Witt Vectors

Zachary Gardner

Unless otherwise stated, A denotes a commutative ring, $I \subseteq A$ denotes an ideal, and p is a fixed rational prime. We say A has characteristic p if $p = 0$ in A. Given such a ring, there is a Frobenius map $x \mapsto x^p$ usually denoted $\varphi : A \to A$. Given $x, y \in A$, the notation $x = y \in A/I$ means that $x \equiv y \bmod I$. The acronym NZD is shorthand for "non-zero-divisor." Given A, its p-adic completion is $\widehat{A} = \widehat{A}_p := \varprojlim A/p^n$. We say A is p-adically complete if the canonical ring map $A \to \widehat{A}$ is an isomorphism.

Much of the motivation behind the construction of Witt vectors comes from the desire to do arithmetic with p-adic integers viewed as power series expansions in p. We will see later that $W(\mathbb{F}_p) = \mathbb{Z}_p$. We start with a simple technical result.

Lemma 0.1. *Let $x, y \in A$ such that $x = y \in A/p^n$. Then, $x^p = y^p \in A/p^{n+1}$ and so $x^{p^n} = y^{p^n} \in A/p^{n+1}$.*

This result in turn tells us something about polynomial arithmetic.

Corollary 0.2. *Let $f \in \mathbb{Z}[t_1, \ldots, t_r]$. Then,*

$$f(t_1^p, \ldots, t_r^p)^{p^n} = f(t_1, \ldots, t_r)^{p^{n+1}} \in \mathbb{Z}/p^{n+1}[t_1, \ldots, t_r].$$

Given $x \in A/p$ and $\tilde{x} \in A/p^{n+1}$ a lift of x, $\tilde{x}^{p^n}$ is independent of the choice of lift by the above lemma and so we obtain a map $\tau_n : A/p \to A/p^{n+1}$ uniquely fitting into the commutative diagram

$$\begin{tikzcd} A/p^{n+1} \arrow[d, two heads] \arrow[dr, "(\cdot)^{p^n}"] & \\ A/p \arrow[r, dotted, "\exists!\, \tau_n"'] & A/p^{n+1} \end{tikzcd}$$

Note that τ_n is multiplicative but not additive.

Our goal now is to construct a coherent framework for doing arithmetic with things of the form $\tau_n(x_0) + p\tau_{n-1}(x_1) + \cdots + p^n\tau_0(x_n)$ for $x_0, \ldots, x_n \in A/p$, where we are using the multiplication maps $p^{i-j} : A/p^j \to A/p^i$ associated to $i \geq j$. Our first order of business is showing that such elements form a subring of A/p^{n+1}.

Lemma 0.3. *There exist unique polynomials $s_i(x, y) \in \mathbb{Z}[x, y]$ for $i \geq 0$ such that, for every $n \geq 0$,*

$$x^{p^n} + y^{p^n} = s_0(x, y)^{p^n} + ps_1(x, y)^{p^{n-1}} + \cdots + p^n s_n(x, y) \in \mathbb{Z}[x, y].$$

These polynomials are given inductively by $s_0(x,y) = x+y$ and

$$s_{n+1}(x,y) = \frac{1}{p^{n+1}}\left(x^{p^{n+1}} + y^{p^{n+1}} - \sum_{i=0}^{n} p^i s_i(x,y)^{p^{n+1-i}}\right).$$

Corollary 0.4. *Let $x, y \in A/p$. Then,*

$$\tau_n(x) + \tau_n(y) = \tau_n(s_0(x,y)) + p\tau_{n-1}(s_1(x,y)) + \cdots + p^n\tau_0(s_n(x,y)).$$

Hence, the set of elements of A/p^{n+1} of the desired form is closed under addition and so forms a subring.

Consider the Witt functor $W : \mathsf{CRing} \to \mathsf{Set}$ defined on objects by $W(A) := \prod_{i\geq 0} A$. The Witt vectors $W(A)$ come equipped with a Teichmüller map $[\cdot] : A \to W(A)$ given by $x \mapsto (x, 0, 0, \ldots)$ and a *verschiebung* or shift operator $V : W(A) \to W(A)$ given by $(x_0, x_1, \ldots) \mapsto (0, x_0, x_1, \ldots,)$.[1] Every element of $W(A)$ can be written uniquely as $\sum_{i\geq 0} V^i[x_i]$ for $x_i \in A$.[2] Using these expansions, we may define the **ghost maps**[3] $\mathrm{gh}_n : W(A) \to A$ for $n \geq 0$ via

$$\sum_{i\geq 0} V^i[x_i] \mapsto \sum_{i=0}^{n} p^i x_i^{p^{n-i}}.$$

As an important special case, note that

$$\mathrm{gh}_n(V^i[x]) = \begin{cases} p^i x^{p^{n-i}}, & i \leq n, \\ 0, & \text{otherwise} \end{cases}$$

given $n, i \geq 0$ and $x \in A$. In particular, $\mathrm{gh}_n \circ [\cdot] = (\cdot)^{p^n}$.

Theorem 0.5. *There exists a unique lift $W : \mathsf{CRing} \to \mathsf{CRing}$ of the functor $W : \mathsf{CRing} \to \mathsf{Set}$ such that, for every $A \in \mathsf{CRing}$, addition and multiplication on $W(A)$ are continuous for the product topology and gh_n is a ring homomorphism for every $n \geq 0$.*[4]

Proof. We provide a sketch. The major steps are as follows.

(1) $\mathrm{gh}_n(W(A)) \subseteq A$ is closed under addition.

(2) $\mathrm{gh}_n(W(A)) \subseteq A$ is a subring.

(3) Assume A has no p-torsion. Then, $(\mathrm{gh}_0, \mathrm{gh}_1, \ldots) : W(A) \to \prod_{i\geq 0} A$ is injective and so there is a unique ring structure on $W(A)$ with the desired properties.

(4) Assume A has no p-torsion and let $I \subseteq A$ be an ideal. Then, $W(I) := \left\{\sum_{i\geq 0} V^i[x_i] : x_i \in I\right\}$ is an ideal of $W(A)$.

[1] Elements in the image of $[\cdot]$ are often called **Teichmüller lifts. It should be noted that this terminology has been waning in popularity since Teichmüller was a notorious Nazi.**

[2] This is a purely symbolic equivalent to the expression $(x_0, x_1, \ldots)$ as $W(A)$ has no arithmetic structure at the moment. Later we will place a ring structure on $W(A)$ with a somewhat nontrivial additive structure.

[3] The underlying polynomials of the ghost maps are sometimes called **Witt polynomials**.

[4] Stated another way, the first part of this result says that W factors uniquely through CRing.

(5) Dropping the assumption on p-torsion, choose p-torsion-free $B \in \mathsf{CRing}$ with $\pi : B \twoheadrightarrow A$. Then, $W(A)$ inherits a ring structure after identifying it with the ring $W(B)/W(\ker \pi)$.

$\square$

Claim 0.6. *The shift operator $V : W(A) \to W(A)$ is additive.*

Claim 0.7. *The Teichmüller map $[\cdot] : A \to W(A)$ is multiplicative.*

Lemma 0.8. *Given $x \in A$, we have $V([x^p]) = p[x]$, with the right-hand side using Witt vector addition.*

Simply apply ghost maps to both sides of the equation and use injectivity. One consequence of this result is as follows. Suppose that k is a characteristic p perfect ring and let $(\cdot)^{1/p^i} := \varphi^{-i}$. Then, a generic element of $W(k)$ can be written as

$$\sum_{i \geq 0} V^i[x_i] = \sum_{i \geq 0} p^i[x_i^{1/p^i}] \in W(k),$$

the latter sum using Witt vector addition.

Corollary 0.9. *Suppose A is reduced. Then, p is an NZD in $W(A)$.*

Properties of the maps τ_n guarantee that there is a unique factorization

$$\begin{tikzcd} W(A) \arrow[r, "\mathrm{gh}_n"] \arrow[d, two heads] & A \arrow[d, two heads] \\ W(A/p) \arrow[r, dotted, "\exists!\, \tilde{\theta}_n"'] & A/p^{n+1} \end{tikzcd}$$

Indeed, letting $x \in A$ with $\overline{x} \in A/p$ its image, we have

$$\tilde{\theta}_n(V^i[\overline{x}]) = \mathrm{gh}_n(V^i[x]) \bmod p^{n+1} = p^i x^{p^{n-i}} \bmod p^{n+1} = p^i \tau_{n-i}(\overline{x})$$

and so $\tilde{\theta}_n$ is given by $\sum_{i \geq 0} V^i[y_i] \mapsto \sum_{i=0}^{n} p^i \tau_{n-i}(y_i)$.

Theorem 0.10. *Let k be a characteristic p perfect ring (equivalently, a perfect commutative $\mathbb{F}_p$-algebra). Then, the following hold.*

(1) *$W(k)$ is p-adically complete.*

(2) *p is an NZD in $W(k)$ and, hence, $W(k)$ is a flat $\mathbb{Z}_p$-module.*

(3) *$pW(k) = VW(k) = \ker \mathrm{gh}_0$.*

Corollary 0.11. *Let k be a characteristic p perfect field. Then, $W(k)$ is a characteristic 0 DVR with maximal ideal $pW(k)$.*

Example 0.12. $W(\mathbb{F}_p) \cong \mathbb{Z}_p$. *This can be shown abstractly by showing that $\mathbb{Z}_p$ satisfies the universal property of $W(\mathbb{F}_p)$ described below. More concretely, there is an explicit isomorphism given by*

$$\sum_{i \geq 0} V^i[x_i] \mapsto (x_0, x_0 + px_1, x_0 + px_1 + p^2 x_2, \ldots).$$

Let k be a perfect ring and $f : k \to A/p$ a ring map. Then, for each $n \geq 1$ there is a commutative diagram

$$\begin{tikzcd} W(k) \arrow[r, dotted, "\exists!\, f_n"] \arrow[d, two heads, "\mathrm{gh}_0"'] & A/p^{n+1} \arrow[d, two heads] \\ k \arrow[r, "f"'] & A/p \end{tikzcd}$$

The map f_n is characterized by the fact that

$$f_n([x]) = f_n([x^{1/p^n}])^{p^n} = \tau_n(f(x^{1/p^n}))$$

and so we have the factorization

$$W(k) \xrightarrow{W(\varphi^{-n})} W(k) \xrightarrow{W(f)} W(A/p) \xrightarrow{\tilde{\theta}_n} A/p^{n+1}$$

Corollary 0.13. *Let A be p-adically complete with ring map $f : k \to A/p$. Then, there exists a unique lift $\tilde{f} : W(k) \to A$ of f in the sense that the diagram*

$$\begin{tikzcd} W(k) \arrow[r, dotted, "\exists! \tilde{f}"] \arrow[d, two heads, "\mathrm{gh}_0"'] & A \arrow[d, two heads] \\ k \arrow[r, "f"'] & A/p \end{tikzcd}$$

commutes. Moreover, $\tilde{f}$ is continuous with respect to the p-adic topologies on $W(k)$ and A.

Note that, in the case that A is not p-adically complete, we still get a lift $W(k) \to \widehat{A}$ and $\widehat{A}/p \cong A/p$ canonically.

TO DO: truncated Witt vectors, F map, proofs