Christopher Deninger - Witt vectors (elementary construction of)

An alternative to Witt vectors (joint w/ Joachim Cuntz)

ring in a perfect p-algebra

In the 1930's Witt, Teichmüller and Schmidt studied
p-adically complete discrete valuation rings $V$ (modern algebra.
exciting!). Problem. Given a perfect field $F$ of characteristic $p$,
find $V$ (as above) such that $V/pV = F$ and $\text{disc}(V)$ should have
deg. 0

Example $R = \mathbb{F}_p$, $V = \mathbb{Z}_p$ p-adic integers (pretty well understood).
Every $v \in \mathbb{Z}_p$ can be written uniquely $v = \sum_{n \geq 0} a_n p^n$, $a_n \in \mathbb{F}_p$.

Our way below $F = \mathbb{Z}/p\mathbb{Z}$ an more system [how to generalize to $R$?]

Here $\mathbb{Z}_p$ contains $\mathbb{F}_p$ contains $\mathbb{F}^\times = \mathbb{Q}^\times / \mathbb{Z}^\times$.

and reduce: $a_n \in \mathbb{Z}_p$ multiplication from $\mathbb{F}_p$ into $\mathbb{Z}_p$ and $\mathbb{F}_p$ gets a map $\phi: \mathbb{F}_p \rightarrow \mathbb{F}_p$ by taking the inverse and adding $\phi = 0$; still multiplicative map.

By construction $\psi$ is a multiplicative splitting of the projection.

Thus every $v \in \mathbb{Z}_p$ has a unique representation

$$v = \sum_{n \geq 0} a_n \mathbb{F}_p$$
If \( w = \sum_{i} w_i p_i \) and \( w' = \sum_{j} w'_j p_j \), then to obtain the \( w + w' \) in

\[ w + w' = \sum_{i} (w_i + w'_i) p_i \]

from \( x \) and \( y \), same for \( x \) and \( y' \).

Will found the solution: Introduce the following polynomials:

\[ w_i(x_i - x) = x_i^n + p x_i^{n-1} + \ldots + p^n x_i \]

Then there are unique polynomials \( s_i(x_i - x_i, y_i - y_i) \) over \( G \):

\[ w_i(s_i - s_i) = w_i(x_i - x) + w_i(y_i - y) \]

Will proved: Then \( S_i \) has well in \( Z \) and \( s_i = S_i(x_i - x_i, y_i - y_i) \)

Similar for multiplication.

Example: \( S_0 = x_0 + y_0 \)

Will ring: Let \( R \) be a common ring. \( WR = R^N \) with

\[ (x_0, x_1, \ldots) + (y_0, y_1, \ldots) = (s_0, s_1, \ldots), \]

similar for multiplication.
This is a comm. unital ring.

Same for \( W(R) = \mathbb{R}^{2n} \), \( W(R) : = \mathbb{R}^{2n} \).

and we have \( W(R) \rightarrow W(R) \), projection homomorphism.

\[ \begin{align*}
\phi : & \mathbb{R} \rightarrow W(R), \quad x \rightarrow (x, 0, \ldots) \text{ multiplication} \\
\psi : & W(R) \rightarrow \mathbb{R}, \quad 
\end{align*} \]

\[ \begin{align*}
W(R) & \rightarrow W(R), \quad (x_0, x_1, \ldots) \rightarrow (0, x_0, x_1, \ldots) \text{ addition} \\
F : & W(R) \rightarrow W(R), \quad (x_0, x_1, \ldots) \rightarrow (x_0^2, x_1^2, \ldots) \text{ if \( F_{p,q} \)-alg}
\end{align*} \]

Universal property of \( W(R) \) for perfect \( F_{p,q} \)-algebra \( R \) (see \( x \rightarrow x^2 \) above)

need definitions: (Serre, Correspondence, loc.cit.)

Def: A comm. ring \( A \) is a \( p \)-ring if it is Noetherian and complete with a topology defined by a sequence of ideals \( (0) \subseteq \mathfrak{P} \subseteq \mathfrak{P}_1 \subseteq \mathfrak{P}_2 \subseteq \ldots \) such that:

1. \( \mathfrak{P}_n / \mathfrak{P}_{n-1} = \mathfrak{P} \)
2. \( A/\mathfrak{P}_n = \mathbb{R} \) is a perfect \( F_{p,q} \)-alg.

A strict \( p \)-ring if \( p \) is an odd prime.

Theorem (Teichmüller, Lazard). For a \( p \)-ring \( A \) there is a unique multiplicative splitting \( A \rightarrow R \).

Then (Lazard) let \( R \) be a \( p \)-ring or perfect \( F_{p,q} \)-algebra \( R \).

Then there exists a unique homomorphism of rings \( \phi : W(R) \rightarrow A \) such that \( W(R) \rightarrow A \cong R \) commutes.
Explicitly, \[ \mathcal{A}(x, y, \ldots) = \sum_{i=0}^{\infty} a_i(x^{p^i})y^i. \]

If \( A \) is a strict \( p \)-ring, then \( \mathcal{A} \) is a homomorphism.

\( W(R) \) is a strict \( p \)-ring at residue algebra \( \mathfrak{A} \).

77 years: For a perfect \( F_p \)-algebra \( A \), there is an alternative candidate for \( W(R) \) which has the universal property in the theorem!

Consider \( R \) as a multiplicative monoid, take the monoid algebra
\[ 2R \overset{\pi}{\rightarrow} \mathbb{E}_{2R} \] is a ring homomorphism.

\[ 0 \rightarrow I \rightarrow 2R \rightarrow R 
\]

\[ \mathbb{E}_{2R} \overset{\text{coproduct}}{\rightarrow} \mathbb{E}_R \]

\[ \mathbb{E}_R \overset{\mathbb{E}_{\pi}}{\rightarrow} A \]

\[ 2R \overset{\pi}{\rightarrow} A \]

\[ H(1) \in A_m = \ker (A \rightarrow \mathbb{F}_p) \]

\[ x(1^m) \in A^m = A_m \rightarrow x(a) \rightarrow \mathbb{Z}/2m \rightarrow A/\ker(x) \]

\[ 2 : C(R) \rightarrow A = \ker A/\ker(x) \]

Hence \( W(R) = C(R) \), \( W_n(R) = \mathbb{Z}/2^m \).

Direct proof that \( C(R) \) is a strict \( p \)-ring:

\[ \text{Ex} \ R = \mathbb{F}_p(\mathbb{Z}/2^m) \]

\[ C(R) = 2R = \lim_{\longrightarrow} \frac{2R}{I^m} \text{ is a } p \text{-ring with } 2R \text{ polynomials in } I^m \text{ variables.} \]

\[ M_n = \mathbb{F}_p(\mathbb{Z}/2^m) \rightarrow \mathbb{F}_p(\mathbb{Z}/2^m) = \mathbb{F}_p(\mathbb{Z}/2^m) \]

For strict we need:

\[ 2R \rightarrow 2R \rightarrow (\mathbb{E}_{2R}(I)) = \mathbb{E}_R(I) \]
Consider $S: \mathbb{Z} R \to \mathbb{Z} R, \; S(a) = \frac{1}{p}(xa - x1)$. Then

(i) $S(x+y) = S(x) + S(y) = S(x) + S(y)$

(ii) $S(xy) = S(x)S(y) + S(x)S(y)$

Eq. (ii) $S(x+y) = S(x) + S(y) \mod I^n$ if $x, y \in I^n$

(iii) $S(I^n) = I^{n-1}$ for $n \geq 1$

Lemma 2 a perfect $F_p$-algebra, $n > 1$

(i) $pa \in I^n \forall a \in \mathbb{Z} R$ for $a \in I^n$

(ii) $I^n = I + p^2 R$ for any $a \in \mathbb{Z} R$

Proof: (i) $S(I^n) = I^{n-1}$

$\Rightarrow S(pa) \in I^{n-1}$ by def.

$S(pa) = \frac{1}{p}(p(a) - p(a)) = p(a) - p^{-1}a = S(a) \mod I^n$

$\Rightarrow S(a) \in I^{n-1} \forall a \in I^n$

2. For $x \in \mathbb{Z} R$, $x = (x - k) \mod I^n p^2 R$

For $x \in I^n$ we get $x \in I + p^2 R$ then $I^n = I + p^2 R$

Case $n = 1$:

Proof: $p$ $(\mathbb{Z} R)$ is a direct sum $\mathbb{Z} p \oplus \mathbb{Z} p$.

For $j \geq n \geq 1$ we have an exact sequence

$$0 \to \mathbb{Z} / \mathbb{Z} \to \mathbb{Z} / \mathbb{Z} J \to \mathbb{Z} / \mathbb{Z} J / I^n \to 0$$

$$0 \to \mathbb{Z} / \mathbb{Z} I^n \to \mathbb{Z} / \mathbb{Z} J \to \mathbb{Z} / \mathbb{Z} J / I^n \to 0$$
\( N_{ij} \rightarrow N_j \) zero map \( \alpha \in \mathbb{R} \in (I^n) \) \( \Rightarrow \alpha \in I^n \)

Lemma 11
\( \alpha \in I^n \) Hence \( (N_j) \) is Hilbert (affine) and \( \lim N_j = 0 \)

Question: 3.ings wll vector? 
\( F - s \in \mathbb{R} \quad 2^\mathbb{R} \rightarrow U, (I^n) \times 2^\mathbb{R} / \mathbb{I} \)

Then (\text{injective even}) \( \text{If } R \) is an \( F - s \in \mathbb{R} \), then 
\( \alpha : 2^\mathbb{R} \rightarrow U, R \) is surjective

If \( \alpha \in \mathbb{R} \) \( \beta \), then ker \( \alpha = I^n = \mathbb{I}^{(I^n)} = 0 \mathbb{I}^{(I^n)} \)

\( U(R) = \mathbb{R} \times 2^\mathbb{R} / \mathbb{I} \) \( \text{(*)} \)

W.H. complex?

Start \( w / \mathbb{Z} 2^\mathbb{R} \) relations on differentials

Consider \( 2^\mathbb{R} \) instead (work in progress)

Pirziller injective?

\( N \) in ? but not zero e.g. for \( \alpha \)

Verschlebung?
\( 2^\mathbb{R} \rightarrow 2^\mathbb{R} = F \quad V = pH \) in perfect core, don't need to see Verschlebung in \( \text{(c)} \)