Cambridge University Press
978-1-107-18858-7 — Galois Representations and (Phi, Gamma)-Modules
Peter Schneider
Excerpt
More Information

1

Relevant Constructions

The purpose of this first chapter is to develop the techniques that will be used in the third chapter to prove the equivalence of categories between p-adic Galois representations and etale (φ_L, Γ_L)-modules. On the one hand, the source category refers to the absolute Galois group of a local field L of characteristic zero with (finite) residue field of characteristic p. On the other hand the coefficient ring of the (φ_L, Γ_L)-modules in the target category is a complete discrete valuation ring whose residue field is a local field of characteristic p. Therefore it should not come as a surprise that much of this chapter will be devoted to setting up formalisms which allow us to pass between fields (or even rings) of characteristic zero and those of characteristic p.

Historically, the first such formalism was Witt's functorial construction of the ring of Witt vectors $W(B)$ for any (commutative) ring B (see [B-AC], §9.1). If $B = k$ is a perfect field of characteristic p then $W(k)$ is a complete discrete valuation ring with maximal ideal $pW(k)$, residue field k, and field of fractions of characteristic zero. For example, we have $W(\mathbb{F}_p) = \mathbb{Z}_p$. Moreover, the pth power map on k lifts naturally to a 'Frobenius' endomorphism F of $W(k)$. Since we will work over a finite, possibly ramified, extension L of $\mathbb{Q}_p$ we need a generalization of Witt's original construction. Suppose that o is the ring of integers in L and $\mathbb{F}_q$ its residue field. The rings of ramified Witt vectors $W(B)_L$, for any o-algebra B, have all the features of the usual Witt vectors but are designed in such a way that $W(\mathbb{F}_q) = o$. This generalization is not well covered in the literature, although most details can be extracted from the rather technical treatment in [Haz]. In Section 1.1 we therefore give a complete and detailed, but nevertheless streamlined, discussion of ramified Witt vectors.

In Section 1.2 we recall the theory of unramified extensions of a complete discretely valued field K. Its importance lies in the fact that if K^{nr}/K denotes the maximal unramified extension and k_K^{sep}/k_K the separable algebraic closure of the residue field k_K of K then one has a natural isomorphism of Galois groups $\mathrm{Gal}(K^{\mathrm{nr}}/K) \xrightarrow{\cong} \mathrm{Gal}(k_K^{\mathrm{sep}}/k_K)$. For us this means that the absolute Galois group of k_K can be identified naturally with a quotient of the absolute Galois group of K.

The coefficient ring of (φ_L, Γ_L)-modules carries an endomorphism φ_L as well as a group of operators $\Gamma_L \cong o^\times$. Their ultimate origin lies in the theory of Lubin–Tate formal group laws, which we explain in detail in Section 1.3. If we fix a prime element π of o then there is, up to an isomorphism, a unique Lubin–Tate formal group law in two variables $F(X,Y) \in o[[X,Y]]$ that contains the ring o in its ring of endomorphisms. In particular, the prime element π corresponds to an endomorphism which later on will give rise to the φ_L. By adjoining to L the torsion points of this formal group law we obtain an abelian extension L_∞/L. The action of the Galois group $\Gamma_L := \mathrm{Gal}(L_\infty/L)$ on these torsion points is given by a character $\chi_L : \Gamma_L = \mathrm{Gal}(L_\infty/L) \xrightarrow{\cong} o^\times$. In an appendix to this section we determine explicitly the higher ramification theory of the extension L_∞/L.

Section 1.4 is the technical heart of the matter. Let $\mathbb{C}_p$ be the completion of the algebraic closure of $\mathbb{Q}_p$. Already Fontaine introduced a very simple recipe for how to construct out of $\mathbb{C}_p$ an algebraically closed complete field $\mathbb{C}_p^\flat$ of characteristic p. It was Scholze, however, who saw the general principle behind this recipe. He introduced the notion of a perfectoid field K in characteristic zero and used Fontaine's recipe to associate with it a complete perfect field $K^\flat$ in characteristic p, calling it the tilt of K. For us a very important example of a perfectoid field will be the completion $\hat{L}_\infty$ of the extension L_∞/L. The tilting procedure is natural. Hence the absolute Galois group G_L of L acts on the tilt $\mathbb{C}_p^\flat$. The absolute Galois group H_L of L_∞ fixes $\hat{L}_\infty$ and consequently also the tilt $\hat{L}_\infty^\flat$. In this way we obtain, on the one hand, a residual action of $\Gamma_L = G_L/H_L$ on $\hat{L}_\infty^\flat$. On the other hand, using the torsion points of our Lubin–Tate formal group law we will exhibit an explicit element ω in $\hat{L}_\infty^\flat$. We then embed the Laurent series field $k((X))$ in one variable over the residue field k of L into $\hat{L}_\infty^\flat$ by sending the variable X to ω. Its image is a local field $\mathbf{E}_L$ of characteristic p. The Γ_L-action on $\hat{L}_\infty^\flat$ preserves $\mathbf{E}_L$. This field $\mathbf{E}_L$ is called the field of norms of L because it can also be constructed via a projective limit with respect to the norm maps in the tower L_∞/L. It was used in this form in Fontaine's original approach to the theory of (φ_L, Γ_L)-modules. However, the route we will take is instead via Scholze's tilting correspondence. The main result that we prove in this section is Theorem 1.4.24, which says that the tilting $K \mapsto K^\flat$ induces a bijection between the perfectoid intermediate fields $\hat{L}_\infty \subseteq K \subseteq \mathbb{C}_p$ and the complete perfect intermediate fields $\hat{L}_\infty^\flat \subseteq F \subseteq \mathbb{C}_p^\flat$. The proof will be given through the construction of an inverse map $F \mapsto F^\sharp$. If o_F is the ring of integers of F then $F^{\sharp}$ is the field of fractions of the quotient of $W(o_F)_L$ by an explicit element $\mathbf{c} \in W(o_{\hat{L}_\infty^\flat})_L$, which depends only on L.

A ring like o_F has its own valuation topology. This leads to a natural topology on the ramified Witt vectors $W(o_F)_L$. It is called the weak topology since it is coarser than the p-adic topology on $W(o_F)_L$. It plays an important technical role in proofs, and it induces the relevant topology on the coefficient ring of (φ_L, Γ_L)-modules. In Section 1.5 we introduce this weak topology in a slightly more general setting and provide the tools to work with it.

In Section 1.6 we deduce from the tilting correspondence that the G_L-action on $\mathbb{C}_p$ induces a topological isomorphism of profinite groups between the absolute Galois group H_L of L_∞ and the absolute Galois group $H_{\mathbf{E}_L}$ of the local field $\mathbf{E}_L$. This is the crucial fact which, for our purposes, governs the passage between characteristic zero and characteristic p.

Finally, in preparation for the coefficient ring of (φ_L, Γ_L)-modules, in Section 1.7 we consider the p-adic completion $\mathscr{A}_L$ of the ring of Laurent series $o((X))$ in one variable X over o. Its elements are 'infinite' Laurent series of a certain kind. We will show that the endomorphisms of our Lubin–Tate formal group law, which correspond to elements in o, extend to operators on $\mathscr{A}_L$. In this way we obtain an endomorphism φ_L corresponding to the prime element π as well as an action of $\Gamma_L \cong o^\times$ on $\mathscr{A}_L$. We will also see that, on the one hand, $\mathscr{A}_L$ carries a weak topology of its own and, on the other, it is a complete discrete valuation ring with prime element π and residue field $k((X))$.

Throughout, we fix a prime number p and a finite field extension $L/\mathbb{Q}_p$ of the field of p-adic numbers. Let $o \subseteq L$ be the ring of integers with residue class field k of cardinality $q = p^f$. We also fix, once and for all, a prime element π of the discrete valuation ring o.

By Alg we denote the category of (commutative unital) o-algebras.

1.1 Ramified Witt Vectors

For any integer $n \geq 0$ we call

$$\Phi_n(X_0, \ldots, X_n) := X_0^{q^n} + \pi X_1^{q^{n-1}} + \cdots + \pi^n X_n$$

the nth *Witt polynomial*. These Witt polynomials satisfy the recursion $\Phi_0(X_0) = X_0$ and

$$\begin{aligned} \Phi_{n+1}(X_0, \ldots, X_{n+1}) &= \Phi_n(X_0^q, \ldots, X_n^q) + \pi^{n+1} X_{n+1} \\ &= X_0^{q^{n+1}} + \pi \Phi_n(X_1, \ldots, X_{n+1}) . \end{aligned} \tag{1.1.1}$$

Let B be in Alg.

Lemma 1.1.1 *For any $m,n \geq 1$ and $b_1, b_2 \in B$ we have that*

$$b_1 \equiv b_2 \bmod \pi^m B \implies b_1^{q^n} \equiv b_2^{q^n} \bmod \pi^{m+n} B .$$

Proof By induction it suffices to consider the case $n = 1$. The polynomial $P(X,Y) := \sum_{i=0}^{q-1} X^i Y^{q-1-i}$ satisfies $(X-Y)P(X,Y) = X^q - Y^q$. Hence it suffices to show that $P(b_1,b_2) \in \pi B$. But our assumption implies $P(b_1,b_2) \equiv P(b_1,b_1) = qb_1^{q-1} \bmod \pi^m B$. □

Lemma 1.1.2 *For $m \geq 1$, $n \geq 0$, and $b_0,\ldots,b_n,c_0,\ldots,c_n \in B$ we have:*

(i) *if $b_i \equiv c_i \bmod \pi^m B$ for $0 \leq i \leq n$ then*

$$\Phi_i(b_0,\ldots,b_i) \equiv \Phi_i(c_0,\ldots,c_i) \bmod \pi^{m+i} B \qquad \textit{for } 0 \leq i \leq n;$$

(ii) *if $\pi 1_B$ is not a zero divisor in B then in (i) the reverse implication holds as well.*

Proof Both assertions will be proved by induction with respect to n. Since the case $n = 0$ is trivial we assume that $n \geq 1$.

(i) By assumption and Lemma 1.1.1 we have $b_i^q \equiv c_i^q \bmod \pi_L^{m+1}$ for $0 \leq i \leq n-1$. The induction hypothesis then implies that

$$\Phi_{n-1}(b_0^q,\ldots,b_{n-1}^q) \equiv \Phi_{n-1}(c_0^q,\ldots,c_{n-1}^q) \bmod \pi^{m+n} B .$$

Inserting this into the recursion formula (1.1.1) gives

$$\Phi_n(b_0,\ldots,b_n) - \pi^n b_n \equiv \Phi_n(c_0,\ldots,c_n) - \pi^n c_n \bmod \pi^{m+n} B .$$

But, as a consequence of the assumption we have $\pi^n b_n \equiv \pi^n c_n \bmod \pi^{m+n} B$. It follows that $\Phi_n(b_0,\ldots,b_n) \equiv \Phi_n(c_0,\ldots,c_n) \bmod \pi^{m+n} B$.

(ii) By the induction hypothesis we have $b_i \equiv c_i \bmod \pi^m B$ for $0 \leq i \leq n-1$. As above we deduce that

$$\Phi_n(b_0,\ldots,b_n) - \pi^n b_n \equiv \Phi_n(c_0,\ldots,c_n) - \pi^n c_n \bmod \pi^{m+n} B .$$

But, by assumption, we have the corresponding congruence for the left summands alone. Hence we obtain $\pi^n(b_n - c_n) \in \pi^{m+n} B$ and therefore $b_n - c_n \in \pi^m B$ by the additional assumption that $\pi 1_B$ is not a zero divisor. □

Let

$$B^{\mathbb{N}_0} := \{(b_0, b_1, \ldots) : b_n \in B\}$$

be the countably infinite direct product of the algebra B with itself (so that addition and multiplication are componentwise). We introduce the following maps:

$$\begin{aligned} f_B \colon B^{\mathbb{N}_0} &\longrightarrow B^{\mathbb{N}_0} \\ (b_0, b_1, \ldots) &\longmapsto (b_1, b_2, \ldots) \ , \end{aligned}$$

which is an endomorphism of o-algebras,

$$\begin{aligned} v_B \colon B^{\mathbb{N}_0} &\longrightarrow B^{\mathbb{N}_0} \\ (b_0, b_1, \ldots) &\longmapsto (0, \pi b_0, \pi b_1, \ldots) \ , \end{aligned}$$

which respects the o-module structure but neither multiplication nor the unit element,

$$\begin{aligned} \Phi_n \colon B^{\mathbb{N}_0} &\longrightarrow B \\ (b_0, b_1, \ldots) &\longmapsto \Phi_n(b_0, \ldots, b_n) \ , \end{aligned}$$

for $n \geq 0$, and

$$\begin{aligned} \Phi_B \colon B^{\mathbb{N}_0} &\longrightarrow B^{\mathbb{N}_0} \\ \mathbf{b} &\longmapsto (\Phi_0(\mathbf{b}), \Phi_1(\mathbf{b}), \Phi_2(\mathbf{b}), \ldots) \ . \end{aligned}$$

Lemma 1.1.3

(i) *If $\pi 1_B$ is not a zero divisor in B then Φ_B is injective.*
(ii) *If $\pi 1_B \in B^\times$ then Φ_B is bijective.*

Proof Let $\mathbf{b} = (b_n)_n$, $\mathbf{u} = (u_n)_n \in B^{\mathbb{N}_0}$. As a consequence of the recursion relations (1.1.1) the relation $\Phi_B(\mathbf{b}) = \mathbf{u}$ is equivalent to the system of equations

$$\begin{aligned} u_0 &= b_0, \\ u_n &= \Phi_{n-1}(b_0^q, \ldots, b_{n-1}^q) + \pi^n b_n \quad \text{for } n \geq 1. \end{aligned} \tag{1.1.2}$$

Under the assumption in (i) (resp. in (ii)) the element $\mathbf{b}$ is therefore, in an inductive way, uniquely determined by $\mathbf{u}$ (resp. can be recursively computed from $\mathbf{u}$). $\square$

Remark 1.1.4 *The system of equations* (1.1.2) *in fact shows the following: Let $\mathbf{b} = (b_n)_n, \mathbf{u} = (u_n)_n \in B^{\mathbb{N}_0}$ be such that $\Phi_B(\mathbf{b}) = \mathbf{u}$. Let $C \subseteq B$ be a subalgebra with the property that the additive map $B/C \xrightarrow{\pi \cdot} B/C$ is injective. Then we have, for any $m \geq 0$,*

$$u_0, \ldots, u_m \in C \Longleftrightarrow b_0, \ldots, b_m \in C \ .$$

Proposition 1.1.5 *Suppose that B has an endomorphism σ of o-algebras such that*

$$\sigma(b) \equiv b^q \bmod \pi B \qquad \text{for any } b \in B.$$

We then have the following.

(i) *Let $b_0, \ldots, b_{n-1} \in B$ for some $n \geq 1$ and put $u_{n-1} := \Phi_{n-1}(b_0, \ldots, b_{n-1})$; an element $u_n \in B$ then satisfies*

$$u_n = \Phi_n(b_0, \ldots, b_n) \text{ for some } b_n \in B \Longleftrightarrow \sigma(u_{n-1}) \equiv u_n \bmod \pi^n B\ .$$

(ii) *$B' := \mathrm{im}(\Phi_B)$ is an o-subalgebra of $B^{\mathbb{N}_0}$ which satisfies*

- $B' = \{(u_n)_n \in B^{\mathbb{N}_0} : \sigma(u_n) \equiv u_{n+1} \bmod \pi^{n+1} B \text{ for any } n \geq 0\}$,
- $f_B(B') \subseteq B'$, $v_B(B') \subseteq B'$.

Proof (i) By our assumption on σ we have $\sigma(b_i) \equiv b_i^q \bmod \pi B$ for any $0 \leq i \leq n-1$. Applying Lemma 1.1.2(i) with $m = 1$ gives

$$\sigma(u_{n-1}) = \Phi_{n-1}(\sigma(b_0), \ldots, \sigma(b_{n-1})) \equiv \Phi_{n-1}(b_0^q, \ldots, b_{n-1}^q) \bmod \pi^n B\ .$$

The existence of an element $b_n \in B$ such that

$$u_n = \Phi_n(b_0, \ldots, b_n) = \Phi_{n-1}(b_0^q, \ldots, b_{n-1}^q) + \pi^n b_n$$

is equivalent to $u_n - \Phi_{n-1}(b_0^q, \ldots, b_{n-1}^q) \in \pi^n B$, hence to $u_n - \sigma(u_{n-1}) \in \pi^n B$.

(ii) By (i), the image B', as a subset of $B^{\mathbb{N}_0}$, has the asserted description. The other claims are easily derived from this. □

First of all we apply this last result to the ring o with its identity endomorphism. We obtain, for any $\lambda \in o$, an element $\Omega(\lambda) = (\Omega_0(\lambda), \Omega_1(\lambda), \ldots) \in o^{\mathbb{N}_0}$ such that

$$\Phi_o(\Omega(\lambda)) = (\lambda, \ldots, \lambda, \ldots)\ .$$

By Lemma 1.1.3(i) this $\Omega(\lambda)$ is uniquely determined by λ. For any o-algebra B we use the canonical homomorphism $o \to B$ to view $\Omega(\lambda)$ also as an element in $B^{\mathbb{N}_0}$.

Example $\Omega_0(\lambda) = \lambda$, $\Omega_1(\lambda) = \pi^{-1}(\lambda - \lambda^q)$, $\Omega_2(\lambda) = \pi^{-2}(\lambda - \lambda^{q^2}) - \pi^{-1-q}(\lambda - \lambda^q)^q$.

Next we consider the polynomial o-algebra

$$A := o[X_0, X_1, \ldots, Y_0, Y_1, \ldots]$$

in two sets of countably many variables. Obviously $\pi 1_A$ is not a zero divisor in A. We consider on A the o-algebra endomorphism θ defined by

$$\theta(X_i) := X_i^q \quad \text{and} \quad \theta(Y_i) := Y_i^q \qquad \text{for any } i \geq 0.$$

Remark 1.1.6 $\theta(a) \equiv a^q \bmod \pi A$ *for any* $a \in A$.

Proof The subset $\{a \in A : \theta(a) \equiv a^q \bmod \pi A\}$ is a subring of A which, since $k^\times$ has order $q-1$, contains o as well as, by the definition of θ, all the variables X_i and Y_i. Hence it must be equal to A. □

Let $\mathbf{X} := (X_0, X_1, \dots)$ and $\mathbf{Y} := (Y_0, Y_1, \dots)$ in $A^{\mathbb{N}_0}$. Because of Lemma 1.1.3(i) and Proposition 1.1.5(ii) there exist uniquely determined elements $\mathbf{S} = (S_n)_n$, $\mathbf{P} = (P_n)_n$, $\mathbf{I} = (I_n)_n$, and $\mathbf{F} = (F_n)_n$ in $A^{\mathbb{N}_0}$ such that

$$\begin{aligned}\Phi_A(\mathbf{S}) &= \Phi_A(\mathbf{X}) + \Phi_A(\mathbf{Y}),\\ \Phi_A(\mathbf{P}) &= \Phi_A(\mathbf{X})\Phi_A(\mathbf{Y}),\\ \Phi_A(\mathbf{I}) &= -\Phi_A(\mathbf{X}),\\ \Phi_A(\mathbf{F}) &= f_A(\Phi_A(\mathbf{X}))\ ,\end{aligned}$$

respectively such that

$$\begin{aligned}\Phi_n(S_0, \dots, S_n) &= \Phi_n(X_0, \dots, X_n) + \Phi_n(Y_0, \dots, Y_n),\\ \Phi_n(P_0, \dots, P_n) &= \Phi_n(X_0, \dots, X_n)\Phi_n(Y_0, \dots, Y_n),\\ \Phi_n(I_0, \dots, I_n) &= -\Phi_n(X_0, \dots, X_n),\\ \Phi_n(F_0, \dots, F_n) &= \Phi_{n+1}(X_0, \dots, X_{n+1})\end{aligned} \tag{1.1.3}$$

for any $n \geq 0$. Remark 1.1.4 implies that

$$\begin{aligned}S_n, P_n &\in o[X_0, \dots, X_n, Y_0, \dots, Y_n],\\ I_n &\in o[X_0, \dots, X_n],\\ F_n &\in o[X_0, \dots, X_{n+1}].\end{aligned}$$

Lemma 1.1.7 $F_n \equiv X_n^q \bmod \pi A$ *for any* $n \geq 0$.

Proof We have

$$\begin{aligned}\Phi_n(F_0, \dots, F_n) = \Phi_{n+1}(X_0, \dots, X_{n+1}) &= \Phi_n(X_0^q, \dots, X_n^q) + \pi^{n+1} X_{n+1}\\ &\equiv \Phi_n(X_0^q, \dots, X_n^q) \bmod \pi^{n+1} A\ .\end{aligned}$$

Hence the assertion follows from Lemma 1.1.2(ii). □

The polynomials S_n, P_n, I_n, F_n can be computed inductively from the system of equations (1.1.3).

Example

(1) $S_0 = X_0 + Y_0$, $S_1 = X_1 + Y_1 - \sum_{i=1}^{q-1} \pi^{-1} \binom{q}{i} X_0^i Y_0^{q-i}$.
(2) $P_0 = X_0 Y_0$, $P_1 = \pi X_1 Y_1 + X_0^q Y_1 + X_1 Y_0^q$.
(3) $F_0 = X_0^q + \pi X_1$, $F_1 = X_1^q + \pi X_2 - \sum_{i=0}^{q-1} \binom{q}{i} \pi^{q-i-1} X_0^{qi} X_1^{q-i}$.

Exercise Show that:

(1) $S_n - X_n - Y_n \in o[X_0, \ldots, X_{n-1}, Y_0, \ldots, Y_{n-1}]$.
(2) If $p \neq 2$ then $I_n = -X_n$ for any $n \geq 0$.

Let B again be an arbitrary o-algebra. On the one hand we have the o-algebra $(B^{\mathbb{N}_0}, +, \cdot)$ defined as a direct product. Any o-algebra homomorphism $\rho : B_1 \longrightarrow B_2$ induces the o-algebra homomorphism

$$\begin{aligned} \rho^{\mathbb{N}_0} :\ B_1^{\mathbb{N}_0} &\longrightarrow B_2^{\mathbb{N}_0} \\ (b_n)_n &\longmapsto (\rho(b_n))_n \ . \end{aligned}$$

On the other hand we define on the set $W(B)_L := B^{\mathbb{N}_0}$ a new 'addition'

$$(a_n)_n \boxplus (b_n)_n := (S_n(a_0, \ldots, a_n, b_0, \ldots, b_n))_n$$

and a new 'multiplication'

$$(a_n)_n \boxdot (b_n)_n := (P_n(a_0, \ldots, a_n, b_0, \ldots, b_n))_n \ .$$

Moreover, we put

$$\mathbf{0} := (0, 0, \ldots) \quad \text{and} \quad \mathbf{1} := (1, 0, 0, \ldots) \ .$$

Because of (1.1.3) the map

$$\Phi_B : W(B)_L \longrightarrow B^{\mathbb{N}_0}$$

satisfies the identities

$$\begin{aligned} \Phi_B(\mathbf{a} \boxplus \mathbf{b}) &= \Phi_B(\mathbf{a}) + \Phi_B(\mathbf{b}), \\ \Phi_B(\mathbf{a} \boxdot \mathbf{b}) &= \Phi_B(\mathbf{a}) \cdot \Phi_B(\mathbf{b}) \ . \end{aligned} \tag{1.1.4}$$

In addition we obviously have

$$\Phi_B(\mathbf{0}) = 0 \quad \text{and} \quad \Phi_B(\mathbf{1}) = 1 \ . \tag{1.1.5}$$

For any o-algebra homomorphism $\rho : B_1 \longrightarrow B_2$ the map $W(\rho)_L := \rho^{\mathbb{N}_0} : W(B_1)_L \longrightarrow W(B_2)_L$ commutes with $\boxplus$ and $\boxdot$ and satisfies $W(\rho)_L(\mathbf{1}) = \mathbf{1}$ and the commutative diagram

$$\begin{tikzcd} W(B_1)_L \arrow[r, "\Phi_{B_1}"] \arrow[d, "W(\rho)_L"'] & B_1^{\mathbb{N}_0} \arrow[d, "\rho^{\mathbb{N}_0}"] \\ W(B_2)_L \arrow[r, "\Phi_{B_2}"] & B_2^{\mathbb{N}_0} \ . \end{tikzcd}$$

Proposition 1.1.8

(i) *$(W(B)_L, \boxplus, \boxdot)$ is a (commutative) ring with zero element* $\mathbf{0}$ *and unit element* $\mathbf{1}$*; the additive inverse of $(b_n)_n$ is $(I_n(b_0,\ldots,b_n))_n$.*
(ii) *The map $\Omega : o \longrightarrow (W(B)_L, \boxplus, \boxdot)$ is a ring homomorphism, making $(W(B)_L, \boxplus, \boxdot)$ into an o-algebra.*
(iii) *The map $\Phi_B : W(B)_L \longrightarrow B^{\mathbb{N}_0}$ is a homomorphism of o-algebras; in particular, for any $m \geq 0$,*

$$\begin{aligned}\Phi_m : W(B)_L &\longrightarrow B\\ (b_n)_n &\longmapsto \Phi_m(b_0,\ldots,b_m)\end{aligned}$$

is a homomorphism of o-algebras.
(iv) *For any o-algebra homomorphism $\rho : B_1 \longrightarrow B_2$ the map*

$$W(\rho)_L : W(B_1)_L \longrightarrow W(B_2)_L$$

is an o-algebra homomorphism as well.

Proof From the preliminary discussion above it remains to prove the assertions (i) and (ii). For that we consider the o-algebra $B_1 := o[\{X_b\}_{b\in B}]$ together with the surjective o-algebra homomorphism $\rho : B_1 \longrightarrow B$ defined by $\rho(X_b) := b$. On the algebra B_1 we have the endomorphism defined by $\sigma(X_b) := X_b^q$, which has the property that $\sigma(b) \equiv b^q \bmod \pi B_1$ for any $b \in B_1$ (compare the proof of Remark 1.1.6). Moreover $\pi 1_{B_1}$ is not a zero divisor in B_1. In this situation Lemma 1.1.3(i) and Proposition 1.1.5(ii) imply that

$$\Phi_{B_1} : W(B_1)_L \xrightarrow{\cong} B_1'$$

is a bijection onto the o-subalgebra B_1' in $B_1^{\mathbb{N}_0}$. Therefore, by (1.1.4) and (1.1.5), the associativity law, the distributivity laws, etc. in $B_1^{\mathbb{N}_0}$ transform into the corresponding laws for $\boxplus$ and $\boxdot$ in $W(B_1)_L$. Hence $(W(B_1)_L, \boxplus, \boxdot)$ is a commutative ring with unit element $\mathbf{1}$. The formula for the additive inverse follows analogously from (1.1.3). Since $\Phi_{B_1} \circ \Omega : o \longrightarrow B_1'$ is obviously a ring homomorphism it also follows that $\Omega : o \longrightarrow W(B_1)_L$ is one. Since the map $W(\rho)_L : W(B_1)_L \longrightarrow W(B)_L$ is surjective and respects $\boxplus$, $\boxdot$, $\mathbf{1}$, and the $\Omega(\lambda)$, the o-algebra axioms for $W(B)_L$ are a consequence of those for $W(B_1)_L$. □

Definition 1.1.9 $(W(B)_L, \boxplus, \boxdot)$ is called the ring of ramified Witt vectors with coefficients in B.

Exercise Show that the o-algebra $(W(B)_L, \boxplus, \boxdot)$, up to natural (in B) isomorphism, does not depend on the choice of the prime element π. Hint: The description of B' in Proposition 1.1.5(ii) uses only the ideal πB.

If $L = \mathbb{Q}_p$ and $\pi = p$ one simply speaks of the ring of Witt vectors $W(B) := W(B)_{\mathbb{Q}_p}$. The elements $\Phi_n(b_0, \ldots, b_n) \in B$ are called the *ghost components* of the Witt vector $(b_n)_n \in W(B)_L$.

In addition we have on $W(B)_L$ the maps

$$\begin{aligned} F : W(B)_L &\longrightarrow W(B)_L \\ (b_n)_n &\longmapsto (F_n(b_0, \ldots, b_{n+1}))_n \end{aligned}$$

and

$$\begin{aligned} V : W(B)_L &\longrightarrow W(B)_L \\ (b_n)_n &\longmapsto (0, b_0, b_1, \ldots) . \end{aligned}$$

Using (1.1.3) and (1.1.1) we obtain the commutativity of the diagrams

$$\begin{tikzcd} W(B)_L \arrow[r, "\Phi_B"] \arrow[d, "F"'] & B^{\mathbb{N}_0} \arrow[d, "f_B"] \\ W(B)_L \arrow[r, "\Phi_B"] & B^{\mathbb{N}_0} \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} W(B)_L \arrow[r, "\Phi_B"] \arrow[d, "V"'] & B^{\mathbb{N}_0} \arrow[d, "v_B"] \\ W(B)_L \arrow[r, "\Phi_B"] & B^{\mathbb{N}_0}. \end{tikzcd} \tag{1.1.6}$$

Proposition 1.1.10

(i) *F is an endomorphism of the o-algebra $W(B)_L$.*
(ii) *V is an endomorphism of the o-module $W(B)_L$.*
(iii) $F(V(\mathbf{b})) = \pi\mathbf{b}$ *for any* $\mathbf{b} \in W(B)_L$.
(iv) $V(\mathbf{a} \boxdot F(\mathbf{b})) = V(\mathbf{a}) \boxdot \mathbf{b}$ *for any* $\mathbf{a}, \mathbf{b} \in W(B)_L$.
(v) $F(\mathbf{b}) \equiv \mathbf{b}^q \bmod \pi W(B)_L$ *for any* $\mathbf{b} \in W(B)_L$.

Proof (Expressions in the assertions such as $\pi\mathbf{b}$ and $\mathbf{b}^q$ refer of course to the new o-algebra structure of $W(B)_L$.) Using the same technique as in the proof of Proposition 1.1.8 this reduces to corresponding identities for f_B and v_B in $B^{\mathbb{N}_0}$, which are easy to check. □

Definition 1.1.11 We call F and V the Frobenius and the Verschiebung on $W(B)_L$, respectively.

For any $m \geq 0$ define

$$V_m(B)_L := \mathrm{im}(V^m) = \{(b_n)_n \in W(B)_L : b_0 = \cdots = b_{m-1} = 0\} .$$

We obviously have

$$W(B)_L = V_0(B)_L \supseteq V_1(B)_L \supseteq \cdots \qquad \text{and} \qquad \bigcap_m V_m(B)_L = 0 .$$

By Proposition 1.1.10(ii) and (iv) every $V_m(B)_L$ is an ideal in $W(B)_L$.