Universal Group-theoretic Characterisation of Witt Vectors

विद्या वाचस्पति की
उपाधि की अपेक्षाओं की आंशिक पूर्ति में प्रस्तुत शोध प्रबंध

A thesis submitted in partial fulfillment of the requirements of the degree of Doctor of Philosophy

द्वारा / By

छात्र का नाम / Name of Student (in Hindi & English)

बिस्वनाथ सामंत / Biswanath Samanta

पंजीकरण सं. / Registration No.: 20203743

शोध प्रबंध पर्यवेक्षक / Thesis Supervisor:

Dr. Supriya Pisolkar

IISER PUNE

भारतीय विज्ञान शिक्षा एवं अनुसंधान संस्थान पुणे

INDIAN INSTITUTE OF SCIENCE EDUCATION AND RESEARCH PUNE

2025

Dedicated to
My Parents and My Wife

Certificate

Certified that the work incorporated in the thesis entitled "*Universal Group-theoretic Characterisation of Witt Vectors*", submitted by *Biswanath Samanta* was carried out by the candidate, under my supervision. The work presented here or any part of it has not been included in any other thesis submitted previously for the award of any degree or diploma from any other university or institution.

Date: December 08, 2025

Dr. Supriya Pisolkar
Thesis Supervisor

Declaration

I declare that this written submission represents my ideas in my own words and where others' ideas have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. I understand that violation of the above will be cause for disciplinary action by the institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

Biswanath.

Date: December 08, 2025 *Biswanath Samanta*

Roll Number: 20203743

Acknowledgements

I begin by thanking my Ph.D. supervisor Dr. Supriya Pisolkar, for her constant support, patience, and guidance. She was always available for discussions and took the time to explain things to me with great patience. Her mathematical guidance has given me a strong foundation to begin my independent research, and she also encouraged me to explore different areas. She created a smooth and friendly atmosphere for my work, and I am sincerely grateful to her.

Besides my supervisor, I would like to thank the rest of my research advisory committee: Dr. Ramla Abdellatif, Dr. Anand Sawant, and Dr. Vivek Mohan Mallick for their insightful comments and encouragement. I had the opportunity to discuss mathematics with many people, and I am thankful for their support and help. I would especially like to thank Prof. Amit Hogadi for teaching me different parts of mathematics and for giving me a lot of his time. I would also like to thank Prof. Anupam Kumar Singh and Prof. Soumen Maity for many helpful discussions, both mathematical and administrative, and for their constant motivation. I also thank my coursework teachers: Prof. Rama Mishra, Dr. Kaneenika Sinha, Dr. Rabeya Basu, and Prof. Mainak Poddar for their guidance. I am grateful to all of them.

I am thankful to CSIR for providing financial support through the research fellowship. I would also like to acknowledge the support of the institute, including the library staff and the administrative staff, for their cooperation. Special thanks are due to Ms. Sayalee Damle, Mrs. Suvarna Bharadwaj, and Mr. Yogesh Kolap for their help.

All the mathematics students at IISER Pune deserve appreciation for their enthusiasm in discussing mathematics with me. I would like to thank all my friends in the department for helping me with many things I was not good at, whether in mathematics or in other matters. A special mention goes to Visakh, Namrata, Ramandeep, Kunal, Sujeet, Dhruv, Darshan, Divyasree, Mridul, Arup, Dhrubajyoti, Kaustabh, Srijan, and Ayon. I also thank all my friends at IISER Pune with whom I shared many good moments. Many of you will recognise yourselves, and I hope you will forgive me for not naming each one of you individually.

Finally, I must express my deepest gratitude to my wife for providing me with unconditional support and constant encouragement throughout my years of study and research. Her patience, understanding, and belief in me have helped me stay focused and motivated during difficult times. I would also like to thank my parents for everything they have done to bring me to this level. Their love, sacrifices, and continuous support have shaped my journey in many ways. I am also grateful to my sister for always believing in me and for being very proud of my achievements. The love and support of my family have truly made a difference in my life.

December 08, 2025 *Biswanath Samanta*

Contents

Abstract

Let $\mathsf{Ab}, \mathsf{CRings}, \mathsf{Rings}$ respectively denote the category of abelian groups, unital commutative rings and unital associative rings. For a prime p, we have the classical construction of a p-typical Witt vector functor $W : \mathsf{CRings} \to \mathsf{CRings}$ given by E. Witt. There are multiple constructions of the group of p-typical Witt vectors of associative (possibly non-commutative) rings. It is known that all these constructions match with classical Witt functor W, when restricted to the CRings. One of the natural questions we have tried to answer in this thesis is - Is there a universal Witt functor on the Rings?

The first part of the thesis is devoted to the commutative set-up. Note that for $R \in \mathsf{CRings}$, the group $W(R)$ is endowed with a Verschiebung operator $W(R) \xrightarrow{V} W(R)$ and a Teichmüller map $R \xrightarrow{\langle\ \rangle} W(R)$. One of the properties satisfied by $V, \langle\ \rangle$ is that the map $R \to W(R)$ given by $x \mapsto V\langle x^p \rangle - p\langle x \rangle$ is an additive map. In this thesis, we show that for $p \neq 2$, this property essentially characterises the functor W. Unlike other known characterisations, this is a group-theoretic characterisation, in the sense that it does not use the ring structure of $W(R)$. This is important because most of the constructions of a Witt functor defined on non-commutative rings do not have a ring structure. Hence, we can use our group theoretic characterisation of W to answer the above question.

The second part of the thesis is devoted to the associative rings. We first define a notion of a pre-Witt functor which abstracts the above group theoretic property. We give a construction of a pre-Witt functor $E : \mathsf{Rings} \to \mathsf{Ab}$ adapting the construction of the Witt functor given by Cuntz-Deninger for the commutative rings. We prove that E when restricted to CRings matches with the functor W. We then define a Witt functor $\hat{E} : \mathsf{Rings} \to \mathsf{Ab}$ and give a universal group theoretic characterisation of $\hat{E}$ modulo an explicit conjecture about non-commutative polynomials. We prove that $\hat{E}$ admits a natural surjection to the Hesselholt's Witt functor W_H, without using the conjecture. We also suspect that the Witt functor W_H is the universal Morita invariant Witt functor.

Notation

$\mathbb{N}$	The set of natural numbers $\{1, 2, 3, \dots\}$.
$\mathbb{N}_0$	The set $\{0, 1, 2, \dots\}$.
Ab	The category of abelian groups.
CRings	The category of commutative rings.
Rings	The category of associative rings.
W	The classical Witt vector functor on CRings.
W_H	Hesselholt's generalisation of W to Rings.
E_c	An alternative construction of W given by Cuntz and Deninger.
E	Our modification of E_c that extends it to Rings.
$[R, R]$	The additive subgroup of R generated by commutators.
$R/[R, R]$	The additive abelianisation of R (not equal to R^{ab}).
$W_n(R)$	The ring of truncated Witt vectors of length n with coefficients in R.
V, F	The Verschiebung and Frobenius maps.
$\langle x \rangle$	The Teichmüller lift of x.
H^{sat}	The p-saturation of a subgroup $H \subseteq G$, $H^{\mathrm{sat}} = \{\, g \in G : p^{\ell} g \in H \text{ for some } \ell \geq 0 \,\}$.

Chapter 1

Introduction

Let CRings denote the category of commutative rings, Rings the category of associative rings, and Ab the category of abelian groups. Let p denote a prime number.

On the category CRings, there is the classical functor of p-typical Witt vectors (see [28], [24])

$$W : \mathsf{CRings} \to \mathsf{CRings}.$$

The Witt vector functor is a fundamental tool in arithmetic geometry and homotopy theory. An explicit description of $W(R)$ is given in [24, Chap. 2, §6], where the addition and multiplication are defined using the Witt polynomials. We note here that if R is a commutative ring of characteristic p, then $W(R)$ is a commutative ring of characteristic 0.

It is known that W has the following universal property in the context of strict p-rings.

Theorem 1.0.1 ([24, Chap. 2, §6]). *Let κ be a perfect ring of characteristic p. Then $W(\kappa)$ is the strict p-ring with residue ring κ.*

There is also a known categorical characterisation of W involving δ-rings.

Theorem 1.0.2 ([18]). *The Witt vector functor W is the right adjoint to the forgetful functor from the category of δ-rings to* CRings.

We emphasise that both of these characterisations rely crucially on the ring structure of $W(R)$. For associative (possibly non-commutative) rings, there are several interesting constructions of Witt vectors (see [11], [13], [8], [6]). Most of these constructions, however, do not equip the resulting Witt vectors with a natural ring structure. Nevertheless, they all agree with the classical definition when the underlying ring is commutative.

This naturally leads to the question of how these various constructions are related, and whether there exists a universal approach to defining the Witt vector functor on the category Rings. In this thesis, our focus will be on the following two particularly important constructions.

The first construction is due to L. Hesselholt ([11], [13]), which extended the classical construction to the following functor

$$W_H : \mathsf{Rings} \to \mathsf{Ab}.$$

The construction uses non-commutative analogue of the Witt polynomials to define group structure.

The second construction is due to Cuntz-Deninger [6], providing an alternative definition of the classical Witt vector functor

$$E : \mathsf{CRings} \to \mathsf{CRings},$$

which extends to associative rings; see [6, page 564]. The construction uses free presentations of rings and therefore does not require universal polynomials to define the ring structure.

For an associative ring R, $W_H(R)$ forms an abelian group, whereas $E(R)$ is a ring. Let

$$HH_0(E(R)) := E(R)/[E(R), E(R)].$$

The following question is posed by L. Hesselholt:

Question 1.0.3. Is $W_H(R)$ isomorphic to $HH_0(E(R))$?

This question was answered negatively by Hogadi and Pisolkar in [17] for $p = 2$, and later by Pisolkar in [21] for any prime p.

Theorem 1.0.4. [21, Theorem 1.1] *Let $A := \mathbb{Z}\{X, Y\}$ be the free ring with two variables. Then there is no continuous surjective group homomorphism from $W_H(A) \to HH_0(E(A))$ which is compatible with V and $\langle\,\rangle$.*

For associative rings, most constructions of Witt vectors do not have a ring structure.

Therefore, we consider $W(R)$ only as an abelian group instead of a ring; that is, we treat

$$W : \mathsf{CRings} \to \mathsf{Ab}.$$

This viewpoint allows a characterisation of W that extends naturally to the non-commutative setting. A more detailed discussion appears in Chapter 5.

In order to seek a universal Witt vector functor on Rings, it is natural to first ask whether the classical functor W admits a universal group-theoretic description. More precisely, we are led to the following question:

Question 1.0.5. Can we obtain a universal group-theoretic characterisation of W?

As mentioned earlier, we have the following natural question for the associative rings.

Question 1.0.6. Does there exist a universal construction of a Witt vector functor on Rings?

These are the central questions addressed in this thesis. Now we present the main results of the thesis.

(I) A universal group-theoretic characterisation of p-typical Witt vectors for commutative rings

(S. Pisolkar and B. Samanta; A group-theoretic characterisation of p-typical Witt vectors; J. Algebra **677** (2025), 1–12)

Let p denote a fixed odd prime throughout. To address Question 1.0.5, we first observe the important group-theoretic properties satisfied by the classical Witt functor W. These properties are recorded below.

Properties 1.0.7. *For $R \in \mathsf{CRings}$, there exist functorial maps*

- *(Verschiebung) $V : W(R) \to W(R)$ (group homomorphism)*
- *(Teichmüller map) $\langle - \rangle : R \to W(R)$ (set map)*

which satisfy the following properties

1. $\langle 0 \rangle = 0$. *If* $p \neq 2$ *then* $\langle -x \rangle = -\langle x \rangle$ *for all* $x \in R$.
2. $x \mapsto V\langle x^p \rangle - p\langle x \rangle$ *is an additive map from* $R \to W(R)$.
3. $W(R)$ *is complete w.r.t the filtration* $\{V^n W(R) \mid n \in \mathbb{N}_0\}$.
4. *If* A *is* p*-torsion free then* $W(A)$ *is also* p*-torsion free (see Lemma 2.2.20).*

We now abstract the properties 1.0.7 in the following definition.

Definition 1.0.8. [pre-Witt functor] A functor $F : \mathsf{CRings} \to \mathsf{Ab}$ is called a pre-Witt functor, if for every R, $F(R)$ is endowed with a functorial endomorphism $F(R) \xrightarrow{V} F(R)$ and a functorial map $R \xrightarrow{\langle\ \rangle} F(R)$ such that the properties 1.0.7 are satisfied.

We show that these properties essentially characterise the Witt vector functor W, which is summarized in the following theorem.

Theorem 1.0.9. [22, Theorem 1.6] *The classical functor of* p*-typical Witt vectors* W *is a universal pre-Witt functor.*

To prove this, we use the alternative definition of W due to Cuntz-Deninger, denoted by E. A crucial step in the argument is a linear-independence statement for Teichmüller-type elements in the abelian group $X(R)$ introduced in [6].

For $R \in \mathsf{CRings}$, write

$$\langle x \rangle := (x, x^p, x^{p^2}, \dots) \in X(R) \subset R^{\mathbb{N}_0}$$

for $x \in R$; see Definition 3.2.1 for details.

Lemma 1.0.10. *Let* $p \neq 2$. *Let* $A = \mathbb{Z}[S]$ *be a commutative polynomial ring over a set* S. *Let* $\{f_i\}_{i=1}^r$ *be a finite set of distinct non-zero elements of* A. *Further assume that* $f_i \neq -f_j$ *for any* $i \neq j$. *Then the subset* $\{\langle f_i \rangle\}_{i=1}^r$ *of* $X(A)$ *is* $\mathbb{Z}$*-linearly independent.*

We first define a functor $C : \mathsf{CRings} \to \mathsf{Ab}$ by enforcing the properties listed in 1.0.7. We show that C is a universal pre-Witt functor. Using Lemma 1.0.10, we prove that C

is isomorphic to E, which establishes Theorem 1.0.9. A detailed proof is presented in Chapter 4.

(II) A group-theoretic characterisation of p-typical Witt vectors for associative rings (Preprint)

(Authors: Supriya Pisolkar, Biswanath Samanta)

In order to answer Question 1.0.6, we extend the ideas of [22] to the case of associative (possibly non-commutative) rings. To approach this, we first observed the following change in Property 1.0.7(4) for associative rings in the construction given by Hesselholt [11].

(4′) If R and $\bar{R}$ are p-torsion free then $W_H(R)$ is p-torsion free, where $\bar{R} := \frac{R}{\langle [R,R] \rangle}$ and $\langle [R,R] \rangle$ is the ideal generated by the commutator subgroup $[R,R]$. (For details see Properties 5.1.1)

Definition 1.0.11. (Pre-Witt functor on Rings) A functor $F : \mathsf{Rings} \to \mathsf{Ab}$ is called a pre-Witt functor on Rings, if for every ring $R \in \mathsf{Rings}$, $F(R)$ is endowed with a functorial endomorphism $V : W(R) \to W(R)$ and a functorial map $\langle\ \rangle : R \to W(R)$ which satisfy the first three properties of 1.0.7 and the property (4′) above.

We give a new construction of a pre-Witt functor, denoted E, which is a slight modification of the construction of Cuntz–Deninger [6, page 564]. We now state the main results of this work.

Theorem 1.0.12. *E is a pre-Witt functor. Moreover:*

1. *The restriction of E to CRings is canonically isomorphic to the classical Witt functor W.*

2. *There exists a unique natural transformation $E \to W_H$, which is surjective.*

Furthermore, we formulate a conjectural characterisation of the functor E on Rings. This reduces to an explicit conjecture about non-commutative polynomial rings. This is the non-commutative analogue of the Lemma 1.0.10. Unfortunately, at present, we have only computational evidence supporting this statement, and therefore we record it as a conjecture.

Conjecture 1.0.13. *Let $p \neq 2$. Let $A = \mathbb{Z}\{S\}$ be a non-commutative polynomial ring over a set S. Let $\{f_i\}_{i=1}^r$ be a finite set of distinct non-zero elements of A. Further assume that $f_i \neq -f_j$ for any $i \neq j$. Then the subset $\{\langle f_i \rangle\}_{i=1}^r$ of $X(A)$ is $\mathbb{Z}$-linearly independent.*

We discuss more about this conjecture and provide computational evidence in Section 5.5. Assuming this conjecture, we obtain a universal characterisation of the functor E, which is summarized in the following theorem.

Theorem 1.0.14. *Assuming Conjecture 1.0.13, E is a universal pre-Witt functor on* Rings*.*

One of the main motivations for this work and also [22] was the following question.

Question 1.0.15. Can W_H be characterized by universal properties?

For a commutative ring R, the group of p-typical Witt vectors $W(R)$ has an additional property, i.e. that sum and difference of elements in $W(R)$ is given by explicit Witt polynomials. This implies the existence of a canonical bijection $R^{\mathbb{N}_0} \to W(R)$ of sets. A similar statement also holds for $W_H(R)$ for associative rings R, except that instead of a bijection, we have an epimorphism $R^{\mathbb{N}_0} \to W_H(R)$ (see [13, Page 56]). Motivated by this, we call a pre-Witt functor F a Witt functor if the sum and difference of elements in $F(R)$ are given by non-commutative Witt polynomials (see Definition 5.4.2).

It is natural to ask if there is a universal Witt functor on Rings. To answer this, we define a Witt functor $\hat{E}$ that is a suitable quotient of the pre-Witt functor E by a closed subgroup defined by certain Witt polynomials (see Definition 5.4.5). We have the following conjectural characterization of the functor $\hat{E}$.

Theorem 1.0.16. *The Conjecture 1.0.13 implies that $\hat{E}$ is a universal Witt functor for $p \neq 2$. In particular there is a unique natural transformation from $\hat{E} \to W_H$*

One can show that $\hat{E}$ is not isomorphic to W_H and moreover it is not Morita invariant.

We would like to pose the following question related to 1.0.15.

Question 1.0.17. Is W_H a universal Morita-invariant Witt functor?

Outline of the Thesis

In the next chapter which is Chapter 2, we recall the definition and fundamental properties of classical p-typical Witt vectors. We describe some applications and uses of p-typical Witt vectors. We conclude this chapter with a short discussion on big Witt vectors.

In Chapter 3, we discuss generalisations of the classical Witt vector construction to associative rings. Although several such constructions appear in the literature, in this thesis we focus on two particularly important ones: the construction of Hesselholt and the construction of Cuntz–Deninger.

In Chapter 4, we prove Theorem 1.0.9, which provides a universal group-theoretic characterisation of the classical Witt vector functor W on CRings. Our approach uses the alternative construction of W due to Cuntz-Deninger [6], denoted by E_c. We first define a functor $C : \mathsf{CRings} \to \mathsf{Ab}$ that attempts to enforce the properties listed in 1.0.7. We have proved that C is universal pre-Witt functor on CRings. We have then proved the universality of W by proving C is isomorphic to E_c.

In Chapter 5, we prove Theorem 1.0.12 and Theorem 1.0.14. We introduce the notion of a pre-Witt functor on Rings, defined by four properties 5.1.1 satisfied by Hesselholt's construction of W_H. We give a construction of a pre-Witt functor $E : \mathsf{Rings} \to \mathsf{Ab}$ adapting the construction of the Witt functor given by Cuntz-Deninger for commutative rings. We have proved that the restriction of E to CRings is the classical Witt functor W. We have defined $\hat{E}$ as a quotient of E. Furthermore, we also show that assuming Conjecture 1.0.13, $\hat{E}$ is the universal Witt functor. We prove that $\hat{E}$ admits a natural surjection to the Hesselholt's Witt functor W_H, without using the conjecture. In Section 5.5, we also provide evidence for Conjecture 1.0.13.

Chapter 2

Classical Witt Vectors

In this chapter, we recall the theory of Witt vectors, following the standard references, including Serre's Local Fields [24] and Hazewinkel's exposition in [10]. The chapter begins with a brief motivation for Witt vectors and the associated Witt polynomials arising from the structure of $\mathbb{Z}_p$. After this, we recall the definition and basic properties of classical p-typical Witt vectors. This construction is equipped with some important maps, namely the Verschiebung operator V and the Teichmüller map $\langle\,\rangle$, and we recall these together with their fundamental properties. The chapter concludes with a short discussion of big Witt vectors and their relation to the p-typical construction.

2.1 Motivation from p-adic integers

In this section, we follow the classical approach to Witt vectors and use the structure of the ring of p-adic integers $\mathbb{Z}_p$ as a motivating example. There are several equivalent ways to define the ring $\mathbb{Z}_p$ of p-adic integers. It may be viewed as the completion of $\mathbb{Z}$ with respect to the p-adic metric, or equivalently, as the inverse limit of the system of rings $\mathbb{Z}/p^n\mathbb{Z}$ for $n \geq 1$. A fundamental property of p-adic integers is the existence of systems of representatives for the residue field $\mathbb{F}_p$ in $\mathbb{Z}_p$. The following lemma formalizes this notion:

Lemma 2.1.1. *If S is a system of representatives of $\mathbb{F}_p$ in $\mathbb{Z}_p$, then every element of $\mathbb{Z}_p$ can be written uniquely as $\sum_{i=0}^{\infty} s_i p^i$ where $s_i \in S$.*

A natural and familiar choice for such a system of representatives is

$$S = \{0, 1, ..., p-1\}.$$

This leads to a bijection between the countable product of $\mathbb{F}_p$ and $\mathbb{Z}_p$:

$$\prod_{i\geq 0} \mathbb{F}_p \xrightarrow{\cong} \mathbb{Z}_p$$

given by the mapping $(a_0, a_1, ...) \mapsto \sum_{i\geq 0} a_i p^i$.

However, a natural question arises: can we express addition and multiplication of p-adic numbers using closed algebraic formulas in terms of their digits a_i? At first glance, this might seem like an easy question, but the problem is in fact quite subtle. The main difficulty comes from the familiar issue of carrying digits when performing arithmetic in base p, much like in ordinary decimal addition. These carries make it hard to write clean algebraic expressions for the operations directly in terms of the digits.

To deal with this difficulty, we can use an idea based on Hensel's lemma. Applying it to the polynomial $f(x) = x^{p-1} - 1$ gives us a special set of representatives for the elements of $\mathbb{F}_p$, called the Teichmüller representatives. This construction defines a map $\tau : \mathbb{F}_p \to \mathbb{Z}_p$, with the convention $\tau(0) = 0$. The map τ is multiplicative and satisfies the identity $\tau(x)^p = \tau(x)$ for all $x \in \mathbb{F}_p$.

By choosing our representatives to be $S = \tau(\mathbb{F}_p)$, we make it easier to understand and work with arithmetic in $\mathbb{Z}_p$. In fact, this choice helps us write algebraic formulas for addition and multiplication of p-adic numbers. This idea was first studied by Hensel and Teichmüller, and was later fully developed by Witt.

To prove this claim, let us consider elements of $\mathbb{Z}_p$ in Teichmüller digit expansions. Assume

$$\sum_{i=0}^{\infty} a_i p^i + \sum_{i=0}^{\infty} b_i p^i = \sum_{i=0}^{\infty} c_i p^i. \tag{2.1}$$

Now going modulo p, we have $c_0 = a_0 + b_0 \pmod{p}$; this implies

$$c_0^p = (a_0 + b_0)^p \pmod{p^2}.$$

Going modulo p^2, we get

$$c_0 + pc_1 = (a_0 + pa_1) + (b_0 + pb_1) \pmod{p^2}.$$

By the property $\alpha^p = \alpha$ for all $\alpha \in S = \tau(\mathbb{F}_p)$, we get

$$c_0^p + pc_1 = (a_0^p + pa_1) + (b_0^p + pb_1) \pmod{p^2}.$$

Now substitute $c_0^p = (a_0 + b_0)^p \pmod{p^2}$ and as $a_0^p + b_0^p - (a_0 + b_0)^p$ is divisible by p, we get

$$c_1 = a_1 + b_1 + \frac{a_0^p + b_0^p - (a_0 + b_0)^p}{p} \pmod{p}.$$

Continuing this process we can solve the equation (2.1) for $c_2, c_3, \ldots \in S$ □

In each step, we find polynomials with integer coefficients, call them $s_0, s_1, \ldots$ such that

$$\sum_{i=0}^{\infty} a_i p^i + \sum_{i=0}^{\infty} b_i p^i = \sum_{i=0}^{\infty} s_i(a_0, a_1, \ldots; b_0, b_1, \ldots) p^i.$$

We can do the same for multiplication of two elements of $\mathbb{Z}_p$. That is we can find polynomials $m_0, m_1, \ldots$ with integer coefficients such that

$$\Big(\sum_{i=0}^{\infty} a_i p^i\Big) \cdot \Big(\sum_{i=0}^{\infty} b_i p^i\Big) = \sum_{i=0}^{\infty} m_i(a_0, a_1, \ldots; b_0, b_1, \ldots) p^i.$$

As Teichmüller representative is multiplicative, this will be easier than addition.

This defines a ring structure on $\prod_{i=0}^{\infty} F_p$ which makes it as a characteristic 0 ring. This also makes the set bijection

$$\prod_{i=0}^{\infty} F_p \to \mathbb{Z}_p$$

defined by

$$(a_0, a_1, \ldots) \mapsto \sum \tau(a_i) p^i$$

into a ring isomorphism. If we define Witt polynomial to be $\omega_n = \sum_{i=0}^{n} p^i x_i^{p^{n-i}}$ and view them $\omega_n : \prod_{i=0}^{n} \mathbb{F}_p \to \mathbb{F}_p$. As Teichmüller representative commutes with pth power, it is easy to see that the ring structure is uniquely determined by the relation

$$\omega_n(x + y) = \omega_n(x) + \omega_n(y) \text{ and } \omega_n(xy) = \omega_n(x)\omega_n(y)$$

for all $n \in \mathbb{N}_0$.

Remark 2.1.2. Although the preceding discussion used the ring $\mathbb{F}_p$, the polynomials $s_0, s_1, \dots$ and $m_0, m_1, \dots$ obtained have integer coefficients. Hence they make sense over an arbitrary commutative ring R, and they determine corresponding operations on $R^{\mathbb{N}}$. The resulting ring is called the Witt ring of R, denoted by $W(R)$.

2.2 p-typical Witt vectors

The exposition in this section follows standard references [24] and [10]. Let $(X_0, X_1, ..., X_n, ...)$ be a sequence of indeterminates, and consider the following polynomials (called "Witt polynomials"):

$$\begin{aligned}
\omega_0 &= X_0 \\
\omega_1 &= X_0^p + pX_1 \\
&\vdots \\
\omega_n &= \sum p^i X_i^{p^{n-i}} = X_0^{p^n} + pX_1^{p^{n-1}} + ... + p^n X_n.
\end{aligned}$$

The following theorem guarantees the existence of polynomials of integer coefficients similar to $\{s_i\}$ and $\{m_i\}$ in our motivating example.

Theorem 2.2.1. [24, Chap. 2 §6] *For every $\Phi \in \mathbb{Z}[X, Y]$, there exists a unique sequence $(\varphi_0, \varphi_1, ..., \varphi_n, ...)$ with $\varphi_i \in \mathbb{Z}[X_0, X_1, ..., X_i, Y_0, Y_1, ..., Y_i]$ such that for all $n \geq 0$,*

$$\omega_n(\varphi_0, \varphi_1, ..., \varphi_n) = \Phi(\omega_n(X_0, ..., X_n), \omega_n(Y_0, ..., Y_n)).$$

Proof. From the given expression, it is easy to see the existence and uniqueness of each φ_i as an element of the ring $\mathbb{Z}[1/p][X_0, X_1, \dots, X_i, Y_0, Y_1, \dots, Y_i]$. The hard part is to show that these elements actually have integer coefficients. For a reference, see [24, Chap. 2 §6]. □

Definition 2.2.2. In the above theorem if we take $\Phi(X, Y) = X + Y$ and $\Phi(X, Y) = X \cdot Y$, we get back the polynomials $\{s_i\}$ and $\{m_i\}$ respectively. For any commutative ring with unity R, consider the set $R^{\mathbb{N}_0}$ and define addition and multiplication of two elements $\underline{x} = (x_0, x_1, ..., x_n, ...)$ and $\underline{y} = (y_0, y_1, ..., y_n, ...)$ of $R^{\mathbb{N}_0}$ by

$$\underline{x} +_w \underline{y} = (s_0(x_0, y_0), s_1(x_0, x_1, y_0, y_1), ...)$$

$$\underline{x} \cdot_w \underline{y} = (m_0(x_0, y_0), m_1(x_0, x_1, y_0, y_1), ...).$$

Theorem 2.2.3. [24, Chap. 2 §6, Thm. 7] *The laws of composition defined above make $R^{\mathbb{N}_0}$ into a commutative ring with unity (called the ring of Witt vectors with coefficients in R and denoted by $W(R)$).*

Definition 2.2.4 (Truncated Witt vectors)**.** Fix a natural number n. Since in Theorem 2.2.1, φ_n depends only on $\{X_i\}_{i=0}^n$ and $\{Y_i\}_{i=0}^n$. We can use $\{s_i\}_{i=0}^{n-1}$ and $\{m_i\}_{i=0}^{n-1}$ to give a ring structure on R^n. The resulting ring is called ring of Witt vectors of length n with coefficients from R and is denoted by $W_n(R)$.

Definition 2.2.5 (Ghost map)**.** For any commutative ring with unity R, we define the ghost map

$$\omega : W(R) \to (R^{\mathbb{N}_0}, +, \cdot)$$

defined by

$$\begin{aligned}\omega(x_0, x_1, ...) &:= (\omega_0(x_0), \omega_1(x_0, x_1), \omega_2(x_0, x_1, x_2), \dots) \\ &= (x_0, x_0^p + px_1, ..., x_0^{p^n} + px_1^{p^{n-1}} + ... + p^n x_n, ...)\end{aligned}$$

For $\underline{x} \in W(R)$, the values $\omega_n(\underline{x})$ for $n \in \mathbb{N}_0$ are called the ghost components of $\underline{x}$, and the coordinates x_n are the Witt components. If p is invertible in R, then the ghost map $\omega : W(R) \to R^{\mathbb{N}_0}$ is an isomorphism of rings. If R is p-torsion-free, then ω is injective. In this case, the ring structure on $W(R)$ agrees with the one obtained by pulling back the componentwise ring structure on $R^{\mathbb{N}_0}$ along the ghost map ω.

The construction of Witt vectors W is functorial. For $R \in \mathsf{CRings}$, we have already shown how to define a ring structure on $W(R)$. Given a ring homomorphism $g : R' \to R$, the induced map

$$W(g) : W(R') \to W(R)$$

is defined by

$$W(g)(x_0, x_1, \dots) = (g(x_0), g(x_1), \dots).$$

In fact, the categorical definition of Witt vectors is given in the following theorem.

Theorem 2.2.6. [14, Prop. 1.2] *There exists unique ring structure on the domain of the ghost map* $\omega : W(R) \to (R^{\mathbb{N}_0}, +, \cdot)$ *making it a natural transformation of functors from* $W(-)$ *to* $(-)^{\mathbb{N}_0}$ *on* CRings.

Example 2.2.7. We have the following classical examples of Witt rings.

1. $W(\mathbb{F}_p) \cong \mathbb{Z}_p$. We have discussed this in the motivating example.

2. If $\mathbb{F}_q$ denotes the finite field with p^n many elements then $W(\mathbb{F}_q) \cong \mathbb{Z}_p[\mu_{q-1}]$ is the ring of integers of the unique unramified extension of degree n of the p-adic numbers $\mathbb{Q}_p$.

We now discuss the basics of strict p-rings and their connection to the ring of Witt vectors.

Definition 2.2.8 (p-ring)**.** A ring R that is Hausdorff and complete for the topology defined by a decreasing sequence $\mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \dots \supset \mathfrak{a}_n \supset \dots$ of ideals such that $\mathfrak{a}_n \cdot \mathfrak{a}_m \subset \mathfrak{a}_{n+m}$ and whose residue ring $\kappa = R/\mathfrak{a}_1$ is a perfect ring of characteristic p.

Ring of integers of local fields and complete discrete valuation ring are examples of p-rings.

Definition 2.2.9 (Strict p-ring)**.** A p-ring R is called a strict p-ring if $\mathfrak{a}_n = p^n R$ and if p is not a zero-divisor in R.

Example 2.2.10. We have the following examples of strict p-ring [24, page 37].

1. Ring of integers of absolutely unramified local fields of mixed characteristic.

2. $\hat{S} = \hat{\mathbb{Z}}[X_\alpha^{p^{-\infty}}]$ with residue ring $\hat{S}/p\hat{S} = \mathbb{F}_p[X_\alpha^{p^{-\infty}}]$, which is perfect ring of characteristic p.

Theorem 2.2.11. [24, Chap.2 §5, Thm. 5] *For any perfect ring* κ *of characteristic* p*, there exists a unique strict* p*-ring* $H(\kappa)$ *with residue ring* κ*.*

Theorem 2.2.12. [24, Chap.2 §6, Thm. 8] *For a perfect ring κ of characteristic p, $W(\kappa)$ is isomorphic to the strict p-ring $H(\kappa)$.*

Corollary 2.2.13. *For any perfect field κ of characteristic $p > 0$, the ring $W(\kappa)$ of Witt vectors is a complete discrete valuation ring with uniformizer p (i.e., it is absolutely unramified) and residue field κ.*

Important maps on ring of Witt vectors

In this subsection, we recall several fundamental maps on the ring of Witt vectors, namely the Verschiebung operator, the Teichmüller lift, and the Frobenius map. We also record the basic relations among these operators and describe how they interact with one another.

Definition 2.2.14 (Verschiebung operator or Shift operator)**.** The Verschiebung operator is a map

$$V : W(R) \to W(R)$$

defined by

$$V(x_0, x_1, \dots) = (0, x_0, x_1, \dots).$$

Lemma 2.2.15. *The Verschiebung operator $V : W(R) \to W(R)$ is an additive map.*

Proof. The explicit formulas for addition and multiplication in Witt vectors are notoriously complicated, so direct computations are generally avoided. Instead, one typically works via the ghost map, whose injectivity on torsion-free rings allows arguments to be carried out on the simpler ghost components and then lifted back to Witt vectors. In ghost components, $V^\omega : R^{\mathbb{N}_0} \to R^{\mathbb{N}_0}$ is given by $V^\omega(x_0, x_1, \dots) = p(0, x_0, x_1, \dots)$. This makes the following diagram commute:

$$\begin{array}{ccc} W(R) & \xrightarrow{\;V\;} & W(R) \\ \downarrow{\scriptstyle \omega} & & \downarrow{\scriptstyle \omega} \\ R^{\mathbb{N}_0} & \xrightarrow{\;V^\omega\;} & R^{\mathbb{N}_0}. \end{array}$$

As the ring structure on $R^{\mathbb{N}_0}$ is defined pointwise, it is easy to see V^ω is additive. If R is p-torsion-free, ω is injective and hence V is additive. For a general ring, choose a ring surjection $g : R' \to R$ with R' is p-torsion-free. The induced map $W(g) : W(R') \to W(R)$ is again surjective. Since V is additive on the domain, it remains additive on the codomain as well. $\square$

Definition 2.2.16 (Teichmüller map)**.** It is a multiplicative map from

$$\langle\ \rangle : R \to W(R)$$

defined by

$$\langle x \rangle = (x, 0, 0, \dots).$$

In ghost components, it is given by

$$\langle\ \rangle^\omega : R \to R^{\mathbb{N}_0},$$

$$\langle x \rangle = (x, x^p, x^{p^2}, \dots).$$

Definition 2.2.17 (Frobenius map)**.** The unique ring homomorphism

$$F : W(R) \to W(R)$$

whose ghost components are given by

$$F^\omega(x_0, x_1, \dots) = (x_1, x_2, \dots)$$

is called the Frobenius map.

We have the following commutative diagram.

$$\begin{array}{ccc} W(R) & \xrightarrow{F} & W(R) \\ \downarrow{\scriptstyle\omega} & & \downarrow{\scriptstyle\omega} \\ R^{\mathbb{N}_0} & \xrightarrow{F^\omega} & R^{\mathbb{N}_0} \end{array}$$

If R is a ring of characteristic p, then the Frobenius map on Witt vectors is given by

$$F(x_0, x_1, \dots) = (x_0^p, x_1^p, \dots).$$

Definition 2.2.18 (Truncation maps)**.** There are surjective ring homomorphisms, called Truncation maps

$$W_{n+k}(R) \to W_n(R)$$

defined by

$$(a_0, a_1, \dots, a_{n+k-1}) \mapsto (a_0, a_1, \dots, a_{n-1}).$$

We have the following short exact sequence that relates the operator V and the truncation map T.

Proposition 2.2.19. *The sequence*

$$0 \to W_n(R) \xrightarrow{V^k} W_{n+k}(R) \xrightarrow{T^n} W_k(R) \to 0$$

is a exact sequence of rings.

Proof. By definition $V^k(a_0, a_1, \dots, a_{n-1}) = (0, 0, \dots 0, a_0, \dots, a_{n-1}) \in W_{n+k}(R)$. So, V^k is injective. Now $T^n(a_0, \dots, a_{n+k-1}) = (a_0, a_1, \dots, a_{k-1})$, so it is surjective. It is easy to see that $\operatorname{Im}(V^k) = \{(a_0, \dots, a_{n+k-1}) : a_0 = \dots = a_{k-1} = 0\} = \ker(T^n)$. Hence, the above is a short exact sequence. □

The following lemma records the key relations among V, F.

Lemma 2.2.20. *For any commutative ring with unity R, we have the following relations.*

1. $F \circ V = [p]$.
2. *If R is p-torsion free then $W(R)$ is also p-torsion-free.*

Proof. All of these statements can be verified by working in ghost coordinates, using the technique explained in the proof of Lemma 2.2.15.

(1) Consider the ghost components:

$$(F \circ V)^{\omega}(x) = F^{\omega}(V^{\omega}(x)) = F^{\omega}(p(0, x_0, x_1, \dots)) = p(x_0, x_1, \dots) = [p]^{\omega}(x).$$

Thus, $\omega(F \circ V) = \omega([p])$. If R is p-torsion free, then the ghost map ω is injective, so we conclude $F \circ V = [p]$ in $W(R)$. For a general ring R, choose a surjection $R' \twoheadrightarrow R$ where R' is p-torsion free. Then the induced map $W(R') \to W(R)$ is also surjective. Since $F \circ V = [p]$ holds in $W(R')$, it must also hold in $W(R)$.

(2) If R is p-torsion free, then so is $R^{\mathbb{N}_0}$. From Definition 2.2.5, the ghost map $\omega : W(R) \to R^{\mathbb{N}_0}$ is injective in this case. Hence, $W(R)$ must also be p-torsion-free. □

2.3 Applications of Witt vectors

This section outlines several contexts in which Witt vectors arise naturally. We begin with Witt's original motivation for introducing these objects. We then recall the definition and the category of δ-rings, emphasizing that for a p-torsion free ring, a δ-structure is equivalent to the existence of a Frobenius lift. The section concludes with an explanation of how, for $R \in \mathsf{CRings}$, the Witt ring $W(R)$ serves as the universal ring equipped with a Frobenius lift mapping to R.

Witt's original motivation to study these objects

The material in this subsection is based primarily on [28]. To understand what led E. Witt to study such objects, consider the problem of classifying cyclic extensions of a field k of fixed degree n. A foundational tool in this direction is Kummer theory. Its main limitation is that it requires the base field k to contain a primitive nth root of unity. When this assumption fails, or when $\text{char}(k)$ divides n, Kummer theory does not give a complete classification. For instance, one may ask for a description of cyclic extensions of degree p over a field of characteristic p. This question is answered by the following classical result, known as the Artin-Schreier theorem.

Theorem 2.3.1. [1] *If k is a field of char $p > 0$, any cyclic extension L/k of degree p is of the form $L = k(\alpha)$ where α satisfies $x^p - x - a = 0$ for some $a \in k$.*

E. Witt was interested in the classification of cyclic extensions of degree p^n over fields of characteristic p. In studying this problem, he discovered certain polynomials closely related to the addition law for p-adic integers. By organizing these polynomials systematically, he obtained a description of cyclic extensions of degree p^n. The main result from this work is now known as the Artin-Schreier-Witt theorem.

Theorem 2.3.2. [28] *Let k be a field of characteristic $p > 0$. Then any cyclic extension L/k of degree p^n is of the form*

$$L = k(\beta_0, \beta_1, ..., \beta_{n-1})$$

where $\beta = (\beta_0, \beta_1, ..., \beta_{n-1}) \in W_n(k_s)$ satisfies $F\beta - \beta - a = 0$ for some $a = (a_0, a_1, ..., a_{n-1}) \in W_n(k)$.

Let k be a field of characteristic $p > 0$. Then any cyclic extension L/k of degree p^n is of the form

In other words, L is the splitting field of a system of equations

$$x_0^p = \omega_0(\underline{x} + \underline{a}), x_1^p = \omega_1(\underline{x} + \underline{a}), \ldots x_{n-1}^p = \omega_{n-1}(\underline{x} + \underline{a})$$

for some $\underline{a} = (a_0, a_1, \ldots, a_{n-1}) \in k^n$.

Connection with δ-rings

André Joyal has shown the connection between the theory of Witt vectors and the theory of δ-rings and Frobenius lifts. Within this framework, Witt vectors provide a "universal way" to lift the Frobenius endomorphism modulo p for any ring R. This perspective has since become central in p-adic Hodge theory and prismatic cohomology. The material in this section is based primarily on [18].

Definition 2.3.3. For a integer prime p and for a commutative ring R, a Frobenius lift

ϕ on R is a ring homomorphism which makes the following diagram commute.

$$\begin{CD} R @>{\phi}>> R \\ @VVV @VVV \\ R/pR @>{x\mapsto x^p}>> R/pR \end{CD}$$

Given two rings with Frobenius lifts (R_1, ϕ_1) and (R_2, ϕ_2), a homomorphism between them is a ring homomorphism $f : R_1 \to R_2$ which makes the following diagram commutes.

$$\begin{CD} R_1 @>{f}>> R_2 \\ @V{\phi_1}VV @VV{\phi_2}V \\ R_1 @>{f}>> R_2 \end{CD}$$

Let Ring_ϕ denote the category of rings equipped with a Frobenius lift. The category Ring_ϕ admits arbitrary limits, but these do not commute with the forgetful functor to Ring. This is one of the reasons we prefer the category of δ-rings.

Definition 2.3.4. A δ-ring is a pair (R, δ) where R is a commutative ring with unity and $\delta : R \to R$ is a set map satisfying the following conditions for all $x, y \in R$.

1. $\delta(1) = 0$
2. $\delta(xy) = x^p\delta(y) + y^p\delta(x) + p\delta(x)\delta(y)$
3. $\delta(x + y) = \delta(x) + \delta(y) - \sum_{i=1}^{p-1} \frac{(p-1)!}{i!(p-i)!} x^i y^{p-i}$

The last condition implies that

$$p(\delta(x + y) - \delta(x) - \delta(y)) = x^p + y^p - (x + y)^p$$

and conversely if R is a p-torsion-free.

Example 2.3.5. There is a unique way to equip $\mathbb{Z}$ with the structure of a δ-ring, namely via the map

$$\delta(x) = \frac{x - x^p}{p}.$$

Lemma 2.3.6. *Fix a commutative ring R.*

1. *Suppose that $\delta : R \to R$ is a δ-structure on R (that is, (R, δ) is a δ-ring). Then the map $\phi : R \to R$ given by*

$$\phi(x) = x^p + p\delta(x)$$

   is a ring homomorphism that induces the Frobenius endomorphism on R/pR.

2. *If R is a p-torsion-free, then this construction defines a bijection between δ-structures on R and Frobenius lifts on R.*

Let Ring_δ denote the category of rings equipped with a δ-structure, where morphisms are ring homomorphisms compatible with the respective δ-structures. The category Ring_δ admits arbitrary limits and colimits, and these commute with the forgetful functor to Ring. Consider the forgetful functor

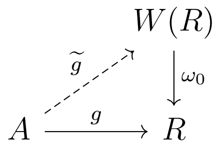
$$F : \mathsf{Ring}_\delta \to \mathsf{Ring}.$$

For a δ-ring (R, δ), the functor simply forgets the δ-structure, so that $F(R, \delta) = R$. Applying Freyd's Adjoint Functor Theorem to F, we find that it admits a right adjoint. The right adjoint is precisely the p-typical Witt vectors, as defined earlier in this chapter.

Remark 2.3.7. One can interpret this adjointness in terms of the lifting of maps. Let R be a commutative ring and A a δ-ring. Since W is right adjoint to F, we have

$$\mathrm{Hom}_{\mathsf{Ring}}(A, R) = \mathrm{Hom}_{\mathsf{Ring}_\delta}(A, W(R)).$$

In other words, if A is a δ-ring with a ring homomorphism to R, then there exists a unique map of δ-rings $A \to W(R)$ such that the following diagram commutes:



2.4 Big Witt vectors

We take a short digression to relate the p-typical Witt vector functor to the big Witt vector functor and to the theory of λ-rings. In this section, we discuss the notion of generalised (or big) Witt vectors as developed by P. Cartier. The material in this section is due to P. Cartier [5] and L. Hesselholt [14]. A more modern viewpoint is given by Borger [2]. In this section, we do not fix a prime p.

Definition 2.4.1. A non-empty subset $S \subset \mathbb{N}$ is called truncation set if $n \in S$, and if d is a divisor of n, then $d \in S$.

Definition 2.4.2 (Ghost map)**.** For any commutative ring with unity R, we have ghost map

$$\omega : R^S \to R^S$$

that takes the vector $a = (a_n : n \in S)$ to the sequence $\omega(a) = (\omega_n(a) : n \in S)$ with

$$\omega_n(a) = \sum_{e|n} e a_e^{n/e}.$$

This is injective when R is S-torsion free.

In the approach to Witt vectors taken here, all necessary congruences are given in the following lemma, commonly attributed to Dwork, whose non-commutative version we will discuss in Lemma 3.1.5.

Lemma 2.4.3. [14, Lemma 1.1.] *Suppose that for every prime number $p \in S$, there exists a ring homomorphism $\phi_p : R \to R$ such that for all $x \in R$*

$$\phi_p(x) \equiv x^p \pmod{pR}.$$

Then for a sequence $x = (x_n : n \in S)$, the following are equivalent.

1. *The sequence x is in the image of the ghost map $\omega : R^S \to R^S$.*
2. *For every prime $p \in S$ and every $n \in S$ with $\nu_p(n) \geq 1$,*

$$\phi_p(x_{n/p}) \equiv x_n \pmod{p^{\nu_p(n)}R}.$$

Proposition 2.4.4. [14, Prop. 1.2.] *There exists a unique ring structure on the domain of the ghost map*

$$\omega : R^S \to (R^S, +, \cdot)$$

making it a natural transformation of functors from CRings *to* CRings*.*

Definition 2.4.5 (Big Witt vectors)**.** For a truncation set S and $R \in$ CRings, the set R^S equipped with the unique ring structure mentioned in Proposition 2.4.4 is called the ring of big Witt vectors. This is denoted by $W_S(R)$.

Therefore, the ghost map is a ring homomorphism

$$\omega : W_S(R) \to R^S.$$

For $x = (x_n : n \in S) \in R^S$, the values $\omega_n(x)$ for $n \in S$ are called the *ghost components* of x, and the coordinates x_n are called the *Witt components*.

Remark 2.4.6. Fix a prime number p. If we take the truncation set

$$S = \{1, p, p^2, \dots\},$$

then we recover the p-typical Witt vectors defined earlier in this chapter.

The construction of Witt vectors W is functorial. As in the classical case, there are several fundamental maps on the ring of big Witt vectors, namely the Verschiebung operator, the Teichmüller lift, and the Frobenius maps. If $S \subset \mathbb{N}$ is a truncation set and $n \in \mathbb{N}$, then the set

$$S/n := \{\, e \in \mathbb{N} : ne \in S \,\}$$

is again a truncation set, possibly empty.

Definition 2.4.7 (Verschiebung operator)**.** For every $n \in \mathbb{N}$, the nth Verschiebung operator is an additive map

$$V_n : W_{S/n}(R) \to W_S(R)$$

defined by for $x = (x_e : e \in S/n)$, $V_n(x) = (y_m : m \in S)$ where

$$y_m = \begin{cases} x_e & \text{if } m = ne, \\ 0 & \text{otherwise.} \end{cases}$$

Definition 2.4.8 (Frobenius map)**.** For every $n \in \mathbb{N}$, there exists a unique natural ring homomorphism

$$W_S(R) \xrightarrow{F_n} W_{S/n}(R)$$

called the nth Frobenius that makes the following diagram, where the map F_n^ω takes the sequence $x = (x_m : m \in S)$ to the sequence $F_n^\omega(x) = (x_{ne} : e \in S/n)$, commute.

$$\begin{array}{ccc} W_S(R) & \xrightarrow{F_n} & W_{S/n}(R) \\ \downarrow{\scriptstyle\omega} & & \downarrow{\scriptstyle\omega} \\ R^S & \xrightarrow{F_n^\omega} & R^{S/n}. \end{array}$$

Definition 2.4.9. The Teichmüller representative is the map

$$R \xrightarrow{\langle\rangle_S} W_S(R)$$

whose mth component is r, if $m = 1$, and 0, otherwise. It is a multiplicative map.

Lemma 2.4.10. *Every element $x \in W_S(R)$ can be written as $\sum_{n \in S} V_n\langle x_n \rangle$.*

Proof. Observe that both elements have the same image under the ghost map. Hence, they are equal whenever R is S-torsion free. For a general ring R, choose an S-torsion free ring R' together with a surjective ring homomorphism $R' \to R$. This induces a surjective homomorphism

$$W_S(R') \to W_S(R).$$

Since the claim holds in the domain, it also holds in the codomain. □

The notion of λ-rings is motivated by the operations that naturally arise in the theory of Witt vectors. It provides a framework in which the big Witt vector functor can be understood as a universal construction.

Definition 2.4.11 (λ-rings)**.** A λ-ring is a commutative ring R together with functions

$$\lambda^n : R \to R \quad (n \geq 0),$$

called λ-operators such that for all $x, y \in R$, the following axioms are satisfied:

1. $\lambda^0(x) = 1$,
2. $\lambda^1(x) = x$,
3. $\lambda^n(1) = 0$ for all $n \geq 2$,
4. $\lambda^n(x+y) = \sum_{i+j=n} \lambda^i(x)\lambda^j(y)$,
5. $\lambda^n(xy) = P_n(\lambda^1(x), \dots, \lambda^n(x); \lambda^1(y), \dots, \lambda^n(y))$,
6. $\lambda^n(\lambda^m(x)) = P_{n,m}(\lambda^1(x), \dots, \lambda^{nm}(x))$.

Here, P_n and $P_{n,m}$ are universal polynomials with integer coefficients as in [30, Example 1.9] and [30, Example 1.7]. Their explicit formulas are quite involved, so we avoid writing them down here and refer to the cited source for the full details.

Example 2.4.12. [30, page 9] Some of the examples of λ-rings are given below.

1. The ring $\mathbb{Z}$ with λ-structure is given by

$$\lambda^i(n) = \text{ coefficient of } t^i \text{ in } (1+t)^n.$$

2. The ring $W(R)$ of big Witt vectors on R is a λ-ring.

Definition 2.4.13. The category of λ-rings is defined as follows. The objects are λ-rings. For two λ-rings R and S, a morphism is a ring homomorphism $f : R \to S$ satisfying

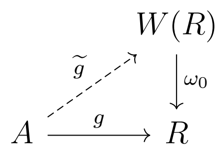
$$f \circ \lambda^i = \lambda^i \circ f \qquad \text{for all } i \geq 0.$$

The category is denoted by CRings_λ. The category CRings_λ admits arbitrary limits and colimits, and these commute with the forgetful functor to CRings. Applying Freyd's Adjoint Functor Theorem, one finds that it admits a right adjoint, which is precisely the big Witt vector functor.

Remark 2.4.14. One can interpret this adjointness in terms of the lifting of maps. Let R be a commutative ring and A a δ-ring. Since W is right adjoint to F, we have

$$\mathrm{Hom}_{\mathsf{CRings}}(A, R) = \mathrm{Hom}_{\mathsf{CRings}_\lambda}(A, W(R)).$$

In other words, if A is a λ-ring with a ring homomorphism to R, then there exists a unique map of λ-rings $A \to W(R)$ such that the following diagram commutes:



Corollary 2.4.15 (Universal property of big Witt Vectors)**.** *$W_S(R)$ is the universal ring with a commutating family of Frobenius $\{F_p$: for primes $p \in S\}$ mapping to R. That is for any torsion free ring A with a commutating family of Frobenius $\{\phi_p$: for primes $p \in S\}$ mapping to R then the $\exists$ unique ring homomorphism $A \to W_S(R)$ compatible with the Frobenius.*

Chapter 3

Witt vectors of associative rings

In this chapter, we discuss generalisations of the classical Witt vector construction to associative rings. Although several constructions appear in the literature, our focus will be on two important constructions. The first is the functor

$$W_H : \mathsf{Rings} \to \mathsf{Ab},$$

introduced by Hesselholt in [11, 13] using non-commutative analogues of the classical Witt sum and difference polynomials. The second construction is the functor

$$E : \mathsf{Rings} \to \mathsf{Rings},$$

introduced by Cuntz–Deninger in [6], which does not rely on universal polynomials for addition and multiplication. Instead, the construction is based on torsion-free presentations of rings. This chapter gives a brief overview of these constructions and records the necessary modifications that will be important in later chapters.

3.1 Hesselholt's construction

The goal of this section is to present the construction of the functor W_H, following the work of L. Hesselholt in [11, 13]. Although Hesselholt denotes this functor by W, we will use the notation W_H to distinguish it from the classical Witt vector functor, for which we reserve the symbol W. We begin with a simple observation that motivates the construction.

Let R be any ring and p a prime. If R is commutative, then for all $a, b \in R$, we have

$$(a+b)^p \equiv a^p + b^p \pmod{pR}.$$

In the associative case,

$$(a+b)^p \equiv a^p + b^p \pmod{pR + [R, R]},$$

where $[R, R]$ denotes the subgroup generated by all commutators.

Remark 3.1.1. This identity suggests a framework for extending Witt vectors to associative rings. A natural approach to do this would involve defining Witt-like polynomials modulo $pA + [A, A]$, mimicking the ghost components from the commutative case.

Circular words

Let S be a totally ordered poset, and consider the free (non-commutative) ring $A = \mathbb{Z}\{S\}$. Two words in A are said to be conjugate if one can be obtained from the other by a cyclic permutation of its letters.

Definition 3.1.2 (Circular words)**.** The equivalence classes of ordinary words under the natural action of the cyclic group are called circular words.

For each circular word, the lexicographically least element will be called its preferred representative. We use $\widetilde{w}$ to denote an ordinary word and w to denote a circular word.

Lemma 3.1.3. *Let S be a totally ordered poset and let $A = \mathbb{Z}\{S\}$ denote the free ring generated by S. Then we have the following:*

1. *Two words are conjugate if and only if their difference is a commutator.*
2. *The abelian group $A/[A, A]$ is freely generated by the set of circular words in S.*
3. *An element $\alpha \in A$ lies in $[A, A]$ if and only if all the lexicographically least words (in the additive expansion of α) appear with coefficient zero.*

Proof. (1) Let $\widetilde{\omega}_1 = s_1 s_2 \cdots s_n$ and $\widetilde{\omega}_2 = s_i s_{i+1} \cdots s_n s_1 s_2 \cdots s_{i-1}$ be conjugate words in A. Writing $x = s_1 \cdots s_{i-1}$ and $y = s_i \cdots s_n$, we observe that

$$\widetilde{\omega}_1 - \widetilde{\omega}_2 = xy - yx,$$

which is a commutator. Conversely, if $\widetilde{\omega}_1 - \widetilde{\omega}_2 = xy - yx$ for some words x, y, then $\widetilde{\omega}_1 = xy$ and $\widetilde{\omega}_2 = yx$ must be words of the same length. Suppose $|y| = m$. Then $\widetilde{\omega}_2$ is obtained from $\widetilde{\omega}_1$ by applying a cyclic permutation m times. In particular, the two words are conjugate.

(2) This follows immediately from part (1), together with the fact that $A = \mathbb{Z}\{S\}$ is a free abelian group with basis given by words in S. The conjugacy classes of words (i.e., circular words) thus form a basis for $A/[A, A]$.

(3) Given a circular word w, let $\sigma_0(w)$ be the lexicographically least representative in its conjugacy class, and extend σ_0 linearly to all of $A/[A, A]$. This gives a section

$$\sigma_0 : A/[A, A] \to A$$

of the natural projection $\pi : A \to A/[A, A]$. Then σ_0 is an injective group homomorphism satisfying $\pi \circ \sigma_0 = \mathrm{id}$, and hence:

$$\begin{aligned} \alpha \in [A, A] &\iff \sigma_0(\pi(\alpha)) = 0 \\ &\iff \text{all the lexicographically least words in } \alpha \text{ have coefficients zero.} \end{aligned}$$

□

Definition 3.1.4 (Ghost map)**.** For any associative ring R, the ghost map

$$\omega : R^{\mathbb{N}_0} \to (R/[R, R])^{\mathbb{N}_0}$$

is given by

$$\omega(x_0, x_1, ...) = (\overline{\omega_0(x_0)}, \overline{\omega_1(x_0, x_1)}, ...),$$

where $\omega_0(x_0) = x_0$, $\omega_1(x_0, x_1) = x_0^p + px_1$, $\omega_2(x_0, x_1, x_2), \ldots, \omega_n(x_0, \ldots, x_n) = x_0^{p^n} + px_1^{p^{n-1}} + ... + p^n x_n$ and so on.

If $R/[R,R]$ is p-torsion-free, then the map ω is injective. We have the following noncommutative analogue of Dwork's lemma.

Lemma 3.1.5. [11, Lemma 1.3.2] *If a ring R has an additive homomorphism $\phi : R \to R$ such that*

- *$\phi([R,R]) \subset [R,R]$ and*
- *for all $x \in R$ and for all $n \geq 1$,*

$$\phi(x^{p^{n-1}}) \equiv x^{p^n} \pmod{p^n R + [R,R]}.$$

Then a sequence $(w_0, w_1, \dots)$ is in the image of the ghost map $\omega : R^{\mathbb{N}_0} \to (R/[R,R])^{\mathbb{N}_0}$ if and only if $\phi(w_{n-1}) \equiv w_n \pmod{p^n R + [R,R]}$ for all $n \in \mathbb{N}_0$.

Fix a prime p. Let S be a totally ordered poset. Consider the free ring $A = \mathbb{Z}\{S\}$. Define $\phi : A \to A$ by $\phi(\sum a_{\widetilde{w}} \widetilde{w}) = \sum a_{\widetilde{w}} \widetilde{w}^p$. Then ϕ is a group homomorphism satisfying the hypothesis of Lemma 3.1.5. Recall that the projection $\pi : A \to A/[A,A]$ has a preferred section σ_0 which which sends a circular word w to the lexicographically least representative in its class and extends by linearity. Then as a corollary of the above lemma, we get the following.

Corollary 3.1.6. *(1) There is a preferred set-theoretic section $\sigma : \omega(A^{\mathbb{N}_0}) \to A^{\mathbb{N}_0}$ of the ghost map $\omega : A^{\mathbb{N}_0} \to (A/[A,A])^{\mathbb{N}_0}$.*

(2) Since ϕ is additive homomorphism, image of ω is a subgroup of $(A/[A,A])^{\mathbb{N}_0}$.

Non-commutative sum and difference polynomials

We consider the free ring $U = \mathbb{Z}\{a_0, b_0, a_1, b_1, ...\}$ with the generators ordered as indicated. Let $\phi : U \to U$ be as above. Since, image of ω forms a subgroup of $(U/[U,U])^{\mathbb{N}_0}$. There must exists $(c_0, c_1, ...)$ such that $\omega(c_0, c_1, ...) = \omega(a_0, a_1, ...) + \omega(b_0, b_1, ...)$.

Definition 3.1.7. We define non-commutative polynomials $s_i, d_i \in \mathbb{Z}\{a_0, b_0, ..., a_i, b_i\}$ by

$$(s_0, s_1, s_2, ...) := \sigma(\omega(a_0, a_1, ...) + \omega(b_0, b_1, ...)),$$

$$(d_0, d_1, d_2, ...) := \sigma(\omega(a_0, a_1, ...) - \omega(b_0, b_1, ...)).$$

Then s_i is a non-commutative polynomial in the variables $a_0, b_0, \ldots a_i, b_i$ and similarly for d_i. If we map U to the commutative polynomial ring with the same set of generators then s_i and d_i are mapped to the classical Witt sum and difference polynomials defined in Definition 2.2.2.

Let $R \in \mathsf{Rings}$. For $\underline{a} = (a_0, a_1, ..., a_{n-1}), \underline{b} = (b_0, b_1, ..., b_{n-1}) \in R^n$, define

$$\underline{a} * \underline{b} = (s_0(a_0, b_0), ..., s_{n-1}(a_0, b_0, ..., a_{n-1}, b_{n-1}))$$

Then this gives a binary operation on R^n with zero element $\underline{0} = (0, ..., 0)$. Consider ghost map

$$\omega : (R^n, *) \to (R/[R, R])^n,$$

which is a composition preserving map. The map ω is not injective, even when $R/[R, R]$ is p-torsion free. Hence identifying $(R^n, *)$ with $W_n(R)$ does not match with our classical Definition 2.2.5.

Definition 3.1.8. [13, page 56] We define abelian groups $W_n(R)$ inductively, such that ghost map ω factors through $W_n(R)$.

$$\begin{array}{ccc} R^n & \xrightarrow{\omega} & \left(\frac{R}{[R,R]}\right)^n \\ {\scriptstyle q}\downarrow & \nearrow{\scriptstyle \bar{\omega}} & \\ W_n(R) & & \end{array}$$

such that

1. $W_1(R) = R/[R, R]$
2. the induced map (also called ghost map) $\bar{\omega}$ is a homomorphism of groups and is injective if $R/[R, R]$ is p-torion-free.

Definition 3.1.9 (Definition of W_H)**.** From the construction of $W_n(R)$, we have an inverse system $\{T : W_n(R) \to W_{n-1}(R)\}$, where

$$T : W_n(R) \to W_{n-1}(R)$$

defined by $T(a_0, a_1, \dots a_{n-1}) = (a_0, a_1, \dots a_{n-2})$ for all $n \in \mathbb{N}$. We define

$$W_H(R) := \varprojlim_n W_n(R).$$

Then clearly the ghost map $\omega : R^{\mathbb{N}_0} \to (R/[R,R])^{\mathbb{N}_0}$ factors through

$$\begin{array}{ccc} R^{\mathbb{N}_0} & \xrightarrow{\omega} & \left(\frac{R}{[R,R]}\right)^{\mathbb{N}_0} \\ \Big\downarrow q & \nearrow \bar{\omega} & \\ W_H(R) & & \end{array}$$

where q is surjective and $\bar{\omega}$ is injective whenever $R/[R,R]$ is p-torsion free. By abuse of notation, we denote an element $q(a_0, a_1, ...)$ of $W_H(R)$ simply by $(a_0, a_1, ...)$.

We have the additive Verschiebung operator

$$V : W_H(R) \to W_H(R)$$

defined by

$$V(x_0, x_1, \dots) = (0, x_0, x_1, \dots),$$

and the Teichmüller map

$$\langle\ \rangle : R \to W_H(R)$$

given by

$$\langle x \rangle = (x, 0, 0, \dots).$$

We also have their truncated versions: $V : W_n(R) \to W_{n+1}(R)$ and $\langle\ \rangle : R \to W_n(R)$. There is a short exact sequence relating the operator V and the truncation map T, analogous to Proposition 2.2.19.

Proposition 3.1.10. [11, Prop. 1.6.3] *The sequence*

$$0 \to W_n(R) \xrightarrow{V^k} W_{n+k}(R) \xrightarrow{T^n} W_k(R) \to 0$$

is exact.

We conclude this section with a result that will be used in later chapters of this thesis.

Lemma 3.1.11. *For any* $(r_0, r_1, \dots) \in W_H(R)$*, we have*

$$(r_0, r_1, \dots) = \sum_{i=0}^{\infty} V^i \langle r_i \rangle.$$

Proof. Applying ghost map, both sides become $(r_0, r_0^p + pr_1, \dots)$. Therefore, if $R/[R, R]$ is p-torsion-free, then the ghost map is injective, and hence they are equal (see also [17, Lemma 3.3]). For a general ring R, choose a surjective ring homomorphism $R' \twoheadrightarrow R$ such that $R'/[R', R']$ is p-torsion free. Then the induced map $W(R') \to W(R)$ is a surjective continuous homomorphism compatible with both V and $\langle \cdot \rangle$. Since the claim holds for the domain R', it follows for the target R as well. □

3.2 Cuntz-Deninger's construction

Cuntz and Deninger [6] provided an alternative construction of the classical p-typical Witt vectors that avoids the use of universal polynomials to define the ring structure. Their construction applies more generally to any truncation set S, but in this thesis, we will restrict our attention to the p-typical case where $S = \{1, p, p^2, \dots\}$. Although on CRings, Cuntz and Deninger denote this functor by E, we will use the notation E_c to distinguish it from the Witt vector functor of associative rings, for which we reserve the symbol E. The material in this section is based on [6].

We briefly recall the construction of the ring $E_c(R)$ and collect some results for the reader's convenience. For $R \in \mathsf{CRings}$, and with the truncation set $S = \{1, p, p^2, \dots\}$, we identify the ring R^S with $R^{\mathbb{N}_0}$ via the correspondence $(a_1, a_p, a_{p^2}, \dots) \sim (a_0, a_1, a_2, \dots)$. From now on, we consider $R^{\mathbb{N}_0}$ equipped with the product topology, where each copy of

R has the discrete topology.

Definition 3.2.1. For $R \in \mathsf{CRings}$ and p a prime number, we have

1. (Verschiebung) A map $V : R^{\mathbb{N}_0} \to R^{\mathbb{N}_0}$ defined by $V(a_0, a_1, \dots) := p(0, a_0, a_1, \dots)$.
2. (Teichmüller map) $\langle\ \rangle : R \to R^{\mathbb{N}_0}$ defined by $\langle r \rangle := (r, r^p, r^{p^2}, \dots)$.
3. $X(R)$ is the closed subgroup of $R^{\mathbb{N}_0}$ generated by

$$\{V^n \langle r \rangle \mid n \in \mathbb{N}_0,\ r \in R\}.$$

Note that $X(R)$ is invariant under the Verschiebung operator V. For an ideal $I \subseteq R$, the subgroup $X(I)$ is defined in the same way. It is important to note that the operators V (Verschiebung) and $\langle \cdot \rangle$ (Teichmüller lift) appearing here are not the same as those in the construction of L. Hesselholt.

Definition 3.2.2. Fix $R \in \mathsf{CRings}$. Consider the presentation

$$0 \to I \to A \xrightarrow{\pi} R \to 0$$

where A is p-torsion free. Let $[\ ]$ be a fixed set-theoretic section of π. Let

$$E_c(R, \pi) := \frac{X(A)}{X(I)}$$

Then $E_c(R, \pi)$ is a Hausdorff topological abelian group equipped with the operators V and $\langle \cdot \rangle$, inherited from those on $X(R)$. The subgroup $X(I)$ is stable under V, so it induces an operator (again denoted by V) on $E_c(R)$. Similarly, the Teichmüller map induces a well-defined map

$$\langle \cdot \rangle : R \to E_c(R),$$

which sends x to the class of $\langle [x] \rangle$ in $E_c(R)$. Thus, the construction of E_c defines a functor from CRings to Ab.

Also we have a natural surjection

$$E_c(R) := X(A)/X(I) \to X(R)$$

induced by $\pi : A \to R$.

Lemma 3.2.3. [6, Cor. 2.5] *The definition of $E_c(R,\pi)$ is independent of the choice of p-torsion-free presentation of R.*

Lemma 3.2.4. [6, Cor. 2.10] *For any p-torsion-free ring R, we have $E_c(R) \cong X(R)$.*

This subsection concludes with the observation (see [6, pg. 561]) that the usual Witt vectors can be recovered via the bijection ψ_S (see [6, Thm. 2.4]). The construction is further extended from the category CRings to the category Rings, resulting a functor $E : \mathsf{Rings} \to \mathsf{Rings}$. In this thesis, we will not use this generalisation directly. Instead, we will modify the construction to obtain a more suitable functor for our purposes. A detailed discussion is postponed to Chapter 5.

Chapter 4

A group-theoretic characterisation of p-typical Witt vectors for commutative rings

In this chapter, we present our first main result, Theorem 1.0.9, which provides a universal group-theoretic characterisation of the p-typical Witt vectors. This chapter is based on joint work that appears in [22].

For a prime p and a commutative ring R with unity, let $W(R)$ denote the group of p-typical Witt vectors. This group is equipped with a Verschiebung operator

$$V\colon W(R) \to W(R)$$

and a Teichmüller map

$$\langle \cdot \rangle \colon R \to W(R).$$

One of the key properties these maps satisfy is that the map

$$x \mapsto V\langle x^p \rangle - p\langle x \rangle$$

is additive. We show that for any odd prime p, this property essentially characterises the functor W. We recall the statement of the theorem from the introduction.

Theorem 1.0.9. [22, Theorem 1.6] *The classical functor of p-typical Witt vectors W is a universal pre-Witt functor.*

Most constructions of the group of p-typical Witt vectors of associative rings do not have a ring structure, and hence this characterisation is more suitable for generalisation to the setup of associative (possibly non-commutative) rings , which we deal in Chapter 5.

4.1 Preliminaries and Main Tools

Let p be a fixed odd prime throughout. To prove Theorem 1.0.9, we first observe the following important group-theoretic properties satisfied by the classical Witt functor W. We recall the properties from the introduction.

Properties 1.0.7. *For $R \in \mathsf{CRings}$, there exist functorial maps*

- *(Verschiebung) $V : W(R) \to W(R)$ (group homomorphism)*
- *(Teichmüller map) $\langle - \rangle : R \to W(R)$ (set map)*

which satisfy the following properties

1. *$\langle 0 \rangle = 0$. If $p \neq 2$ then $\langle -x \rangle = -\langle x \rangle$ for all $x \in R$.*
2. *$x \mapsto V\langle x^p \rangle - p\langle x \rangle$ is an additive map from $R \to W(R)$.*
3. *$W(R)$ is complete w.r.t the filtration $\{V^n W(R) \mid n \in \mathbb{N}_0\}$.*
4. *If A is p-torsion free then $W(A)$ is also p-torsion free (see Lemma 2.2.20).*

Proof. We will prove these properties using the ghost map, whose injectivity on p-torsion free rings allows us to work with ghost components and then lift the arguments back to Witt vectors.

(1) In ghost coordinates, the Teichmüller lift of $-x \in R$ is

$$\langle -x \rangle = (-x, (-x)^p, (-x)^{p^2}, \dots) = (-x, -x^p, -x^{p^2}, \dots) = -\langle x \rangle,$$

as p is odd. Hence the same is true in $W(R)$.

(2) Again, working in ghost coordinates: for $x \in R$,

$$V\langle x^p\rangle - p\langle x\rangle = p(0, x^p, x^{p^2}, \dots) - p(x, x^p, x^{p^2}, \dots) = -p(x, 0, 0, \dots),$$

which is clearly additive in x.

(3) We have the truncation maps

$$T : W(R) \to W_n(R)$$

defined by

$$(a_0, a_1, \dots) \mapsto (a_0, a_1, \dots, a_{n-1}).$$

This is a surjective ring homomorphism with kernel

$$\{(a_0, a_1, \dots) \in W(R) : a_0 = a_1 = \cdots = a_{n-1} = 0\} = V^n(W(R)).$$

Hence, $W(R)/V^n(W(R)) \simeq W_n(R)$ for all $n \in \mathbb{N}$. Passing to quotients, we get $\{T : W_{n+1}(R) \to W_n(R)\}$ forms an inverse system with

$$W(R) \cong \varprojlim W(R)/V^n(W(R)),$$

which shows that $W(R)$ is complete with respect to the V-adic filtration.

(4) It follows from the fact that the ghost map is injective when A is p-torsion free. □

Remark 4.1.1. The above properties do not use the ring structure on $W(R)$. For example, the Teichmüller map $R \xrightarrow{\langle\ \rangle} W(R)$ is multiplicative. However, since we do not intend to use the ring structure of $W(R)$, only a weaker consequence of multiplicativity is stated in the form of (1).

We now abstract the properties 1.0.7 in the following definition. We recall the definition from the introduction.

Definition 1.0.8. [pre-Witt functor] A functor $F : \mathsf{CRings} \to \mathsf{Ab}$ is called a pre-Witt functor, if for every R, $F(R)$ is endowed with a functorial endomorphism $F(R) \xrightarrow{V} F(R)$ and a functorial map $R \xrightarrow{\langle\ \rangle} F(R)$ such that the properties 1.0.7 are satisfied.

Remark 4.1.2. $R \mapsto W(R)$ is an example of a pre-Witt functor.

Remark 4.1.3. For every ring R, $W(R)$ admits one more functorial endomorphism, viz., the Frobenius endomorphism $W(R) \xrightarrow{\mathbf{F}} W(R)$. However, $\mathbf{F}$ is uniquely determined by the requirements $\mathbf{F}\langle x\rangle = \langle x^p\rangle$ and $\mathbf{F}V = p$.

Remark 4.1.4. For $R \in \mathsf{CRings}$, and for all $x \in R$, we have the identity

$$V\langle x^p\rangle - p\langle x\rangle = (V\mathbf{F} - \mathbf{F}V)\langle x\rangle.$$

In ghost coordinates, we compute:

$$\begin{aligned}(V\mathbf{F} - \mathbf{F}V)\langle x\rangle &= V(x^p, x^{p^2}, \dots) - p\mathbf{F}(0, x, x^p, \dots) \\ &= p(0, x^p, x^{p^2}, \dots) - p(x, x^p, x^{p^2}, \dots) \\ &= -p(x, 0, 0, \dots) \\ &= V\langle x^p\rangle - p\langle x\rangle.\end{aligned}$$

Therefore the identity $V\langle x^p\rangle - p\langle x\rangle = (V\mathbf{F} - \mathbf{F}V)\langle x\rangle$ holds for all $x \in R$. This shows that the Frobenius map plays a nontrivial role and is not being neglected in the construction.

The outline of the proof is as follows. In the second section, we recall the definition of the functor $E_c : \mathsf{CRings} \to \mathsf{Ab}$ with a slight modification that will become apparent in the next chapter. The functor E_c is essentially an alternative construction of W (see [6, page 561]). In the third section, for $p \neq 2$, we give a construction of a functor $C : \mathsf{CRings} \to \mathsf{Ab}$ which is obtained by enforcing the properties 1.0.7. At this stage however, it is not straightforward to check that C satisfies property (4) of 1.0.7. Hence we introduce a temporary notion of *weak pre-Witt functor*, in which a weaker version of 1.0.7(4) is used (see Definition 4.3.5). We will then prove that C is a universal weak pre-Witt functor. The fourth section will be devoted to proving that C and E_c are isomorphic. This shows that C is a universal pre-Witt functor. This is used to finish the proof of Theorem 1.0.9.

4.2 The functor E_c : $\mathsf{CRings} \to \mathsf{Ab}$

In this section we will highlight a few points of the functor E_c that will be needed to prove our main theorem. Although in the original paper [6], the authors have denoted this functor by E, we will denote this by E_c. We will reserve the notation E for the functor we are going to define in the next chapter. Throughout this subsection we will assume that $R \in \mathsf{CRings}$.

Definition 4.2.1. [6, Prop. 1.2] For $R \in \mathsf{CRings}$ and p a prime number, we have

1. (Verschiebung) $V : R^{\mathbb{N}_0} \to R^{\mathbb{N}_0}$ given by $V(r_0, r_1, ...) := p(0, r_0, r_1, ...)$.
2. (Teichmüller map) For $r \in R$ define $\langle r \rangle := (r, r^p, r^{p^2}, ...)$
3. Let $X(R)$ to be the closed subgroup of $R^{\mathbb{N}_0}$ generated by $\{V^n\langle r\rangle \mid n \in \mathbb{N}_0,\ r \in R\}$. Here we give discrete topology to R and product topology on $R^{\mathbb{N}_0}$.

Let $A := \mathbb{Z}[R]$ be the commutative polynomial ring on the set R. For $x \in R$ we denote the corresponding variable in A by $[x]$. Let

$$E_c(R) := \frac{X(A)}{X_I(A)}$$

where I is the kernel of the natural surjection $A \to R$ and $X_I(A) \subset X(A)$ is the closed subgroup generated by

$$\{V^n\langle a\rangle - V^n\langle b\rangle \mid n \in \mathbb{N}_0,\ a, b \in A \text{ such that } a - b \in I\}.$$

Thus we have a natural surjection $E_c(R) := \frac{X(A)}{X_I(A)} \to X(R)$. $E_c(R)$ is naturally endowed with an endomorphism V and a map $\langle\ \rangle : R \to E_c(R)$ which sends x to the class of $\langle [x] \rangle$ in $E_c(R)$.

Lemma 4.2.2. *Every element of $X(R)$ can be written as $\sum_{n=0}^{\infty} V^n\langle a_n\rangle$.*

Proof. Since $X(R)$ is the quotient of $X(\mathbb{Z}[R])$, it suffices to prove the statement when R is a polynomial ring. When R is a polynomial ring, $X(R) = E_c(R)$ [6, Cor. 2.10] and

$E_c(R) \cong W(R)$ [6, page 561]. The result then follows from the corresponding well known bijection $R^{\mathbb{N}_0} \to W(R)$ which is indeed given by the formula

$$(a_0, a_1, ...) \mapsto \sum_n V^n\langle a_n\rangle.$$

□

Lemma 4.2.3. *The closed subgroup $X_I(A)$ coincides with the closed subgroup $X(I)$ as given in Definition 3.2.1.*

Proof. We recall that, $X_I(A)$ is generated by $\{V^n\langle a\rangle - V^n\langle b\rangle \mid a,\ b \in A$ such that $a-b \in I,\ n \in \mathbb{N}_0\}$ while $X(I)$ is generated by $\{V^n\langle a\rangle \mid n \in \mathbb{N}_0,\ a \in I\}$. By taking one of a or b to zero we get $X_I(A) \subset X(I)$. For the reverse inclusion, let $\langle a\rangle - \langle b\rangle \in X_I(A)$. By Lemma 4.2.2, $\langle a\rangle - \langle b\rangle = \sum_{i=0}^n V^i\langle c_i\rangle$ for some $c_i \in A$. Assumption $a - b \in I$ implies $c_i \in I\, \forall i$. Hence, $\langle a\rangle - \langle b\rangle \in X(I)$. This proves that, $X_I(A) = X(I)$. Thus the group $E_c(R)$ defined above for commutative rings is exactly the same as defined in 3.2.2. □

Remark 4.2.4. The subgroups $X(I)$ and $X_I(A)$ will not coincide for a non-commutative ring. For example, take a non-commutative polynomial ring $A := \mathbb{Z}\{X, Y\}$ and $I := (X, Y)$ then $(X) - (Y)$ is in $X_I(A)$ but not $X(I)$.

Lemma 4.2.5. *For $R \in$ CRings, let $\widetilde{X}(R) \subset X(R)$ be the subgroup generated by $\{V^n\langle r\rangle \mid n \in \mathbb{N}_0,\ r \in R\}$. Then*

1. *The natural map $X(R) \to \varprojlim_n \frac{X(R)}{V^n(X(R))}$ is an isomorphism.*

2. *The natural map $\frac{\widetilde{X}(R)}{V^n(\widetilde{X}(R))} \to \frac{X(R)}{V^n(X(R))}$ is an isomorphism.*

In particular we have a canonical isomorphism $X(R) \cong \varprojlim_n \frac{\widetilde{X}(R)}{V^n(\widetilde{X}(R))}$.

Proof. By Lemma 4.2.2, observe that for any $n \in \mathbb{N}$,

$$(\{0\}^n \times R \times R \times \cdots) \cap X(R) = V^n(X(R)).$$

Therefore, the collection $\{V^n(X(R))\}_{n=0}^{\infty}$ forms a basis of neighbourhoods of $X(R)$. Thus, the topology on $X(R)$ induced from $R^{\mathbb{N}_0}$ coincides with the topology induced by the V-filtration. Since $R^{\mathbb{N}_0}$ is complete and $X(R)$, being closed in $R^{\mathbb{N}_0}$, is also complete, it follows that

$$X(R) \cong \varprojlim_n \frac{X(R)}{V^n(X(R))}.$$

Statement (2) follows from the fact that the natural map $\widetilde{X}(R) \hookrightarrow X(R) \to X(R)/V^n(X(R))$ is surjective with kernel $V^n(\widetilde{X}(R))$. □

Lemma 4.2.6. *X : $\mathsf{CRings} \to \mathsf{Ab}$ is a pre-Witt functor.*

Proof. Since we will use this argument multiple times, we provide the full details here once.

The first two properties of the pre-Witt functor follow directly from Definition 4.2.1 as follows. For $p \neq 2$, for all $x \in R$,

$$\langle -x \rangle = ((-x), (-x)^p, (-x)^{p^2}, \dots) = (-x, -x^p, \dots) = -(x, x^p, \dots) = -\langle x \rangle.$$

This proves property (1). For (2), let $B(x) := V\langle x^p \rangle - p\langle x \rangle$. Then,

$$\begin{aligned} B(x+y) &= p(0, (x+y)^p, (x+y)^{p^2}, \dots) - p(x+y, (x+y)^p, \dots) \\ &= p(-(x+y), 0, 0, \dots) = B(x) + B(y). \end{aligned}$$

Property (3) follows from Lemma 4.2.5. Finally, property (4) follows from the fact that $X(R)$ is a subgroup of $R^{\mathbb{N}_0}$.

Hence, X is a pre-Witt functor. □

We now recall an important result proved by Cuntz and Deninger, which shows that the property (4) of 1.0.7 is satisfied by $E_c(R)$.

Lemma 4.2.7. [6, Cor. 2.10] *If R is p-torsion free then $E_c(R) = X(R)$. In particular, $E_c(R)$ is p-torsion free.*

The following lemma, is an easy consequence of the above result.

Lemma 4.2.8. *The group $E_c(R)$ is topologically generated by $\{V^n\langle x\rangle |\ x \in R\ , n \geq 0\}$. Moreover, the functor $E_c : \mathsf{CRings} \to \mathsf{Ab}$ satisfies the properties in 1.0.7 and hence is a pre-Witt functor.*

Proof. Since $X(\mathbb{Z}[R])$ is topologically generated by the set $\{V^n\langle a\rangle \mid a \in \mathbb{Z}[R],\ n \geq 0\}$, and $E_c(R)$ is a quotient of $X(\mathbb{Z}[R])$, it follows that $E_c(R)$ is topologically generated by the images of these elements under the canonical map $X(\mathbb{Z}[R]) \to E_c(R)$. This proves the first part.

For the second part, by Lemma 4.2.6, the functor X satisfies the first two properties listed in 1.0.7. Since $E_c(R)$ is a quotient of $X(\mathbb{Z}[R])$, it also satisfies these two properties. By Lemma 4.2.5, $X(\mathbb{Z}[R])$ is an abelian group that is complete and Hausdorff with respect to the V-filtration. Since $X_I(\mathbb{Z}[R])$ is a closed subgroup, it follows from [4, Chap. IX, §3.1, Prop. 4] that $E_c(R)$ is V-complete. This establishes property (3) in 1.0.7. Property (4) follows from Lemma 4.2.7. □

4.3 The functor $C : \mathsf{CRings} \to \mathsf{Ab}$

Fix a prime $p \neq 2$ throughout this section. In this section, we first define a functor $C : \mathsf{CRings} \to \mathsf{Ab}$ which attempts to enforce the properties 1.0.7. It is less straightforward to see that C satisfies 1.0.7(4) and hence we introduce a temporary notion of a weak pre-Witt functor (see Definition 4.3.5). We will in fact show in the next section that C is a pre-Witt functor (see Theorem 4.4.3). In this section, however, we limit ourselves to showing that C is a universal weak pre-Witt functor (see Theorem 5.3.7).

Definition 4.3.1. For any commutative ring R and a prime $p \neq 2$, we first define a group $G(R)$ as follows. Let

1. $\widetilde{G}(R)$ be the free abelian group generated by symbols $\{V_r^n \mid n \in \mathbb{N}_0,\ 0 \neq r \in R\}$. Define $V_0^n := 0$ for all $n \geq 0$.
2. A set map $R \xrightarrow{\langle\ \rangle} \widetilde{G}(R)$ given by $\langle r\rangle := V_r^0$.
3. A homomorphism $\widetilde{G}(R) \xrightarrow{V} \widetilde{G}(R)$ defined by $V(V_r^n) := V_r^{n+1}$.

4. $H(R) \subset \widetilde{G}(R)$ be the subgroup generated by the elements of the form $\{(V^n_{(x+y)^p} - pV^{n-1}_{x+y}) - (V^n_{x^p} - pV^{n-1}_x) - (V^n_{y^p} - pV^{n-1}_y)\}$ and $\{V^n_r + V^n_{-r}\}$ for $x, y, r \in R$ and $n \in \mathbb{N}_0$.

5. $\widetilde{H}(R)$ be the p-saturation of $H(R)$, i.e. $\widetilde{H}(R) := \{\alpha \in \widetilde{G}(R) \mid p^\ell \alpha \in H(R) \text{ for some } \ell > 0\}$.

6. Let $G^0(R)$ denote the completion of $\widetilde{G}(R)/\widetilde{H}(R)$ by the V-filtration. Let $G(R)$ be the quotient of $G^0(R)$ modulo the closed subgroup generated by p-power torsion elements. Note that the construction of $G(R)$ is functorial in R.

Definition 4.3.2 (The functor C)**.** Let $R \in \mathsf{CRings}$ and $0 \to I \to \mathbb{Z}[R] \to R \to 0$ be the canonical free presentation of R. Define

$$C(R) := \frac{G(\mathbb{Z}[R])}{G_I(\mathbb{Z}[R])}$$

where $G_I(\mathbb{Z}[R])$ is the closed subgroup generated by

$$\{V^n_x - V^n_y \mid x, y \in \mathbb{Z}[R] \text{ such that } x - y \in I,\ n \geq 0\}.$$

We have a well defined group homomorphism $V : C(R) \to C(R)$ and a well defined map of sets $R \xrightarrow{\langle\ \rangle} C(R)$ induced by the corresponding maps on $G(\mathbb{Z}[R])$.

Any ring homomorphism $f : R \to S$, gives a group homomorphism $G(R) \to G(S)$ induced by $V^n_r \mapsto V^n_{f(r)}$ which is compatible with V and hence a continuous group homomorphism $C(f) : C(R) \to C(S)$.

Remark 4.3.3. There is a straightforward modification of the definition of C for $p = 2$. However we only restrict ourselves to the condition $p \neq 2$ due to it's requirement in Lemma 1.0.10. We have not yet explored the case $p = 2$.

The next result is about $C(A)$ when A is a polynomial algebra.

Lemma 4.3.4. *If $A = \mathbb{Z}[S]$ is a free commutative algebra, then $C(A) \cong G(A)$. In particular, $C(A)$ is p-torsion free.*

Proof. Since A is a free algebra, the natural surjection $\pi : \mathbb{Z}[A] \to A$ has a section which is also a ring homomorphism. We denote this section as $j : A \to \mathbb{Z}[A]$. Then we have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & 0 & \longrightarrow & A & \xrightarrow{id} & A & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle j} & & \downarrow{\scriptstyle id_A} & & \\ 0 & \longrightarrow & I & \longrightarrow & \mathbb{Z}[A] & \xrightarrow{\pi} & A & \longrightarrow & 0. \end{array}$$

By functoriality of G, we have a group homomorphism

$$G(j) : G(A) \to G(\mathbb{Z}[A])$$

Composing with the quotient map, we get a morphism

$$\phi : G(A) \to C(A)$$

It suffices to show that ϕ is an isomorphism. The injectivity of ϕ is straight forward because $\pi \circ j = id_A$ and hence ϕ has a retract induced by $G(\pi)$. For surjectivity we note that for $\alpha \in G(\mathbb{Z}[A])$, $\phi(\beta) = \alpha$ where $\beta := G(\pi)(\alpha)$. □

Since we define C formally to satisfy properties of pre-Witt functor, C should be universal pre-Witt functor on CRings. Unfortunately, it appears less straightforward to check that C actually satisfies the property 1.0.7(4) and is a pre-Witt functor. To overcome this hurdle, we introduce a notion of 'weak pre-Witt' functor below, whose role is somewhat temporary (see Theorem 4.4.3). We will prove in the next section that C is a universal pre-Witt functor.

Definition 4.3.5 (weak pre-Witt functor)**.** A functor F : CRings $\to$ Ab is said to be a weak pre-Witt functor if it satisfies the properties (1), (2) and (3) of 1.0.7 and the following property, which is a weaker version of 1.0.7(4):

(4′) If A is free (i.e. a polynomial ring) then $F(A)$ is p-torsion free.

Any pre-Witt functor is a weak pre-Witt functor. In particular, the functors W, X and E_c are weak pre-Witt functors.

Theorem 4.3.6. *Let $p \neq 2$. The functor C : CRings $\to$ Ab is a universal weak pre-Witt functor. In particular, there is a natural transformation $C \xrightarrow{\eta} E_c$ which is compatible with $V, \langle\ \rangle$.*

Proof. As $C(R)$ is a quotient of $G(\mathbb{Z}[R])$ and by point (6) of Definition 4.3.1, C satisfies (1), (2) of 1.0.7. Now, by point (6) of Definition 4.3.1, $G(\mathbb{Z}[R])$ V-complete. So, $C(R)$ is also V-complete by [4, chap IX, §3.1, prop. 4]. Lemma 4.3.4 implies that the property (4′) of the Definition 4.3.5 is also satisfied by C. Hence C is a weak pre-Witt functor. It remains to show its universality. Let F be any weak pre-Witt functor. For a commutative ring R, take the presentation $0 \to I \to \mathbb{Z}[R] \xrightarrow{\pi} R \to 0$. We define the homomorphism,

$$\eta : \widetilde{G}(\mathbb{Z}[R]) \to F(\mathbb{Z}[R]), \text{ given by } V_a^n \mapsto V^n\langle a\rangle \text{ for all } a \in \mathbb{Z}[R],\ n \geq 0.$$

Since F satisfies properties (1)-(2) of 1.0.7, $\eta(\widetilde{H}(\mathbb{Z}[R])) = 0$ in $F(\mathbb{Z}[R])$. So, we get a homomorphism (again denoted by η),

$$\eta : \widetilde{G}(\mathbb{Z}[R])/\widetilde{H}(\mathbb{Z}[R]) \to F(\mathbb{Z}[R]).$$

As η is compatible with V, and F satisfies 1.0.7(3), taking V-completion, we get the transformation $\eta : G^0(\mathbb{Z}[R]) \to F(\mathbb{Z}[R])$. Since $F(\mathbb{Z}[R])$ is p-torsion free, η induces a map, which we continue to denote by $\eta : G(\mathbb{Z}[R]) \to F(\mathbb{Z}[R])$. Now, consider the composition $F(\pi) \circ \eta$, where $F(\pi) : F(\mathbb{Z}[R]) \to F(R)$. This composition, still denoted by η, factors through $C(R)$. Indeed, for $a, b \in \mathbb{Z}[R]$ such that $a - b \in I, \eta(V_a^n - V_b^n) = V^n\langle\pi(a)\rangle - V^n\langle\pi(b)\rangle = 0$, so $\eta(G_I(\mathbb{Z}[R])) = 0$ in $F(R)$. Therefore, we get the natural transformation $\eta : C(R) \to F(R)$. Hence, C is universal weak pre-Witt functor. □

4.4 Proof of theorem 1.0.9

In this section we will prove the main theorem 1.0.9. Note that, for $R \in \mathsf{CRings}$, we have the canonical isomorphism $E_c(R) \to W(R)$ by [6, Page 561]. Thus, in view of the above Theorem 5.3.7, it is enough to prove that C is a pre-Witt functor and that $C(R) \cong E_c(R)$ for all $R \in \mathsf{CRings}$ (see Theorem 4.4.3). The first step towards proving this is to show that, for a free commutative polynomial algebra A, $C(A) \cong X(A)$. The crucial observation for this is the Lemma 1.0.10. Before proving the Lemma 1.0.10, we will begin by stating an interesting fact about integers.

Lemma 4.4.1. *Let p be any prime and $\{c_1, c_2, ..., c_n\}$ be distinct nonzero integers. Let*

$$M(c_1, c_2, ...c_n) := \begin{bmatrix} c_1 & c_2 & \dots & c_n \\ c_1^p & c_2^p & \dots & c_n^p \\ \vdots & \vdots & \vdots & \vdots \\ c_1^{p^{n-1}} & c_2^{p^{n-1}} & \dots & c_n^{p^{n-1}} \end{bmatrix}$$

Then columns of $M(c_1, ..., c_n)$ are $\mathbb{Z}$-linearly independent in the following cases:

1. *c_i are positive integers for all i.*
2. *$p \neq 2$ and $|c_i|$ are distinct, i.e. $c_i \neq -c_j$ for any $i \neq j$.*

Proof. Clearly columns of $M(c_1, ..., c_n)$ are $\mathbb{Z}$-linearly independent iff $det(M(c_1, ..., c_n)) \neq 0$. The first statement is a well known fact and follows from the exercise as given in [23, page 43]. One can see a beautiful proof of this fact at [26]. The second statement can be deduced from (1) as follows. Since p is odd, $det(M(c_1, c_2, .., c_n))$ differs from $det(M(|c_1|, |c_2|, ..., |c_n|)$ at most by a sign. The condition in (2) ensures that $|c_i|$ are distinct and now apply (1) to get the result. □

We now recall the following lemma from the introduction and give the proof.

Lemma 1.0.10. *Let $p \neq 2$. Let $A = \mathbb{Z}[S]$ be a commutative polynomial ring over a set S. Let $\{f_i\}_{i=1}^r$ be a finite set of distinct non-zero elements of A. Further assume that $f_i \neq -f_j$ for any $i \neq j$. Then the subset $\{\langle f_i \rangle\}_{i=1}^r$ of $X(A)$ is $\mathbb{Z}$-linearly independent.*

Proof. As there are only finitely many variables in each f_i, we may assume $A = \mathbb{Z}[X_1, ..., X_n]$. Since $\mathbb{Z}$ is an infinite integral domain, it is well known that a polynomial $f \in A$ is zero iff $f(\underline{a}) = 0$ for all $\underline{a} \in \mathbb{Z}^n$. Applying this to the polynomial $g := \Pi_{i<j\leq r}(f_i - f_j)(f_i + f_j) \cdot \Pi_i f_i$, which is non-zero by hypothesis, we can choose an element $\underline{a} \in \mathbb{Z}^n$ such that $g(\underline{a}) \neq 0$. This implies that $c_i := f_i(a)$ are distinct nonzero integers such that $c_i \neq -c_j$ for $i \neq j$. The linear independence of $\langle f_i \rangle$ now directly follows from Lemma 4.4.1. □

Lemma 4.4.2. *Let $A = \mathbb{Z}[S]$ be a free polynomial algebra. There exists a canonical isomorphism $C(A) \cong X(A)$.*

Proof. We know that X is a pre-Witt functor by Lemma 4.2.6. Since C is a universal weak pre-Witt functor there exists a natural transformation $\eta : C \to X$. For a polynomial algebra A, we have the group homomorphism $\eta : C(A) \to X(A)$ which is given by $V_a^n \mapsto V^n\langle a\rangle$. By Lemma 4.2.2 this map is surjective. By Lemma 4.3.4 we know that $G(A) \cong C(A)$, thus composing with the group homomorphism $\widetilde{G}(A)/\widetilde{H}(A) \to G(A)$, we get the map

$$\overline{\eta} : \widetilde{G}(A)/\widetilde{H}(A) \to G(A) \to X(A)$$

The image of $\overline{\eta}$ lands in $\widetilde{X}(A)$. Thus we have the group epimorphism

$$\widetilde{\eta} : \widetilde{G}(A)/\widetilde{H}(A) \to \widetilde{X}(A); \quad V_a^n \mapsto V^n\langle a\rangle.$$

We will now prove the theorem in following steps.

Step 1: To prove the theorem it is enough to show that $\widetilde{\eta}$ is an isomorphism: This is because, if $\widetilde{\eta}$ is an isomorphism then since $\widetilde{\eta}$ is compatible with V, after taking the V-completion we get that

$$G^0(A) \cong X(A).$$

Since $X(A)$ has no p-torsion, this implies, using Lemma 4.3.4

$$C(A) \cong G(A) \cong X(A).$$

Thus, it is enough to show that the group epimorphism $\widetilde{\eta}$ is injective. This we will prove in the next step.

Step 2: To show that $\widetilde{\eta}$ is injective, we in fact consider the map (again denoted by $\widetilde{\eta}$);

$$\widetilde{\eta} : \widetilde{G}(A) \to \widetilde{X}(A)$$

We will show that $\mathrm{Ker}(\widetilde{\eta}) = \widetilde{H}(A)$. It is easy to observe from the definition of $\widetilde{H}(A)$ that $\widetilde{H}(A) \subseteq \mathrm{Ker}(\widetilde{\eta})$.

Let $\alpha = \sum_{i=1}^{\ell} c_i V_{a_i}^{n_i} \in \mathrm{Ker}(\widetilde{\eta})$. We will prove that $\alpha \in \widetilde{H}(A)$, i.e. $p^k\alpha \in H(A)$ for some $k \geq 0$. We will establish this in following two steps.

Step 2a: We first prove the case when $n_i = 0$ for all i, i.e.

$$\alpha = \sum_{i=1}^{\ell} c_i V_{a_i}^0$$

We may assume without loss of generality that a_i are all distinct. Moreover if $a_r = -a_s$ for some $r \neq s$ then

$$V_{a_r}^0 = -V_{a_s}^0 \bmod H(A).$$

Thus we may replace the expression $c_r V_{a_r}^0 + c_s V_{a_s}^0$ with $(c_s - c_r) V_{a_s}^0$. In particular we may assume that not only a_i are distinct, but $a_i \neq -a_j$ for any $i \neq j$. In this case, c_i must be zero for all i by Lemma 1.0.10. Thus $\alpha = 0$ and hence is in $\widetilde{H}(A)$.

Step 2b: For $n_i \geq 0$, we prove the claim by induction on $n_\alpha := \max_i\{n_i\} - \min_i\{n_i\}$. Since $\widetilde{X}(A) \xrightarrow{V} \widetilde{X}(A)$ and $\widetilde{H}(A) \xrightarrow{V} \widetilde{H}(A)$ are both injective maps, we may assume without loss of generality that $\min_i\{n_i\} = 0$. The starting step of induction is proved in Step 1. Now by rearranging, we may assume that $n_i = 0$ for $1 \leq i \leq s$ and $n_i > 0$ for $s < i \leq \ell$. Thus without loss of generality we have

$$\alpha = \sum_{i=1}^{s} c_i V_{a_i}^0 + \sum_{i>s}^{\ell} c_i V_{a_i}^{n_i}$$

We need to show $p^k \alpha \in H(A)$, for some $k \geq 0$.

$$\begin{aligned} p\alpha &= \sum_{i=1}^{s} p c_i V_{a_i}^0 + \sum_{i>s}^{\ell} p c_i V_{a_i}^{n_i} \\ &= \sum_{i=1}^{s} c_i (p V_{a_i}^0 - V_{a_i^p}^1) + \sum_{i=1}^{s} c_i V_{a_i^p}^1 + \sum_{i>s}^{\ell} p c_i V_{a_i}^{n_i} \\ &= \beta + \sum_{i=1}^{s} c_i V_{a_i^p}^1 + \sum_{i>s}^{\ell} p c_i V_{a_i}^{n_i} \\ &=: \beta + \gamma \end{aligned}$$

Since $\alpha \in \mathrm{Ker}(\widetilde{\eta})$ we have

$$p\widetilde{\eta}(\alpha) = \widetilde{\eta}(\beta) + \widetilde{\eta}(\gamma) = (p \sum_{i=1}^{s} c_i a_i, \cdots) = (0, 0, 0, \cdots).$$

This implies that $\sum_{i=1}^{s} c_i a_i = 0$, since $X(A)$ is p-torsion free.

We now claim that $\beta \in H(A)$: To prove this claim we will use the defining relations of $H(A)$.

Consider the map $\phi : A \to \widetilde{G}(A)$ given by $a \mapsto V^1_{a^p} - pV^0_a$ which is a linear map, i.e.

$$\phi(\sum_{i=1}^{s} c_i a_i) \equiv \sum_{i=1}^{s} c_i \phi(a_i) (\text{mod } H(A))$$

Thus, $\beta \equiv 0(\text{mod } H(A))$. This proves that $\beta \in H(A)$ and hence is in $\widetilde{H}(A)$. Thus, $\beta \in \mathrm{Ker}(\widetilde{\eta})$. This implies that $\gamma \in \mathrm{Ker}(\widetilde{\eta})$. Moreover observe that $n_\gamma < n_\alpha$, hence by the induction hypothesis, $\gamma \in \widetilde{H}(A)$. Thus, $p^r\gamma \in H(A)$ for some $r \geq 0$. Thus, $p^{r+1}\alpha \in H(A)$. Thus, $\mathrm{Ker}(\widetilde{\eta}) \subseteq \widetilde{H}(A)$.

This proves that $\widetilde{G}(A)/\widetilde{H}(A) \cong \widetilde{X}(A)$ and hence the theorem. □

Theorem 4.4.3. *The natural transformation $C \to E_c$ is an isomorphism of functors.*

Proof. Let A be a commutative polynomial ring. Since $E_c(A) \cong X(A)$ by [6, Cor. 2.10] and $X(A) \cong C(A)$ by Lemma 4.4.2, we get that $C(A) \cong E_c(A)$. For a general commutative ring R, consider the presentation,

$$0 \to I \to \mathbb{Z}[R] \to R \to 0.$$

The functor C being universal, we have a commutative diagram with exact rows.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & G_I(\mathbb{Z}[R]) & \longrightarrow & G(\mathbb{Z}[R]) & \longrightarrow & C(R) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow \phi & & \downarrow & & \\ 0 & \longrightarrow & X_I(\mathbb{Z}[R]) & \longrightarrow & X(\mathbb{Z}[R]) & \longrightarrow & E_c(R) & \longrightarrow & 0 \end{array}$$

Now by Lemma 4.3.4 and Lemma 4.4.2, the vertical map

$$\phi : G(\mathbb{Z}[R]) \to X(\mathbb{Z}[R])$$

is an isomorphism. The definition of $G_I(\mathbb{Z}[R])$ and $X_I(\mathbb{Z}[R])$ shows that the preimage of $X_I(\mathbb{Z}[R])$ under ϕ is exactly $G_I(\mathbb{Z}[R])$. Hence, the induced map $C(R) \to E_c(R)$ is an isomorphism. □

Theorem 4.4.4. *The functor C : $\mathsf{Rings} \to \mathsf{Ab}$ is a universal pre-Witt functor on* CRings.

Proof. It follows from the construction of C that, C satisfies properties (1), (2) and (3) of Properties 1.0.7. As $C(R) \cong E_c(R)$ and E is a pre-Witt functor, C is also a pre-Witt functor. Its universality follows from Theorem 5.3.7 as every pre-Witt functor is also a weak pre-Witt functor. □

We now recall the main theorem and give the proof.

Theorem 1.0.9. [22, Theorem 1.6] *The classical functor of p-typical Witt vectors W is a universal pre-Witt functor.*

Proof of Theorem 1.0.9. By Theorem 4.4.4 we know that C is a universal pre-Witt functor. By the canonical isomorphism $E_c(R) \to W(R)$ [6, Page 561] and by Theorem 4.4.3, W is a universal functor satisfying four properties in 1.0.7. □

Chapter 5

A group-theoretic characterisation of p-typical Witt vectors for associative rings

In the Chapter 4, a universal group-theoretic characterisation of W was given. In this chapter, we extend the ideas of Chapter 4 to the case of associative (possibly non-commutative) rings. This chapter is based on joint work with my PhD advisor.

We define the notion of a pre-Witt functor on Rings and give an explicit construction of a universal pre-Witt functor by adapting the construction of the Witt functor E by Cuntz-Deninger (see [6]). We then define the notion of a Witt functor and give a characterisation of universal Witt functor $\hat{E}$ modulo an explicit conjecture about non-commutative polynomials (see Theorem 1.0.16). In Section 5.5, we give evidence for the Conjecture 1.0.13. Without assuming Conjecture 1.0.13, we show that $\hat{E}$ admits a natural surjection to the Hesselholt's Witt functor W_H (see Theorem 5.4.8).

5.1 Pre-Witt functor on Rings

On the category CRings we have classical p-typical Witt functor

$$W : \mathsf{CRings} \to \mathsf{Ab}.$$

In Chapter 4, we have proved the following theorem. We restate it here from the introduction.

Theorem 1.0.9. [22, Theorem 1.6] *The classical functor of p-typical Witt vectors W is a universal pre-Witt functor.*

The key point of the above characterization is that it uses only the group structure on $W(R)$, and not the ring structure. This is important because most of the known constructions of Witt vectors for associative (possibly non-commutative) rings (see [11], [13], [6]) produce only abelian groups and do not endow them with a ring structure. A natural question, which we address in this chapter, is the following: what is the universal Witt functor on the category Rings obtained by mimicking these properties?

This motivates the following definition, which is exactly same as Definition 1.0.11.

Definition 5.1.1 (pre-Witt functor)**.** A pre-Witt functor is a functor $F : \mathsf{Rings} \to \mathsf{Ab}$ which has functorial maps

1. Verschiebung operator: $V : F(R) \to F(R)$ (group homomorphism)
2. Teichmüller map : $\langle\ \rangle : R \to F(R)$ (a set map)

which satisfy the following properties

1. $\langle 0 \rangle = 0$. If $p \neq 2$ then $\langle -x \rangle = -\langle x \rangle$ for all $x \in R$.
2. $x \mapsto V\langle x^p \rangle - p\langle x \rangle$ is an additive map from $R \to F(R)$.
3. $F(R)$ is complete with respect to the filtration $\{V^n F(R) \mid n \in \mathbb{N}_0\}$.
4. R and $\bar{R}$ are p-torsion free $\implies$ $F(R)$ is p-torsion free, where $\bar{R} := \frac{R}{\langle [R,R] \rangle}$ and $\langle [R,R] \rangle$ is the ideal generated by the commutator subgroup $[R,R]$.

The two main examples of pre-Witt functors considered in this chapter are

1. The functor $E : \mathsf{Rings} \to \mathsf{Ab}$ which is obtained by adapting the construction of Cuntz and Deninger (see Definition 5.2.4)
2. The Witt functor $W_H : \mathsf{Rings} \to \mathsf{Ab}$ defined by Hesselholt (see Definition 3.1.9).

Remark 5.1.2. Here, one notes that the property 5.1.1(4) has been slightly changed as compared to the property(4) satisfied by W in the commutative case. The main reason for imposing both R and $\bar{R}$ to be p-torsion free, is that we want the universal pre-Witt functor to coincide with the classical Witt functor W when restricted to CRings. Moreover since for a commutative ring $\bar{R}$ is same as R, this property specializes correctly to the commutative case. In addition, Hesselholt's Witt functor W_H satisfies these properties.

We now state the main results of this chapter, we recall it from the introduction.

Theorem 1.0.12. *E is a pre-Witt functor. Moreover:*

1. *The restriction of E to* CRings *is canonically isomorphic to the classical Witt functor W.*
2. *There exists a unique natural transformation $E \to W_H$, which is surjective.*

We show that modulo an explicit conjecture (1.0.13) related to non-commutative polynomials, E is in fact a universal pre-Witt functor.

Theorem 1.0.14. *Assuming Conjecture 1.0.13, E is a universal pre-Witt functor on* Rings*.*

In order to find a universal Witt functor on Rings, we define a Witt functor $\hat{E}$ that is a suitable quotient of the pre-Witt functor E by a closed subgroup defined by the certain Witt polynomials (see Definition 5.4.5). We have the following conjectural characterization of the functor $\hat{E}$. We recall it from the introduction.

Theorem 1.0.16. *The Conjecture 1.0.13 implies that $\hat{E}$ is a universal Witt functor for $p \neq 2$. In particular there is a unique natural transformation from $\hat{E} \to W_H$*

Theorems 1.0.14 and 1.0.16 rely on the following conjecture concerning non-commutative polynomials. This conjecture is a direct analogue of Lemma 1.0.10, which played a crucial role in the proof of the main result of Chapter 4. The recall the statement below from the introduction and it uses the notation introduced in Section 5.2.

Conjecture 1.0.13. *Let $p \neq 2$. Let $A = \mathbb{Z}\{S\}$ be a non-commutative polynomial ring over a set S. Let $\{f_i\}_{i=1}^{r}$ be a finite set of distinct non-zero elements of A. Further* *assume that $f_i \neq -f_j$ for any $i \neq j$. Then the subset $\{\langle f_i \rangle\}_{i=1}^r$ of $X(A)$ is $\mathbb{Z}$-linearly independent.*

The outline of the proof is as follows. In the Section 5.2 we give the definition of the functor $E : \mathsf{Rings} \to \mathsf{Ab}$ and prove the first part of Theorem 1.0.12. In Section 5.3, we prove Theorem 1.0.14. In Section 5.4 we define the notion of a Witt functor and give the definition of the functor $\hat{E}$ and prove Theorem 1.0.12(2) and Theorem 1.0.16. In Section 5.5 we discuss evidence for the Conjecture 1.0.13.

5.2 Definition and properties of $E : \mathsf{Rings} \to \mathsf{Ab}$

In this section we define the functor E (see Definition 5.2.4) used in Theorem 1.0.12. We adapt the construction of p-typical Witt vectors by Cuntz and Deninger (see [6]) to enforce properties 5.1.1. We begin by recalling the definitions and results about the functor $X : \mathsf{Rings} \to \mathsf{Ab}$ as in [6]. Let $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$.

Definition 5.2.1 ($X(R)$)**.** Let $R \in \mathsf{Rings}$. We have

1. (Verschiebung) $V : R^{\mathbb{N}_0} \to R^{\mathbb{N}_0}$ given by $V(r_0, r_1, ...) := p(0, r_0, r_1, ...)$.
2. (Teichmüller map) For $r \in R$ define $\langle r \rangle := (r, r^p, r^{p^2}, ...)$.
3. $\widetilde{X}(R)$ be the subgroup generated by $\{V^n \langle r \rangle \mid n \in \mathbb{N}_0,\ r \in R\}$. Define a topology on $R^{\mathbb{N}_0}$ using the sequence of decreasing subgroups $\{V^n \widetilde{X}(R)\}_{n \in \mathbb{N}}$.
4. Define $X(R)$ as the closure of $\widetilde{X}(R)$ in $R^{\mathbb{N}_0}$ with respect to this topology. Note that $X(R)$ is invariant under V.

Properties of $X(R)$:

1. $X : \mathsf{Rings} \to \mathsf{Ab}$ is a functor.
2. For a non-commutative ring R, the topology on $X(R)$ induced by $\{V^n \widetilde{X}(R)\}$ is finer than the one coming from product topology on $\mathbb{R}^{\mathbb{N} \cup \{0\}}$. Indeed, let $A := \mathbb{Z}\{x, y, z\}$. Then the element $\langle x + y \rangle + \langle -x \rangle + \langle -y \rangle + V\langle z \rangle$ is not in $V^n(\widetilde{X}(A))$ for any $n \geq 1$. Hence, $(\{0\} \times A^{\mathbb{N}}) \cap \widetilde{X}(A)$ is not open in the V-topology.

3. For $R \in \mathsf{Rings}$, $X(R) \cong \varprojlim_n \frac{X(R)}{V^n(X(R))}$. Thus, $X(R)$ has V-topology and every element of $X(R)$ can be written as $\sum_{n_i} V^{n_i}\langle a_{n_i}\rangle$ where for $M \in \mathbb{N}$, there will only be finitely many $n_i \leq M$ counted with repetitions.

Definition 5.2.2 (X_I and X_I^{sat})**.** For $R \in \mathsf{Rings}$, consider the free presentation

$$0 \to I \to A \to R \to 0$$

where $A := \mathbb{Z}\{R\}$ be the non-commutative polynomial ring on the set R. Let $X_I(A) \subset X(A)$ be the closed subgroup generated by

$$\{V^n\langle a\rangle - V^n\langle b\rangle \mid n \geq 0,\ a, b \in A \ \text{ such that } a - b \in I\}.$$

We will denote X_I as a short for $X_I(A)$. We denote the p-saturation of X_I by

$$X_I^{\mathsf{sat}} := \{\alpha \in X(A) \mid \ p^{\ell}\alpha \in X_I \text{ for some } \ell \in \mathbb{N} \cup \{0\}\}$$

It is easy to see that $X_I \subseteq X_I^{\mathsf{sat}}$.

Remark 5.2.3. For $R \in \mathsf{CRings}$, the closed subgroup $X(I)$ generated by $\{V^n\langle a\rangle \mid n \in \mathbb{N}_0,\ a \in I\}$ as given in [6, Prop.1.2] coincides with the closed subgroup $X_I(A)$ generated by

$$\{V^n\langle a\rangle - V^n\langle b\rangle \mid a,\ b \in A \text{ such that } a - b \in I, n \in \mathbb{N} \cup \{0\}\}.$$

The subgroups $X(I)$ and $X_I(A)$ will not coincide for a non-commutative ring. For example, take a non-commutative polynomial ring $A := \mathbb{Z}\{X, Y\}$ and $I := (X, Y)$ then $(X) - (Y)$ is in $X_I(A)$ but not $X(I)$. This is the reason why we need to modify the definition of E so that it works in the non-commutative set-up.

Definition 5.2.4 ($E(R)$)**.** For $R \in \mathsf{Rings}$ we denote by $\bar{R}$ the quotient ring $\frac{R}{\langle [R,R]\rangle}$ where $\langle [R, R]\rangle$ is the ideal generated by the commutator subgroup $[R, R]$. Suppose there exists a morphism $\phi : S \to R$ in Rings where S, $\bar{S}$ are p-torsion free. We consider the free presentations of R and S as follows.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & J & \longrightarrow & \mathbb{Z}\{S\} & \xrightarrow{\pi_2} & S & \longrightarrow & 0 \\ & & \downarrow & & \downarrow \widetilde{\phi} & & \downarrow \phi & & \\ 0 & \longrightarrow & I & \longrightarrow & \mathbb{Z}\{R\} & \xrightarrow{\pi_1} & R & \longrightarrow & 0 \end{array} \tag{1}$$

Here, $\widetilde{\phi}$ is a lift of ϕ. Applying the functor X we get the following diagram.

$$\begin{array}{ccccccc} X_J & \longrightarrow & X(\mathbb{Z}\{S\}) & \longrightarrow & X(S) & \longrightarrow & 0 \\ \downarrow & & \downarrow \widetilde{\phi} & & \downarrow \phi & & \\ X_I & \longrightarrow & X(\mathbb{Z}\{R\}) & \longrightarrow & X(R) & \longrightarrow & 0 \end{array} \tag{2}$$

Following the notation as in the Definition 5.2.2, we define

$$\widetilde{X_I} := \text{ the closed subgroup of } X(\mathbb{Z}\{R\}) \text{ generated by } \{X_I, \Sigma_I\}$$

where for a lift $\widetilde{\phi}$ as above

$$\Sigma_I \ := \Big\{\alpha \in X(\mathbb{Z}\{R\}) \ \Big| \ \alpha = \widetilde{\phi}(\beta) \text{ for some } \beta \in X_J^{\text{sat}}\Big\}.$$

We leave it to the reader to check that the set Σ_I is independent of the lift $\widetilde{\phi}$. Finally, we define

$$E(R) := \frac{X(\mathbb{Z}\{R\})}{\widetilde{X_I}}$$

Remark 5.2.5. We would like to note the following observations regarding $E(R)$ which directly follow from the definition. Some of these are technical in nature however they are needed later.

1. The group $E(R)$ is naturally endowed with an endomorphism $V : E(R) \to E(R)$ and a set map $\langle\ \rangle : R \to E(R)$ (both induced from that on $X(R)$). Here, $\langle r\rangle := \langle [r]\rangle$, where $[r] \in \mathbb{Z}\{R\}$ is a lift of r. It is easy to see from the definition of X_I that, $\langle [r]\rangle($ modulo $X_I)$ is independent of choice of a lift of r in $\mathbb{Z}\{R\}$.

2. For $R \in$ Rings, $X_I \subseteq \widetilde{X_I} \subseteq X_I^{\mathsf{sat}}$. Indeed, for $\alpha \in \widetilde{X_I}$, there exists $\beta \in X_J^{\mathsf{sat}}$ such that $\widetilde{\phi}(\beta) = \alpha$. As $\beta \in X_J^{\mathsf{sat}}$, $p^r\beta \in X_J$ for some $r \in \mathbb{N} \cup \{0\}$. Since $\widetilde{\phi}(X_J) \subseteq X_I$ we get that $p^r\alpha \in X_I$. Thus $\alpha \in X_I^{\mathsf{sat}}$.

3. For $R \in \mathsf{Rings}$, if R and $\bar{R}$ are both p-torsion free then $\widetilde{X_I} = X_I^{\mathsf{sat}}$. In particular, $E(R)$ is p-torsion free. To prove this, it is now enough to show that $\widetilde{X_I} \supseteq X_I^{\mathsf{sat}}$. This is straightforward by taking $S = R$ in the definition of Σ_I.

We will now show that E is a pre-Witt functor. Before showing this, we will prove the following important Lemma. The idea of the proof of this lemma will be used repetitively later in this paper.

Let $R \in \mathsf{Rings}$. In the definition of $E(R)$ (5.2.4), we chose the canonical free presentation $0 \to I \to \mathbb{Z}\{R\} \to R \to 0$ in order to define $E(R) := X(\mathbb{Z}\{R\})/\widetilde{X_I}$. However if

$$0 \to K \to B \to R \to 0$$

is any other free presentation we can also define the group

$$E_B(R) := \frac{X(B)}{\widetilde{X_K}}$$

where $\widetilde{X_K}$ is defined similarly. We now show that the definition of $E(R)$ is independent of the choice of free presentation of R.

Lemma 5.2.6. *$E(R) \cong E_B(R)$.*

Proof. Suppose that we have following two free presentations of R.

$$0 \to I \to A := \mathbb{Z}\{R\} \to R \to 0$$

$$0 \to K \to B \to R \to 0$$

We need to show that $E(R) \cong E_B(R)$. We prove this result in following steps.

Step(1) : In this step we will show that there exists a group homomorphism $\widetilde{\psi} : X(A) \to X(B)$, such that $\widetilde{\psi}(\widetilde{X_I}) \subseteq \widetilde{\psi}(\widetilde{X_K})$. Hence it induces a well-defined morphism $\widetilde{\psi} : E(R) \to E_B(R)$.

Consider the set maps $R \xrightarrow{[\cdot]_1} A$ and $R \xrightarrow{[\cdot]_2} B$. Define $\widetilde{\psi} : X(A) \to X(B)$ as

$$\psi(V^n\langle [r]_1 \rangle) := V^n\langle [r]_2 \rangle.$$

This induces a well defined group homomorphism $\widetilde{\psi} : X(A)/X_I \to X(B)$. It remains to show that $\widetilde{\psi}(\widetilde{X_I}) \subseteq \widetilde{X_K}$. It is enough to show that $\widetilde{\psi}(\Sigma_I) \subseteq \Sigma_K$.

Suppose there exists a morphism $\phi : S \to R$ where S and $\bar{S}$ are p-torsion free. Consider the diagrams similar to the one in Definition 5.2.4.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & J & \longrightarrow & \mathbb{Z}\{S\} & \longrightarrow & S & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \widetilde{\phi}} & & \downarrow{\scriptstyle \phi} & & \\
0 & \longrightarrow & I & \longrightarrow & A & \longrightarrow & R & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \widetilde{\psi}} & & \downarrow{\scriptstyle id} & & \\
0 & \longrightarrow & K & \longrightarrow & B & \longrightarrow & R & \longrightarrow & 0
\end{array}$$

We get the following induced diagram,

$$\begin{array}{ccccccc}
X_J & \longrightarrow & X(\mathbb{Z}\{S\}) & \longrightarrow & X(S) & \longrightarrow & 0 \\
\downarrow & & \downarrow{\scriptstyle \widetilde{\phi}} & & \downarrow{\scriptstyle \phi} & & \\
X_I & \longrightarrow & X(A) & \longrightarrow & X(R) & \longrightarrow & 0 \\
\downarrow & & \downarrow{\scriptstyle \widetilde{\psi}} & & \downarrow{\scriptstyle id} & & \\
X_K & \longrightarrow & X(B) & \longrightarrow & X(R) & \longrightarrow & 0
\end{array}$$

For $\alpha \in \Sigma_I$, $\alpha = \widetilde{\phi}(\beta)$ for some $\beta \in X_J^{\mathsf{sat}}$. Thus $\widetilde{\psi}(\alpha) = \widetilde{\psi} \circ \widetilde{\phi}(\beta)$ and hence $\widetilde{\psi}(\alpha) \in \Sigma_K$. Thus we have a well defined homomorphism which we again denote as,

$$\widetilde{\psi} : E(R) \to E_B(R)$$

Step 2: We will now show that $\widetilde{\psi} : E(R) \to E_B(R)$ is an isomorphism. To prove this, we will establish a group homomorphism $\chi : E_B(R) \to E(R)$ and show that $\widetilde{\psi} \circ \chi = id_{E_B(R)}$ and $\chi \circ \psi = id_{E(R)}$. Since A and B both are free rings, we will reverse the roles of A and B in the step(1), to get a group homomorphism $\chi : E_B(R) \to E(R)$. For $b \in \mathbb{Z}\{B\}$,

$$\widetilde{\psi} \circ \chi(V^n\langle b\rangle) = V^n\langle \widetilde{\psi} \circ \chi(b)\rangle \equiv V^n\langle b\rangle (\text{mod } X_I) \text{ as } \widetilde{\psi} \circ \chi(b) - b \in I.$$

$\square$

The following result, which is consequence of the above lemma, plays an important role in the proof of Theorem 1.0.12.

Lemma 5.2.7. *For a non-commutative free polynomial algebra A, $E(A) \cong X(A)$.*

Proof. This follows by taking the free presentation $0 \to 0 \to A \xrightarrow{\text{id}} A \to 0$ and using the Lemma 5.2.6 □

Theorem 5.2.8. $E : \mathsf{Rings} \to \mathsf{Ab}$ *is a pre-Witt functor.*

Proof. We first observe that E is a functor. Let $f : R_1 \to R_2$ be a morphism in Rings. Consider the free presentations of R_1 and R_2,

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I & \longrightarrow & \mathbb{Z}\{R_1\} & \longrightarrow & R & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle f} & & \\ 0 & \longrightarrow & K & \longrightarrow & \mathbb{Z}\{R_2\} & \longrightarrow & R & \longrightarrow & 0 \end{array}$$

Following similar arguments as in the proof of the Step(1) of Lemma 5.2.6 we get a group homomorphism $X(\mathbb{Z}\{R_1\}) \to X(\mathbb{Z}\{R_2\})/\widetilde{X_K}$ which factors via $E(R_1)$.

In order to show that E is a pre-Witt functor we need to prove the four properties stated in 5.1.1. The first two properties are easily seen to be satisfied by $E(R)$ since they are satisfied by $X(\mathbb{Z}\{R\})$. For the third property, we know that for $R \in \mathsf{Rings}$, $X(\mathbb{Z}\{R\})$ is V-complete. Moreover, $\widetilde{X_I}$ is a closed subgroup of $X(\mathbb{Z}\{R\})$ where X_I and Σ_I are V-invariant. Thus $E(R)$ is V-complete. For the fourth property, assume that R and $\bar{R}$ are p-torsion free. By the Remark 5.2.5(3), $\widetilde{X_I} = X_I^{\mathsf{sat}}$, hence $E(R)$ is p-torsion free. Thus E is a pre-Witt functor. □

The remaining section is devoted to proving the following theorem which shows that the functor E when restricted to commutative rings, gives the classical p-typical Witt functor. This proves a part (1) of Theorem 1.0.12.

Theorem 5.2.9. *For $R \in \mathsf{CRings}$, $E(R) \cong W(R)$.*

Proof. Let $R \in \mathsf{CRings}$. We denote by $E_c : \mathsf{CRings} \to \mathsf{Ab}$ the pre-Witt functor defined in Section 4.2. Note that in [22], it was denoted by $E : \mathsf{CRings} \to \mathsf{Ab}$, however to avoid conflict with E : Rings $\to$ Ab (see Definition 5.2.4), we denote it by E_c instead. We know that $E_c(R) \cong W(R)$ (see [6, Page 561]), hence it suffices to show that $E(R) \cong E_c(R)$ whenever $R \in$ CRings. We will prove the result in following steps.

Step 1: In this step we will prove that there exists a group homomorphism say $\widetilde{f}$: $X(\mathbb{Z}\{R\}) \to E_C(R)$ which factors via $E(R)$. Consider following two presentations of R.

$$0 \to I \to \mathbb{Z}\{R\} \xrightarrow{\pi_1} R \to 0 \quad \text{and} \quad 0 \to K \to \mathbb{Z}[R] \xrightarrow{\pi_2} R \to 0.$$

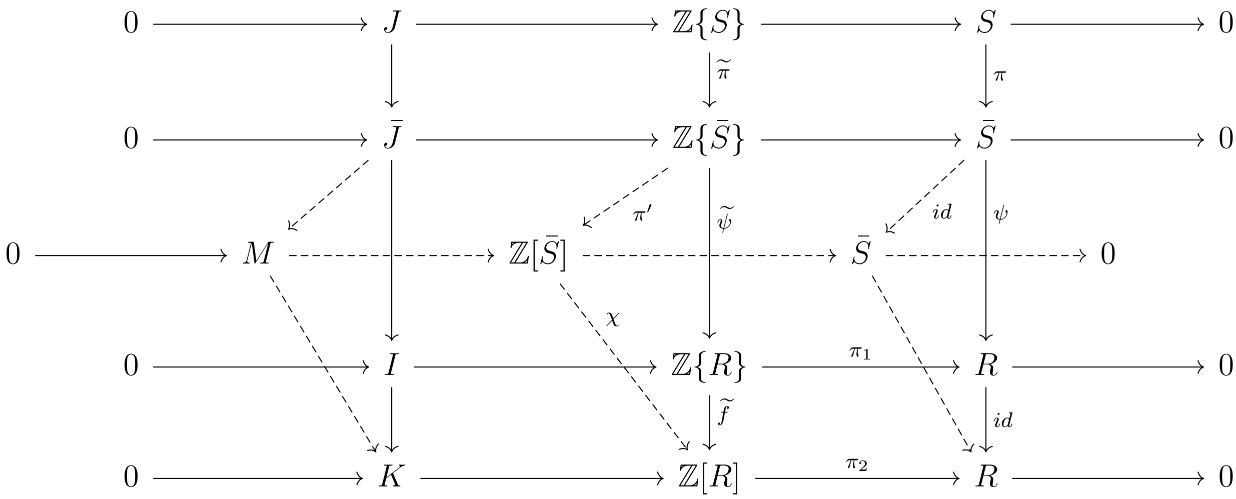
Since R is commutative, π_1 factors via $\mathbb{Z}[R]$. Thus, $\exists\ \widetilde{f} : \mathbb{Z}\{R\} \to \mathbb{Z}[R]$ such that $\pi_1 = \pi_2 \circ \widetilde{f}$ and we get the following commutative diagram.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I & \longrightarrow & \mathbb{Z}\{R\} & \xrightarrow{\pi_1} & R & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \widetilde{f}} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 0 & \longrightarrow & K & \longrightarrow & \mathbb{Z}[R] & \xrightarrow{\pi_2} & R & \longrightarrow & 0 \end{array}$$

Applying the functor X, we get the induced homomorphism $\widetilde{f} : X(\mathbb{Z}\{R\}) \to E_C(R)$ given by $\widetilde{f}(V^n\langle\alpha\rangle) := V^n\langle\widetilde{f}(\alpha)\rangle$.

Enough to show that $\widetilde{f}(\widetilde{X_I}) \subseteq X_K$. Since $\widetilde{f}(X_I) \subseteq X_K$, it remains to show that $\widetilde{f}(\Sigma_I) \in X_K$.

Suppose $\alpha \in \Sigma_I$, i.e. $\exists\ S \in$ Rings such that S and $\bar{S}$ are p-torsion free and $\exists\ S \xrightarrow{\phi} R$. Moreover, $\widetilde{\phi}(\beta) = \alpha$ for some $\beta \in X_J^{\mathsf{sat}}$. As R is commutative ring, ϕ factors through $\bar{S}$, i.e. $\exists\ \psi : \bar{S} \to R$ such that $\psi \circ \pi = \phi$. Thus, we need to consider the extended diagram in Rings.



Considering the diagram after applying the functor X (see Diagram(2) in Definition 5.2.4), it is easy to see that $\widetilde{\pi}(X_J^{\mathsf{sat}}) \subseteq X_{\bar{J}}^{\mathsf{sat}}$, $\widetilde{\psi}(X_{\bar{J}}^{\mathsf{sat}}) \subseteq X_I^{\mathsf{sat}}$ and $\widetilde{f}(X_I^{\mathsf{sat}}) \subseteq X_K^{\mathsf{sat}}$. Also note that $\mathbb{Z}[R]$ being commutative, $\widetilde{f} \circ \widetilde{\psi}$ factors via $\mathbb{Z}[\bar{S}]$. Since $\mathbb{Z}[\bar{S}]$ (resp. $\mathbb{Z}[R]$) is a commutative p-torsion free ring, by Corollary [6, Cor. 2.10], $X_M^{\mathsf{sat}} = X_M$ (resp. $X_K^{\mathsf{sat}} = X_K$). Thus,

$$\widetilde{f}(\alpha) = \widetilde{f} \circ \widetilde{\phi}(\beta) = \widetilde{f} \circ \widetilde{\psi} \circ \widetilde{\pi}(\beta) = \chi \circ \pi' \circ \widetilde{\pi}(\beta) \in X_K$$

Therefore there exists a well defined group homomorphism,

$$\widetilde{f} : E(R) := \frac{X(\mathbb{Z}\{R\})}{\widetilde{X_I}} \longrightarrow \frac{X(\mathbb{Z}[R])}{X_K} =: E_c(R).$$

Step 2: We now will establish a group homomorphism say $\widetilde{g} : E_c(R) \to E(R)$ such that $\widetilde{g} \circ \widetilde{f} = id_{E(R)}$ and $\widetilde{f} \circ \widetilde{g} = id_{E_c(R)}$.

Consider the short exact sequence and the following diagram.

$$\begin{array}{ccccccccc}
 & & & & 0 & & 0 & & \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & I & \longrightarrow & K & & \\
 & & & & \downarrow & \overset{\widetilde{g}}{\dashleftarrow} & \downarrow & & \\
0 & \longrightarrow & N & \longrightarrow & \mathbb{Z}\{R\} & \longrightarrow & \mathbb{Z}[R] & \longrightarrow & 0 \\
 & & & & \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle \pi_2} & & \\
 & & 0 & \longrightarrow & R & \xrightarrow{id} & R & \longrightarrow & 0 \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & 0 & & 0 & &
\end{array}$$

Since $\mathbb{Z}[R]$ is a free commutative ring, there exists a set-theoretic section, say $\widetilde{g} : \mathbb{Z}[R] \to \mathbb{Z}\{R\}$, which we will now describe. We have set theoretic sections $R \xrightarrow{[\cdot]_1} \mathbb{Z}\{R\}$ and $R \xrightarrow{[\cdot]_2} \mathbb{Z}[R]$. We fix an ordering on the set $\mathrm{Im}(R) \subset \mathbb{Z}\{R\}$ and define a set map $\widetilde{g} : \mathbb{Z}[R] \to \mathbb{Z}\{R\}$ by

$$\sum_{j=1}^{m} a_{i_1 i_2 \cdots i_j} [r_{i_1}]_2^{n_1} \cdots [r_{i_j}]_2^{n_j} \mapsto \sum_{j=1}^{m} a_{i_1 i_2 \cdots i_j} [r_{i_1}]_1^{n_1} \cdots [r_{i_j}]_1^{n_j}$$

We get a induced well defined set map on the quotients $\widetilde{g} : X(\mathbb{Z}[R])/X_K \to X(\mathbb{Z}\{R\})/X_N$. This is also an additive group homomorphism. Note that $N \subseteq I$, thus $X_N \subseteq X_I \subseteq \widetilde{X_I}$. Thus we get a group homomorphism

$$\widetilde{g} : E_c(R) := X(\mathbb{Z}[R])/X_K \longrightarrow X(\mathbb{Z}\{R\})/X_I \twoheadrightarrow X(\mathbb{Z}\{R\})/\widetilde{X_I} =: E(R)$$

Now for $\alpha \in X(\mathbb{Z}[R])$, $\widetilde{f} \circ \widetilde{g}(V^n\langle\alpha\rangle) = \widetilde{f} V^n(\langle\widetilde{g}(\alpha)\rangle) = V^n(\langle\widetilde{f} \circ \widetilde{g}(\alpha)\rangle) \equiv V^n\langle\alpha\rangle (\mod X_I)$. Similarly, for a class $\beta \in E_C(R)$, $\widetilde{f} \circ \widetilde{g}(V^n\langle\beta\rangle) = V^n\langle\widetilde{f} \circ \widetilde{g}(\beta)\rangle = V^n\langle\beta\rangle$. □

The proof of the Theorem 1.0.12(2) is postponed to Section 5.4. In the next section, assuming Conjecture 1.0.13, we show that E is a universal pre-Witt functor if $p \neq 2$.

5.3 Proof of Theorem 1.0.14

As part of the proof of Theorem 1.0.14, we construct a functor C : $\mathsf{Rings} \to \mathsf{Ab}$ which is obtained by enforcing the properties 5.1.1 (1)-(3). It is less straightforward to see that C satisfies 5.1.1(4). We introduce a temporary notion of a weak pre-Witt functor (see Definition 5.3.6) to show that C is a universal weak pre-Witt functor (see Theorem 5.3.7). Essentially, this section has a lot of conceptual overlap with Section 4.3. We will follow the arguments used in Section 4.3.

Definition 5.3.1 (The functor C)**.** For any associative ring R and a prime $p \neq 2$, we first define a group $G(R)$ as follows. Let

1. $\widetilde{G}(R)$ be the free abelian group generated by symbols $\{V_r^n \mid n \in \mathbb{N}_0,\ 0 \neq r \in R\}$. Define $V_0^n := 0$ for all $n \geq 0$.
2. A set map $R \xrightarrow{\langle\ \rangle} \widetilde{G}(R)$ given by $\langle r \rangle := V_r^0$.
3. A homomorphism $\widetilde{G}(R) \xrightarrow{V} \widetilde{G}(R)$ defined by $V(V_r^n) := V_r^{n+1}$.
4. $H(R) \subset \widetilde{G}(R)$ be the subgroup generated by the set:
$$\bigcup_n \Big(\{(V^n_{(x+y)^p} - pV^{n-1}_{x+y}) - (V^n_{x^p} - pV^{n-1}_x) - (V^n_{y^p} - pV^{n-1}_y) \mid x, y \in R\} \bigcup \{V^n_r + V^n_{-r} \mid r \in R\}\Big)$$
5. $\widetilde{H}(R)$ be the p-saturation of $H(R)$, i.e. $\widetilde{H}(R) := \{\alpha \in \widetilde{G}(R) \mid p^\ell \alpha \in H(R) \text{ for some } \ell > 0\}$.
6. Let $G^0(R)$ denote the completion of $\widetilde{G}(R)/\widetilde{H}(R)$ by the V-filtration. Let $G(R)$ be the quotient of $G^0(R)$ modulo the closed subgroup generated by p-power torsion elements. Note that the construction of $G(R)$ is functorial in R.

Consider the free presentation $0 \to I \to A \to R \to 0$ where $A := \mathbb{Z}\{R\}$. For $x \in R$ we denote the corresponding variable in A by $[x]$. Let $G_I(A) \subset G(A)$ is the closed subgroup generated by
$$\{V_a^n - V_b^n \mid n \geq 0,\ a, b \in A \ \text{ such that } a - b \in I\}.$$

Suppose there exists a morphism $\phi : S \to R$ in Rings where S, $\bar{S}$ are p-torsion free. We consider the free presentations of R and S as follows.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & J & \longrightarrow & \mathbb{Z}\{S\} & \xrightarrow{\pi_2} & S & \longrightarrow & 0 \\ & & \downarrow & & \downarrow \widetilde{\phi} & & \downarrow \phi & & \\ 0 & \longrightarrow & I & \longrightarrow & A = \mathbb{Z}\{R\} & \xrightarrow{\pi_1} & R & \longrightarrow & 0 \end{array} \tag{1}$$

Following the notation as in the Definition 5.2.4, we define

$$C(R) := \frac{G(A))}{\widetilde{G_I}}$$

where $\widetilde{G_I}$ is the closed subgroup of $G(A)$ generated by $\{G_I, \Sigma_I\}$ where

$$\Sigma_I \ := \ \left\{ \alpha \in G(A) \ \middle| \ \alpha = \widetilde{\phi}(\beta) \text{ for some } \beta \in G_J^{\mathrm{sat}} \right\}.$$

It is similar to Definition 5.2.4; see the diagram and definition in Definition 5.2.4 for comparison.

Remark 5.3.2. We have a well-defined group homomorphism $V : C(R) \to C(R)$ and a well defined map of sets $R \xrightarrow{\langle\ \rangle} C(R)$ induced by the corresponding maps on $G(\mathbb{Z}[R])$. Any ring homomorphism $f : R \to S$, gives a group homomorphism $G(R) \to G(S), V_r^n \mapsto V_{f(r)}^n$ which is compatible with V and hence a group homomorphism $C(f) : C(R) \to C(S)$.

Let $R \in$ Rings. In the definition of $C(R)$ we chose the canonical free presentation $0 \to I \to \mathbb{Z}\{R\} \to R \to 0$. However if $0 \to K \to B \to R \to 0$ is any other free presentation we can also define the group

$$C_B(R) := \frac{G(B)}{\widetilde{G_K}}$$

Following the arguments as in Lemma 5.2.6 and Lemma 5.2.7 we can prove the following results.

Lemma 5.3.3. $C(R) \cong C_B(R)$.

Corollary 5.3.4. *If $A = \mathbb{Z}\{S\}$ is a free algebra, then $C(A) \cong G(A)$.*

Eventually, we will show the following.

Theorem 5.3.5. *For $p \neq 2$, C is a universal pre-Witt functor.*

Unfortunately, it is less straightforward to check that C actually satisfies property 1.0.7(4) and is a pre-Witt functor. To overcome this hurdle, we introduce a notion of "weak pre-Witt" functor below, whose role is somewhat temporary. The main strategy is to show that C is universal weak pre-Witt (see Theorem 5.3.7), and then show that C is isomorphic to E.

Definition 5.3.6 (weak pre-Witt functor)**.** A functor $F : \mathsf{Rings} \to \mathsf{Ab}$ is said to be a weak pre-Witt functor if it satisfies the properties (1), (2) and (3) of Definition 5.1.1 and the following property, which is a weaker version of 5.1.1(4):

(4′) If A is a free polynomial ring in Rings then $F(A)$ is p-torsion free

Any pre-Witt functor is a weak pre-Witt functor. In particular, the functor E (see Definition 5.2.4), the Witt functor W_H defined in [11], [13] are weak pre-Witt functors.

Theorem 5.3.7. *Let $p \neq 2$. The functor C : $\mathsf{Rings} \to Ab$ is a universal weak pre-Witt functor. In particular, there is a natural transformation $C \xrightarrow{\eta} E$ which is compatible with $V, \langle\ \rangle$.*

Proof. It follows from the construction of C that, C satisfies properties (1), (2) and (3) of Definition 5.1.1. The Lemma 5.3.4 implies that C also satisfies the property (4′) of the Definition 5.3.6. Hence C is a weak pre-Witt functor. It remains to show its universality. We will prove that, given any pre-Witt functor F, there exists a natural transformation $\eta : C \to F$. The idea is to first establish a group homomorphism in the case of a free algebra and then extend the result to any $R \in \mathsf{Rings}$. We will prove this in the following steps.

Step 1: We will show that, for a free non-commutative polynomial ring A there exists a group homomorphism $C(A) \to F(A)$. Consider the presentation

$$0 \to 0 \to A \xrightarrow{id} A \to 0$$

We define the homomorphism,

$$\eta : \widetilde{G}(A) \to F(A) \text{ given by } V_a^n \mapsto V^n\langle a\rangle \ \forall\ a \in A,\ n \geq 0.$$

Since F satisfies the properties (1)-(2) of Definition 5.3.6, $\eta(\widetilde{H}(A)) = 0$ in $F(A)$. So, we get a homomorphism,

$$\widetilde{\eta} : \widetilde{G}(A)/\widetilde{H}(A) \to F(A).$$

As η is compatible with V, taking V-completion, we get the induced group homomorphism, denoted as $\eta_A : G(A) \to F(A)$.

Step 2: To show that for $R \in \mathsf{Rings}$, there exists a group homomorphism $C(R) \to F(R)$.

Consider the presentation $0 \to I \to \mathbb{Z}\{R\} \xrightarrow{\pi_1} R \to 0$ of R. By Step (1), we have a group homomorphism $F(\pi_1) \circ \eta_{\mathbb{Z}\{R\}} : G(\mathbb{Z}\{R\}) \to F(R)$.

It is easy to see that for $a, b \in \mathbb{Z}\{R\}$ such that $a - b \in I$, $G(\pi_1)(V_a^n - V_b^n) = V^n\langle\pi_1(a)\rangle - V^n\langle\pi_1(b)\rangle = 0$, thus $F(\pi_1) \circ \eta_{\mathbb{Z}\{R\}}(G_I) = 0$. Hence, there exists a group homomorphism $\eta : G(\mathbb{Z}\{R\})/G_I \to F(R)$. It remains to show that $F(\pi_1) \circ \eta_{\mathbb{Z}\{R\}}(\widetilde{G_I}) = 0$.

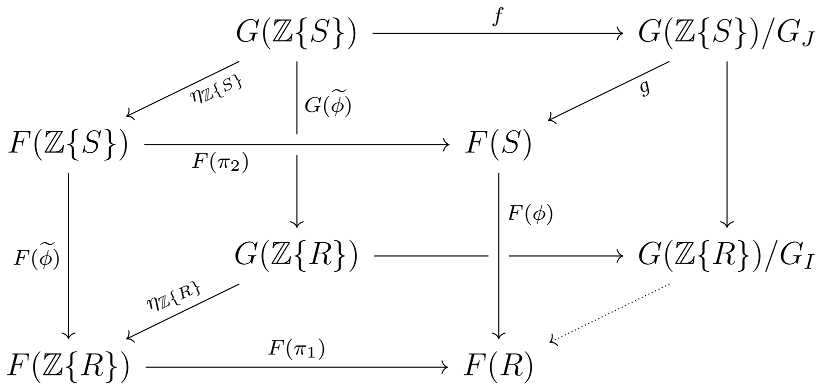
Let $S \in \mathsf{Rings}$ such that $S, \bar{S}$ are p-torsion free and $\phi : S \to R$ be a ring homomorphism. We now recall here the definition of Σ and the diagram (1) as in the given in Definition 5.2.4.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & J & \longrightarrow & \mathbb{Z}\{S\} & \xrightarrow{\pi_2} & S & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle\widetilde{\phi}} & & \downarrow{\scriptstyle\phi} & & \\ 0 & \longrightarrow & I & \longrightarrow & \mathbb{Z}\{R\} & \xrightarrow{\pi_1} & R & \longrightarrow & 0 \end{array} \qquad (1)$$

Consider the map $f : G(\mathbb{Z}\{S\}) \to G(\mathbb{Z}\{S\})/G_J$. Then

$$\Sigma := \{\alpha \in G(\mathbb{Z}\{R\}) \mid \alpha = G(\widetilde{\phi})(\beta),\ \beta \text{ is a p-torsion in } G(\mathbb{Z}\{S\})/G_J\}$$

We have the following diagram



Let $\alpha \in \Sigma$. Then $\alpha = G(\widetilde{\phi})(\beta)$ for some $\beta \in G_J^{\mathsf{sat}}$. Thus $p^\ell \beta \in G_J$ for some $\ell \geq 0$. In other words, $f(\beta)$ is a p-torsion element in $G(\mathbb{Z}\{S\})/G_J$. Since $\eta_{\mathbb{Z}\{S\}}(G_J) \subseteq F_J$, we have the induced group homomorphism denoted by $g : G(\mathbb{Z}\{S\})/G_J \to F(S)$, which takes $f(\beta)$ to a p-torsion element in $F(S)$. Since F is a pre-Witt functor and $S, \bar{S}$ are p-torsion free, $F(S)$ is p-torsion free. Thus $g \circ f(\beta) = 0$. Thus,

$$(F(\phi) \circ g \circ f)(\beta) = (F(\phi) \circ F(\pi_2) \circ \eta_{\mathbb{Z}\{S\}})(\beta) = 0$$

Since F is functor, we have the commutativity of the front square and thus,

$$(F(\phi) \circ F(\pi_2) \circ \eta_{\mathbb{Z}\{S\}})(\beta) = (F(\pi_1) \circ F(\widetilde{\phi}) \circ \eta_{\mathbb{Z}\{S\}})(\beta) = 0$$

By step (1), the left outermost square commutes. Hence,

$$(F(\pi_1) \circ F(\widetilde{\phi}) \circ \eta_{\mathbb{Z}\{S\}})(\beta) = (F(\pi_1) \circ \eta_{\mathbb{Z}\{R\}} \circ G(\widetilde{\phi})(\beta) = 0$$

By definition $\alpha = G(\widetilde{\phi})(\beta)$, hence

$$F(\pi_1) \circ \eta_{\mathbb{Z}\{R\}}(\beta) = 0$$

Since $\eta_{\mathbb{Z}\{R\}}(G_I) \subseteq F_I$, the morphism $F(\pi_1) \circ \eta_{\mathbb{Z}\{R\}}$ already factors through $G(\mathbb{Z}\{R\})/G_I$. Thus, we have a morphism

$$C(R) := G(\mathbb{Z}\{R\})/\langle G_I, \Sigma \rangle \to F(R)$$

□

In the remaining section, we show that C is in fact naturally isomorphic to E, which implies that E is universal. The first step towards proving this result would be to show that for a free non-commutative polynomial algebra A , $C(A) \cong X(A)$.

Proposition 5.3.8. *Let $p \neq 2$, and $A = \mathbb{Z}\{S\}$ be a free ring over a set S. The Conjecture 1.0.13 implies that $C(A) \cong X(A)$.*

Proof. The proof of this lemma is similar to the proof of Lemma 4.4.2. Since C is a universal weak pre-Witt functor, by using the Lemma 5.2.7 and the Lemma 5.3.4, one can show that there exists an epimorphism

$$\widetilde{\eta} : \widetilde{G}(A)/\widetilde{H}(A) \to \widetilde{X}(A); \quad V_a^n \mapsto V^n\langle a\rangle.$$

Since the map $\widetilde{\eta}$ is V-complete, it is enough to show that this map is injective. The injectivity is proved by using the Conjecture 1.0.13 and the arguments as in proof of Lemma 4.4.2. Hence we get an isomorphism denoted as $\eta_A : G(A) \to X(A)$ □

Proof of Theorem 1.0.14. To show that E is universal pre-Witt functor, by Theorem 5.3.7 it suffices to show that $E(R)$ is naturally isomorphic to $C(R)$ for $R \in \mathsf{Rings}$. Consider the presentation, $0 \to I \to A := \mathbb{Z}\{R\} \to R \to 0$. By the above Proposition 5.3.8, $C(A) \cong X(A)$. Following the proof of Theorem 5.3.7 with F replaced by X, we have the following commutative diagram.

$$\begin{array}{ccccccc}
G(\mathbb{Z}\{R\}) & \twoheadrightarrow & G(\mathbb{Z}\{R\})/G_I & \twoheadrightarrow & G(\mathbb{Z}\{R\})/\widetilde{G_I} & \longrightarrow & 0 \\
\downarrow{\scriptstyle \eta_{\mathbb{Z}\{R\}}} & & \downarrow & & \downarrow & & \\
X(\mathbb{Z}\{R\}) & \twoheadrightarrow & X(\mathbb{Z}\{R\})/X_I & \twoheadrightarrow & X(\mathbb{Z}\{R\})/\widetilde{X_I} & \longrightarrow & 0
\end{array}$$

Since $\eta_{\mathbb{Z}\{R\}}$ is an isomorphism, we have $\eta_{\mathbb{Z}\{R\}}(G_I) = X_I$ and $\eta_{\mathbb{Z}\{R\}}(\Sigma_I^G) = \Sigma_I^X$. Thus, $\eta_{\mathbb{Z}\{R\}}(\widetilde{G_I}) = \widetilde{X_I}$. This implies that $\eta_{\mathbb{Z}\{R\}}$ induces an isomorphism $\eta_R : C(R) \to E(R)$. □

5.4 Witt functors

The goal of this section is to define the notion of a Witt functor (see Definition 5.4.3) and to describe a universal Witt functor $\hat{E}$, assuming Conjecture 1.0.13. We also finish the proof of Theorem 1.0.12 by showing the existence of a natural transformation $E \to W_H$. Note that such a transformation exists by universality of E (Theorem 1.0.14), however we would like to establish this (see Theorem 5.4.8) without assuming Conjecture 1.0.13.

In the classical case, for $R \in \mathsf{CRings}$, the set $W(R)$ is in bijection with $R^{\mathbb{N}_0}$. This bijection can be explicitly given by

$$(a_0, a_1, ...) \mapsto \sum_n V^n \langle a_n \rangle$$

Let $F : \mathsf{Rings} \to \mathsf{Ab}$ be a pre-Witt functor. For a tuple $(a_0, a_1, ...) \in R^{\mathbb{N}_0}$, denote

$$(a_0, a_1, ...)_w := \sum_n V^n \langle a_n \rangle \in F(R).$$

5.4.1 Witt sum and difference polynomials

Before defining the Witt functor, we first recall the group structure on $W_H(R)$ for $R \in \mathsf{Rings}$ as given in Definition 3.1.9. Note that $W_H(R)$ is equipped with the Verschiebung operator

$$V : W(R) \to W(R) \qquad V(a_0, a_1, \cdots) := (0, a_0, a_1, \cdots)$$

and the Teichmüller map

$$\langle\ \rangle : R \longrightarrow W(R), \qquad \langle a \rangle := (a, 0, 0, \ldots)$$

Remark 5.4.1. The definitions $V : W_H(R) \to W_H(R)$ and $\langle\ \rangle : R \longrightarrow W_H(R)$ differ from that of $V : E(R) \to E(R)$ and $\langle\ \rangle : R \longrightarrow E(R)$ (see Definition 5.2.1 and Remark 5.2.5). Every element of $W_H(R)$ represented (not necessarily uniquely) as $(a_0, a_1 ...)_w$. This is a consequence of the fact that the addition and subtraction of elements of the form $(a_0, a_1 ...)_w$ in the group $W_H(R)$ are given by non-commutative version of Witt polynomials as given below.

Definition 5.4.2 (Witt sum and difference polynomials)**.** For $R \in \mathsf{Rings}$, and elements $(a_0, a_1, ...)_w, (b_0, b_1, ...)_w \in W_H(R)$,

$$(a_0, a_1, ...)_w + (b_0, b_1, ...)_w := (s_0(a_0, b_0), s_1(a_0, b_0, a_1, b_1), ...)$$

$$(a_0, a_1, ...)_w - (b_0, b_1, ...)_w := (d_0(a_0, b_0), d_1(a_0, b_0, a_1, b_1), ...)$$

where s_i and d_i are non-commutative analogues of classical Witt sum and difference polynomials as defined in [11, 1.4.1]. We use the following two variable specialisations of the Witt sum and difference polynomials. For an integer $i \geq 0$ define polynomials $r_i, e_i \in \mathbb{Z}\{X, Y\}$ by

$$r_i(X, Y) := s_i(X, Y, 0, 0, ...0, 0)$$
$$e_i(X, Y) := d_i(X, Y, 0, 0, ...0, 0)$$

It follows that $r_0(X, Y) = X + Y$ and $e_0(X, Y) = X - Y$. In particular, we have the following relations in W_H (and also in the classical case)

$$\langle x\rangle + \langle y\rangle = \langle x + y\rangle + \sum_{i>0} V^i \langle r_i(x, y)\rangle$$
$$\langle x\rangle - \langle y\rangle = \langle x - y\rangle + \sum_{i>0} V^i \langle e_i(x, y)\rangle$$

Definition 5.4.3 (Witt functor)**.** A pre-Witt functor $F : \mathsf{Rings} \to \mathsf{Ab}$ is called a Witt functor if,

$$\langle x\rangle + \langle y\rangle = \langle x + y\rangle + \sum_{i>0} V^i \langle r_i(x, y)\rangle$$
$$\langle x\rangle - \langle y\rangle = \langle x - y\rangle + \sum_{i>0} V^i \langle e_i(x, y)\rangle$$

Example 5.4.4. W_H is a Witt functor.

Definition 5.4.5 (The Witt functor $\hat{E}$)**.** For a ring $R \in \mathsf{Rings}$, let $\mathcal{R}(R) \subset E(A)$ denote the smallest closed subgroup stable under V and containing all elements of the form

$$\{\langle x\rangle + \langle y\rangle - \sum_n V^n \langle r_n(x, y)\rangle \mid x, y \in A\} \bigcup \{\langle x\rangle - \langle y\rangle - \sum_n V^n \langle e_n(x, y)\rangle \mid x, y \in R\}$$

where r_n, e_n are integer polynomials defined in (5.4.2). Let $\hat{E}(R) := \frac{E(R)}{\mathcal{R}(R)}$. Clearly $\hat{E}$ is a Witt functor, since the required relations have been forced by the definition.

The following result is an immediate consequence of the above definition of $\hat{E}$.

Lemma 5.4.6. *Every element of $\hat{E}(R)$ is of the form*

$$\sum_{n=0}^{\infty} V^n \langle a_n \rangle.$$

Moreover, we have the following conjectural characterisation of the functor $\hat{E}$.

Theorem 5.4.7. *For $p \neq 2$, the Conjecture 1.0.13 implies that $\hat{E}$ is a universal Witt functor.*

Proof. By using Conjecture 1.0.13, we have proved that E is a universal pre-Witt functor (see Theorem 1.0.14). $\hat{E}$ is obtained by simply going modulo the extra relations in E required to be a Witt functor. From this, one can easily deduce that $\hat{E}$ is a universal Witt functor. □

The goal of the remaining section is to prove Theorem 1.0.12(2). We will prove the following result without using Conjecture 1.0.13 and Theorem 1.0.14.

Theorem 5.4.8. *There is a unique natural transformation of pre-Witt functors $E \to W_H$ and of Witt functors $\hat{E} \to W_H$.*

We will need the following results in order to the prove Proposition 5.4.8.

Lemma 5.4.9. *Let $A = \mathbb{Z}\{S\}$ be a free algebra. Then there is a natural isomorphism $\hat{E}(A) \cong \frac{X(A)}{R(A)}$ where $R(A) \subset X(A)$ is the smallest V-stable closed subgroup containing*

$$\{\langle x \rangle + \langle y \rangle - \sum_n V^n \langle r_n(x,y) \rangle \mid x, y \in A\} \cup \{\langle x \rangle - \langle y \rangle - \sum_n V^n \langle e_n(x,y) \rangle \mid x, y \in A\}$$

Proof. By Corollary 5.2.7, we know that $E(A) \cong X(A)$. Since this isomorphism is compatible with V and $\langle\ \rangle$, $\mathcal{R}(A)$ is mapped to $R(A)$ □

We now observe the following connection between $\hat{E}(A)$ and $W_H(A)$.

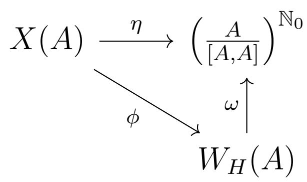
Lemma 5.4.10. *Let $A = \mathbb{Z}\{S\}$ be a free algebra. Then the image of the natural map $\hat{E}(A) \to (\frac{A}{[A,A]})^{\mathbb{N}_0}$ is canonically isomorphic to $W_H(A)$. This gives a canonical surjection $\hat{E}(A) \to W_H(A)$ sending $V^n\langle a\rangle \mapsto V^n\langle a\rangle$.*

Proof. Let $\eta : X(A) \to \left(\frac{A}{[A,A]}\right)^{\mathbb{N}_0}$ be the map given by the composition

$$X(A) \hookrightarrow A^{\mathbb{N}_0} \to \left(\frac{A}{[A,A]}\right)^{\mathbb{N}_0}.$$

We will show that $R(A) \subseteq \mathrm{Ker}(\eta)$.

We know that the ghost map $\omega : W_H(A) \to \left(\frac{A}{[A,A]}\right)^{\mathbb{N}_0}$ is injective (see [13, page 2]). Hence, the image $\omega(W_H(A))$ is canonically isomorphic to $W_H(A)$. We consider the following diagram:



Let $\phi : X(A) \to W_H(A)$ be a map that sends an element $V^n\langle a\rangle$ to $V^n\langle a\rangle$. We also recall that $W_H(A)$ is generated by elements of the form $\{V^n\langle a_n\rangle \mid a_n \in A, n \in \mathbb{N}_0\}$ by [17, Lemma 3.3], hence, ϕ is a surjective map. Also,

$$\omega(\sum_n V^n\langle a_n\rangle) = \omega(a_0, a_1, \cdots) = (\overline{a_0}, \overline{a_0}^p + \overline{a_1}, \cdots)$$

It is easy to verify that,

$$\eta(\sum_n V^n\langle a_n\rangle) = (\overline{a_0}, \overline{a_0}^p + \overline{a_1}, \cdots).$$

Hence, the image of the natural map $X(A) \to (\frac{A}{[A,A]})^{\mathbb{N}_0}$ is canonically isomorphic to $W_H(A)$. Note that the 'relations' defining $R(A)$ (see Definition 5.4.5) are mapped to zero in $W_H(A)$ and hence are mapped to zero in $(\frac{A}{[A,A]})^{\mathbb{N}_0}$. Therefore η induces a map

$$\frac{X(A)}{R(A)} \cong \hat{E}(A) \xrightarrow{\hat{\eta}} \left(\frac{A}{[A,A]}\right)^{\mathbb{N}_0}$$

and a canonical surjection

$$\hat{E}(A) \to W_H(A)$$

□

Proof of Theorem 5.4.8. First, we show that there exists a natural transformation $\eta : E \to W_H$ between the pre-Witt functors. We follow the diagram and arguments as in Theorem 5.3.7, where the roles of C (resp. F) are now played by E (resp. W_H), with E being a weak pre-Witt functor and W_H being a pre-Witt functor.

For $R \in \mathsf{Rings}$, consider the presentation $0 \to I \to A := \mathbb{Z}\{R\} \to R \to 0$. Lemma 5.2.7 and the proof of Lemma 5.4.10 gives a natural morphism $\eta_A : E(A) \cong X(A) \to W_H(A)$ where A is any free non-commutative algebra. Thus, there exists a morphism $\eta_{\mathbb{Z}\{R\}} : E(\mathbb{Z}\{R\}) \to W_H(\mathbb{Z}\{R\})$ given by, $V^n\langle a\rangle \mapsto V^n\langle a\rangle$. In order to show that there exists a natural transformation $\eta_R : E(R) \to W_H(R)$ we need to show that $\eta_{\mathbb{Z}\{R\}}(\widetilde{X_I}) = 0$ in $W_H(R)$. Following diagram as in Theorem 5.3.7, we have the commutativity of the outer leftmost square involving $\eta_{\mathbb{Z}\{S\}} : E(\mathbb{Z}\{S\}) \to W_H(\mathbb{Z}\{S\})$ and $\eta_{\mathbb{Z}\{R\}} : E(\mathbb{Z}\{R\}) \to W_H(\mathbb{Z}\{R\})$. Thus, following the argument of the proof of Step (2) of Theorem 5.3.7 we get that there exists a natural transformation $\eta_R : E(R) \to W_H(R)$ between the pre-Witt functors. It is now straightforward to observe that the 'relations' defining $\hat{E}(R)$ are mapped to zero in $W_H(R)$. Hence we have a unique natural transformation $\hat{E} \to W_H$ of Witt functors. □

Proof of Theorem 1.0.12. Follows from Theorem 5.2.8, Theorem 5.2.9 and Theorem 5.4.8.

□

5.5 Evidence for the Conjecture

The aim of this section is to present computational evidence supporting Conjecture 1.0.13, in addition to the fact that an analogous statement holds in the commutative setting (see Lemma 1.0.10).

For any ring R and any element $x \in R$, we write

$$\langle x \rangle := (x, x^p, x^{p^2}, \dots) \in X(R) \subset R^{\mathbb{N}_0},$$

as in Definition 3.2.1.

We emphasize that the map $\langle \cdot \rangle$ introduced above is not new. For any ring R and prime p, the n-th component r^{p^n} of $\langle r \rangle$ coincides with the n-th ghost component of the Teichmüller lift $\langle r \rangle \in W(R)$ in the ring of p-typical Witt vectors (see Definition 2.2.16). Although $A = \mathbb{Z}\{S\}$ is non-commutative and $W(A)$ is therefore only an abelian group, both the ghost map and the Teichmüller construction remain well-defined in this setting. Conjecture 1.0.13 is therefore equivalent to asking whether the Teichmüller lifts $\{f_1\}, \dots, \{f_r\}$ have $\mathbb{Z}$-linearly independent images under the ghost map.

In the commutative case, the statement reduces to a Vandermonde-type determinant argument; see Lemma 4.4.1 and Lemma 1.0.10. The non-commutative integral setting is significantly harder. When $p = 2$, the conjecture fails in a trivial way (e.g. for constant polynomials), which shows that the restriction $p \neq 2$ is essential. The additional hypothesis $f_i \neq -f_j$ is forced by the identity $\langle -f \rangle = -\langle f \rangle$ for odd primes p. The case $r = 2$ can be handled by an elementary argument using only the components corresponding to $n = 0$ and $n = 1$. However, for $r \geq 3$, the main difficulty lies in controlling the non-commutative multinomial cross-terms arising in higher powers.

Let $A = \mathbb{Z}\{X, Y\}$ and $p = 3$. For nonzero elements $f_1, f_2, f_3 \in A$ with distinct moduli, we wish to verify that $\{\langle f_i \rangle\}$ is a $\mathbb{Z}$-linearly independent subset of $X(A)$. This is immediate in either of the following cases:

1. The elements f_1, f_2, f_3 are $\mathbb{Z}$-linearly independent.
2. The images of f_i in the commutative polynomial ring $\mathbb{Z}[X, Y]$ have distinct moduli (see Lemma 1.0.10).

To obtain nontrivial computational evidence for Conjecture 1.0.13, we therefore considered triples f_1, f_2, f_3 that do not satisfy either of the above conditions. Using SageMath, we verified the conjecture for a range of such examples of degree at most 3. We provide the sage code below.

5.6 Sage Code for Verifying the Conjecture

```
# Non-commutative polynomial ring over ZZ
F.<X,Y> = FreeAlgebra(ZZ, 2)

# Commutative polynomial ring for comparison
R.<x,y> = PolynomialRing(ZZ, 2)

def to_commutative(f):
#Map from free algebra to commutative polynomial ring.

result = R.zero()
for mon, coeff in f.monomial_coefficients().items():
# mon is a word in X,Y
mon_str = str(mon)
x_count = mon_str.count('X')
y_count = mon_str.count('Y')
result += coeff * x**x_count * y**y_count
return result

def power_in_free_algebra(f, n):
#Compute f^n in the free algebra.
if n == 0:
return F.one()
result = f
for _ in range(n - 1):
result = result * f
return result

def ab_sequence(f, p, length):

#Compute the sequence ab(f) = (f, f^p, f^{p^2}, ..., f^{p
    ^{length-1}})
```

```
return [power_in_free_algebra(f, p**i) for i in range(
   length)]

def extract_coefficients(f, monomial_list):

#Extract coefficients of f with respect to a list of
   monomials.
#Returns a vector of coefficients. This works only if the
    monomial_list is in F, not just a list of strings or
   words.

coeff_dict = dict(f)
return vector(ZZ, [coeff_dict.get(m, 0) for m in
   monomial_list])

def get_all_monomials(polys):
#Get all monomials appearing in a list of polynomials.
monomials = set()
for f in polys:
monomials.update(f.monomial_coefficients().keys())
return sorted(monomials, key=str)

def distinct_moduli(f_list):
#Check if f_i != +/-f_j for all i != j.

n = len(f_list)
for i in range(n):
for j in range(i+1, n):
if f_list[i] == f_list[j] or f_list[i] == -f_list[j]:
return False
return True

def Z_linearly_independent(f_list):
```

```
#Check if f_list is Z-linearly independent in the free
   algebra.

# Step 1: collect all monomials appearing
monomials = set()
for f in f_list:
monomials.update(f.monomial_coefficients().keys())
monomials = sorted(monomials, key=str)

# Step 2: build coefficient matrix
M = []
for m in monomials:

row = [f.monomial_coefficients().get(m, 0) for f in
   f_list]
M.append(row)

M = Matrix(ZZ, M)

# Step 3: check kernel over QQ
return M.change_ring(QQ).right_kernel().dimension() == 0

def commutative_distinct_moduli(f_list):
#Check if images in the commutative ring have distinct
   moduli.
images = [to_commutative(f) for f in f_list]
n = len(images)
for i in range(n):
for j in range(i+1, n):
if images[i] == images[j] or images[i] == -images[j]:
return False
return True

def check_Z_linear_independence(sequences,
   max_power_index):
```

```
#Check if {ab(f_i)} are Z-linearly independent, using
   truncation up to max_power_index.

# Step 1: collect all monomials appearing in all powers
monomials = set()
for seq in sequences:
for f in seq[:max_power_index]:
monomials.update(f.monomial_coefficients().keys())
monomials = sorted(monomials, key=str)

# Step 2: build coefficient matrix (stacking all k)
M = []
for k in range(max_power_index):
for m in monomials:
row = [seq[k].monomial_coefficients().get(m, 0) for seq
   in sequences]
M.append(row)

M = Matrix(ZZ, M)

# Step 3: check kernel over QQ
kernel = M.change_ring(QQ).right_kernel()
is_independent = kernel.dimension() == 0

return is_independent, kernel

def verify_conjecture(f_list, p=3, max_power_index=3,
   verbose=True):

#Verify the conjecture for a given list of polynomials.

# Compute ab sequences
sequences = [ab_sequence(f, p, max_power_index) for f in
   f_list]
```

```
# Check Z-linear independence
is_independent, kernel = check_Z_linear_independence(
   sequences, max_power_index)

if is_independent:
print("RESULT:␣{ab(f_i)}␣is␣Z-linearly␣independent.")
print("Conjecture␣HOLDS␣for␣this␣sample.")
else:
print("RESULT:␣{ab(f_i)}␣is␣Z-linearly␣DEPENDENT!")
print("Conjecture␣FAILS␣for␣this␣sample!")
return is_independent

##################################################

# Example usage with a specific sample
print("EXAMPLE:␣Manual␣verification")
print()

# An interesting example.
f1 = X + Y
f2 = X - Y
f3 = 2*X    # f3 = f1 + f2, so Z-linearly dependent

verify_conjecture([f1, f2, f3], p=3, max_power_index=3)
print()
print()
```

Here is the output:

```
RESULT: {ab(f_i)} is Z-linearly independent.
Conjecture HOLDS for this sample.
```

```
# Another example with non-commutative structure
print("EXAMPLE:␣Manual␣Verification-2")
print()
```

```
f1 = X*Y
f2 = Y*X
f3 = X*Y + Y*X # f3 = f1 + f2, so Z-linearly dependent

verify_conjecture([f1, f2, f3], p=3, max_power_index=3)
```

Here is the output:

```
RESULT: {ab(f_i)} is Z-linearly independent.
Conjecture HOLDS for this sample.
```

Bibliography

[1] Emil Artin and Otto Schreier, *Eine kennzeichnung der reell abgeschlossenen körper*, Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg **5** (1927), 225–231.

[2] James Borger, *The basic geometry of Witt vectors, I: The affine case*, Algebra Number Theory **5** (2011), no. 2, 231–285. MR 2833791

[3] ———, *The basic geometry of Witt vectors. II: Spaces*, Math. Ann. **351** (2011), no. 4, 877–933. MR 2854117

[4] Nicolas Bourbaki, *Elements of mathematics: General topology. part 2,[chapters 5-10].*, Hermann, 1966.

[5] Pierre Cartier, *Groupes formels associés aux anneaux de witt généralisés*, C.R. Acac. Sci. Paris Sér. A-B **265** (1967), A129–A132.

[6] Joachim Cuntz and Christopher Deninger, *Witt vector rings and the relative de rham witt complex*, Journal of Algebra **440** (2015), 545–593.

[7] The Sage Developers, *Sagemath, the Sage Mathematics Software System (version 10.1)*, https://www.sagemath.org, 2023.

[8] Emanuele Dotto, Achim Krause, Thomas Nikolaus, and Irakli Patchkoria, *Witt vectors with coefficients and characteristic polynomials over non-commutative rings*, Compositio Mathematica **158** (2022), no. 2, 366–408.

[9] Michiel Hazewinkel (ed.), *Handbook of algebra. Vol. 1*, Handbook of Algebra, vol. 1, Elsevier/North-Holland, Amsterdam, 1996. MR 1421796

[10] ———, *Witt vectors. part 1*, arXiv preprint arXiv:0804.3888 (2008).

[11] Lars Hesselholt, *Witt vectors of non-commutative rings and topological cyclic homology*, Acta Math. **178** (1997), no. 1, 109–141.

[12] ———, *Galois cohomology of witt vectors of algebraic integers*, Mathematical Proceedings of the Cambridge Philosophical Society, vol. 137, Cambridge University Press, 2004, pp. 551–557.

[13] ———, *Correction to "witt vectors of non-commutative rings and topological cyclic homology"*, Acta mathematica **195** (2005), no. 1, 55–60.

[14] ———, *The big de rham–witt complex*, Acta Math **214** (2015), 135–207.

[15] Amit Hogadi and Supriya Pisolkar, *On the cohomology of witt vectors of p-adic integers and a conjecture of hesselholt*, Journal of Number Theory **131** (2011), no. 10, 1797–1807.

[16] ———, *An equicharacteristic analogue of hesselholt's conjecture on cohomology of witt vectors*, Acta Arithmetica **158** (2013), 165–171.

[17] ———, *On the comparison of two constructions of witt vectors of non-commutative rings*, Journal of Algebra **506** (2018), 379–396.

[18] André Joyal, *δ-anneaux et vecteurs de witt*, CR Math. Rep. Acad. Sci. Canada **7** (1985), no. 3, 177–182.

[19] Dmitry Kaledin, *Witt vectors, commutative and non-commutative*, arXiv preprint arXiv:1708.05660 (2017).

[20] Casimir Kothari, *Notes on motivating witt vectors and delta rings*, https://math.uchicago.edu/~ckothari/WittAndDelta.pdf.

[21] Supriya Pisolkar, *Morphisms between two constructions of witt vectors of non-commutative rings*, Proceedings of the American Mathematical Society **148** (2020), no. 7, 2835–2842.

[22] Supriya Pisolkar and Biswanath Samanta, *A universal group-theoretic characterisation of p-typical witt vectors*, Journal of Algebra **677** (2025), 1–12.

[23] George Pólya and Gabor Szegő, *Problems and theorems in analysis. II*, Classics in Mathematics, Springer-Verlag, Berlin, 1998.

[24] Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York-Berlin, 1979.

[25] Leonid Stern, *On the norm groups of global fields*, Journal of Number Theory **32** (1989), no. 2, 203–219.

[26] Ryszard Szwarc, *How to prove that generalized vandermonde matrix is invertible?*, Mathematics Stack Exchange, URL:https://math.stackexchange.com/q/4549001.

[27] Wikipedia, *Witt vectors*, https://en.wikipedia.org/wiki/Witt_vector.

[28] Ernst Witt, *Zyklische körper und algebren der charakteristik p vom grad p^n*, J. reine angw. Math. **176** (1937).

[29] ———, *Vektorkalkül und endomorphismen der einspotenzreihengruppe*, Collected Papers-Gesammelte Abhandlungen, Springer, 1998, pp. 157–194.

[30] Donald Yau, *Lambda-rings*, World Scientific Publishing Company, 2010.