p fixed prime, A commutative ring.

Witt polynomials: For $n \in \mathbb{N}_0$ define $\Phi_n \in \mathbb{Z}[x_0, \ldots, x_n]$:

$$\Phi_n(x_0, \ldots, x_n) := x_0^{p^n} + p x_1^{p^{n-1}} + \cdots + p^n x_n \ .$$

We have $\Phi_0 = x_0$ and the recurrence relations:

$$\Phi_{n+1}(x_0, \ldots, x_{n+1}) = \Phi_n(x_0^p, \ldots, x_n^p) + p^{n+1} x_{n+1} \ ,$$

$$\Phi_{n+1}(x_0, \ldots, x_{n+1}) = x_0^{p^{n+1}} + p\Phi_n(x_1, \ldots, x_{n+1}) \ .$$

Proposition 1. *$s \in \mathbb{N}$, $n \in \mathbb{N}_0$, $a_0, \ldots, a_n$, $b_0, \ldots, b_n \in A$. If $a_i \equiv b_i \pmod{p^s A}$ for $i = 0, \ldots, n$, then*

$$\Phi_i(a_0, \ldots a_i) \equiv \Phi_i(b_0, \ldots b_i) \pmod{p^{s+i} A} \quad \text{for } i = 0, \ldots, n \ .$$

Proof: Exercise. Use $a \equiv b \pmod{p^s A} \Rightarrow a^{p^j} \equiv b^{p^j} \pmod{p^{s+j} A}$, and the recurrence for the Φ_i.

If $\underline{a} = (a_n)_{n \in \mathbb{N}_0} \in A^{\mathbb{N}}$, use obvious interpretation of $\Phi_j(\underline{a})$. Define the map

$$\Phi = \Phi_A \colon A^{\mathbb{N}} \longrightarrow A^{\mathbb{N}}$$

by $\Phi(\underline{a}) := (\Phi_n(\underline{a}))_{n \in \mathbb{N}_0}$.

Proposition 2. *Suppose that p is not a zero divisor in A, and suppose that A has an endomorphism σ with $\sigma(a) \equiv a^p \pmod{pA}$ for all $a \in A$. Then $\Phi \colon A^{\mathbb{N}} \longrightarrow A^{\mathbb{N}}$ is injective with image consisting of those sequences (b_n) for which*

$$\sigma(b_n) \equiv b_{n+1} \pmod{p^{n+1} A} \ , \ \forall n \in \mathbb{N}_0 \ .$$

In particular, Φ is bijective if p is invertible in A.

Proof: The recurrence for the Φ_j shows that $\underline{b} = \Phi(\underline{a})$ if and only if $b_0 = a_0$, and

$$b_n = \Phi_{n-1}(a_0^p, \ldots, a_{n-1}^p) + p^n a_n \ , \quad \forall n \geq 1 \ .$$

So, if p is not a zero divisor in A, the sequence $\underline{a}$ is uniquely determined by $\underline{b}$ if it exists.

Let $\underline{a}$ be given and put $\underline{b} = \Phi(\underline{a})$. As $\sigma(a_j) \equiv a_j^p \pmod{pA}$, Proposition 1 and the recurrence for the Φ_i show that

$$\begin{aligned} \sigma(b_{n-1}) &= \sigma\left(\Phi_{n-1}(a_0, \ldots, a_{n-1})\right) = \Phi_{n-1}(\sigma(a_0), \ldots, \sigma(a_{n-1})) \\ &\equiv \Phi_{n-1}(a_0^p, \ldots, a_{n-1}^p) \pmod{p^n A} \\ &\equiv \Phi_n(a_0, \ldots, a_n) \pmod{p^n A} \\ &\equiv b_n \pmod{p^n A} \ . \end{aligned}$$

If conversely $\underline{b}$ is given with $\sigma(b_n) \equiv b_{n+1} \pmod{p^{n+1} A}$, $\forall n \in \mathbb{N}$, we define a_n recursively such that $b_n = \Phi_{n-1}(a_0, \ldots, a_{n-1})$: Put $a_0 := b_0$ and suppose that $a_0, \ldots a_{n-1}$ have been constructed. Then as above we obtain

$$b_n \equiv \sigma(b_{n-1}) \equiv \Phi_{n-1}(a_0^p, \ldots, a_{n-1}^p) \pmod{p^n A} \ ,$$

whence we deduce the existence of a unique $a_n \in A$ such that

$$b_n = \Phi_{n-1}(a_0^p, \ldots, a_{n-1}^p) + p^n a_n = \Phi_n(a_0, \ldots, a_n) \ .$$

The last statement of the proposition is now clear.

Theorem 1. *Consider the ring $A = \mathbb{Z}[x_0, \ldots, x_n, \ldots; y_0, \ldots, y_n, \ldots]$ of polynomials in countably many variables $x_0, \ldots, x_n, \ldots; y_0, \ldots, y_n, \ldots$, and write $\underline{x} := (x_n)$, $\underline{y} := (y_n)$. Suppose that $f \in \mathbb{Z}[X, Y]$ is a polynomial in 2 variables. Then there exists a unique sequence $\underline{\psi}_f = ((\psi_f)_n)_{n \in \mathbb{N}_0})$ such that*

$$\Phi_A(\underline{\psi}_f) = f(\Phi_A(\underline{x}), \Phi_A(\underline{y})) \ ,$$

i.e. such that

$$\Phi_n((\psi_f)_0, \ldots (\psi_f)_n) = f(\Phi_n(\underline{x}), \Phi_n(\underline{y}))$$

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

Proof: Notice first that p is not a zero divisor in A. Consider the endomorphism σ of A given by $\sigma(z) = z$ for $z \in \mathbb{Z}$, $\sigma(x_j) = x_j^p$, $\sigma(y_j) = y_j^p$ for $j \in \mathbb{N}_0$. Then $\sigma(a) \equiv a^p \pmod{pA}$ for all $a \in A$. Using the recurrence for the Φ_n, we now obtain

$$\begin{aligned} \sigma\left(f(\Phi_n(\underline{x}), \Phi_n(\underline{y}))\right) &= f(\Phi_n(\underline{x}^p), \Phi_n(\underline{y}^p)) \\ &\equiv f(\Phi_{n+1}(\underline{x}), \Phi_{n+1}(\underline{y})) \pmod{p^{n+1}A} \ . \end{aligned}$$

The claim now follows from Proposition 2.

Let $(S_0, \ldots, S_n, \ldots)$, $(P_0, \ldots, P_n, \ldots)$, and $(I_0, \ldots, I_n, \ldots)$ be the sequences of polynomials in $\mathbb{Z}[x_0, \ldots, x_n, \ldots; y_0, \ldots, y_n, \ldots]$ from Theorem 1 corresponding to $f = X + Y$, $f = XY$, and $f = -X$ respectively.

Definition 1. *For a commutative ring A we define the Witt vectors with coefficients in A, denoted by $W(A)$, as the set $A^{\mathbb{N}}$ with compositions $+$ and $\cdot$ given by*

$$\underline{a} + \underline{b} := (S_0(\underline{a}, \underline{b}), \ldots, S_n(\underline{a}, \underline{b}), \ldots)$$

and

$$\underline{a} \cdot \underline{b} := (P_0(\underline{a}, \underline{b}), \ldots, P_n(\underline{a}, \underline{b}), \ldots) \ .$$

Exercise: $W(A)$ is a commutative ring with 1.

Consider the map $t \colon A \longrightarrow W(A)$ given by

$$t(a) := (a, 0, \ldots, 0, \ldots) \ ,$$

which is called the *Teichmüller lift.*

Exercise: The Teichmüller lift is multiplicative with $t(1) = 1$.

We now consider the following situation: A is a commutative ring of characteristic p which is perfect, i.e. $x \mapsto x^p$ is an automorphism of A, B is commutative ring which is separated and complete w.r.t. the p-adic topology, i.e. the topology generated by the sequence of ideals $p^n B$. Suppose that we are given a homomorphism

$\bar{\phi}\colon A \longrightarrow B/pB$. One may then show that there is a unique map $\phi\colon A \longrightarrow B$ such that

$$\bar{\phi} = (\phi \pmod{pB}) ,$$

and which satisfies $\phi(a^p) = \phi(a)^p$, $\forall a \in A$; further, such a ϕ is multiplicative with $\phi(1) = 1$. Here, we shall simply consider the map ϕ with the stated properties as having been given.

Let now $\underline{a} = (a_0, \ldots, a_n, \ldots) \in W(A)$. As A is perfect there is to each $a \in A$ and each $n \in \mathbb{N}_0$ a uniquely determined element $x \in A$ such that $x^{p^n} = a$; we denote this element by $a^{p^{-n}}$. As B is p-adically complete the series

$$\psi(\underline{a}) := \sum_{n=0}^{\infty} p^n \cdot \phi(a_n^{p^{-n}})$$

defines an element of B. Apparently, we have $\psi \circ t = \phi$ where t is the Teichüller lift. We claim that ψ defines a homomorphism $W(A) \longrightarrow B$. One may show that ψ is unique with these properties.

Proof of the claim: We show that ψ is additive. The proof of multiplicativity is similar. So, let $\underline{a} = (a_n),\ \underline{b} = (b_n) \in W(A)$. We shall show that

$$(*) \qquad \psi(\underline{a} + \underline{b}) \equiv \psi(\underline{a}) + \psi(\underline{b}) \pmod{p^{n+1}B}$$

for any $n \in \mathbb{N}_0$; this implies the additivity of ψ as B is separated w.r.t. p-adic topology. So, let $n \in \mathbb{N}_0$ be given. We have

$$\psi(\underline{a} + \underline{b}) = \psi(S_0(\underline{a}, \underline{b}), \ldots, S_n(\underline{a}, \underline{b}), \ldots) = \sum_{j=0}^{\infty} p^j \cdot \phi(S_j(\underline{a}, \underline{b})^{p^{-j}}) ,$$

so that $(*)$ is equivalent to

$$(**) \qquad \sum_{j=0}^{n} p^j \cdot \phi(S_j(\underline{a}, \underline{b})^{p^{-j}}) \equiv \sum_{j=0}^{n} p^j \cdot \left(\phi(a_j^{p^{-j}}) + \phi(b_j^{p^{-j}})\right) \pmod{p^{n+1}B} .$$

Since A is perfect we may utilize the change of variables $a_j \mapsto a_j^{p^n}$ and $b_j \mapsto b_j^{p^n}$, i.e. $(**)$ follows if we can show

$$\sum_{j=0}^{n} p^j \cdot \phi(S_j(\underline{a}^{p^n}, \underline{b}^{p^n})^{p^{-j}}) \equiv \sum_{j=0}^{n} p^j \cdot \left(\phi(a_j^{p^{n-j}}) + \phi(b_j^{p^{n-j}})\right) \pmod{p^{n+1}B}$$

which is equivalent to

$$\sum_{j=0}^{n} p^j \cdot \phi(S_j(\underline{a}^{p^n}, \underline{b}^{p^n}))^{p^{-n} \cdot p^{n-j}} \equiv \sum_{j=0}^{n} p^j \cdot \left(\phi(a_j)^{p^{n-j}} + \phi(b_j)^{p^{n-j}}\right) \pmod{p^{n+1}B}$$

because ϕ is multiplicative. By the definition of Φ_n, this is equivalent to:

$$\Phi_n(\phi(S_0(\underline{a}^{p^n}, \underline{b}^{p^n}))^{p^{-n}}, \ldots, \phi(S_n(\underline{a}^{p^n}, \underline{b}^{p^n}))^{p^{-n}}) \equiv$$
$$\Phi_n(\phi(a_0), \ldots, \phi(a_n)) + \Phi_n(\phi(b_0), \ldots, \phi(b_n)) \pmod{p^{n+1}B}$$

Now, $\bar{\phi}\colon A \longrightarrow B/pB$ is a ring homomorphism and S_j are polynomials so we have

$$\bar{\phi}(S_j(\underline{a}^{p^n}, \underline{b}^{p^n})) = S_j(\bar{\phi}(\underline{a}^{p^n}), \bar{\phi}(\underline{b}^{p^n})) = S_j(\bar{\phi}(\underline{a}), \bar{\phi}(\underline{b}))^{p^n}$$

whence

$$\phi(S_j(\underline{a}^{p^n}, \underline{b}^{p^n}))^{p^{-n}} \equiv \left(S_j(\phi(\underline{a}), \phi(\underline{a}))^{p^n}\right)^{p^{-n}} \equiv S_j(\phi(\underline{a}), \phi(\underline{a})) \pmod{pB} .$$

Then Proposition 1 shows that what we need is equivalent to

$$\Phi_n(S_0(\phi(\underline{a}), \phi(\underline{b})), \ldots, S_n(\phi(\underline{a}), \phi(\underline{b}))) \equiv$$
$$\Phi_n(\phi(a_0), \ldots, \phi(a_n)) + \Phi_n(\phi(b_0), \ldots, \phi(b_n)) \pmod{p^{n+1}B} ,$$

which is just the defining property of the S_j.