Lemma Let $\phi: A \to A$ an endomorphism of a ring; $\phi(a) \equiv a^p \pmod p$. Consider the ghost map

$$A^\infty \to A^\infty$$

$$(a_0, a_1, \dots) \mapsto (w_0(a_0), w_1(a_0, a_1), w_2(a_0, a_1, a_2), \dots)$$

The image of the ghost map consists of $(x_0, x_1, x_2, \dots)$:

$$\phi(x_n) \equiv x_{n+1} \pmod{p^{n+1}} \quad \forall n$$

Proof Lemma 1: if $a \equiv b \pmod p$ then $a^{p^n} \equiv b^{p^n} \pmod{p^{n+1}}$. **Proof**: $a \equiv b \pmod{p^n} \Rightarrow$

$\Rightarrow a^p \equiv b^p \pmod{p^{n+1}}$. Indeed:

$$(a + \varepsilon p^n)^p = a^p + p \cdot \varepsilon \cdot p^n \cdot a^{p-1} + \sum \binom{p}{k} p^{nk} \dots$$

$$\equiv a^p \pmod{p^{n+1}}.$$

Lemma 2: $a_0 \equiv b_0, \dots, a_n \equiv b_n \pmod p \Rightarrow$

$\Rightarrow w_n(a_0, \dots, a_n) \equiv w_n(b_0, \dots, b_n) \pmod{p^{n+1}}$.

Follows from Lemma 1 and from

$$w_n(a_0, \dots, a_n) = a_0^{p^n} + p a_1^{p^{n-1}} + \dots + p^n a_n$$

Now: $w_n(a_0,\dots,a_n) = w_{n-1}(a_0^p,\dots,a_{n-1}^p) + p^n a_n$

$\equiv w_{n-1}(\phi(a_0),\dots,\phi(a_{n-1})) + p^n a_n =$

$= \phi(w_{n-1}(a_0,\dots,a_{n-1})) + p^n a_n \pmod{p^n}$, so

$x_n \equiv \phi(x_{n-1}) \pmod{p^n}$; and, if we are solving $x_n = w_n(a_0,\dots,a_n)$ by induction, we recover a_n (uniquely if A has no p-torsion).

We apply this to $A = \mathbb{Z}[a_0,a_1,\dots;b_0,b_1,\dots]$ and $\phi: a_j \mapsto a_j^p$, $b_j \mapsto b_j^p$. Get solution, uniquely, to

$$w_n(a_0,\dots,a_n) + w_n(b_0,\dots,b_n) = w_n(c_0,\dots,c_n)$$

or $\times$

The image of the ghost map (or Witt map)

$$(a_0, a_1, a_2, \dots) \mapsto (w_0, w_1, w_2, \dots)$$

is closed under $+$ and $\cdot$.

Subring of $\mathbb{A}^\infty$

$$\{(x_0, x_1, \dots) : \phi(x_n) \equiv x_{n+1} \pmod{p^{n+1}}\}$$

Ex: $\forall$ comm. A:

$$W(A) = \{(a_0, a_1, \dots)\}_{a_i \in A}$$

is how a commutative ring.

Frobenius and Verschiebung

$\forall A$:

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

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

$V, F: W \circlearrowright$

add. str.

schemes

$V(a_0, a_1, a_2, a_3, \dots) \mapsto (0, a_0, a_1, a_2, \dots)$

at the ghost level:

$x_n = w_n(a_0, \dots, a_n)$

$(x_0, x_1, x_2, \dots) \mapsto (0, px_0, p^{x_1}, p^{x_2}, \dots)$

$A^\infty \longrightarrow A^\infty$

$(0, a_0, a_1, \dots) \longmapsto 0, \; 0^p + pa_0, \; 0^{p^2} + pw_1(a_0, a_1) + p^2 a_0 + p^2 a_1, \dots$

$F: (x_0, x_1, x_2, \ldots) \longmapsto (x_1, x_2, x_3, \ldots)$

on the ghost level.

Claim: yes, such a thing exists;

morphism of rings;

and $A/\mathbb{F}_p \Rightarrow (a_0^p, a_1^p, a_2^p, \ldots) = F$ on $W(A)$

$$(a_0, a_1, \_) \underset{\times}{+} (b_0, b_1, \_) = (\underbrace{c_0, c_1, c_2, \_}_{\text{universal polynomials as above.}})$$

e.g.

$$(a_0, \_) + (b_0, \_) = (a_0 + b_0,\ a_1 + b_1 + \frac{1}{p}\left[a_0^p + b_0^p - (a_0+b_0)^p\right])$$

$$(a_0, \_) \cdot (b_0, \_) = (a_0 b_0,\ a_0^p b_1 + a_1 b_0^p + p a_1 b_1, \_)$$

$$W(A) = \mathrm{Hom}_{\mathrm{Rgs}}(\mathbb{Z}[a_0, a_1, \_], A)$$

↑ ring scheme