Then of course, $W\text{-}ord(g) = W\text{-}ord(f)$.

Now we can prove the theorem 1.38 :

Proof. Let $\nu \in \overline{\mathfrak{M}}$. Then $f(X) - \nu$ is defined over some finite extension S of R. For the Weierstrass order we have the equation

$$W\text{-}ord(f(X) - \nu) = W\text{-}ord(f(X)) = p^{ht(f)}$$

and $ht(f)$ is finite by Proposition 1.33. By the Weierstrass preparation theorem (Theorem 1.42) therefore $f(X) - \nu = u(X)g(X)$, where $u(X)$ is an invertible power series and $g(X)$ is a distinguished polynomial :

$$g(X) = X^{p^{ht(f)}} + \sum_{i=0}^{p^{ht(f)}-1} g_iX^i, \ g_i \in \mathfrak{M}_S$$

Take $\alpha \in \overline{K}$ so that $g(\alpha) = 0$. Since the coefficients of g lie in S then $\alpha \in \overline{R}$.
As $g_i \in \overline{\mathfrak{M}}$, then also $\alpha \in \overline{\mathfrak{M}}$. But the zeroes of $f(X) - \nu$ are precisely the zeroes of $g(X)$. Hence we have $f(\alpha) = \nu$ for some $\alpha \in \overline{\mathfrak{M}}$. This proves i).
For ii), take $\nu = 0$. Now $g(X)$ has $p^{ht(f)}$ distinct roots, provided that $g(\alpha) = 0$ implies $g'(\alpha) \neq 0$.
Thus $f(X) = 0$ has $p^{ht(f)}$ roots in $\overline{\mathfrak{M}}$, provided $f(\alpha) = 0$ implies $f'(\alpha) \neq 0$ ($\alpha \in \overline{\mathfrak{M}}$).
Differentiating the equation $f(F(X,Y)) = G(f(X), f(Y))$ with respect to Y, we obtain $f'(F(X,Y))F_2(X,Y) = G_2(f(X), f(Y)).f'(Y)$
(here, the suffix 2 denotes the derivative with respect to the second variable). Put $X = \alpha$, $Y = 0$. If $f(\alpha) = 0$, then $f'(\alpha)F_2(\alpha, 0) = G_2(0,0).f'(0) = f'(0) \neq 0$. Therefore $f'(\alpha) \neq 0$. □

The following theorem is really a corollary of Theorem 1.38

Theorem 1.43. *(Lubin, Serre)*
i) $P(F)$ is a divisible group and the integers prime to p induce automorphism of $P(F)$.
ii) $\Lambda(F) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{(h)}$, $h = Ht(F)$ ($^{(h)}$ denotes h-fold product).

Proof. i) For n prime to p, i.e., n a unit of R, $[n]_F$ is an automorphism of F. Hence $P([n]_F)$ is an automorphism of $P(F)$. Apply Theorem 1.38 to $f = [p]_F^r$. The surjectivity of $P([p]_F^r) : P(F) \to P(F)$ implies that $P(F)$ is divisible.
ii) $\Lambda(F)$ is a torsion subgroup of the divisible group $P(F)$ hence divisible. Also $\Lambda(F)$ is p-primary. Hence $\Lambda(F) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{(c)}$, where $c = dim(Ker([p]_F))$. But the cardinality of $Ker([p]_F)$ is $p^{dim(Ker([p]_F))}$, which by Theorem 1.38 is p^h. Therefore $c = h$. □

For each real number ρ, the set $J_\rho = \{\alpha \in \overline{K} | v(\alpha) > \rho\}$ is a fractional ideal of $\overline{R}$. If $\rho \geq 0$ then J_ρ is an ideal of $\overline{R}$ and in particular, $J_0 = \overline{\mathfrak{M}}$. For $\rho \geq 0$, the elements of J_ρ form a subgroup $F(J_\rho)$ of $P(F)$.
We admit the existence of a unique isomorphism $l_F : F \to G_a$, defined over K such that $l'_F(X)$ is defined over R and $l'_F(0) = 1$. Its inverse is denoted e_F. (For details, see [Fro68]).

Theorem 1.44. *(Serre)*
i) l_F converges on $\overline{\mathfrak{M}}$; e_F converges on $J_{\frac{1}{p-1}}$.
ii) The map $\alpha \mapsto l_F(\alpha)$ ($\alpha \in \overline{\mathfrak{M}}$) defines a homomorphism $P(F) \to \overline{K}^+$ of Γ-modules and of $End_R(F)$-modules. The sequence :

$$0 \to \Lambda(F) \to P(F) \to \overline{K}^+ \to 0$$

is exact.
iii) l_F and e_F define inverse isomorphisms $F(J_{\frac{1}{p-1}}) \cong J^+_{\frac{1}{p-1}}$ (where the group operation on $J^+_{\frac{1}{p-1}}$ is the usual addition).

We will need the following lemma to prove Theorem 1.44

Lemma 1.45. *For each real number ρ, there exists an integer $n = n(\rho, F)$ such that, for all $\alpha \in \overline{K}$ with $v(\alpha) \geq \rho$, we have $v([p]_F^n(\alpha)) > \frac{1}{p-1}$.*

Proof. We may assume $\rho < 1$, since otherwise we may take $n = 0$.
Now, $[p]_F(X) \equiv pX$ (mod deg 2). If $v(\alpha) > 0$, then $[p]_F(\alpha) = p\alpha + \alpha^2 r$ for some $r \in \overline{R}$. Thus if $v(\alpha) \geq \rho$, then $v([p]_F(\alpha)) \geq \inf(1 + v(\alpha), 2\rho) \geq \inf(1, 2\rho)$.
We deduce then by induction that $v([p]_F^n(\alpha)) \geq inf(1, 2^n\rho)$, and we then choose n so that $2^n\rho > \frac{1}{p-1}$. □

We can now prove the Theorem

Proof. Write $l_F(X) = \sum\limits_{n=1}^{\infty} a_n X^n$.
Since l'_F is defined over R and $l'_F(0) = 1$, then $v(na_n) \geq 0$ and $a_1 = 1$. We thus have $v(a_n) \geq -v(n)$. Put $n = p^{\sigma(n)}$, then $v(n) \leq \sigma(n)$.
Now $v(a_n\alpha^n) = nv(\alpha) + v(a_n) \geq p^{\sigma(n)}v(\alpha) - v(n) \geq p^{\sigma(n)}v(\alpha) - \sigma(n)$, which tends to ∞ as $n \to \infty$, provided that $v(\alpha) > 0$. Hence $l_F(\alpha)$ converges if $v(\alpha) > 0$.
Write $e_F(X) = \sum\limits_{n=1}^{\infty} b_n X^n$. Choose $\beta \in \overline{R}$ so that $v(\beta) = \frac{1}{p-1}$, e.g. $\beta^{p-1} = p$.
Then $v(a_n\beta^{n-1}) \geq \frac{n-1}{p-1} - v(n)$ which is ≥ 0 when $v(n) = 0$.
If $v(n) > 0$, we continue $\frac{n-1}{p-1} - v(n) \geq \frac{p^{v(n)}-1}{p-1} - v(n) = 1 + p + p^2 + ... + p^{v(n)} - v(n) \geq 0$.
Therefore $(\beta^{-1} \circ l_F \circ \beta)(X) = \sum\limits_{n=1}^{\infty} a_n\beta^{n-1}X^n$ has coefficients in $\overline{R}$, and leading coefficient 1. Its inverse under composition $(\beta^{-1} \circ e_F \circ \beta)(X) = \sum\limits_{n=1}^{\infty} b_n\beta^{n-1}X^n$ is thus also a power series with integral coefficients and leading coefficient 1. Hence $v(b_n\beta^{n-1}) \geq 0$.
Take $\alpha \in J_{\frac{1}{p-1}}$, i.e., such that $v(\alpha) > \frac{1}{p-1}$.
Then $v(b_n\alpha^n) = v(b_n\beta^{n-1}(\frac{\alpha}{\beta})^{n-1}\alpha) = v(b_n\beta^{n-1}) + v((\frac{\alpha}{\beta})^{n-1}) + v(\alpha) \to \infty$ as $n \to \infty$, since $v(\frac{\alpha}{\beta}) > 0$. Thus $e_F(\alpha)$ converges if $\alpha \in J_{\frac{1}{p-1}}$.
Moreover, $v(b_n\alpha^n) > v(\alpha)$, if $n > 1$. Therefore $e_F(\alpha) = \alpha + \alpha'$ where $v(\alpha') > v(\alpha)$. Hence we deduce that, if $\alpha \in J_{\frac{1}{p-1}}$ then $v(e_F(\alpha)) = v(\alpha)$. Similarly, if $\alpha \in J_{\frac{1}{p-1}}$, then $v(l_F(\alpha)) = v(\alpha)$. The maps $\alpha \mapsto e_F(\alpha)$ and $\alpha \mapsto l_F(\alpha)$ thus define inverse bijections $J_{\frac{1}{p-1}} \to J_{\frac{1}{p-1}}$. Under l_F therefore the group of points $F(J_{\frac{1}{p-1}})$ becomes isomorphic to the additive group of $J_{\frac{1}{p-1}}$, and the inverse ismorphism is given by e_F. We have thus established i) and iii).
Since $\overline{K}^+$ is torsion free, then $\Lambda(F) \subseteq Ker(l_F)$.
Let $\alpha \in Ker(l_F)$. By Lemma 1.45, $[p]_F^n(\alpha) \in F(J_{\frac{1}{p-1}})$ for some integer $n > 0$.
Since $l_F([p]_F^n(\alpha)) = 0$, then by iii), $[p]_F^n(\alpha) = 0$. Therefore $\alpha \in \Lambda(F)$. Thus in fact $Ker(l_F) = \Lambda(F)$.
Suppose $a \in \overline{K}^+$, since $\overline{K}^+/J_{\frac{1}{p-1}}$ is a torsion module, then $p^m a \in J_{\frac{1}{p-1}}$ for some m. Thus by iii), there exists $\alpha \in J_{\frac{1}{p-1}}$ such that $l_F(\alpha) = p^m a$. But $P(F)$ is divisible (Theorem 1.43) so there exists $\beta \in P(F)$ such that $[p]_F^m(\beta) = \alpha$. Since $p^m l_F(\beta) = p^m a$, then $l_F(\beta) = a$. We have thus shown that $l_F : P(F) \to \overline{K}^+$ is surjective and so that the sequence

$$0 \to \Lambda(F) \to P(F) \to \overline{K}^+ \to 0$$

of groups is exact. Since l_F is defined over K this is a sequence of Γ-modules. If $f \in End_R(F)$, then both $l_F \circ f$ and $f'(0) \circ l_F$ are homomorphism $F \to G_a$ with derivative $f'(0)$ at 0. They therefore coincide. From the commutative diagram

$$\begin{tikzcd}
P(F) \arrow[r] \arrow[d, "P(f)"] & \overline{K}^{+} \arrow[d, "f'(0)"] \\
P(F) \arrow[r] & \overline{K}^{+}
\end{tikzcd}$$

we deduce that $P(F) \to \overline{K}^{+}$ is a homomorphism of $End_R(F)$-modules. □

The following theorem is a converse of Theorem 1.38. It shows that every finite subgroup of $\Lambda(F)$ arises as the kernel of some isogeny. We will admit it (for details see [Fro68] Chapter IV, section 2, Theorem 4).

Theorem 1.46. *(Lubin)*
Let ϕ be a finite subgroup of $\Lambda(F)$. Let L be the fixed field of the stabilizer of ϕ in $Gal(\overline{K}/K)$ and let S denote the integers of L. Then there exist a formal group G and an isogeny $f : F \to G$ both defined over S, so that :
i) $Ker(f) = \phi$ (we write $Ker(f)$ for $Ker(P(f))$)
ii) If $g : F \to H$ is an isogeny with $Ker(g) \supseteq \phi$ then there exists a unique isogeny $h : G \to H$ such that $g = h \circ f$. If g and H are defined over the integers S_1, of some finite extension L_1 of L, then so is h.

Corollary 1.47. *If there exists an isogeny $F \to G$ defined over some S_1 then there exists an isogeny $G \to F$ defined over S_1.*

Proof. If $f : F \to G$ is an isogeny, then suppose the exponent of $Ker(f)$ is p^r. Then $Ker(f) \subseteq Ker([p]^r_F)$. By Theorem 1.46, there exists an isogeny $h : G \to F$ such that $h \circ f = [p]^r_F$, and h is defined over S_1. □

Corollary 1.48. *Either $Hom_S(F, G) = 0$, or $Hom_S(F, G)$ as an $End_S(F)$-modules is isomorphic to a non-zero ideal of $End_S(F)$, and as an $End_S(G)$-module is isomorphic to a non-zero ideal of $End_S(G)$.*

Proof. Suppose $Hom_S(F, G) \neq 0$. By Corollary 1.47, there exists an isogeny $g : G \to F$ over S. The map $f \mapsto g \circ f$ is an injective homomorphism $Hom_S(F, G) \to End_S(F)$ of $End_S(F)$-modules, whose image is a non-zero ideal.
Analogously for the map $f \mapsto f \circ g$. □

Corollary 1.49. *If $Hom_S(F, G) \neq 0$ then :*
i) The quotient field of $D(End_S(F))$ and of $D(End_S(G))$ coincide.
ii) The rank of $Hom_S(F, G)$ over $\mathbb{Z}_p$ is the rank of $End_S(F)$ (and of $End_S(G)$).

Proof. See [Fro68] Chapter IV, section 2 Corollary 3 □

1.4 The Tate Module

The notation is the same as in the section on group of points. We shall frequently write $[p]_F^n$ in place of $\Lambda([p]_F^n)$. We know that $[p]_F^n$ yields a homomorphism

$$\rho_m^{n+m} : Ker([p]_F^{n+m}) \to Ker([p]_F^m)$$

(here $Ker([p]_F^m$ stands as an abbreviation for $Ker(\Lambda([p]_F^m))$).
These maps, and the groups $Ker([p]_F^m)$ define an inverse system of Abelian groups.

Definition 1.50. The inverse limit of this system is called the Tate module, denoted $T(F)$.

The elements of $T(F)$ can be written as sequences

$$\begin{aligned}&(a_1, a_2, ...)\ a_i \in \Lambda(F)\\ &[p]_F(a_1) = 0,\ [p]_F(a_{i+1}) = a_i\end{aligned}$$

Similarly we have an inverse system, indexed by the integers $m \geq 0$, whose groups all coincide with $\Lambda(F)$ (that means that we put $\Lambda(F)_n = \Lambda(F)$ for all n), the map from $\Lambda(F)_{n+m}$ to $\Lambda(F)_m$ being the endomorphism $[p]_F^n$. Let $V(F)$ be the inverse limit. The element of $V(F)$ can be written as sequences

$$\begin{aligned}&\overline{a} = (a_0, a_1, ...)\ a_i \in \Lambda(F)\\ &[p]_F(a_{i+1}) = a_i\end{aligned}$$

The map $\overline{a} \mapsto a_0$ is a homomorphism $V(F) \to \Lambda(F)$, whose kernel may clearly be identified with $T(F)$, i.e., we get an exact sequence

$$0 \to T(F) \to V(F) \to \Lambda(F) \to 0 \tag{1.1}$$

Equivalent description :
We start with the isomorphism $Hom_{\mathbb{Z}_p}(\frac{1}{p^n}\mathbb{Z}_p/\mathbb{Z}_p, \Lambda(F)) \cong Ker([p]_F^n)$, which takes f into the image $f(\frac{1}{p^n} \bmod \mathbb{Z}_p)$. The direct system $\frac{1}{p^n}\mathbb{Z}_p/\mathbb{Z}_p$ with limit $\mathbb{Q}_p/\mathbb{Z}_p$ gives rise to an inverse system by means of the functor $Hom_{\mathbb{Z}_p}(-, \Lambda(F))$, which under the above isomorphism goes over the inverse system $(Ker([p]_F^m, \rho_m^{n+m})$. Hence in fact

$$Hom_{\mathbb{Z}_p}(\mathbb{Q}_p/\mathbb{Z}_p, \Lambda(F)) \cong T(F) \tag{1.2}$$

Similarly from the direct system $\frac{1}{p^n}\mathbb{Z}_p$ with limit $\mathbb{Q}_p$ one obtains an isomorphism

$$Hom_{\mathbb{Z}_p}(\mathbb{Q}_p, \Lambda(F)) \cong V(F) \tag{1.3}$$

and of course we have the natural isomorphism

$$Hom_{\mathbb{Z}_p}(\mathbb{Z}_p, \Lambda(F)) \cong \Lambda(F)$$

By means of these isomorphisms the sequence (1.1) can now be interpreted as being obtained by applying the functor $Hom_{\mathbb{Z}_p}(-, \Lambda(F))$ to the sequence

$$0 \to \mathbb{Z}_p \to \mathbb{Q}_p \to \mathbb{Q}_p/\mathbb{Z}_p \to 0$$

Alternatively (1.1) may be viewed as obtained from this sequence by tensoring over $\mathbb{Z}_p$ with $T(F)$.
Another consequence of (1.2) and (1.3), together with the isomorphisms

$$Hom_{\mathbb{Z}_p}(\mathbb{Q}_p/\mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p) \cong \mathbb{Z}_p$$
$$Hom_{\mathbb{Z}_p}(\mathbb{Q}_p, \mathbb{Q}_p/\mathbb{Z}_p) \cong \mathbb{Q}_p$$

and Theorem 1.43 ii) is :

Proposition 1.51. *$T(F) \cong \mathbb{Z}_p^{(h)}$ and $V(F) \cong \mathbb{Q}_p^{(h)}$*

We shall in fact view $T(F)$ as a lattice (= free $\mathbb{Z}_p$-module of maximal rank) in the vector space $V(F)$.

The groups and maps of (1.1) are clearly functorial. Here in particular $T(F)$ and $V(F)$, as well as $\Lambda(F)$, are $End_R(F)$-modules, and the maps of (1.1) are homomorphisms of $End_R(F)$-modules. Moreover, an isogeny $f : F \to G$ gives rise to a commutative diagram (1.4)

$$\begin{tikzcd}
T(F) \arrow[r] \arrow[d, "T(f)"] & V(F) \arrow[r] \arrow[d, "V(f)"] & \Lambda(F) \arrow[d, "\Lambda(f)"] \\
T(G) \arrow[r] & V(G) \arrow[r] & \Lambda(G)
\end{tikzcd}$$

Proposition 1.52. *$V(f)$ is an isomorphism and $T(f)$ is injective, with $Coker(T(f)) \cong Ker(\Lambda(f))$ finite.*

Proof. If $dim_{\mathbb{Q}_p}(Ker(V(f))) = s$, then $Ker(\Lambda(f))$ contains the submodule $Ker(V(f))/Ker(T(f)) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^s$. As $Ker(\Lambda(f))$ is finite (Theorem 1.38), $s = 0$ and so $Ker(V(f)) = 0$. Similarly, as $Coker(\Lambda(f)) = 0$ (again by the same theorem) we conclude that $Coker(V(f)) = 0$. Now it follows that $Ker(T(f)) = 0$ and $Ker(\Lambda(f)) \cong Coker(T(f))$ (By Snake lemma). □

From this proposition, it follows that $Im(T(f))$ is a lattice in $V(G)$, a sublattice of $T(G)$. (The term lattice L in a vector space V is always to imply that L is of maximal rank, i.e., spans V).
We shall write $L(f)$ for the inverse image of $T(G)$ under $V(f)$, i.e., for $V(f)^{-1}(T(G))$. This is a superlattice of $T(F)$ in $V(F)$.

The Galois group $\Gamma = Gal(\overline{K}/K)$ acts on $V(F)$ and $T(F)$ as well as on $\Lambda(F)$ and the maps of (1.1) are homomorphisms of Γ-modules. We are assuming throughout that the given formal group F is defined over R, but we do not assume other formal groups $G, H, ...$ to be necessarily defined over R, they may be defined over the integers in some finite extension of R. If however G as well as the isogeny $f : F \to G$ are defined over R, then the diagram (1.4) is one of Γ-module homomorphisms and so both $Im(T(f))$ and $L(f)$ are Γ-modules.

Theorem 1.53. *(Lubin)*
i) Let L be a sublattice of $T(F)$ in $V(F)$. Then there exists an isogeny $f : H \to F$ so that $L = Im(T(f))$, and if L is stable under Γ then H and f may be chosen to be defined over R. If $Im(T(f_1)) \subseteq Im(T(f))$, f_1 being an isogeny $H_1 \to F$ then there is an isogeny $h : H_1 \to H$ with $f_1 = f \circ h$. In particular $Im(T(f))$ determines H and f to within isomorphism.
ii) Let L be a supperlattice of $T(F)$ in $V(F)$. Then there exists an isogeny $g : F \to G$ with $L(f) = L$. If $L(g) \subseteq L(g_1)$, g_1 being an isogeny $F \to G_1$ then there is an isogeny $h : G \to G_1$ so that $h \circ g = g_1$. In particular $L(g)$ determines G and g to within isomorphism.

Proof. First that of ii). $L/T(F)$ is a finite subgroup of $V(F)/T(F) = \Lambda(F)$. Taking quotients mod $T(F)$ we thus get an order preserving bijection from the set of supperlattices L to the set of finite subgroups of $\Lambda(F)$, which also preserves stability under Γ. Note also that if $g : F \to G$ is an isogeny, then $Ker(\Lambda(g)) = L/T(F)$ precisely when $V(g)L = T(G)$, i.e., $L = L(g)$.
ii) now follows from Theorem 1.46

Next the proof of i). Let in the sequel n be an integer with $p^{-n}L = L' \supseteq T(F)$ and so, by ii), there exists an isogeny $g : F \to H$ with $L' = L(g)$, i.e., with $V(g)L' = T(H)$. Now $p^n L' = L \subseteq T(F)$ implies that $p^n Ker(\Lambda(g)) = 0$, i.e., that $Ker(\Lambda(g)) \subseteq Ker([p]_F^n)$. By Theorem 1.46, there is an isogeny $f : H \to F$ with $f \circ g = [p]_F^n$. But then $Im(T(f)) = V(f \circ g)L' = p^n L' = L$ as required. Let $f_1 : H_1 \to F$ be an isogeny with $L_1 = Im(T(f_1)) \subseteq Im(T(f)) = L$. We may suppose that $Im(T(f_1)) \supseteq p^n T(F)$. Let g as above. As by hypothesis, $p^n Ker(\Lambda(f_1)) = 0$, there is an isogeny $g_1 : F \to H_1$ with

$g_1 \circ f_1 = [p]^n_{H_1}$. But then also $f_1 \circ g_1 = [p]_F = f \circ g$. Now we have

$$Ker(\Lambda(g_1)) = p^{-n}Im(T(f_1))/T(f) \subseteq p^{-n}Im(T(f))/T(F) = Ker(\Lambda(g))$$

Therefore by Theorem 1.46, there is an isogeny $h : H_1 \to H$ with $g = h \circ g_1$, i.e., $f \circ h \circ g_1 = f_1 \circ g_1$, and so $f_1 = f \circ h$. This completes the proof of the theorem. □

Remark 1.54. i) Note that in the above construction the choice of n is immaterial (of course within the stated conditions). If say $m \geq n$, then $g_1 = g \circ [p]^{m-n}_F$ replaces g and still $f \circ g_1 = [p]^m_F$.
ii) Note secondly that if L is Γ-stable then so is L'. Choose then g to be defined over R. Hence g^{-1} (inverse under substitution) is defined over K, and thus $f = [p]^n_F \circ g^{-1}$ is defined over K, hence over R.

We can extend the injective map

$$Hom_{\overline{R}}(F,G) \to Hom(V(F),V(G))$$

to a map

$$\mathbb{Q}_p \otimes_{\mathbb{Z}_p} Hom_{\overline{R}}(F,G) \to Hom(V(F),V(G))$$

which we shall still denote by V and which remains injective. Viewing $Hom_{\overline{R}}(F,G)$ as contained in $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} Hom_{\overline{R}}(F,G)$ we have :

Theorem 1.55. *Let $g \in \mathbb{Q}_p \otimes_{\mathbb{Z}_p} Hom_{\overline{R}}(F,G)$. Then $g \in Hom_{\overline{R}}(F,G)$ if and only if $V(g)$ maps $T(F)$ into $T(G)$.*

Proof. The "Only if" is trivial
"If" : Let $p^n g = h \in Hom_{\overline{R}}(F,G)$. Then $Im(T(h)) \subseteq p^n T(G)$, whence by Theorem 1.38, $h = [p]^n_G \circ h_1$, $h_1 \in Hom_{\overline{R}}(F,G)$. But then $g = h_1$. □

Write now $E_F = D(End_{\overline{R}}(F))$ and let L_F be the quotient field of E_F in $\overline{K}$. Then of course D induces an isomorphism

$$\mathbb{Q}_p \otimes_{\mathbb{Z}_p} End_{\overline{R}}(F) \cong L_F$$

We view $T(F)$ as an E_F-module and so $V(F)$ as an L_F-module. By Theorem 1.55

$$E_F = \{a \in L_F | aT(F) \subseteq T(F)\}$$

Let $g : G \to F$ be an isogeny. We know (Corollary 1.49) that $L_F = L_G$, and in fact $V(g)$ is an isomorphism of L_F-modules. Hence :

Corollary 1.56. *(Lubin)*

$$E_G = \{a \in L_F | aIm(T(g)) \subseteq Im(T(g))\}$$

Let R be a discrete valuation ring with finite residue class of p^s elements. Denote by $\mathfrak{M}$ the maximal ideal of R and take π in R so that $\mathfrak{M} = \pi R$.

Lemma 1.57. *Suppose $f(X)$ and $g(X)$ are power series over R satisfying*

$$\begin{aligned} f(X) &\equiv g(X) \equiv \pi X \ \mathit{mod\ deg\ 2} \\ f(X) &\equiv g(X) \equiv X^q \ \mathit{mod}\ \mathfrak{M} \end{aligned}$$

where $q = p^{sl}$ for some positive integer l. Let $L(X_1, ..., X_n)$ be a linear form over R. Then there exists a power series $F(X_1, ..., X_n)$ over R satisfying the conditions :
i) $F(X_1, ..., X_n) = L(X_1, ..., X_n)$ (mod deg 2)
ii) $f(F(X_1, ..., X_n)) = F(g(X_1), ..., g(X_n))$
These conditions determine F uniquely over the quotient field of R.

Proof. Our aim is to construct a sequence (F_m) of polynomials over R in $X_1, ..., X_n$ with the properties :

$$\begin{aligned} &F_m(X_1, ..., X_n) \text{ is of degree } m-1 \\ &F_m(X_1, ..., X_n) \equiv L(X_1, ..., X_n) \text{ (mod deg 2)} \\ &f(F_m(X_1, ..., X_n)) \equiv F_m(g(X_1), ..., g(X_n)) \text{ (mod deg m)} \\ &F_{m+1}(X_1, ..., X_n) = F_m(X_1, ..., X_n) + \Delta(X_1, ..., X_n) \end{aligned}$$

where $\Delta(X_1, ..., X_n)$ is a homogeneous polynomial of degree m.
These conditions imply (here we work with congruences modulo degree $m+1$) that :

$$\begin{aligned} F_{m+1}(g(X_1), ..., g(X_n)) &= F_m(g(X_1), ..., g(X_n)) + \Delta(g(X_1), ..., g(X_n)) \\ &\equiv F_m(g(X_1), ..., g(X_n)) + \Delta(\pi X_1, ..., \pi X_n) \\ &\equiv F_m(g(X_1), ..., g(X_n)) + \pi^m \Delta(X_1, ..., X_n) \end{aligned}$$

If we write $f(X) = \pi X + f_{(2)}(X)$, then we also have

$$\begin{aligned} f(F_{m+1}(X_1, ..., X_n)) &= f(F_m(X_1, ..., X_n) + \Delta(X_1, ..., X_n)) \\ &\equiv \pi F_m(X_1, ..., X_n) + \pi\Delta(X_1, ..., X_n) + f_{(2)}(F_m(X_1, ...X_n)) \\ &\equiv f(F_m(X_1, ..., X_n)) + \pi\Delta(X_1, ..., X_n) \end{aligned}$$

We are therefore required to find Δ satisfying the congruence :

$$F_m(g(X_1), ..., g(X_n)) + \pi^m \Delta(X_1, ..., X_n) \equiv f(F_m(X_1, ..., X_n)) + \pi\Delta(X_1, ..., X_n)$$

In other words, we must solve over the quotient field of R the congruence :

$$\Delta(X_1, ..., X_n) \equiv \frac{1}{\pi}\left(\frac{F_m(g(X_1), ..., g(X_n)) - f(F_m(X_1, ..., X_n))}{1 - \pi^{m-1}}\right)$$

There clearly exists a unique solution. But $1-\pi^{m-1}$ is a unit of R. To show that the solution has coefficients in R we must show that $F_m(g(X_1), ..., g(X_n)) - f(F_m(X_1, ..., X_n))$ has coefficients in $\mathfrak{M}$ (i.e. divisible by π). Since $f(X) \equiv g(X) \equiv X^q \pmod{\mathfrak{M}}$, then $F_m(g(X_1), ..., g(X_n)) - f(F_m(X_1, ..., X_n)) \equiv F_m(X_1^q, ..., X_n^q) - (F_m(X_1, ..., X_n))^q$ (mod $\mathfrak{M}$)

But $(F_m(X_1, ..., X_n))^q \equiv F_m^q(X_1^q, ..., X_n^q)$ (mod $\mathfrak{M}$) (F_m^q denotes the polynomial obtained from F_m by raising all the coefficients to the q-th power). As q is a power of the cardinality of the residue field, we have $F_m^q = F_m$. Hence

$$(F_m(X_1, ..., x_n))^q \equiv F_m(X_1^q, ..., X_n^q) \pmod{\mathfrak{M}}$$

and therefore

$$F_m(g(X_1), ..., g(X_n)) - f(F_m(X_1, ..., X_n)) \equiv 0 \pmod{\mathfrak{M}}$$

as required. □

Now one has :

Theorem 1.58. *(Lubin)*
Let $\mathcal{O}$ be an order over $\mathbb{Z}_p$ (contained in $\overline{R}$). Then there is a formal group F with $ht(F) = [\mathcal{O} : \mathbb{Z}_p]$ so that $E_F = \mathcal{O}$.

We first find an F so that $ht(F) = [\mathcal{O} : \mathbb{Z}_p]$ and so that L_F is the quotient field of $\mathcal{O}$. Let K be the quotient field of $\mathcal{O}$, R the valuation ring of K. We then have :

Proposition 1.59. *There is a formal group F of height $h = [K : \mathbb{Q}_p]$ so that $E_F = R$.*

Proof. (Constructon of Lubin-Tate). Let π generate the maximal ideal $\mathfrak{M}$ of R and let $q = card(R/\mathfrak{M}) = p^s$. By Lemma 1.57, there is a unique $F(X, Y) \in R[[X, Y]]$ with

$$F(X, Y) \equiv X + Y \text{ mod deg } 2$$

and with

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

where $f(X) = \pi X + X^q$. We shall then show below that F is a formal group, so that the map $D : End_E(F) \to R$ is surjective, hence bijective.

Moreover $[p]_F = f^e \circ u$, where e is the ramification index of $K/\mathbb{Q}_p$ and u is a unit of $End_R(F)$. Therefore $ht([p]_F) = e.s = [K : \mathbb{Q}_p] = h$. Thus F is of height h, and $K \subseteq L_F$. As $[L_F : \mathbb{Q}_p] | [K : \mathbb{Q}_p] = h$, it follows that $K = L_F$ and $R = E_F$.
Let $a \in R$ and construct along the line of Lemma 1.57, a power series $[a](X)$ over R with

$$[a](X) \equiv aX \text{ mod degree } 2$$

and

$$f \circ [a] = [a] \circ f$$

We have then to show that :

$$\begin{aligned} &F(X,Y) = F(Y,X) \\ &F(F(X,Y),Z) = F(X,F(Y,Z)) \\ &[a](F(X,Y)) = F([a](X),[a](Y)) \end{aligned}$$

and it will follow that F is indeed a commutative formal group and $[a]$ is an endomorphism of F with $D([a]) = a$. In each case this is done via the uniqueness part of Lemma 1.57. Thus e.g. the two sides in the last equation are both solutions of the problem of finding G, so that $G(f(X), f(Y)) = f(G(X,Y))$ and $G(X,Y) \equiv aX + aY$ (mod degree 2). □

Proposition 1.60. *Let F be a formal group of finite height and let $\mathcal{O}$ be an order with quotient field L_F. Then there is a formal group G isogeneous to F so that $\mathcal{O} = E_G$.*

Proof. Let L be any sublattice of $T(F)$ so that $\mathcal{O} = \{a \in L_F \mid aL \subseteq L\}$. Such sublattices exist, e.g., $L = \mathcal{O}x$ with $0 \neq x \in T(F)$. By Theorem 1.53, there is an isogeny $g : G \to F$ so that $L = Im(T(g)$. By Corollary 1.55, $E_G = \mathcal{O}$. □

Theorem 1.58 now follows from the last two propositions.

1.4.1 The Tate module as a module over $\Gamma = Gal(\overline{K}/K)$

We already know that $T(F)$, and hence $V(F)$ is a Γ-module. An element γ of Γ will leave $T(F)$ and hence $V(F)$ elementwise fixed if and only if γ leaves $\Lambda(F)$ fixed. But $\Lambda(F)$ is just a subset of $\overline{K}$, and so we see that the representation of Γ on $V(F)$ (or on $T(F)$) is a faithful representation of its quotient group $Gal(K(\Lambda(F))/K)$.
Let $t : \Gamma \to GL(T(F))$ (automorphism group of $T(F)$) be the homomorphism with $xt(\gamma) = \gamma x$ for $x \in T(F)$. $GL(T(F))$ is a topological group, a fundamental system of neighbourhood of the identity being the subgroup of automorphism $a \equiv 1$ (mod p^n)

(i.e., of form $1 + sp^n$, 1=identity, s an endormorphism of $T(F)$). t is continuous. To see this we only have to note that $t(\gamma) \equiv 1 \pmod{p^n}$ if and only if $\rho_n t(\gamma) = \rho_n t(1)$, where ρ_n is the map $T(F) \to Ker([p]_F^n)$ (we consider here the definion of $T(F)$ as an inverse limit). But $\rho_n t(\gamma) = \rho_n t(1)$ if and only if γ leaves $Ker([p]_F^n) \subseteq \overline{K}$ fixed.
We now consider the Γ-module $V(F)$.

Theorem 1.61. *$V(F)$ is an irreducible Γ-module over $\mathbb{Q}_p$ (i.e., the only $\mathbb{Q}_p$-subspace of $V(F)$ which are Γ-modules are $V(F)$ and 0).*

Proof. Denote by Γ_s the orbit under Γ of an element s in a Γ-set S. What we have to show is that if $0 \neq x \in V(F)$ then the subspace generated by Γx is the whole of $V(F)$. It clearly suffices to consider an $x \in T(F)$, with $x \notin pT(F)$.
Let then M be the $\mathbb{Z}_p$-submodule of $V(F)$ generated by Γx. M is a free $\mathbb{Z}_p$-module of rank $s \leq h$ and we have to show that $s \geq h$.
Write ρ_n for the surjection $T(F) \to Ker([p]_F^n)$ associated with the inverse limit $T(F) = \lim\limits_{\leftarrow} Ker([p]_F^n)$. $M \subseteq T(F)$ and so $\rho_n(M)$ is defined. It is the direct product of at most s cyclic subgroups, and so the number of elements in $\rho_n(M)$, not in $p\rho_n(M)$ is at most $p^{ns} - p^{(n-1)s}$. Write $\alpha_n = \rho_n(x)$. Then each element of $\Gamma\alpha_n$ lies in $\rho_n(M)$, and not in $p\rho_n(M)$. Therefore

$$card(\Gamma\alpha_n) \leq p^{(n-1)s}(p^s - 1).$$

The left hand side is the number of conjugates of α_n over K, and so equal to the degree $[K(\alpha_n) : K]$. We thus get the inequality

$$[K(\alpha_n) : K] \leq p^{(n-1)s}(p^s - 1) \tag{1.4}$$

holding for all n.
Now note that

$$[p]_F(\alpha_1) = 0, \ \alpha_1 \neq 0, \ [p]_F(\alpha_{n+1}) = \alpha_n \tag{1.5}$$

We shall show that this implies the existence of a positive constant c so that

$$[K(\alpha_n) : K] \geq cp^{nh}, \text{ for all } n \tag{1.6}$$

Comparison of (1.5) with (1.7) as $n \to \infty$ yields then the required inequality $s \geq h$.
To get (1.7) from (1.6) we require a lemma, to be proved later.

Lemma 1.62. *Let $\alpha, \beta \in P(F)$, $[p]_F(\alpha) = \beta$*
a) If $v(\beta) \leq 1$, then $v(\alpha) \leq \frac{v(\beta)}{p}$
b) If $v(\beta) \leq \frac{1}{e}$, e being the ramification index of K over $\mathbb{Q}_p$, then $v(\alpha) \leq \frac{v(\beta)}{p^h}$

We apply the lemma to complete the proof of the theorem. Return to (1.6). By Theorem 1.44, $v(\alpha_1) \leq \frac{1}{p-1} \leq 1$. From the lemma, form a), we obtain by induction the inequality $v(\alpha_n) \leq \frac{1}{p^{n-1}}$. Therefore for some n_0, $v(\alpha_{n_0}) \leq \frac{1}{e}$. Now use form b) in the lemma to get for $n \geq n_0$ the inequality $v(\alpha_n) \leq \frac{1}{ep^{(n-n_0)h}}$. On the other hand let e_n be the ramification index of $K(\alpha_n)/K$. Then certainly $e_n v(\alpha_n) \geq \frac{1}{e}$, $\frac{1}{e}$ being the least strictly positive value of v on K. Hence finally,

$$[K(\alpha_n) : K] \geq e_n \geq \frac{1}{ev(\alpha_n)} \geq p^{nh}c, \ c = p^{-n_0 h}$$

□

It remains to prove the lemma

Proof. Let $[p]_F(X) = \sum\limits_{n=1}^{\infty} a_n X^n$. Here $a_1 = p$.
Apply Theorem 1.8 to the ring R/pR and the reduction of $[p]_F(X)$ mod pR. This tell us that $v(a_n) \geq v(p) = 1$ whenever $p \nmid n$, i.e., in particular

$$v(a_n) \geq 1 \text{ for } 0 < n < p \tag{1.7}$$

Similarly, applying the same reasoning to the residue field of R, one gets

$$v(a_n) \geq \frac{1}{e} \text{ for } 0 < n < p^h \tag{1.8}$$

Let now $v(a_j\alpha^j) = \inf\limits_n v(a_n\alpha^n)$. Then $v(\beta) \geq v(a_j\alpha^j)$ and so

$$jv(\alpha) \leq v(a_j) + jv(\alpha) = v(a_j\alpha^j) \leq v(\beta) \tag{1.9}$$

If first $v(\beta) \leq 1$ then for $0 < n < p$, we have by (1.8)

$$v(a_n\alpha^n) = v(a_n) + nv(\alpha) > 1 \geq v(\beta) \geq v(a_j\alpha^j)$$

and so $j \geq p$, whence by (1.10) $pv(\alpha) \leq v(\beta)$
If next $v(\beta) \leq \frac{1}{e}$, then we deduce similarly that $j \geq p^h$, whence again by (4.10) $p^h v(\alpha) \leq v(\beta)$. □

2 The Period rings B_{dR} and B_{cris}

2.1 Witt Vectors

In this section we will recall some properties about Witt vectors and the basic definitions. It will be useful in the sequel for the construction of the rings of period B_{dR} and B_{cris}.
Fix p a prime number and let $\underline{X} = (X_0, X_1, ...)$ be a sequence of indeterminates.

Definition 2.1. Let $n \in \mathbb{Z}_{\geq 0}$, the n-th Witt polynomial is :

$$\Phi_n(\underline{X}) = X_0^{p^n} + pX_1^{p^{n-1}} + p^2X_2^{p^{n-2}} + ... + p^nX_n$$

If A is a ring, the ghost map is :

$$\begin{aligned} \Phi_A : A^{\mathbb{Z}_{\geq 0}} &\to A^{\mathbb{Z}_{\geq 0}} \\ \underline{a} = (a_0, a_1, ...) &\mapsto (\Phi_n(\underline{a}))_{n \in \mathbb{Z}_{\geq 0}} \end{aligned}$$

Lemma 2.2. *Let A be a ring, $x, y \in A$ such that $x \equiv y$ mod pA. Then*

$$x^{p^n} \equiv y^{p^n} \ mod \ p^{n+1}A \ \forall n \in \mathbb{Z}_{\geq 0}$$

.

Proof. We proceed by induction on $n \in \mathbb{Z}_{\geq 0}$.
Assume $n > 0$ and $x^{p^{n-1}} \equiv y^{p^{n-1}}$ mod p^nA. Write $x^{p^{n-1}} = y^{p^{n-1}} + p^nZ$.
Then $x^{p^n} = y^{p^n} + \sum_{k=1}^{p-1} \binom{p}{k} p^{kn} Z^k y^{(p-k)p^{n-1}} + p^{pn}Z^p \equiv y^{p^n}$ mod $p^{n+1}A$ and we are done. □

Lemma 2.3. *(Dwork)*
Assume $\varphi : A \to A$ is a ring homomorphism such that $\varphi(a) \equiv a^p$ mod pA for all $a \in A$. Then a sequence $(x_n)_n \in A^{\mathbb{Z}_{\geq 0}}$ lies in the image of Φ_A if and only if we have $\varphi(x_n) \equiv x_{n+1}$ mod $p^{n+1}A$ for all $n \in \mathbb{Z}_{\geq 0}$.

Proof. Let $\underline{a} = (a_0, a_1, ...) \in A^{\mathbb{Z}_{\geq 0}}$.
As φ is a ring homomorphism, we have : $\varphi(\Phi_n(\underline{a})) = \sum_{i=0}^{n} p^i \varphi(a_i)^{p^{n-i}}$. The previous lemma implies that $\varphi(a_i)^{p^{n-i}} \equiv a_i^{p^{n+1-i}}$ mod $p^{n+1-i}A$. So $p^i\varphi(a_i)^{p^{n-i}} \equiv p^i a_i^{p^{n+1-i}}$ mod $p^{n+1}A$. Thus $\varphi(\Phi_n(\underline{a})) = \sum_{i=0}^{n} p^i a_i^{p^{n+1-i}}$ mod $p^{n+1}A$. But $\sum_{i=0}^{n} p^i a_i^{p^{n+1-i}} = \Phi_{n+1}(\underline{a}) - p^{n+1}a_{n+1}$.
Hence $\varphi(\Phi_n(\underline{a})) \equiv \Phi_{n+1}(\underline{a})$ mod $p^{n+1}A$.

Conversely, assume $(x_n)_n \in A^{\mathbb{Z}_{\geq 0}}$ is such that $\varphi(x_n) \equiv x_{n+1} \bmod p^{n+1}A$ for all n.
We construct $\underline{a} = (a_0, a_1, ...) \in A^{\mathbb{Z}_{\geq 0}}$ inductively such that $x_n = \Phi_n(\underline{a})$ for all $n \in \mathbb{Z}_{\geq 0}$.
Put $a_0 = x_0$. Let $n \in \mathbb{Z}_{\geq 0}$ be such that $a_0, a_1, ..., a_n$ have been constructed such that for all $k \in \{0, ..., n\},\ x_k = \Phi_k(a_0, a_1, ..., a_k)$.
Then $\varphi(x_n) = \varphi(\Phi_n(a_0, a_1, ..., a_n)) = \sum\limits_{i=0}^{n} p^i a_i^{p^{n+1-i}} \bmod p^{n+1}A$ i.e. $x_{n+1} \equiv \sum\limits_{i=0}^{n} p^i a_i^{p^{n+1-i}} \bmod p^{n+1}A$.
This implies that $x_{n+1} - \sum\limits_{i=0}^{n} p^i a_i^{p^{n+1-i}} = p^{n+1}a_{n+1}$ for some $a_{n+1} \in A$.
Hence $x_{n+1} = \Phi_{n+1}(a_0, a_1, ..., a_{n+1})$. □

Proposition 2.4. *There exist unique sequences of polynomials* $(S_n(\underline{X}, \underline{Y}))_{n \in \mathbb{Z}_{\geq 0}}$,$(P_n(\underline{X}, \underline{Y}))_{n \in \mathbb{Z}_{\geq 0}}$ *in* $Z[\underline{X}, \underline{Y}]$ *and* $(I_n(\underline{X}))_{n \in \mathbb{Z}_{\geq 0}}$ *in* $Z[\underline{X}]$ *such that :*

$$\begin{aligned}
&\Phi_n(S_0(\underline{X}, \underline{Y}), ..., S_n(\underline{X}, \underline{Y})) = \Phi_n(\underline{X}) + \Phi_n(\underline{Y}) \\
&\Phi_n(P_0(\underline{X}, \underline{Y}), ..., P_n(\underline{X}, \underline{Y})) = \Phi_n(\underline{X})\Phi_n(\underline{Y}) \\
&\Phi_n(I_0(\underline{X}), ..., I_n(\underline{X})) = -\Phi_n(\underline{X})
\end{aligned}$$

Proof. Put $A = \mathbb{Z}[\underline{X}, \underline{Y}]$. Let $\varphi : A \to A$ be the unique ring endomorphism such that $\varphi(X_i) = X_i^p$ and $\varphi(Y_i) = Y_i^p$ for all $i \in \mathbb{Z}_{\geq 0}$. We have : $\varphi(a) \equiv a^p \bmod pA$,
$\Phi_n(\varphi(\underline{X})) = \Phi_{n+1}(\underline{X}) - p^{n+1}X_{n+1}$ and $\Phi_n(\varphi(\underline{Y})) = \Phi_{n+1}(\underline{Y}) - p^{n+1}Y_{n+1}$.
Hence $\varphi(\Phi_n(\underline{X}) + \Phi_n(\underline{Y})) = \Phi_{n+1}(\underline{X}) + \Phi_{n+1}(\underline{Y}) \bmod p^{n+1}A$. By Dwork's lemma we get that $(\Phi_n(\underline{X}) + \Phi_n(\underline{Y}))_n$ belongs to $Im(\Phi_A)$, hence the existence of $(S_n(\underline{X}, \underline{Y}))_n$.
Similarly we have the existence of $(P_n(\underline{X}, \underline{Y}))_n$ and $(I_n(\underline{X}))_n$. The unicity follows from the injectivity of $\Phi_A : A^{\mathbb{Z}_{\geq 0}} \to A^{\mathbb{Z}_{\geq 0}}$. □

Definition 2.5. Let A be a ring. Put $W(A) = A^{\mathbb{Z}_{\geq 0}}$. If $\underline{a} = (a_0, a_1, ...)$ and $\underline{b} = (b_0, b_1, ...)$ are both in $W(A)$.

$$\begin{aligned}
\text{Put : } \underline{a} + \underline{b} &= (S_n(\underline{a}, \underline{b}))_{n \in \mathbb{Z}_{\geq 0}} \\
\underline{a}.\underline{b} &= (P_n(\underline{a}, \underline{b}))_{n \in \mathbb{Z}_{\geq 0}} \\
-\underline{a} &= (I_n(\underline{a}))_{n \in \mathbb{Z}_{\geq 0}}
\end{aligned}$$

Proposition 2.6. *i)* $A \mapsto (W(A), +, .)$ *is a functor from the category of commutative rings to that of sets endowed with two internal laws.*
ii) If p is not a zero divisor in A (resp. p is not invertible in A), then Φ_A *is injective (resp. bijective).*
iii) $(W(A), +, .)$ *is a commutative ring with zero* $(0, 0, ...)$ *and unit* $(1, 0, 0, ...)$.

Proof. i) and ii) are obvious.
For iii), we will use the following trick that will be useful in other proofs.

Put $B = \mathbb{Z}[X_a]_{a\in A}$, p is not a zero divisor and we have a surjective ring homomorphism $B \to A$ which maps X_a to a. As Φ_B is injective, $W(B)$ is identified with a subring of $B^{\mathbb{Z}_{\geq 0}}$ and since $W(B) \to W(A)$ is surjective, the ring axioms are satisfied in $(W(A), +, .)$. □

Definition 2.7. Let A be a ring. The Teichmüller representative of $a \in A$ is

$$[a] := (a, 0, 0, ...) \in W(A)$$

Proposition 2.8. *Let A be a ring and $a, b \in A$. Then $[a].[b] = [ab]$ in $W(A)$*

Proof. By the same trick as in the previous proof, we may assume that A has no p-torsion, thus Φ_A is injective. This implies that $\Phi_A([a]) = (a, a^p, a^{p^2}, ...)$ is multiplicative in $A^{\mathbb{Z}_{\geq 0}}$. □

Proposition 2.9. *There exists a unique sequence of polynomials $(F_n(\underline{X}))_{n\in\mathbb{Z}_{\geq 0}}$ such that $F_n(\underline{X}) \in \mathbb{Z}[X_0, X_1, ..., X_{n+1}]$ and $\Phi_n(F_0(\underline{X}), ..., F_n(\underline{X})) = \Phi_{n+1}(\underline{X})$ for all $n \in \mathbb{Z}_{\geq 0}$.*

Proof. We have to prove that $(\Phi_1(\underline{X}), \Phi_2(\underline{X}), ...) \in Im(\Phi_A)$ where $A = \mathbb{Z}[\underline{X}]$.
As A is endowed with the lift of Frobenius given by $\varphi(X_i) = X_i^p$, it is enough (by Dwork's lemma) to see that :

$$\Phi_{n+1}(\underline{X}) \equiv \varphi(\Phi_n(\underline{X})) \bmod p^{n+1}A$$

for all $n \in \mathbb{Z}_{\geq 0}$.
Unicity follows from unicity in $\mathbb{Z}[\frac{1}{p}][\underline{X}]$. □

Definition 2.10. Let A be a ring. The Frobenius map on $W(A)$ is :

$$\begin{aligned} F : W(A) &\to W(A) \\ \underline{a} = (a_0, a_1, ...) &\mapsto (F_0(\underline{a}), F_1(\underline{a}), ...) \end{aligned}$$

Proposition 2.11. *Let A be a ring.*
i) $\forall a \in A$, $F([a]) = [a^p]$
ii) $\forall n \in \mathbb{Z}_{\geq 0}$, $F_n(\underline{X}) \equiv X_n^p$ mod $p\mathbb{Z}[X]$
In particular, if $pA = 0$, then $F(a_0, a_1, ...) = (a_0^p, a_1^p, ...)$.

Proof. i) We use again our trick and thus we may assume that A has no p-torsion so the Φ_A is injective. If $a \in A$:

$$\begin{aligned} \Phi_n(F([a])) = \Phi_{n+1}([a]) &= a^{p^{n+1}} \\ &= \Phi_n([a])^p \\ &= \Phi_n([a]^p) \end{aligned}$$

ii) By induction on n, starting with $F_0(X_0,X_1) = X_0^p + pX_1$.
Assume that $n > 0$ and $F_i(\underline{X}) \equiv X_i^p \mod p\mathbb{Z}[\underline{X}]$ for $i \in \{0,1,...,n-1\}$.
Then $F_i(\underline{X})^{p^{n-i}} \equiv X_i^{p^{n+1-i}} \mod p^{n+1-i}\mathbb{Z}[\underline{X}]$, hence $p^iF_i(\underline{X})^{p^{n-i}} \equiv p^iX_i^{p^{n+1-i}} \mod p^{n+1}\mathbb{Z}[\underline{X}]$.
Also

$$\begin{aligned}\Phi_{n+1}(\underline{X}) &= \Phi_n(F_0(\underline{X}),...,F_n(\underline{X}))\\ &= \sum_{i=0}^{n} p^iF_i(\underline{X})^{p^{n-i}}\\ &\equiv p^nF_n(\underline{X}) + \sum_{i=0}^{n-1} p^iX_i^{p^{n-i}} \mod p^{n+1}\mathbb{Z}[\underline{X}]\end{aligned}$$

Therefore we have $\Phi_n(\underline{X}) \equiv p^nF_n(\underline{X}) + \Phi_{n+1}(\underline{X}) - p^nX_n^p - p^{n+1}X_{n+1} \mod p^{n+1}\mathbb{Z}[\underline{X}]$.
But $p^nF_n(\underline{X}) \equiv p^nX_n^p \mod p^{n+1}\mathbb{Z}[\underline{X}]$ i.e. $F_n(\underline{X}) \equiv X_n^p \mod p\mathbb{Z}[\underline{X}]$. □

Definition 2.12. Let A be a ring. The Veirschiebung map is :

$$\begin{aligned}V : W(A) &\to W(A)\\ \underline{a} = (a_0,a_1,...) &\mapsto (0,a_0,a_1,...)\end{aligned}$$

Proposition 2.13. *Let A be a ring and $\underline{a},\underline{b} \in W(A)$.*
i) $\Phi_A(F(\underline{a})) = (\Phi_1(\underline{a}),\Phi_2(\underline{a}),...) = f(\Phi_A(\underline{a}))$ and $\Phi_A(V(\underline{a})) = (0,p\Phi_0(\underline{a}),p\Phi_1(\underline{a}),...) = v(\Phi_A(\underline{a}))$ where $f(x_0,x_1,...) = (x_1,x_2,...)$ and $v(x_0,x_1,...) = (0,px_1,px_2,...)$.
ii) F is a ring endomorphism.
iii) V is a group endormorphism of $(W(A),+)$.
iv) $FV = pId_{W(A)}$ and $VF(\underline{a}) = (0,1,0,...).\underline{a}$.
v) $V(\underline{a}.F(\underline{b})) = V(\underline{a}.\underline{b})$, $V(\underline{a})V(\underline{b}) = pV(\underline{a}.\underline{b})$.
vi) $F(\underline{a}) \equiv \underline{a}^p \mod pW(A)$
vii) $\underline{a} = [a_0] + V(\underline{a'})$, where $\underline{a'} = (a_1,a_2,...) \in W(A)$ therefore we have $\underline{a} = \sum_{n=0}^{\infty} V^n([a_n])$.

Proof. i) is computation
By the usual trick we can assume for ii)-vii) that A is p-torsion free hence that Φ_A is injective.
ii) (resp. iii)) follows from the fact that f (resp. v) is a ring (resp. group) endomorphism of $A^{\mathbb{Z}_{\geq 0}}$.
iv) follows from the fact that $f \circ v = p$ and that $\Phi_A(0,1,0,...) = (0,p,p,...)$
v) follows from the corresponding properties of f and v.
vi) follows from $\Phi_{n+1}(\underline{X}) \equiv \Phi_n(\underline{X})^p \mod p\mathbb{Z}[\underline{X}]$ that implies that f coincides with the p-th power map on $Im(\Phi_{\mathbb{Z}[\underline{X}]})$
vii) follows from $\Phi_0(\underline{a}) = a_0$ and that $\Phi_n(\underline{a}) = a_0^{p^n} + p\Phi_{n+1}(\underline{a'})$ for $n > 0$ which means that $\Phi_n(\underline{a}) = \Phi_n([\underline{a}] + V(\underline{a'}))$ for all n. □

Definition 2.14. Let A be a ring and $n \in \mathbb{Z}_{\geq 0}$. We define a filtration on $W(A)$ by :

$$\begin{aligned} Fil^n W(A) &= V^n W(A) \\ &= \{(0, ..., 0, a_n, a_{n+1}, ...) | (a_k)_{k \geq n} \in A^{\mathbb{Z}_{\geq 0}}\}. \end{aligned}$$

Remark 2.15. $Fil^n W(A)$ is an ideal in $W(A)$.

Definition 2.16. The ring of Witt vectors of length n is : $W_n(A) = W(A)/Fil^n W(A)$

Proposition 2.17. *Let A be a ring and assume that $pA = 0$. Let $\underline{a}, \underline{b} \in W(A)$.*
i) $FV(\underline{a}) = VF(\underline{a}) = p.\underline{a}$ (i.e. $(0, 1, 0, ...) = p$)
ii) $V^n(\underline{a})V^m(\underline{b}) = V^{n+m}(F^m(\underline{a}), F^n(\underline{b}))$.
iii) The p-adic and the $V(W(A))$-adic filtrations are the same and they are finer than the topology defined by $\{Fil^n W(A)\}_n$. In particular, $W(A)$ is separated and complete for the p-adic topology.
iv) If A is perfect (i.e. the Frobenius map on A is an automorphism), then the three topologies coincide, $W(A)/pW(A) \simeq A$ and

$$\begin{aligned} \underline{a} = (a_0, a_1, ...) &= \sum_{n=0}^{\infty} V^n([a_n]) \\ &= \sum_{n=0}^{\infty} V^n F^n([a_n^{p^{-n}}]) = \sum_{n=0}^{\infty} p^n([a_n^{p^{-n}}]) \end{aligned}$$

2.1.1 Witt vectors and p-rings

Definition 2.18. Let A be a ring and R be a ring of characteristic p. The ring A is called p-ring with residue ring R if there exists $\pi \in A$ such that A is separated and complete with respect to the π-adic topology and if $R = A/\pi A$.

Remark 2.19. Since R is of characteristic p, we have $p \in \pi A$.

Definition 2.20. A p-ring with residue field R is called strict if $\pi = p$ and if p is not nilpotent in A. A is called perfect if it is strict and if R is perfect.

Example 2.21. $\mathbb{Z}_p$ is a perfect p-ring since $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$ and $\mathbb{F}_p$ is a perfect field.

Theorem 2.22. *If R is a perfect ring of characteristic p, there exists a strict p-ring $W(R)$, unique up to isomorphism, which residue field is R. Moreover, $W(R)$ has the following universal property : If A is a p-ring with residue field R', $\overline{\theta} : R \to R'$ is a ring homomorphism and $\tilde{\theta} : R \to A$ is a multiplicative application lifting $\overline{\theta}$, there exists a unique ring homomorphism $\theta : W(R) \to A$ such that if $x \in R$ then $\theta([x]) = \tilde{\theta}(x)$.*

Proof. See [Col07] Theorem 2.29 □

Remark 2.23. If R is not perfect, then there still exist strict p-ring A such that $A/pA = R$, but A is not unique anymore. Such a ring is called a Cohen ring.

Proposition 2.24. *If R and R' are both perfect rings of characteristic p, the natural application from $Hom(W(R), W(R'))$ into $Hom(R, R')$ is a bijection.*
In particular, the Frobenius morphism $x \mapsto x^p$ on R can be lifted to a Frobenius automorphism φ of $W(R)$.

Proof. If $\overline{\theta}$ is a morphism from R into R', set $\tilde{\theta}(x) = [\overline{\theta}(x)]$ and $\tilde{\theta}$ is a multiplicative application from R into $W(R')$ lifting $\overline{\theta}$. We deduce by Theorem 2.22 the surjectivity of the natural application from $Hom(W(R), W(R'))$ into $Hom(R, R')$.
If θ is a morphism from $W(R)$ into $W(R')$, we have $\theta([x]) = \lim\limits_{n\to\infty} \theta([x^{p^{-n}}])^{p^n} = [\overline{\theta}(x)]$ since $\theta([x^{p^{-n}}])$ is a lift in $W(R')$ of $\overline{\theta}(x^{p^{-n}}) = (\overline{\theta}(x))^{p^{-n}}$.
The injectivity follows from the fact that $W(R)$ being a strict p-ring, knowing $\theta([x])$ for every $x \in R$ is equivalent to know θ. □

Proposition 2.25. *If A is a p-ring with residue ring R and if $x \in A$, the following statements are equivalent :*
i) x is a unit in A.
ii) The image $\overline{x}$ of x modulo π is a unit in R.

Proof. If y has an inverse x in A, then $\overline{y}$ has an inverse $\overline{x}$ in R.
Reciprocally, if $\overline{y}$ has an inverse $\overline{x}$ in R and if y is any lift of $\overline{y}$ in A, then set $z = 1 - xy \in \pi A$ and $y(\sum\limits_{n=0}^{\infty} z^n)$ is the inverse of x. □

Corollary 2.26. *If A is a strict p-ring to which the residue ring is a field, then $B = A[\frac{1}{p}]$ is a field.*

Proof. If $x \in B\backslash\{0\}$, then there exists a unique $n \in \mathbb{Z}$ such that $p^n x \in A\backslash pA$. The last proposition tells us that $p^n x$ is a unit in A and therefore its reduction modulo π is so. □

2.2 The construction of B_{dR}

In this section, we will explain the construction of the rings of period of Fontaine, B_{dR} and B_{cris}. We will keep more or less the notations of the article of L. Berger [Ber01] that we follow mostly for this section.

2.2.1 The ring $\tilde{E}^+$

Let R be a perfect ring of characteristic p, K a p-adic field for which we will denote k its residue field and $G_K = Gal(\overline{K}/K)$. We will denote also $C = \hat{\overline{K}}$ the p-adic completion of the algebraic closure of K.

Definition 2.27. Let $\tilde{E}^+ = \varprojlim_{x \mapsto x^p} \mathcal{O}_C = \{(x^{(0)}, x^{(1)}, ...) | (x^{(i+1)})^p = x^{(i)}\}$.

We endow this set with the following sum and product : if $x = (x^{(i)})$ and $y = (y^{(i)})$ are two elements of $\tilde{E}^+$, then their sum is defined by $(x+y)^{(i)} = \lim_{j \to \infty} (x^{(i+j)} + y^{(i+j)})^{p^j}$ and their product by $(xy)^{(i)} = x^{(i)} y^{(i)}$.
With this two operations, the set $\tilde{E}^+$ becomes a ring (which is clear since operation are made componentwise and that $\mathcal{O}_C$ is a ring).

If $\sigma \in G_K$, σ acts on $\tilde{E}^+$ in the following way : if $x = (x^{(n)})_{n \geq 0} \in \tilde{E}^+$ then

$$\sigma(x) = (\sigma(x^{(n)}))_{n \geq 0}$$

Proposition 2.28. *The ring $\tilde{E}^+$ is a perfect ring of characteristic p.*

Proof. We need to prove that the Frobenius map on $\tilde{E}^+$ is an automorphism. The ring $\tilde{E}^+$ is by construction an inverse limit with transition map the Frobenius map. Therefore the surjectivity is clear. For the injectivity : suppose $(x^{(i)})^p = 0$. This implies that $x^{(i-1)} = 0$ for all $i \geq 1$. Hence, for $x \in \tilde{E}^+$, $x^p = ((x^{(0)})^p, x^{(0)}, x^{(1)}, ...) = (0, 0, ...)$ we get $x = (0, 0, ...)$
The fact that it is of characteristic p comes from the next proposition. □

Proposition 2.29. *There exists a bijection between $\tilde{E}^+$ and $\varprojlim_{x \mapsto x^p} \mathcal{O}_C/(p)$ defined by : $(x^{(n)})_{n \geq 0} \mapsto (x^{(n)} mod\ p)_{n \geq 0}$ with inverse $(x_n)_{n \geq 0} \mapsto (\lim_{m \to \infty} \hat{x}_{n+m}^{p^m})_{n \geq 0}$ where $\hat{x}_{n+m} \in \mathcal{O}_C$ is a lift of x_{n+m}.*

Proof. First we show that both maps are well defined. For the first map, it is naturally induced by the map $\mathcal{O}_C \to \mathcal{O}_C/(p)$ hence it is well defined. For the second map, let

$x \in \varprojlim_{x \mapsto x^p} \mathcal{O}_C/(p)$. So we have $x = (x_n)_{n\geq 0}$, $x_n \in \mathcal{O}_C/(p)$ and $x_{n+1}^p = x_n$. For any $n \geq 0$, we choose a lifting of x_n in $\mathcal{O}_C$, say $\hat{x}_n$. Thus $\hat{x}_{n+1}^p \equiv \hat{x}_n \text{mod } p$. By Lemma 2.2 we have that for $n, m \in \mathbb{Z}_{\geq 0}, \hat{x}_{n+m+1}^{p^{m+1}} \equiv \hat{x}_{n+m}^{p^m} \text{mod } p^{m+1}$. Hence for every $n \geq 0$, $\lim_{m\to\infty} \hat{x}_{n+m}^{p^m}$ exists in $\mathcal{O}_C$ and thus the limit is independant of the choice of the liftings. Therefore $\lim_{m\to\infty} \hat{x}_{n+m}^{p^m}$ is a lifting of x_n, $(\lim_{m\to\infty} \hat{x}_{n+m+1}^{p^{m+1}})^p = \lim_{m\to\infty} \hat{x}_{n+m}^{p^m}$ and the second map is well defined. We clearly see through the constrution that they are inverse to each other so we are done. □

If $x = (x^{(n)})_{n\geq 0} \in \tilde{E}^+$, we define a valuation v_E on $\tilde{E}^+$ by $v_E(x) = v_p(x^{(0)})$. Therefore $v_E(x) = p^n v_p(x^{(n)})$ for any $n \in \mathbb{Z}_{\geq 0}$.

Proposition 2.30. *The application v_E is a valuation on $\tilde{E}^+$ for which it is complete.*

Proof. If $x = (x^{(n)})_{n\geq 0}$ and $y = (y^{(n)})_{n\geq 0}$ are two elements of $\tilde{E}^+$, then

$$\begin{aligned} v_p((x^{(n)} + y^{(n)})^{p^n}) &= p^n v_p(x^{(n)} + y^{(n)}) \\ &\geq \inf(p^n v_p(x^{(n)}), p^n v_p(y^{(n)})) \\ &= \inf(v_E(x), v_E(y)) \end{aligned}$$

By passing to the limit we get the inequality

$$v_E(x + y) \geq \inf(v_E(x), v_E(y))$$

The other properties that we need to check are clear, hence v_E is a valuation.
Now we want to show that $\tilde{E}^+$ is complete with respect to v_E.
We have $v_E(x - y) \geq p^n$ if and only if $x^{(0)} = y^{(0)}, ..., x^{(n)} = y^{(n)}$ in $\mathcal{O}_C/(p)$. This shows that the basis of neighbourhoods of x for the induced topology of v_E which are $\{y \mid v_E(x - y) \geq p^n\}$ is also a basis of neighbourhoods of x for the topology on $(\mathcal{O}_C/(p))^{\mathbb{Z}_{\geq 0}}$, each of the factors being equipped with the discrete topology. Since a product of discrete spaces is complete, so is $\tilde{E}^+$ (a Cauchy sequence being stationnary in each component). □

Let $\mu_n = \{x \in \overline{K} \mid x^n = 1\}$ the set of n-th root of unity and consider $(\varepsilon^{(n)})_{n\in\mathbb{Z}_{\geq 0}}$ a compatible sequence of primitive p^n-th roots of unity with $\varepsilon^{(0)} = 1$, $\varepsilon^{(n)} \in \mu_{p^n} \subseteq \overline{K}$ such that $\varepsilon^{(1)} \neq 1$ and $(\varepsilon^{(n+1)})^p = \varepsilon^{(n)}$. Let $\varepsilon = (\varepsilon^{(n)})$.
It is clear that ε is an element of $\tilde{E}^+$.

Remark 2.31. Something that we will need later is that the valuation of $\varepsilon - 1$ is $\frac{p}{p-1}$.
Let's compute it :
There are two cases, whether if p is 2 or not since $v_E(\varepsilon - 1) = v_p((\varepsilon - 1)^{(0)})$ and by

definition of the addition in $\tilde{E}^+$ we get $(\varepsilon-1)^{(0)} = \lim\limits_{n\to\infty}(\varepsilon^{(n)}+(-1)^{(n)})^{p^n}$ and $(-1)^{p^n}=1$ if $p=2$ and -1 if p is odd.
If $p=2$, then

$$\begin{aligned} v_p((\varepsilon-1)^{(0)}) &= \lim_{n\to\infty} 2^n v_p(\varepsilon^{(n)}+1) \\ &= \lim_{n\to\infty} 2^n v_p((\varepsilon^{(n)}-1)+2) \\ &= \lim_{n\to\infty} 2^n v_p((\varepsilon^{(n)}-1) \end{aligned}$$

with $\varepsilon^{(n)}$ a 2^n-th root of unity, so we get $v_E(\varepsilon-1) = \lim\limits_{n\to\infty} \frac{2^n}{2^{n-1}(2-1)} = 2$.
For p odd, we get $v_p((\varepsilon-1)^{(0)}) = \lim\limits_{n\to\infty} p^n v_p(\varepsilon^{(n)}-1)$ with $\varepsilon^{(n)}$ a p^n-th root of unity, so we get $v_E(\varepsilon-1) = \lim\limits_{n\to\infty} \frac{p^n}{p^{n-1}(p-1)} = \frac{p}{p-1}$.

2.2.2 The ring $\tilde{A}^+$

We denote by $\tilde{A}^+$ the ring of Witt vectors $W(\tilde{E}^+)$ with coefficients in the perfect field ring $\tilde{E}^+$. Any element of $\tilde{A}^+$ can be written in a unique way as $x = \sum\limits_{n=0}^{\infty} p^n[x_n]$ where $(x_n)_{n\geq 0}$ is a sequence in $\tilde{E}^+$. The actions of G_K and of the Frobenius φ on $\tilde{E}^+$ can be lifted in a unique way in actions of G_K and φ on $\tilde{A}^+$. We have :

$$\varphi\left(\sum_{n=0}^{\infty} p^n[x_n]\right) = \sum_{n=0}^{\infty} p^n[x_n^p] \text{ and } \sigma\left(\sum_{n=0}^{\infty} p^n[x_n]\right) = \sum_{n=0}^{\infty} p^n[\sigma(x_n)] \text{ if } \sigma \in G_K$$

There is natural map $\tilde{E}^+ \to \mathcal{O}_C$ defined by $x = (x^{(i)})_{i\geq 0} \mapsto x^{(0)}$ which induced a homomorphism from $\tilde{E}^+$ to $\mathcal{O}_C/(p)$ (by taking the reduction modulo p) which is surjective and commutes with the action of G_K.

Proposition 2.32. *The map $\theta : \tilde{A}^+ \to \mathcal{O}_C$ defined by $\theta\left(\sum\limits_{k=0}^{\infty} p^k[x_k]\right) = \sum\limits_{k=0}^{\infty} p^k x_k^{(0)}$ is a ring homomorphism.*

Proof. Since $\tilde{A}^+ = W(\tilde{E}^+)$, consider the map

$$\theta_n(= \theta \bmod p^n) : W_n(\tilde{E}^+) = W(\tilde{E}^+)/(p^n) \to \mathcal{O}_C/(p^n)$$

defined by $\theta_n\left(\sum\limits_{k=0}^{n-1} p^k[x_k]\right) = \sum\limits_{k=0}^{n-1} p^k x_k^{(0)}$.
We only need to show that $\theta_n(x+y) = \theta_n(x)+\theta_n(y)$ since $\theta_n(xy) = \theta_n(x)\theta_n(y)$ depends

$\mathbb{Z}$-bilinearly on (x, y) and so via Teichmüller expansions the verification of this identity is reduced to the case $x = [a]$ and $y = [b]$ with $a, b \in \tilde{E}^+ : \theta([a][b]) = \theta([ab]) = (ab)^{(0)} = a^{(0)}b^{(0)} = \theta([a])\theta([b])$. Hence we just need to check that each θ_n is additive.
Writing $x = (x_0, ..., x_{n-1}) \in W(\tilde{E}^+)$ we have :

$$\begin{aligned}\theta_n(x) = \sum_{i=0}^{n-1} p^i x_i^{(0)} &= x_0^{(0)} + px_1^{(0)} + ... + p^{n-1}x_{n-1}^{(0)} \\ &= (x_0^{(n)})^{p^n} + p(x_1^{(n-1)})^{p^{n-1}} + ... + p^{n-1}(x_{n-1}^{(1)})^p \\ &= \sum_{i=0}^{n-1} p^i (x_i^{(n-i)})^{p^{n-i}} \\ &= \Phi_n(x_0^{(n)} \text{mod } p^n, ..., x_{n-1}^{(1)} \text{mod } p^n)\end{aligned}$$

where Φ_n is the n-th ghost map (notice that $\Phi_{n-1} = \Phi_n$ since we work mod p^n).
We have that Φ_n is additive. By Lemma 2.2, we get that $\Phi_n(x_0, ...x_{n-1})$ depends only on the x_i mod p.
That means that Φ_n factors as $\overline{\Phi}_n \circ \pi_n$ where $\pi_n : W_n(\mathcal{O}_C/(p^n)) \twoheadrightarrow W_n(\mathcal{O}_C/(p))$ is the natural quotient map and $\overline{\Phi}_n : W_n(\mathcal{O}_C/(p)) \to \mathcal{O}_C/(p^n)$ maps $(\overline{x}_0, ..., \overline{x}_{n-1})$ to $\sum_{i=0}^{n-1} p^i x_i^{p^{n-i}}$ where $x_i \in \mathcal{O}_C/(p^n)$ is a lift of $\overline{x_i}$. Clearly π_n is surjective and it is additive by functoriality of the additive structure on W_n. Thus, as Φ_n is also additive we get that $\overline{\Phi}_n$ is so. Considering now $p_n : \tilde{E}^+ \to \mathcal{O}_C/(p)$ the projection $r \mapsto r^{(n)}$ mod p, we have $\theta_n = \overline{\Phi}_n \circ W_n(p_n)$. The map $W_n(p_n)$ is additive since p_n is a ring homomorphism and the additive structure on W_n is functorial in ring homomorphism. So $\overline{\Phi}_n$ is additive and we conclude that θ_n is also additive, we are done. □

Lemma 2.33. *The ring homomorphism θ is surjective.*

Proof. Once again via Teichmüller expansions it is enough to show that for any $y \in \mathcal{O}_C$ there exists $x \in \tilde{E}^+$ such that $\theta([x]) = y$. But C is algebraically closed, therefore there exists a solution to $x^{(0)} - y = 0$, hence we are done. □

There are two natural topologies on $\tilde{A}^+$. The strong topology which is the p-adic topology (a basis of neighbourhood of 0 are the $p^k\tilde{A}^+$ for $k \in \mathbb{Z}_{\geq 0}$), makes the application $\sum_{n=0}^{\infty} p^n[x_n] \mapsto (x_n)_{n\geq 0}$ a homeomorphism from $\tilde{A}^+$ into $(\tilde{E}^+)^{\mathbb{Z}_{\geq 0}}$, where $\tilde{E}^+$ is equipped with the discrete topology.

The natural topology on $\tilde{A}^+$ is the one which makes $\sum_{n=0}^{\infty} p^n[x_n] \mapsto (x_n)_{n\geq 0}$ a homeomorphism from $\tilde{A}^+$ into $(\tilde{E}^+)^{\mathbb{Z}_{\geq 0}}$ where this time $\tilde{E}^+$ is equipped with the topology defined

by v_E. This topology, the weak topology, is weaker than the p-adic topology, but $\tilde{A}^+$ is still complete for this topology since $\tilde{E}^+$ is complete for v_E.
As G_K acts continuously on $\tilde{E}^+$ for the topology defined by v_E, it acts continuously on $\tilde{A}^+$ equipped with the weak topology.

Proposition 2.34. *Choose $\tilde{p} \in \tilde{E}^+$ such that $\tilde{p}^{(0)} = p$ (so $\tilde{p} = (p, p^{\frac{1}{p}}, p^{\frac{1}{p^2}}, ...)$ and $v_E(\tilde{p}) = v_p(\tilde{p}^{(0)}) = 1$). Let $\xi = [\tilde{p}] - p = (\tilde{p}, -1, 0, ...) \in \tilde{A}^+$. Then :*
i) $Ker(\theta)$ is a principal ideal of $\tilde{A}^+$ generated by ξ.
ii) An element $x = (x_0, x_1, ...) \in Ker(\theta)$ is a generator of $Ker(\theta)$ if and only if x_1 is a unit in $\tilde{A}^+$.

Proof. Computing $\theta(\xi) = \theta([\tilde{p}]) - \theta(p) = \tilde{p}^{(0)} - p = 0$ we see that $\xi \in Ker(\theta)$. Moreover, $\tilde{A}^+/(Ker(\theta)) = \mathcal{O}_C$ has no non trivial p-torsion, so we have $Ker(\theta) \cap p^n \tilde{A}^+ = p^n Ker(\theta)$ and since $\tilde{A}^+$ is p-adically separated and complete ($\tilde{E}^+$ is perfect so $W(\tilde{E}^+) = \tilde{A}^+$ is a strict p-ring), it is enough to show that $Ker(\theta) \subseteq (\xi, p) (= (\tilde{p}, p))$ to prove the first assertion.
Let $x = (x_0, x_1, ...) \in Ker(\theta)$. Then $\theta(x) = 0 \Leftrightarrow \sum_{k=0}^{\infty} p^k x_k^{(0)} = 0 \Leftrightarrow x_0^{(0)} \equiv 0 \bmod p$, that is $v_E(x_0) = v_p(x_0^{(0)}) \geq 1 = v_E(\tilde{p})$, hence $x_0 \in \tilde{p}\tilde{A}^+$. Thus $x \in ([x_0], p) \subseteq ([\tilde{p}], p)$ and we are done for i).
Let $x = (x_0, x_1, ...) \in Ker(\theta)$. Since ξ generates $Ker(\theta)$ we can write x as $x = \xi.x'$ with $x' = (x'_0, x'_1, ...)$. So $x = (P_n(\xi, x'))_{n \geq 0} = (\tilde{p}x'_0, \tilde{p}^p x'_1 - x_0'^p, ...)$ therefore we get $x = (\tilde{p}x'_0, \tilde{p}^p x'_1 - x_0'^p, ...)$ and so $x_1 = \tilde{p}^p x'_1 - x_0'^p$. So x_1 is a unit of $\tilde{E}^+$ if and only if x'_0 is a unit of $\tilde{E}^+$. But if x'_0 is a unit of $\tilde{E}^+$ then $x' = (x'_0, x'_1, ...)$ is a unit of $\tilde{A}^+$ and if x' is a unit of $\tilde{A}^+$ then x is a principal generator of $Ker(\theta)$ (since $\tilde{A}^+$ is a domain). □

Example 2.35. Let $\omega = \frac{[\varepsilon]-1}{[\varepsilon^{\frac{1}{p}}]-1} = 1 + [\varepsilon^{\frac{1}{p}}] + ... + [\varepsilon^{\frac{1}{p}}]^{p-1} \in \tilde{A}^+$. We have $\theta(\omega) = 0$ since $\theta([\varepsilon]) = 1$ and $\theta([\varepsilon^{\frac{1}{p}}]) = \varepsilon^{(1)} \neq 1$. Moreover, the image $\overline{\omega}$ of ω in $\tilde{E}^+$ is $\frac{\varepsilon-1}{\varepsilon^{\frac{1}{p}}-1} = (\varepsilon - 1)^{1-\frac{1}{p}}$ and so $v_E(\overline{\omega}) = (1 - \frac{1}{p})v_E(\varepsilon - 1) = 1$.
This shows that ω is a generator of $Ker(\theta)$.

Proposition 2.36. *The weak topology on $\tilde{A}^+$ is also the $(p, Ker(\theta))$-adic topology.*

Proof. [Col07] Proposition 2.39 □

2.2.3 The ring B_{dR}

Let $\tilde{B}^+ = \tilde{A}^+[\frac{1}{p}]$. We can extend θ by $\mathbb{Q}_p$-linearity into a ring morphism from $\tilde{B}^+$ into $\mathcal{O}_C[\frac{1}{p}] = C$. We denote this extension by θ_K. Thanks to Proposition 2.34, we see that $Ker(\theta_K)$ is still principal generated by ξ.

Corollary 2.37. *For all $i \geq 0$ we have : $\tilde{A}^+ \cap (Ker(\theta_K))^i = (Ker(\theta))^i$.*
Moreover $\bigcap_{i=0}^{\infty} (Ker(\theta))^i = \bigcap_{i=0}^{\infty} (Ker(\theta_K))^i = 0$

Proof. The proof goes by a simple induction on i. For the case $i = 1$ it is immediate since $\tilde{A}^+/Ker(\theta) = \mathcal{O}_C$ has no non trivial p-torsion.
Recall that $\theta_K : \tilde{B}^+ = \tilde{A}^+[\frac{1}{p}] \to \mathcal{O}_C[\frac{1}{p}] = C$. Any element of $\tilde{B}^+$ admits a p-power multiple in $\tilde{A}^+$ and so $\bigcap_{i=0}^{\infty} (Ker(\theta_K))^i = \bigcap_{i=0}^{\infty} (Ker(\theta))^i[\frac{1}{p}]$. It suffices now to show that it vanishes.
Let $x = (x_0, x_1, ...) \in \tilde{A}^+$ such that $x \in \bigcap_{i=0}^{\infty} (Ker(\theta))^i$. It is then divisible by any power of the generator of $Ker(\theta)$ (in particular by ξ), so x_0 is divisible by any power of $\tilde{p}$ (in $\tilde{E}^+$). But $v_E(\tilde{p}) = 1 > 0$ and so, since $\tilde{E}^+$ is v_E-adically separated we have that $x_0 = 0$. Hence $x = px'$ with $x' \in \tilde{A}^+$ since $\tilde{E}^+$ is perfect. Thus $x' \in \tilde{A}^+ \cap (Ker(\theta_K))^i = (Ker(\theta))^i$ for all i. So we see that each element of $\bigcap_{i=0}^{\infty} (Ker(\theta))^i$ in $\tilde{A}^+$ lies in $\bigcap_{n=0}^{\infty} p^n \tilde{A}^+$, which vanishes since $\tilde{A}^+$ is a strict p-ring. □

Definition 2.38. The de Rham ring

$$B_{dR}^+ := \varprojlim_j \tilde{B}^+/(Ker(\theta_K))^j$$

is the ring obtained by completing $\tilde{B}^+$ for the $Ker(\theta_K)$-adic topology.

Remark 2.39. Since $B_{dR}^+ = \varprojlim_j \tilde{B}^+/(Ker(\theta_K))^j$, it is mapped onto each quotient $\tilde{B}^+/(Ker(\theta_K))^j$ via the evident natural map and in particular for $j = 1$, θ_K induces a surjective map $\theta_{dR}^+ : B_{dR}^+ \twoheadrightarrow C$.
We get from the definitions that $Ker(\theta_{dR}^+) \cap \tilde{A}^+ = Ker(\theta)$ and moreover that
$Ker(\theta_{dR}^+) \cap \tilde{B}^+ = Ker(\theta_K)$ (since θ_{dR}^+ restricts to θ_K on the subring $\tilde{B}^+$).

Proposition 2.40. *The ring B_{dR}^+ is a complete discrete valuation ring with residue field C, and any generator of $Ker(\theta_K)$ in $\tilde{B}^+$ is a uniformizer of B_{dR}^+. The natural map $B_{dR}^+ \to \tilde{B}^+/(Ker(\theta_K))^j$ is identified with the projection $B_{dR}^+ \to B_{dR}^+/(Ker(\theta_{dR}^+))^j$ for all $j \geq 1$.*

Proof. Since $Ker(\theta_K)$ is a nonzero principal maximal ideal (with residue field C) in the domain $\tilde{B}^+$, for $j \geq 1$ we see that $\tilde{B}^+/(Ker(\theta_K))^j$ is an Artin local ring whose only ideals are $(Ker(\theta_K))^i/(Ker(\theta_K))^j$ for $j \geq i \geq 0$. In particular, an element of B_{dR}^+ is a unit if and only if it has nonzero image under θ_{dR}^+. In other words, the maximal ideal

$Ker(\theta^+_{dR})$ consists of precisely the non-units, so B^+_{dR} is a local ring. Consider a non-unit $b \in B^+_{dR}$, so its image in each, $\tilde{B}^+/(Ker(\theta_K))^j$ has the form $b_j\xi$ with b_j uniquely determined modulo $(Ker(\theta_K))^{j-1}$ (with ξ as above). In particular, the residue classes $b_j \bmod (Ker(\theta_K))^{j-1}$ are a compatible sequence and so define an element $b' \in B^+_{dR}$ with $b = \xi b'$. The construction of b' shows that it is unique. Hence, the maximal ideal of B^+_{dR} has the principal generator ξ, and ξ is not a zero divisor in B^+_{dR}. It now follows that for each $j \geq 1$ the multiples of ξ^j in B^+_{dR} are the elements killed by the surjective projection to $\tilde{B}^+/(Ker(\theta_K))^j$. In particular, B^+_{dR} is ξ-adically separated, so it is a discrete valuation ring with uniformizer ξ. We have identified the construction of B^+_{dR} as the inverse limit of its Artinian quotients, so it is a complete discrete valuation ring. □

We denote by v_H the valuation defined by ξ on B^+_{dR}. Since $Ker(\theta_K)$ is stable by G_K, the action of G_K on $\tilde{B}^+$ extends continuously on B^+_{dR}. However, the action of φ does not extend since φ does not preserve the kernel of θ_K (as $\varphi(\xi) = [\tilde{p}^p] - p \notin Ker(\theta_K)$). The natural topology on B^+_{dR} is not the topology defined by v_H ; this one is too strong for G_K to act continuously on B^+_{dR}. The natural topology on B^+_{dR} is the one for which $p^k\tilde{A}^+ + \xi^n B^+_{dR},\ k, n \geq 0$, gives us a basis of neighbourhoods of 0. This topology is weaker than the topology induced by v_H but G_K acts continuously on B^+_{dR} equipped with it.

Definition 2.41. The field of p-adic periods (also called the de Rham period ring) is $B_{dR} := Frac(B^+_{dR})$ equipped with its natural G_K-action and G_K-stable filtration via the $\mathbb{Z}$-powers of the maximal ideal of B^+_{dR}.

For $i \in \mathbb{Z}$, let $Fil^i B_{dR}$ be the i-th power of the maximal ideal of B^+_{dR}.
Then, if $i \geq 0$, $Fil^i B_{dR} = \mathfrak{m}^i_{B^+_{dR}}$. For $i \in \mathbb{Z}$, $Fil^i B_{dR}$ is the free B^+_{dR}-module generated by ξ^i : $Fil^0 B_{dR} = B^+_{dR}$ and $Fil^i B_{dR} = \xi^i B^+_{dR}$.

2.2.4 The p-adic analogous of $2i\pi$

In the following we will show that B^+_{dR} admits a uniformizer t, canonical up to $\mathbb{Z}_p^*$-multiple, on which G_K acts by the cyclotomic character, and that the set of such t's is naturally $\mathbb{Z}_p^*$-equivariantly bijective with the set of $\mathbb{Z}_p$-bases of $\mathbb{Z}_p(1) = \varprojlim \mu_{p^n}(\overline{K})$. Such elements t do not live in $\tilde{B}^+$ so it was essential for us to pass to the completion B^+_{dR} to find such a uniformizer. Moreover, we will see that the element t is in fact a p-adic analogous of $2i\pi$.
Let's construct this t. Recall that we have $\varepsilon = (\varepsilon^{(n)})_{n\geq 0}$ a compatible sequence of primitive p^n-th roots of unity.

Since $\theta([\varepsilon]-1)=\varepsilon^{(0)}-1=0$ we have that $[\varepsilon]-1\in Ker(\theta)\subseteq Ker(\theta^+_{dR})$. So $[\varepsilon]-1$ is "small" for the topology of B^+_{dR} and the following series :

$$\sum_{n=1}^{\infty}(-1)^{n+1}\frac{([\varepsilon]-1)^n}{n}$$

will converge in B^+_{dR}, to our desired t. Of course, one should think of t as $t=log([\varepsilon])$ and notice that it lies in the maximal ideal of B^+_{dR}.

Proposition 2.42. *Let t be the element defined as above. Then :*

$$t\in Fil^1B_{dR} \text{ and } t\notin Fil^2B_{dR}$$

In other words, t generates the maximal ideal of B^+_{dR} (i.e. it is a uniformizer).

Proof. $Fil^1B_{dR}=\xi B^+_{dR}$ and as $[\varepsilon]-1\in Ker(\theta)$, it is clear that $\frac{([\varepsilon]-1)^n}{n}\in Fil^1B_{dR}$ $\forall n\geq 1$, hence $t\in Fil^1B_{dR}$.
$Fil^2B_{dR}=\xi^2B^+_{dR}$ and for the same reason it is clear that $\frac{([\varepsilon]-1)^n}{n}\in Fil^2B_{dR}$ $\forall n\geq 2$, so to prove that $t\notin Fil^2B_{dR}$ we only need to show that $[\varepsilon]-1\notin Fil^2B_{dR}$.
$[\varepsilon]-1\in Ker(\theta)$ implies that we can write $[\varepsilon]-1$ as $[\varepsilon]-1=x\xi$ with $x\in\tilde{A}^+$. So showing that $[\varepsilon]-1\notin Fil^2B_{dR}$ is equivalent to show that $\theta(x)\neq 0$, that is $x\notin\xi\tilde{A}^+$.
Suppose that $[\varepsilon]-1\in\xi^2\tilde{A}^+$ so we can write it as $[\varepsilon]-1=x\xi^2$ with $x\in\tilde{A}^+$ and $x=(x_0,x_1,...)$.
Since $\xi=(\tilde{p},-1,0,...)$, we have $\xi^2=(\tilde{p}^2,...)$ and thus $x\xi^2=(\tilde{p}^2x_0,...)$.
But $[\varepsilon]-1=(\varepsilon-1,...)$ so $\varepsilon-1=\tilde{p}^2x_0$. We have $v_E(\tilde{p}^2x_0)\geq v_E(\tilde{p}^2)=2$ and therefore we should have $v_E(\varepsilon-1)\geq 2$. We know by the Remark 2.31 that if p is odd then $v_E(\varepsilon-1)=\frac{p}{p-1}$ so we get a first contradiction and if $p=2$ we need to do a little computation (we will work in $W_2(\tilde{E}^+)$).
Suppose $p=2$, then $\xi^2=(\tilde{p}^2,0,...)$ and $x\xi^2=(\tilde{p}^2x_0,\tilde{p}^4x_1,...)$.
Moreover, for $p=2$ we have $-1=(1,1,...)$ in $\mathbb{Z}_2=W(\mathbb{F}_2)$ since $-1=1+2.1$ mod 4, hence $[\varepsilon]-1=(\varepsilon-1,\varepsilon-1,...)$ in $\tilde{A}^+$. Thus if $x\xi^2=[\varepsilon]-1$, then $\varepsilon-1=\tilde{p}^4x_1$ and $v_E(\varepsilon-1)\geq v_E(\tilde{p}^4)=4$. We get again a contradiction since by Remark 2.31 $v_E(\varepsilon-1)=2$ if $p=2$. So we are done. □

Remark 2.43. Note that since the begining we have made a choice for our ε so a natural question is : what happend if we choose a different compatible sequence of p^n-th root of unity, say ε' ?
If we make such another choice then $\varepsilon'=\varepsilon^a$ for a unique $a\in\mathbb{Z}_p^*$ using the natural structure on units in $\tilde{E}^+$. Since the Teichmüller map from $\tilde{E}^+$ to $\tilde{A}^+$ is continuous for the

v_E-adic topology of $\tilde{E}^+$ we have $[\varepsilon'] = [\varepsilon^a] = [\varepsilon]^a$ in $\tilde{A}^+$. Hence $t' = log([\varepsilon']) = log([\varepsilon]^a)$. We would like to have $t' = a.log([\varepsilon])$, but this is not trivial since the logarithm is defined as a convergent sum relative to the topology on B_{dR}^+ that does not use the v_E-adic topology of $\tilde{E}^+$ whereas the exponentiation procedure $[\varepsilon]^a$ involves the v_E-adic topology of $\tilde{E}^+$ in an essential manner. It is possible to introduce a topological ring structure on B_{dR}^+, finer than its discrete valuation topology and such that the map $\tilde{A}^+ \to B_{dR}^+$ is continuous (details can be found in [BC]). Once this done, we get $t' = log([\varepsilon']) = a.log([\varepsilon]) = at$ with $a \in \mathbb{Z}_p^*$. So we see that the line $\mathbb{Z}_p t$ in the maximal ideal of B_{dR}^+ is independant of the choice of ε and making a choice of $\mathbb{Z}_p$-basis of this line is the same as making a choice of ε. Also, choosing ε is a choice of $\mathbb{Z}_p$-basis of $\mathbb{Z}_p(1)$.

If we look for a p-adic analogous of $2i\pi$ in $\mathbb{C}_p$, the completion of the algebraic closure of $\mathbb{Q}_p$, it should be defined by the formula $2i\pi = \lim_{n\to\infty} p^n log(\varepsilon^{(n)})$. The issue is that we have $log_p(\varepsilon^{(n)}) = 0$ for any $n \in \mathbb{Z}_{\geq 0}$ and so our formula gives us $2i\pi = 0$ which is absurd. If we look at the previous formula with a Galois point of view, and that we use the formula $\sigma(\varepsilon^{(n)}) = (\varepsilon^{(n)})^{\chi(\sigma)}$, for $\sigma \in G_{\mathbb{Q}_p}$, we see that the minimum required to be a p-adic analogous of $2i\pi$ is to satisfy the formula $\sigma(2i\pi) = \chi(\sigma)2i\pi$ for any $\sigma \in G_{\mathbb{Q}_p}$. However we have the following results that tell us that such an analogous cannot exist in $\mathbb{C}_p$ (we admit them, for details see [Col07]) :

Theorem 2.44. *If $k \in \mathbb{Z}$, then $\{x \in \mathbb{C}_p \mid \sigma(x) = \chi(\sigma)^k x$, for any $\sigma \in G_{\mathbb{Q}_p}\} = \{0\}$ if $k \neq 0$ and is equal to $\mathbb{Q}_p$ if $k = 0$.*

Corollary 2.45. *Let K be a finite extension of $\mathbb{Q}_p$.*
If $k \in \mathbb{Z}$, then $\{x \in \mathbb{C}_p \mid \sigma(x) = \chi(\sigma)^k x$, for any $\sigma \in G_K\} = \{0\}$ if $k \neq 0$ and is equal to K if $k = 0$.

As we have seen earlier, $t = log([\varepsilon]) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{([\varepsilon]-1)^n}{n}$ converges in B_{dR}^+.
If $\sigma \in G_{\mathbb{Q}_p}$, we have

$$\begin{aligned}\sigma(t) = \sigma(log([\varepsilon])) = log([\sigma(\varepsilon)]) &= log([\varepsilon^{\chi(\sigma)}]) \\ &= log([\varepsilon]^{\chi(\sigma)}) \\ &= \chi(\sigma) log([\varepsilon]) \\ &= \chi(\sigma) t\end{aligned}$$

This shows us that t is a p-adic analogous of $2i\pi$ and that it is a period for the cyclotomic character. We have $\theta_{dR}^+(t) = 0$ which explain why we did not see it in $\mathbb{C}_p$.
We could have defined $B_{dR} = B_{dR}^+[\frac{1}{t}]$ and so $Fil^i B_{dR} = t^i B_{dR}^+$.

2.3 The construction of B_{cris}

As we have already said, the ring B_{dR}^+ is too coarse a ring since there is no extension of the natural Frobenius $\varphi : \tilde{B}^+ \to \tilde{B}^+$ to a continuous map $\varphi : B_{dR}^+ \to B_{dR}^+$. One would still like to have a Frobenius map, and there is a natural way to complete $\tilde{B}^+$ such that the completion is still endowed with a Frobenius map.

Definition 2.46. The ring A_{cris}^0 is defined to be the divided power envelope of $\tilde{A}^+$ with respect to $Ker(\theta)$, that is : $A_{cris}^0 = \tilde{A}^+[\frac{\alpha^m}{m!}]_{m\geq 1,\ \alpha\in Ker(\theta)}$

Remark 2.47. Since $\frac{(ax)^n}{n!} = a^n\frac{x^n}{n!}$, we can define A_{cris}^0 as $A_{cris}^0 = \tilde{A}^+[\frac{\xi^m}{m!}]_{m\geq 1}$ with ξ the principle generator of $Ker(\theta)$.

Definition 2.48. We define A_{cris} to be the p-adic completion of A_{cris}^0 :

$$A_{cris} = \varprojlim_n A_{cris}^0/p^n A_{cris}^0$$

.

Remark 2.49. By the definition of A_{cris} we see that it is p-adically separated and complete.

We would like to warn the reader that proving even basic properties about A_{cris} requires a lot of effort and knowledge in algebra so we will be less precise in this section.
One can prove that there exists a unique continuous map j such that the following diagram commutes using the p-adic topology on A_{cris} and the finer topology that we talked about earlier on B_{dR}^+ :

$$\begin{tikzcd}
A_{cris} \arrow[r, "j"] \arrow[d] & B_{dR}^+ \arrow[d] \\
A_{cris}^0 \arrow[r] & \tilde{B}^+
\end{tikzcd}$$

The uniqueness of j comes from the fact that one can show that A_{cris}^0 is dense in A_{cris} and B_{dR}^+ is Hausdorff. Moreover the map j can be proved to be injective, so A_{cris} is a domain and $A_{cris}^0 \to A_{cris}$ is indeed injective.
The image of A_{cris} in B_{dR}^+ can be described as the subring of elements

$$\left\{ \sum_{n=0}^{\infty} x_n \frac{\xi^n}{n!} \mid x_n \in \tilde{A}^+,\ x_n \to 0 \text{ for the } p\text{-adic topology} \right\}$$

in which the infinite sums are taken with respect to the discretely-valued topology of B_{dR}^+ (the convergence of the sums is due to the fact that $\xi \in \mathfrak{m}_{B_{dR}^+}$).

Definition 2.50. The ring B^+_{cris} is defined to be the $\tilde{B}^+$-subalgebra :

$$B^+_{cris} := A_{cris}[\frac{1}{p}]$$

.

Remark 2.51. The ring B^+_{cris} is a subring of B^+_{dR}, consisting of the limits of sequences of B^+_{dR} which satisfy some growth conditions. For example $\sum\limits_{n=0}^{\infty} p^{-n^2} t^n$ converges in B^+_{dR} but not in B^+_{cris}. This ring is equipped with a continuous Frobenius.

Proposition 2.52. *One has $t \in A_{cris}$ and $t^{p-1} \in pA_{cris}$.*

Proof. Choose a generator ξ of $Ker(\theta)$. We know that $[\varepsilon] - 1 \in Ker(\theta)$ therefore we can write $[\varepsilon] - 1 = x\xi$ for $x \in \tilde{A}^+$. Looking at t now in B^+_{dR} we have :

$$\begin{aligned} t = \sum_{n=1}^{\infty}(-1)^{n+1}\frac{([\varepsilon]-1)^n}{n} &= \sum_{n=1}^{\infty}(-1)^{n+1}\frac{(x\xi)^n}{n} \\ &= \sum_{n=1}^{\infty}(-1)^{n+1}(n-1)!x^n.\frac{\xi^n}{n!} \end{aligned}$$

with $(n-1)!x^n \to 0$ for the p-adic topology of $\tilde{A}^+$. Hence $t \in A_{cris}$ inside of B^+_{dR}.
The fact that $t^{p-1} \in pA_{cris}$ depends on t mod p since $t \in A_{cris}$. So the infinite sum expression for t allows us to check whether or not $t^{p-1} \in pA_{cris}$ by replacing t with a suitable finite truncation of the sum on $\sum\limits_{n=1}^{\infty}(-1)^{n+1}(n-1)!x^n\frac{\xi^n}{n!}$ (we would like to drop the terms with coefficient $(n-1)!$ divisible by p). Hence we can restrict to the sum over $1 \leq n \leq p$.
The terms for $1 \leq n < p$ are A_{cris}-multiple of $[\varepsilon] - 1$, and the term for $n = p$ is $(-1)^{p+1}\frac{([\varepsilon]-1)^p}{p} = (-1)^{p+1}\frac{([\varepsilon]-1)^{p-1}}{p}([\varepsilon]-1)$ so $t = ([\varepsilon]-1)(a+(-1)^{p+1}\frac{([\varepsilon]-1)^{p-1}}{p})$ for some $a \in A_{cris}$. Hence to prove that $t^{p-1} \in pA_{cris}$ it remains to check (and apply twice) that $([\varepsilon]-1)^{p-1} \in pA_{cris}$. But $p\tilde{A}^+ \subseteq pA_{cris}$ and $[\varepsilon] - 1 \equiv [\varepsilon - 1]$ mod $p\tilde{A}^+$. So it suffices to show that $[(\varepsilon-1)^{p-1}] \in pA_{cris}$.
We know that $v_E(\varepsilon - 1) = \frac{p}{p-1}$, so for $\tilde{p} \in \tilde{E}^+$ defined as usual we have

$$v_E((\varepsilon-1)^{p-1}) = p = v_E(\tilde{p}^p)$$

Hence, $(\varepsilon - 1)^{p-1} = \tilde{p}^p x$ for some unit $x \in \tilde{E}^+$, so $[(\varepsilon-1)^{p-1}]$ is a $(\tilde{A}^+)^*$-multiple of $[\tilde{p}^p] = (\xi + p)^p \equiv \xi^p \text{mod } pA_{cris}$. But $\xi^p = p.(\frac{\xi^p}{p!})(p-1)! \in pA_{cris}$. So we are done. □

Proposition 2.53. *For any $a \in Ker(A_{cris} \twoheadrightarrow \mathcal{O}_C)$ we have $\frac{a^m}{m!} \in A_{cris}$ $\forall m \geq 1$.*

Proof. Fix a choice of m. By definition, a in A_{cris} is a sum of terms $a_n \frac{\xi^n}{n!}$ with $n \geq 1$, $a_n \in \tilde{A}^+$ and $a_n \to 0$ in $\tilde{A}^+$ for the p-adic topology. therefore it is enough to treat the case when this infinite sum is replaced with a finite truncation, big enough, so that the tail lies in $p^N A_{cris}$ with $m!$ which divides p^N. By the binomial theorem we have $\frac{(x+y)^m}{m!} = \sum\limits_{i=0}^{m} \frac{x^i}{i!} \frac{y^{m-i}}{(m-i)!}$. Thus, it suffices when a is a finite sum to treat the case when a is a single term, i.e. $a = \frac{x\xi^n}{n!}$ with $x \in \tilde{A}^+$. But $\frac{(xy)^m}{m!} = x^m \frac{y^m}{m!}$ so finally we are reduced to the case $a = \frac{\xi^n}{n!}$ with $n \geq 1$ and we wish to prove that the divided power $\frac{a^m}{m!}$ lies in A_{cris}. By the universal identity of divided power in any $\mathbb{Q}$-algebra we get that $\frac{a^m}{m!} \in A_{cris}$ for $a = \frac{\xi^n}{n!}$ and all $m \geq 1$, as required. □

Definition 2.54. The crystalline period ring B_{cris} is defined as the $\tilde{B}^+$-subalgebra

$$B_{cris} := B_{cris}^+[\frac{1}{t}] = A_{cris}[\frac{1}{t}]$$

inside of $B_{dR}^+[\frac{1}{t}] = B_{dR}$.

For the end of this section, we will state few properties about the different Frobenius automorphism that we have.
Recall that we have our usual $\tilde{p} \in \tilde{E}^+$ such that $\tilde{p}^{(0)} = p$ and $\xi = [\tilde{p}] - p \in Ker(\theta)$. Recall also that $B_{cris} = A_{cris}[\frac{1}{t}]$ with A_{cris} defined to be the p-adic completion of $A_{cris}^0 = \tilde{A}[\frac{\xi^m}{m!}]_{m \geq 1}$. We start with the following lemma :

Lemma 2.55. *The $\tilde{A}^+$-subalgebra $A_{cris}^0 \subseteq \tilde{B}^+$ is φ-stable.*

Remark 2.56. Here φ is the Frobenius automorphism of $\tilde{B}^+$.

Proof. Since $\varphi(\xi) = [\tilde{p}^p] - p = [\tilde{p}]^p - p = (\xi + p)^p - p = \xi^p + px$ for some $x \in \tilde{A}^+$, we have : $\varphi(\xi) = p(x + (p-1)!(\frac{\xi^p}{p!}))$. Therefore $\varphi(\xi^m) = p^m(x + (p-1)!(\frac{\xi^p}{p!}))^m$ for all $m \geq 1$. But $\frac{p^m}{m!} \in \mathbb{Z}_p$ for all $m \geq 1$, so $\varphi(\frac{\xi^m}{m!}) \in A_{cris}^0$ for all $m \geq 1$. □

The endomorphism of A_{cris}^0 induced by φ on $\tilde{B}^+$ extends uniquely to a continuous endomorphism of the p-adic completion A_{cris}, and hence to an endomorphism of $B_{cris}^+ = A_{cris}[\frac{1}{p}]$ that extends the Frobenius automorphism of the subring $\tilde{B}^+$. Recall that we constructed earlier a uniformizer of $\tilde{B}^+$ called t defined as $t = log([\varepsilon])$ and that it belongs to A_{cris} . Moreover we have the following lemma :

Lemma 2.57. $\varphi(t) = pt$.

Proof. We have $t = \sum\limits_{n=1}^{\infty}(-1)^{n+1}\frac{([\varepsilon]-1)^n}{n}$. Therefore $\varphi(t) = \sum\limits_{n=1}^{\infty}(-1)^{n+1}\frac{(\varphi([\varepsilon])-1)^n}{n} = \sum\limits_{n=1}^{\infty}(-1)^{n+1}\frac{([\varepsilon]^p-1)^n}{n}$ since φ on A_{cris} extends the Frobenius map on $\tilde{A}^+$. Therefore $\varphi(t) = \sum\limits_{n=1}^{\infty}(-1)^{n+1}\frac{([\varepsilon]-1)^n}{n} = log([\varepsilon]^p)$. By Remark 2.43 we know that it is $p.log([\varepsilon]) = pt$. So we are done. □

This lemma allows us to extend the Frobenius to B_{cris} by setting $\varphi(t^{-1}) = p^{-1}t^{-1}$.

3 p-adic Periods of Formal Groups

3.1 The infinitesimal thickening

Let Λ be a ring and V a Λ-algebra

Definition 3.1. A pro-infinitesimal Λ-thickening of V is a couple (D, θ) where D is a Λ-algebra and θ a surjective Λ-algebra homomorphism $\theta_D = \theta : D \to V$ such that, if $I_D = I$ denotes the kernel of θ, then D is separated and complete for the I-adic topology.

Definition 3.2. If D is a pro-infinitesimal Λ-thickening of V and if I_D is nilpotent, D is called an infinitesimal Λ-thickening of V. If m is an integer such that $I_D^{m+1} = 0$, we say that the thickening has order $\leq m$.

Definition 3.3. Let $\mathfrak{p}$ be an ideal of Λ and assume V to be separated and complete with respect to the $\mathfrak{p}$-adic topology. We say that (D,θ) is a formal $\mathfrak{p}$-adic pro-infinitesimal Λ-thickening if it is a pro-infinitesimal Λ-thickening of V such that D is separated and complete for the $(I, \mathfrak{p})$-adic topology.

Remark 3.4. These notions depend on the topology defined by the powers of $\mathfrak{p}$ and not on the ideal $\mathfrak{p}$ itself.

Theorem 3.5. *Let Λ be a ring, V a separated and complete Λ-algebra for the $\mathfrak{p}$-adic topology. Assume that for every $a \in V$, there exist $x, y \in V$ such that $a = x^p + py$. Then the ring V admits a universal formal $\mathfrak{p}$-adic pro-infinitesimal Λ-thickening.*

3.2 The ring $A_{inf,K}$ and $A_{cris,K}$

Let K be a finite extension of $\mathbb{Q}_p$, $\mathcal{O}_K$ its ring of integers, K_0 the maximal unramified extension of $\mathbb{Q}_p$ in K and $\mathcal{O}_{K_0}$ its ring of integers.

Definition 3.6. $A_{inf,K}$ is the subring of B_{dR}^+ generated by $\tilde{A}^+$ and $\mathcal{O}_K$, that is

$$A_{inf,K} = \mathcal{O}_K \otimes_{\mathcal{O}_{K_0}} \tilde{A}^+$$

In fact $A_{inf,K}$ is the universal p-adic infinitesimal $\mathcal{O}_K$-thickening of $\mathcal{O}_C$. Since $A_{inf,K}$ can be described as $\mathcal{O}_K \otimes_{\mathcal{O}_{K_0}} \tilde{A}^+$ we deduce that $Ker(\theta) \cap A_{inf,K}$ is a principal ideal of $A_{inf,K}$.
Let $\pi_K = \pi$ (respectively $\rho_K = \rho$) a uniformizer of $\mathcal{O}_K$ (respectively a generator of $Ker(\theta) \cap A_{inf,K}$).
We define for any $k \in \mathbb{Z}_{\geq 0}$ the following subring of B_{dR}^+ :

$$A_{inf,K}^k = A_{inf,K}[[\pi^{-k}\rho]].$$

We have for $k = 0$, $A^k_{inf,K} = A_{inf,K}$ and $A^k_{inf,K}$ is a closed subring of B^+_{dR} for any $k \geq 0$.

We recall that for a generator u of $Ker(\theta_K) \cap \tilde{A}^+$ we have A_{cris}, the subring of B^+_{dR} composed by elements x of the form $\sum\limits_{n=0}^{\infty} x_n u^n$ where $(n!x_n)_{n\in\mathbb{Z}_{\geq 0}}$ is a sequence of elements of $\tilde{A}^+$ which tends to 0.
B^+_{cris} was defined by $B^+_{cris} = A_{cris}[\frac{1}{p}]$ and let φ be the Frobenius endomorphism of B^+_{cris} obtained by extending by continuity the Frobenius action $(x_0, ..., x_n, ...) \mapsto (x_0^p, ..., x_n^p, ...)$ of $\tilde{A}^+$.

Definition 3.7. If K is a finite extension of $\mathbb{Q}_p$, we define $A_{cris,K}$ by the subring of B^+_{dR} generated by A_{cris} and $\mathcal{O}_K$, that is $A_{cris,K} = A_{cris} \otimes_{\mathcal{O}_{K_0}} \mathcal{O}_K$. We define also $B^+_{cris,K} = A_{cris,K}[\frac{1}{p}]$.

If $K_0 = K \cap \mathbb{Q}_p^{nr}$ is the maximal unramified extension of $\mathbb{Q}_p$ in K, we have
$B^+_{cris,K} \cong K \otimes_{K_0} B^+_{cris}$ and we denote φ_K the endomorphism $id \otimes_{K_0} \varphi^{[K_0:\mathbb{Q}_p]}$ of $B^+_{cris,K}$.
We set for $k \in \mathbb{Z}_{\geq 0}$: $A^k_{cris,K} = A_{cris,K}$ if $k = 0$ and $A^k_{cris,K} = A^k_{inf,K}$ if $k \geq 1$.

Lemma 3.8. *Let e be the absolute ramification index of K, p^s be the smallest power of p greater or equal than e and $r(e) = sup\{em - p^{m-s} \mid m - s \in \mathbb{Z}_{\geq 0}\}$.*
If $u \in (A^k_{inf,K} \cap Ker(\theta))$ and $l, n \in \mathbb{Z}_{\geq 0}$ with $l \leq n$ then $\frac{u^n}{l} \in \pi^{-r(e)} A^k_{cris,K}$.

Proof. We prove the lemma for $k = 0$ because we only need this case in the sequel and that the case $k \geq 1$ is supposed to be easier.
Since $k = 0$ we have $A^k_{inf,K} = A_{inf,K}$ and $A^k_{cris,K} = A_{cris,K}$.
If $x = (x^{(n)}) \in \tilde{E}^+$ such that $x^{(0)} = \pi$, then $[x] - \pi$ is a generator of $A_{inf,K} \cap Ker(\theta)$ and we can reduce to the case $l = n = p^m$ and $u = [x] - \pi$.
As $v_E(x^{p^s}) = v_p(x^{(0)^{p^s}}) = p^s v_p(\pi) > 1$, and since θ is surjective, we can find $y \in \tilde{A}^+$ such that $\alpha = [x]^{p^s} - py$ in $\tilde{A}^+ \cap Ker(\theta)$. So $u^{p^s} = ([x] - \pi)^{p^s} = [x]^{p^s} - py + \pi\beta,\ \beta \in A_{inf,K}$.

$$\text{If } m \geq s,\ \frac{u^{p^m}}{p^m} = \frac{(u^{p^s})^{p^{m-s}}}{p^m} = \frac{(\alpha + \pi\beta)^{p^{m-s}}}{p^m}$$
$$= \sum_{k=0}^{p^{m-s}} \frac{\binom{p^{m-s}}{k} \alpha^{p^{m-s}-k} (\pi\beta)^k}{p^m}$$

Expending the binomial coefficient and setting $i = p^{m-s} - k$ and $j = k$ (so $i + j = p^{m-s}$) we get

$$\frac{u^{p^m}}{p^m} = \sum_{i+j=p^{m-s}} \frac{\alpha^i}{i!} \frac{\beta^j}{j!} \pi^j \frac{(p^{m-s} - 1)!}{p^s}$$

We have $\frac{\alpha^i}{i!} \in A_{cris,K}$ because $\alpha \in Ker(\theta)$ and $A_{cris,K} = A_{inf,K}[\frac{\gamma^m}{m!}]$ for $\gamma \in Ker(\theta)$ (Proposition 2.53). Since $r(e) = sup\{em - p^{m-s} \mid m - s \in \mathbb{Z}_{\geq 0}\}$, factoring out $\pi^{p^{m-s}} p^{s-m} \in \pi^{r(e)}\mathcal{O}_K$ and noticing that β^j belongs to $A_{inf,K}$, we therefore deduce that $\frac{u^{p^m}}{p^m} \in \pi^{-r(e)} A_{cris,K}$. □

Corollary 3.9. *If $F \in K[[z_1, ..., z_d]]$ satisfies :*
i) $F(0) = 0$
ii) $dF = \sum_{i=1}^{d} f_i dz_i$ with $f_i \in A^k_{cris,K}[[\pi^{-k}z_1, ..., \pi^{-k}z_d]]$
and if $u = (u_1, ..., u_d) \in \left(A^k_{inf,K} \cap Ker(\theta)\right)^d$ then $F(u) \in \pi^{-r(e)} A^k_{cris,K}$.

Proof. If $u = (u_1, ..., u_d) \in \left(A^k_{inf,K} \cap Ker(\theta)\right)^d$ then $u_i \in A^k_{inf,K} \cap Ker(\theta)$ for all $i = 1, ..., d$ and so for some $n_i, l_i \in \mathbb{Z}_{\geq 0}$ $\frac{u_i^{n_i}}{l_i} \in \pi^{-r(e)} A^k_{cris,K}$ (by Lemma 3.8).
As $F(0) = 0$ the fact that $F(u) \in \pi^{-r(e)} A^k_{cris,K}$ really depends on $f_i(u_i)$.
If $\frac{u_i^{n_i}}{l_i} \in \pi^{-r(e)} A^k_{cris,K}$ then $f_i(u_i) \in \pi^{-r(e)} A^k_{cris,K}$ and hence we get $F(u) \in \pi^{-r(e)} A^k_{cris,K}$ as required. □

Lemma 3.10. *If $x \in B^+_{dR}$ satisfies $|\theta(x) - 1|_p < 1$ then the series*

$$log_p(x) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} (x-1)^n$$

converges in B^+_{dR}.

Proof. If $x \in B^+_{dR}$ satisfies $|\theta(x) - 1|_p < 1$, then $x - 1 \in Ker(\theta)$, and we can write $x - 1 = a\xi,\ a \in A_{inf,K},\ \xi$ a generator of $Ker(\theta)$.

$$\begin{aligned} log_p(x) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} (x-1)^n &= \sum_{n=1}^{\infty} (-1)^{n-1} \frac{(a\xi)^n}{n} \\ &= \sum_{n=1}^{\infty} (-1)^{n-1} (n-1)! a^n \frac{\xi^n}{n!} \end{aligned}$$

and since $(n-1)!a^n \to 0$ as $n \to \infty$ we deduce that $log_p(x)$ converges in B^+_{dR}. □

3.3 Dieudonné Module of a Formal Group

Let K be a fintie Galois extension of $\mathbb{Q}_p$ and $K_0 = K \cap \mathbb{Q}_p^{nr}$ the maximal unramified extension of $\mathbb{Q}_p$ inside K, and let k_K be the residue field of K.

Definition 3.11. A Dieudonné module is a triplet (V, ϕ, Fil) where V is a K_0-vector space of dimension h, ϕ an endomorphism of V which is φ-semilinear, injective and topologically nilpotent, satisfying moreover that if M is a lattice of V stable by ϕ then $pM \subseteq \phi M$. Fil is a decreasing filtration on $V_K = K \otimes_{K_0} V$ satisfying $Fil^0(V_K) = V_K$, $Fil^2(V_K) = 0$ and $Fil^1(V_K)$ is a K-vector space of dimension the dimension of $M/\phi M$ as k_K-vector space.

If $D_1 = (V_1, \phi_1, Fil)$ and $D_2 = (V_2, \phi_2, Fil)$ are both Dieudonné modules, the morphisms from D_1 into D_2 are by definition the K_0-linear applications f from V_1 into V_2 satisfying $f \circ \phi_1 = \phi_2 \circ f$ and $f(Fil^1(V_{1,K})) \subseteq Fil^2(V_{2,K})$.

Let Γ be a commutative formal group defined over $\mathcal{O}_K$, of dimension d and finite height h. To such a formal group, we can associate a Dieudonné module in the following way:

Let $\mathcal{O}_K[[X]] = \mathcal{O}_K[[X_1, ..., X_d]]$ be the affine algebra of Γ and denote $\oplus$ the law of formal group. If $\omega = \sum_{i=1}^{d} \alpha_i(X_1, ..., X_d) dX_i$ where $\alpha_i(X) \in K[[X]]$ is a closed differential form, denote F_ω the unique element of $K[[X]]$ satisfying $dF_\omega = \omega$ and $F_\omega(0) = 0$. Let $F_\omega^2 \in K[[X, Y]]$ be the formal series given by the formula

$$F_\omega^2(X, Y) = F_\omega(X \oplus Y) - F_\omega(X) - F_\omega(Y).$$

Definition 3.12. A closed differential form ω is called exact if F_ω has bounded coefficients (or equivalently if there exists $r \in \mathbb{Z}_{\geq 0}$ such that $\pi^r F_\omega \in \mathcal{O}_K[[X_1, ..., X_d]]$).

Definition 3.13. A closed differential form ω is called of second kind if F_ω^2 has bounded coefficients (or equivalently if there exists $r \in \mathbb{Z}_{\geq 0}$ such that $\pi^r F_\omega^2 \in \mathcal{O}_K[[X, Y]]$).

Definition 3.14. A closed differential form ω is called invariant if $F_\omega^2 = 0$.

Denote by Ω_Γ the K-vector space of invariant differential forms. It is a K-vector space of dimension d. Denote $K[[X]]_0$ the subspace of $K[[X]]$ of formal series F satisfying $F(0) = 0$.

Definition 3.15. An element of $K[[X]]_0$ such that $dF \in \Omega_\Gamma$ is called a logarithm of Γ.

Denote $H^1_{dR}(\Gamma)$ the K-vector space which is the quotient of the space of the differential form of second kind by the one of exact differential forms. It is a K-vector space of dimension h equipped with the filtration $Fil^0(H^1_{dR}(\Gamma)) = H^1_{dR}(\Gamma)$, $Fil^1(H^1_{dR}(\Gamma)) = \Omega_\Gamma$ and $Fil^2(H^1_{dR}(\Gamma)) = 0$.

Let $V(\Gamma)$ the K_0-vector subspace of $H^1_{dR}(\Gamma)$ generated by the differential forms ω with coefficients in K_0, equipped with the endomorphism ϕ obtained by the formula :

$$\phi(\omega) = \omega^{\varphi}((X_1)^p, ..., (X_d)^p).$$

The triplet $D(\Gamma) = (V(\Gamma), \phi, Fil)$ where Fil is the filtration on $V(\Gamma)_K = K \otimes_{K_0} V(\Gamma) = H^1_{dR}(\Gamma)$ introduced earlier, is a Dieudonné module and we will call it the Dieudonné module of Γ. We have $H^1_{dR}(\Gamma) \cong K \otimes_{K_0} D(\Gamma)$.
We have that two formal groups defined over $\mathcal{O}_K$ are isogeneous if and only if they have isomorphic Dieudonné module.

3.4 Tate's module and the period map

Let $T_p(\Gamma) = \varprojlim_n \Gamma_{p^n}$, where Γ_{p^n} is the subgroup of points of p^n-torsion of $\Gamma(\mathfrak{M}_{\overline{K}})$, be the Tate module of Γ ; as we already know, it is a $\mathbb{Z}_p$-module of rank h equipped with a continuous action of $G_K = Gal(\overline{K}/K)$.

Lemma 3.16. *i) If $x = (x_1, ..., x_d) \in (A_{inf,K})^d$ is such that $|\theta(x_i)|_p < 1$ for $1 \leq i \leq d$, then $F_\omega([p]_\Gamma x) - pF_\omega(x) \in \pi^{-s} A_{inf,K}$.*
ii) Let $r(e)$ be the integer introduced in Lemma 3.8. If there exists $y = (y_1, ..., y_d)$ such that $y_i - x_i \in A_{inf,K} \cap Ker(\theta)$ then $F_\omega(y) - F_\omega(x) \in \pi^{-s-r(e)} A_{cris,K}$.

Proof. i) Note first that we have :

$$\begin{aligned} \pi^s F^2_\omega([k-1]_\Gamma x, x) + \pi^s(F_\omega([k-1]_\Gamma x) - (k-1)F_\omega(x)) &= \pi^s(F_\omega([k-1]_\Gamma x \oplus x) - F_\omega([k-1]_\Gamma x) \\ &\quad - F_\omega(x)) + \pi^s(F_\omega([k-1]_\Gamma x) - (k-1)F_\omega(x)) \\ &= \pi^s(F_\omega([k]_\Gamma x) - kF_\omega(x)) \end{aligned}$$

We show now by induction on k that : $\pi^s(F_\omega([k]_\Gamma x) - kF_\omega(x)) \in \mathcal{O}_K[[X_1, ..., X_d]]$
For $k = 0$:
$\pi^s(F_\omega([0]_\Gamma x) - 0F_\omega(x)) = 0 \in \mathcal{O}_K[[X_1, ..., X_d]]$
Now suppose it is true for $k \geq 0$, that is : $\pi^s(F_\omega([k]_\Gamma x) - kF_\omega(x)) \in \mathcal{O}_K[[X_1, ..., X_d]]$ for $k \geq 0$.
$\pi^s(F_\omega([k+1]_\Gamma x) - (k+1)F_\omega(x)) = \pi^s F^2_\omega([k]_\Gamma x, x) + \pi^s(F_\omega([k]_\Gamma x) - kF_\omega(x))$ (by our remark). We have that $\pi^s F^2_\omega([k]_\Gamma x, x) \in \mathcal{O}_K[[X_1, ..., X_d]]$ since ω is of second kind and $\pi^s(F_\omega([k]_\Gamma x) - kF_\omega(x)) \in \mathcal{O}_K[X_1, ..., X_d]]$ by induction hypothesis.
Hence $\pi^s(F_\omega([k]_\Gamma x) - kF_\omega(x)) \in \mathcal{O}_K[X_1, ..., X_d]]$ for any $k \geq 0$.
By taking $k = p$ we get $\pi^s(F_\omega([p]_\Gamma x) - pF_\omega(x)) \in \mathcal{O}_K[X_1, ..., X_d]]$ which implies

$F_\omega([p]_\Gamma x) - pF_\omega(x) \in \pi^{-s}\mathcal{O}_K[[X_1,...,X_d]]$. So now, taking $x = (x_1,...,x_d) \in (A_{inf,K})^d$ such that $|\theta(x_i)|_p < 1$ for $1 \leq i \leq d$ we get indeed $F_\omega([p]_\Gamma x) - pF_\omega(x) \in \pi^{-s}A_{inf,K}$ as required.
ii) It is an immediate consequence of Corollary 3.9.
Indeed, if $y = (y_1,...,y_d)$ with $y_i - x_i \in A_{inf,K} \cap Ker(\theta)$ then $y - x \in (A_{inf,K} \cap Ker(\theta))^d$.
We have by definition $F(0) = 0$ and $dF_\omega = \omega = \sum\limits_{i=1}^{d} \alpha_i dX_i$ with $\alpha_i \in K[[X_1,...,X_d]]$. So as shown later we have $\pi^s\omega \in \mathcal{O}_K[[X_1,..,X_d]]$ which implies that $\pi^s\alpha_i \in \mathcal{O}_K[[X_1,...,X_d]]$.
By Corollary 3.9, we obtain $\pi^s F_\omega(y-x) \in \pi^{-r(e)}A_{cris,K}$ so in particular,

$$F_\omega(y) - F_\omega(x) \in \pi^{-s-r(e)}A_{cris,K}.$$

□

We state now the main proposition :

Proposition 3.17. *Let ω be a differential form of second kind, $u = (0, u_1..., u_n, ...) \in T_p(\Gamma)$ and $\hat{u}_n \in (A_{inf,K})^d$ such that $\theta(\hat{u}_n) = u_n$. Then :*
i) the sequence $-p^n F_\omega(\hat{u}_n)$ converges in $B^+_{cris,K}$ to a limit which depends only on u and the range of ω in $H^1_{dR}(\Gamma)$.
ii) the period map defined as

$$\begin{aligned} H^1_{dR}(\Gamma) \times T_p(\Gamma) &\to B^+_{cris,K} \\ (\omega, u) &\mapsto \int_u \omega = \lim_{n\to\infty} p^n F_\omega(\hat{u}_n) \end{aligned}$$

is bilinear, respects the filtrations (i.e. $\int_u \omega \in Fil^1(B_{dR}+)$ if $\omega \in Fil^1(H^1_{dR}(\Gamma))$ and commutes with the action of $Gal(\overline{K}/K)$ (i.e. $g(\int_u \omega) = \int_{g(u)} \omega$ if $g \in Gal(\overline{K}/K)$).
iii) If $\omega \in D(\Gamma)$, then $\int_u \omega \in B^+_{cris}$ and $\varphi(\int_u \omega) = \int_u \phi(\omega)$.

Proof. ω is a differential form of second kind, so by defintion there exists $r \in \mathbb{Z}_{\geq 0}$ such that $\pi^r F^2_\omega \in \mathcal{O}_K[[X_1,...,X_d,Y_1,...,Y_d]]$. Moreover by definition of F^2_ω, $F^2_\omega = F_\omega(X \oplus Y) - F_\omega(X) - F_\omega(Y)$. As $dF_\omega = \omega$ we get

$$\begin{aligned} dF^2_\omega(X,Y) &= dF_\omega(X \oplus Y) - dF_\omega(X) - dF_\omega(Y) \\ &= \omega(X \oplus Y) - \omega(X) - \omega(Y) \end{aligned}$$

and so $\pi^r F^2_\omega \in \mathcal{O}_K[[X_1,...,X_d]]$ implies that $\pi^r(\omega(X\oplus Y) - \omega(X) - \omega(Y)) \in \mathcal{O}_K[[X_1,...,X_d,Y_1,...,Y_d]]$.
$\omega(X \oplus Y) - \omega(X) - \omega(Y) = \sum\limits_{i=1}^{d} \alpha_i(X \oplus Y)d(X \oplus Y)_i - \sum\limits_{i=1}^{d} \alpha_i(X)dX_i - \sum\limits_{i=1}^{d} \alpha_i(Y)dY_i$.
Therefore, there exists $s \geq r$ such that $\pi^s\omega \in \mathcal{O}_K[[X_1,...,X_d]]$ (take $X_i = Y_i$ in the

previous equality to see it).
Now, let $x = (x_1, ..., x_d) \in B^+_{dR}$ such that $|\theta(x)|_p < 1$ for $i = 1, ..., d$ then $|\theta(x_i) - 1|_p \leq \max\{|\theta(x_i)|_p, |1|_p\} < 1$ and so, as in Lemma 3.10, $F_\omega(x)$ converges in B^+_{dR} (it is the formal logarithm of ω).
In particular, as $\theta(\hat{u}_n) = u_n$ and $[p]^n_\Gamma u_n = 0$, $|u_n|_p < 1$, we have that $F_\omega(\hat{u}_n)$ converges in B^+_{dR}.
Write :

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

By i) of Lemma 3.16, as $\hat{u}_{n+1} \in (A_{inf,K})^d$ and that $|\theta(\hat{u}_{n+1})|_p = |u_{n+1}|_p < 1$, we have $pF_\omega(\hat{u}_{n+1}) - F_\omega([p]_\Gamma \hat{u}_{n+1}) \in \pi^{-s} A_{inf,K}$
By ii) of Lemma 3.16, as $\theta([p]_\Gamma \hat{u}_{n+1}) = [p]_\Gamma u_{n+1} = u_n = \theta(\hat{u}_n)$ we have $[p]_\Gamma u_{n+1} - u_n \in A_{inf,K} \cap Ker(\theta)$ and so $F_\omega([p]_\Gamma([p]_\Gamma \hat{u}_{n+1}) - F_\omega(\hat{u}_n) \in \pi^{-s-r(e)} A_{cris,K}$.
We obtain $p^n(pF_\omega(\hat{u}_{n+1}) - F_\omega([p]_\Gamma \hat{u}_{n+1}) \in \pi^{n-s} A_{cris,K}$ and $p^n(F_\omega([p]_\Gamma([p]_\Gamma \hat{u}_{n+1}) - F_\omega(\hat{u}_n) \in \pi^{n-s-r(e)} A_{cris,K}$.
As $B^+_{cris,K} = A_{cris,K}[\frac{1}{p}]$ and that $F_\omega(\hat{u}_n)$ converges in B^+_{dR}, we obtain that $-p^n F_\omega(\hat{u}_n)$ converges in $B^+_{cris,K}$.
We clearly see that the limit does not depend on $\hat{u}_n$ but on $u = (0, u_1, ..., u_n, ...)$ and on the range of ω in $H^1_{dR}(\Gamma)$ (we do not wish that ω is exact).
We have finally proved i) of the proposition.

We want to show now the bilinearity of the period map.
The linearity with respect to ω is clear since $dF_{\lambda\omega} = \lambda\omega = \lambda dF_\omega$ so $F_{\lambda\omega} = \lambda F_\omega$ by unicity of F_ω. Still by the unicity of F_ω we deduce $dF_{\omega+\omega'} = \omega + \omega' = dF_\omega + dF_{\omega'}$.
For the linearity with respect to u, we note that since $[p]^n_\Gamma u_n \to 0$ as $n \to \infty$ and that $-p^n F^2_\omega(\hat{u}_n, \hat{u}'_n) = p^n F_\omega(\hat{u}_n) + p^n(\hat{u}'_n) - p^n F_\omega(\hat{u}_n \oplus \hat{u}'_n)$ we have

$$p^n F_\omega(\hat{u}_n \oplus \hat{u}'_n) \to p^n F_\omega(\hat{u}_n) + p^n F_\omega(\hat{u}'_n) \text{ as } n \to \infty$$

and thus $\int_{u+u'} \omega = \int_u \omega + \int_{u'} \omega$.
Hence we have proved the bilinearity.
We want to show now that the period map commutes with the action of $Gal(\overline{K}/K)$ (i.e. $g(\int_u \omega) = \int_{g(u)} \omega$ if $g \in Gal(\overline{K}/K)$).
Let $g \in Gal(\overline{K}/K)$ and $\hat{u}_n \in (A_{inf,K})^d$ such that $\theta(\hat{u}_n) = u_n$, then $g(\hat{u}_n) \in (A_{inf,K})^d$ and $\theta(g(\hat{u}_n)) = g(u_n)$ because θ is G_K-equivariant $(\theta(g(\hat{u}_n)) = g(\theta(\hat{u}_n)) = g(u_n))$.
As $F_\omega \in K[[X_1, .., X_d]]$ we have $F_\omega(g(\hat{u}_n)) = g(F_\omega(\hat{u}_n))$ and so $g(\int_u \omega) = \int_{g(u)} \omega$.
We finally prove that the period map respects filtrations (i.e. $\int_u \omega \in Fil^1(B^+_{dR})$ if $\omega \in Fil^1(H^1_{dR}(\Gamma))$.
Let $\omega \in Fil^1(H^1_{dR}(\Gamma)) = \Omega_\Gamma$, that means, $F^2_\omega = 0$, which implies that $F_\omega(X \oplus Y) =$

$F_\omega(X) + F_\omega(Y)$ and so in particular $F_\omega([k]_\Gamma X) = kF_\omega(X)$.
Taking $k = p^n$ and $X = u_n$, we get : $F_\omega([p^n]_\Gamma u_n) = p^n F_\omega(u_n)$ and so $F_\omega(u_n) = p^{-n} F_\omega([p^n]_\Gamma u_n) = 0$ since $[p^n]_\Gamma u_n = 0$. Hence $F_\omega(\hat{u}_n) \in Fil^1(B^+_{cris,K})$.

iii) We want to show now that if $\omega \in D(\Gamma)$ then $\int_u \omega \in B^+_{cris}$ and $\varphi(\int_u \omega) = \int_u \phi(\omega)$.
If $u_n = (x_{n,1}, ..., x_{n,d})$, consider $y_{n,i} \in \tilde{E}^+$ such that $y^{(0)}_{n,i} = x_{n,i}$ (therefore we have $y_{n,i} = (x_{n,i}, x^{\frac{1}{p}}_{n,i}, x^{\frac{1}{p^2}}_{n,i}, ...))$. Set $\hat{u}_n = ([y_{n,1}], ..., [y_{n,d}])$. If $\omega \in D(\Gamma)$, that means, $\omega \in K_0[[X_1, ..., X_d]]$ and $\omega \in H^1_{dR}(\Gamma)$. Since $B^+_{cris,K} \cong K \otimes_{K_0} B^+_{cris}$ and $H^1_{dR}(\Gamma) = K \otimes_{K_0} D(\Gamma)$, we have $F_\omega(\hat{u}_n) \in B^+_{cris}$.
Moreover,

$$\begin{aligned} dF_{\phi(\omega)}(\hat{u}_n) = \phi(\omega)(\hat{u}_n) &= \omega^\varphi((X_1)^p, ..., (X_d)^p)(\hat{u}_n) \\ &= \omega^\varphi \varphi(\hat{u}_n) \\ &= \varphi(\omega(\hat{u}_n)) = \varphi(dF_\omega(\hat{u}_n)) \end{aligned}$$

And therefore, by unicity of F_ω we get $\varphi(F_\omega(\hat{u}_n)) = F_{\phi(\omega)}(\hat{u}_n)$. By passing to the limit, as $F_\omega(\hat{u}_n) \in B^+_{cris}$ which is closed in $B^+_{cris,K}$, we get that $\lim_{n\to\infty} F_\omega(\hat{u}_n) \in B^+_{cris}$. We also know, by i), that the sequence $-p^n F_\omega(\hat{u}_n)$ converges in $B^+_{cris,K}$ to a limit which depends on u and on the range of ω in $H^1_{dR}(\Gamma)$ and so we have indeed $\int_u \omega \in B^+_{cris}$ if $\omega \in D(\Gamma)$.
Moreover, as $\varphi(F_\omega(\hat{u}_n)) = F_{\phi(\omega)}(\hat{u}_n)$, we have that :

$$\begin{aligned} \varphi(\int_u \omega) &= \varphi(\lim_n p^n F_\omega(\hat{u})) \\ &= \lim_n p^n F_{\phi(\omega)}(\hat{u}) \\ &= \int_u \phi(\omega) \end{aligned}$$

as required. □

We will give an example of a concrete computation when we consider the multiplactive group and show the analogous for the complex case.

Example 3.18. Consider $G_m = Spec(\mathbb{C}[z, \frac{1}{z}])$. Let γ a generator of $H_1(\mathbb{C}^*, \mathbb{Z}), \omega = \frac{dz}{z} \in H^0(G_m, \Omega^1_{G_m/\mathbb{C}})$ and $\varepsilon_n = e^{\frac{2i\pi}{p^n}}$, where $\Omega^1_{G_m/\mathbb{C}}$ is the quotient of the Kähler differential module of G_m by the submodule generated by the da, for $a \in \mathbb{C}$ (that means that we see the elements of $\mathbb{C}$ as constants and that we can apply the usual rules of derivation).

We know that :

$$\int_\gamma \omega = p^n \int_1^{\varepsilon_n} \omega = p^n \int_0^{\frac{2\pi}{p^n}} \frac{de^{i\Theta}}{e^{i\Theta}}$$
$$= 2i\pi$$

This is the classical period.
Now, suppose that $G_m = Spec(K[z, \frac{1}{z}])$ and let $\gamma = (\varepsilon_n)_n$ be a generator of $T_p(G_m) = \lim\limits_{\leftarrow} \mu_{p^n}(\overline{\mathbb{Q}_p})$ and $\omega = \frac{dz}{z} \in H^0(G_m, \Omega_{G_m/K})$. We have $F_\omega = log$ and by definition :

$$p^n \int_1^{\varepsilon_n} \omega = p^n log(\varepsilon_n) = log(\varepsilon_n^{p^n})$$
$$= 0$$

So we see one more time that there is no p-adic analogous of $2i\pi$ in a finite extension of $\mathbb{Q}_p$.
Consider now $\tilde{\varepsilon_n} = [(\varepsilon_{n+m})_{m \in \mathbb{Z}_{\geq 0}}] \in B_{dR}^+$ and let $t = log(\tilde{\varepsilon}_0) \in B_{dR}^+ \backslash \{0\}$. Of course, $\tilde{\varepsilon}_n \neq \varepsilon_n$ but $\theta_{dR}^+(\tilde{\varepsilon}_n) = \varepsilon_n$. Moreover :

$$p^n \int_1^{\tilde{\varepsilon}_n} \omega = p^n log(\tilde{\varepsilon}_n) = log(\tilde{\varepsilon}_0)$$
$$= t$$

And we see that we find our element t.

References

[BC] Olivier Brinon and Brian Conrad. Cmi summer school notes on p-adic hodge theory. http://math.stanford.edu/ conrad/papers/notes.pdf. (Preliminary version).

[Ber01] Laurent Berger. An introduction to the theory of p-adic representations, 2001.

[Bre00] Christophe Breuil. Integration sur les varietes p-adiques. *Asterisque*, 266:489–549, 2000.

[Col92] Pierre Colmez. Periodes p-adiques des varietes abeliennes. *Mathematische Annalen*, 292:629–644, 1992.

[Col93] Pierre Colmez. Periodes des varietes abeliennes à multiplication complexe. In *Annals of Mathematics*, volume 138, pages 625–683. Annals of Mathematics, 1993.

[Col98] Pierre Colmez. Integration sur les varietes p-adiques. *Asterisque*, 248, 1998.

[Col07] Pierre Colmez. Periodes et representations galoisiennes, notes du cours de m2. https://webusers.imj-prg.fr/ pierre.colmez/Orsay.pdf, 2007.

[FO] Jean-Marc Fontaine and Yi Ouyang. Theory of p-adic galois representations.

[Fon94] Jean-Marc Fontaine. Le corps des periodes p-adiques. *Asterisque*, 223:59–111, 1994.

[Fro68] A. Frohlich. *Formal Groups*. Springer, 1968.

[Sil08] Joseph H. Silverman. *The arithmetic of Elliptic curves*, volume 106. Springer, 2nd edition, 2008.

Index