WITT VECTORS FROM DEFORMATION THEORY

LÉO NAVARRO CHAFLOQUE

Abstract. We give an deformation theoretic perspective on Witt vectors. More precisely, we find by deformation theory a canonical deformation of a perfect ring in characteristic p to a $\mathbb{Z}/p^2\mathbb{Z}$-algebra and then write down the addition and multiplication law on this algebra using the deformation theory perspective. We find that these laws are the usual laws of the Witt vectors. Also, in the first section, we outline the fundamental lemma of deformation theory to use it for our purposes, and to serve as a quick reference for other occasions.

Contents

1. Recollection on deformation theory

In order to get a quick and correct definition of the *cotangent complex*, we use animated categories although we will not use this theory in this note. See [CS23, Section 5.1] for an account.

Definition 1.1 (Cotangent complex)**.** Consider the functor $A \mapsto \Omega^1_{A|R}$ from CAlg_R to $\mathrm{CAlgMod}_R$ the category of pairs (A, N) where A is R-algebra and N is an A-module. We denote by $A \mapsto (A, L_{A|R})$ the natural extension to $\mathrm{Ani}(\mathrm{CAlg}_R) \to \mathrm{Ani}(\mathrm{CAlgMod}_R)$[1]. We say that $L_{A|R}$ is the *cotangent complex* of A over R.

Remark. The "natural extension" preserves geometric realizations *aka* colimts on Δ^{op} and has the same value has $\Omega^1_{\bullet|R}$ on polynomial algebras. Therefore to compute the cotangent complex $L_{A|R}$, we may take a simplicial object $S_\bullet$ in CAlg_R which consists of polynomial algebras with an homotopy equivalence $S_\bullet \to A$. A typical choice is the bar resolution from the free-forgetful adjunction, see [Sta, Section 08PL]. Then because the value of the cotangent complex is the same as $\Omega^1_{\bullet|R}$ on polynomial algebras, we get a simplicial module which we may realize as a complex by the Dold-Kan equivalence, namely by taking the homology of the associated simplicial module. For our sake we will actually only care about $\tau_{\leq 1} L_{A|R}$ which may be realized for any presentation $R[S] \to A$ of R-algebras with kernel I as the complex with target in degree zero

$$\tau_{\leq 1} L_{A|R} = \left(I/I^2 \to \bigoplus_{s \in S} A ds \right)$$

[1]Objects of $\mathrm{Ani}(\mathrm{CAlgMod}_R)$ may be regarded as pairs of an object in $A \in \mathrm{Ani}(\mathrm{CAlg}_R)$ and $N \in \mathrm{Ani}(\mathrm{Mod}_A)$.

where the map is given by sending a polynomial f to the image of $d(f)$ by $R[S] \to A$. Using the following truncation $I \to R[S]$ of a resolution of A by polynomial algebras we can express the truncation of the universal derivation $A \to L_{A|R}$ as the below map of complexes.

$$\begin{array}{ccc} I & \longrightarrow & R[S] \\ \downarrow & & \downarrow{\scriptstyle d} \\ I/I^2 & \xrightarrow{d} & \bigoplus_{s \in S} Ads \end{array}$$

Definition 1.2 (Square zero extensions)**.** Let R be a ring, $R \to A$ an A-algebra and N an A-module. We say that A' is an *an R-algebra square zero extension of A by N* if we have an exact sequence

$$0 \to N \to A' \to A \to 0$$

where the map $A' \to A$ is a surjective ring map with square zero kernel and $N \to A'$ is onto this kernel and this map is an A'-module morphism. A morphism of R-algebras square zero extensions of A by N is a map

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \longrightarrow & A' & \longrightarrow & A & \longrightarrow & 0 \\ & & & \searrow & \downarrow & \nearrow & & & \\ & & & & A'' & & & & \end{array}$$

and therefore automatically an isomorphism by the five lemma.

We write down the following so that it can be an handy reference, and sketch a proof which should clarify most of common claims.

Lemma 1.3 (Fundamental lemma of deformation theory)**.** *Let R be a ring, $R \to A$ an A-algebra and N an A-module.*

(1) The map

$$\pi_0(\mathrm{Map}_A(L_{A|R}, N[1])) \to \{\text{Equ. classes of } R\text{-algebras square zero extensions of } A \text{ by } N\}$$

sending a derivation $d\colon A \to L_{A|R} \to N[1]$ to the homotopy fiber

$$\begin{array}{ccc} A' & \longrightarrow & A \\ \downarrow & & \downarrow{\scriptstyle (\mathrm{id},0)} \\ A & \xrightarrow{(\mathrm{id},d)} & A \oplus_0 N[1] \end{array}$$

is a bijection.

(2) Under the identification of 1-truncated connective objects of $\mathcal{D}(A)$ with A-module groupoids, the object

$$\mathrm{Map}_A(L_{A|R}, N[1])$$

of $\mathcal{D}(A)$ is identified with the A-module groupoid of R-algebras square zero extensions of A by N.

(3) Let $R[S] \to A$ be a presentation with kernel I. Then we have an identification of $\pi_0(\mathrm{Map}_A(L_{A|R}, N[1])) = \mathrm{Ext}^1(L_{A|R}, N)$ as

$$\frac{\mathrm{Hom}_A(I/I^2, N)}{\prod_S N}$$

where by the last quotient we mean maps which comes from the composition $I/I^2 \to \bigoplus_{s\in S} Ads \to N$, where the first map is given by taking a polynomial $f \in I$ to the evaluation of df.

(4) *Keeping the setup of the previous statement, given $d\colon I \to N$ representing an element in $\mathrm{Ext}^1(L_{A|R}, N)$, the homotopy fiber square above is realized has*
$$\frac{R[S]/I^2 \oplus_0 N}{(-i, d(i))_{i\in I}}.$$

Proof. Because $\mathrm{Map}_A(L_{A|R}, N[1]) = \mathrm{Map}_A(\tau_{\leq 1}L_{A|R}, N[1])$, note that it is direct from the above description of $\tau_{\leq 1}L_{A|R}$ that
$$\pi_0(\mathrm{Map}_A(L_{A|R}, N[1]) = \frac{\mathrm{Hom}_A(I/I^2, N)}{\prod_S N}$$
where by the last quotient we mean maps which comes from the composition $I/I^2 \to \bigoplus_{s\in S} Ads \to N$.

We now sketch the two directions of the equivalence.

First, consider
$$0 \to N \to A' \to A \to 0$$
an R-algebra square zero extension of A by N. We get from this short exact sequence a map in $\mathcal{D}(R)$
$$A \to N[1].$$
By usual homological algebra we can represent this map using any lift $R[S] \to A'$ of the surjection $R[S] \to A$ which restriction to I will corestrict to N, describing the map $A \to N[1]$ as depicted below.
$$\begin{array}{ccc} I & \longrightarrow & R[S] \\ \downarrow & & \downarrow \\ N & \longrightarrow & 0 \end{array}$$
Because N is square zero, this map factors through $\tau_{\leq 1}L_{R|A}$
$$\begin{array}{ccc} I & \longrightarrow & R[S] \\ \downarrow & & \downarrow \\ I/I^2 & \longrightarrow & \bigoplus_{s\in S} Ads \\ \downarrow & & \downarrow \\ N & \longrightarrow & 0 \end{array}$$
giving the desired map $L_{R|A} \to N[1]$.

As for the other direction, given a map $L_{A|R} \to N[1]$ in $\mathcal{D}(A)$, one can consider the composition $d\colon A \to L_{A|R} \to N[1]$. If we look at the above, then we should define $A' = \mathrm{fib}(A \to N[1])$, but this is has no ring structure a priori. To do this, we realize this fiber has the fiber square of (1-truncated) animated rings

$$\begin{array}{ccc} A' & \longrightarrow & A \\ \downarrow & & \downarrow {\scriptstyle (\mathrm{id},0)} \\ A & \xrightarrow{(\mathrm{id},d)} & A \oplus_0 N[1] \end{array}$$

where $A \oplus_0 N[1]$ denotes the quasi-ideal $(N \xrightarrow{0} A)$.[2] Let us realize concretely this fiber. Using the quasi-ideal resolution of $A = (I \to R[S])$ where the target is in degree zero we get using the description of the cocone in homological algebra that A' is represented by the quasi-ideal

$$I \to R[S] \oplus_0 N$$

with target in degree zero and where the map is given by $i \mapsto (-i, d(i))$. Because this map is injective, we get that this fiber square (now described as the coker of the above map) is discrete. Moreover, as $d(I^2) = 0$, we see that we can write A' has the quotient

$$A' = \frac{R[S]/I^2 \oplus_0 N}{(-i, d(i))_{i \in I}},$$

as claimed in the statement. The proof found in [Sta, Section 08S3] fills the details to show that both ways are actually inverses to each other.

As for statement (2), the statement on the objects of the groupoid is the above, and as for the arrows, this follows from the identification of isomorphisms of square zero extensions with $\mathrm{Hom}_A(\Omega^1_{A|R}, N) = \pi_1(\mathrm{Map}_A(L_{A|R}, N[1]))$. One sees this using that the difference of two isomorphisms will always define a derivation $A \to N$. □

Example 1.4. We classify all square zero extensions of $\mathbb{F}_p$ by $N = \mathbb{F}_p$. We have in this case the presentation

$$\mathbb{Z} \to \mathbb{F}_p$$

Therefore (but even without the truncation)

$$\tau_{\leq 1} L_{\mathbb{F}_p|\mathbb{Z}} = (p)/(p^2)[1]$$

It follows that

$$\pi_0(\mathrm{Map}((p)/(p^2)[1], \mathbb{F}_p[1])) = \mathrm{Hom}((p)/(p^2), \mathbb{F}_p)$$

Under the identification $\mathbb{F}_p \to (p)/(p^2)$ sending 1 to p, we get

$$\mathrm{Ext}^1(L_{\mathbb{F}_p|\mathbb{Z}}, \mathbb{F}_p) = \mathbb{F}_p.$$

If we take the derivation corresponding to 0 we get

$$\frac{\mathbb{Z}/p^2\mathbb{Z} \oplus_0 \mathbb{F}_p}{(p, 0)} \cong \mathbb{F}_p[\epsilon].$$

For the derivation corresponding to 1 (or any non-zero $\lambda \in \mathbb{F}_p$) we get, because the abelian group map $\mathbb{F}_p \to \mathbb{Z}/p^2\mathbb{Z}$ sending 1 to p is injective, that the corresponding square zero extension is

$$\mathbb{Z}/p^2\mathbb{Z}.$$

[2]See for example ([Dri21, Section 3.3]) for the notion of quasi-ideal.

Note that the "derived derivation" associated to $\lambda \in \mathbb{F}_p$ can be described at the level of chain complexes (resolving $\mathbb{F}_p$ by free modules)

$$\begin{array}{ccccc} 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{p} & \mathbb{Z} \\ \downarrow & & \lambda\downarrow & & \downarrow \\ 0 & \longrightarrow & \mathbb{F}_p & \longrightarrow & 0 \end{array}$$

Note that there are $p-1$ isomorphism classes of *square zero extensions* with ring isomorphism class being $\mathbb{Z}/p^2\mathbb{Z}$. Note the following phenomenon.

Lemma 1.5. *Let $R \to A$ be a map of rings and N be an A-module. Then isomorphism classes as "A-extensions" of square zero extensions of A-algebras with kernel N is isomorphic to the pointed quotient*

$$\mathrm{Ext}^1(L_{A|R}, N)/\operatorname{Aut}_A(N).$$

Proof. We need to precise what we mean by isomorphisms of "A-extensions". We mean that if $A' \to A$ and $A'' \to A$ are square extensions with kernel identified with N then we are looking at isomorphism classes given by diagrams as described below.

$$\begin{array}{ccc} A' & & \\ \downarrow\varphi & \searrow & \\ A'' & \longrightarrow & A \end{array}$$

Note that this induces by restricting to N an A-automorphism of N. Giving an A-automorphism of N also provides such an isomorphism, one case use for example the explicit form of a square extension given above.

□

2. Witt vectors from deformation theory

After this quick recollection, we have the tools to construct the Witt vectors $W_2(R)$ for a perfect algebra R using purely deformation theory.

Example 2.1. Let R be perfect in characteristic p. We have

$$L_{\mathbb{F}_p|\mathbb{Z}} \otimes R \to L_{R|\mathbb{F}_p} \to L_{R|\mathbb{Z}}$$

Because R is perfect, the Frobenius pullback is both zero and an isomorphism implying $L_{R|\mathbb{F}_p} = 0$. In consequence

$$L_{R|\mathbb{Z}} \cong ((p)/(p^2) \otimes^L R)[1] \cong R[1]$$

because $\mathbb{F}_p$ is flat over $\mathbb{F}_p$. In consequence isomorphism classes of square zero extensions with kernel $N = R$, in the sense of Lemma 1.5, are canonically in correspondence with,

$$R/R^{\times}.$$

Note also that the canonical class of zero is the only one in characteristic p because $L_{R|\mathbb{F}_p} = 0$. All the others are over $\mathbb{Z}/p^2\mathbb{Z}$: indeed, note that p is necessarily in the kernel, from which the assertion follows. This last remark also shows that we could have replace $\mathbb{Z}$ with $\mathbb{Z}/p^2\mathbb{Z}$ in the above considerations. Note also that the class of 1 is canonical.

Lemma 2.2. *Let R be a perfect $\mathbb{F}_p$-algebra. Let $\mathbb{F}_p[S] \to R$ be any presentation with $S \subset R$ a subset of generators stable under the Frobenius. Let J be the kernel. Then J/J^2 is a free R-module on S elements, these elements being*

$$(x_s - x^p_{s^{1/p}})_{s \in S}$$

Proof. Because $L_{R|\mathbb{F}_p} = 0$, it implies that

$$J/J^2 \to \bigoplus_{s \in S} Rds$$

is an isomorphism. As the elements in the statement of the lemma are in J and their derivative *i.e.* the image *via* the map is ds, we are done.

□

Remark. The "stable under the Frobenius" hypothesis is not necessary. We can take $f_{s^{1/p}}$ to be any lift of $s^{1/p}$, and look at the image of this polynomial along $x_s \mapsto x_s^p$. Denote this suggestively as $x^p_{s^{1/p}}$, then the lemma also holds with this notation.

The next lemma is pretty soothing. In the proof, we really see that we formally "multiply by p the elements of R, inside $\mathbb{Z}/p^2\mathbb{Z}[R]$, which appeals to some "lifting in mixed characteristic".

Lemma 2.3. *Let R be a perfect $\mathbb{F}_p$-algebra. Let $\mathbb{Z}/p^2\mathbb{Z}[S] \to R$ be any presentation with $S \subset R$ a subset of generators closed by the action of the Frobenius. For $r \in R$ denote by $f_r \in \mathbb{Z}[S]$ any lift. Let I be the kernel. Then*

$$R \xrightarrow{\cdot p} I/I^2$$

sending $r \to pf_r$ is an isomorphism of R-modules onto the kernel of

$$I/I^2 \to \bigoplus_{s \in S} Rds.$$

In consequence I/I^2 is the following free R-module (the second term may be further identified with $\bigoplus_{s \in S} Rds$)

$$(p \cdot R) \oplus \bigoplus_{s \in S} R(x_s - x^p_{s^{1/p}}).$$

Proof. First, note that this well defined. Indeed if f_r and f'_r are two lifts of r, then

$$p(f_r - f'_r) \in I^2.$$

The R-module map aspect becomes obvious. Using the last Lemma 2.2, we get that the kernel mentioned in the statement is the kernel of the surjection

$$I/I^2 \to J/J^2.$$

This is the image of $I \cap p\mathbb{Z}/p^2\mathbb{Z}[S] = p\mathbb{Z}/p^2\mathbb{Z}[S]$ in the quotient. We show that the $R \xrightarrow{\cdot p} I/I^2$ is onto the latter image. Because any polynomial is a lift of some elements of R, the claim follows. To show the injectivity, it suffices to produce a set theoretic inverse. To a polynomial $pg(x_{s_1}, \dots, x_{s_n}) \in p\mathbb{Z}/p^2\mathbb{Z}[S]$, associate $g(s_1, \dots, s_n) \in R$. We need to show that this well defined. Take $pg(x_{s_1}, \dots, x_{s_n})$ and $pg'(x_{s'_1}, \dots, x_{s'_n})$ such that

$$g(s_1, \dots, s_n) = g'(s'_1, \dots, s'_n).$$

But then the difference

$$g(x_{s_1}, \dots, x_{s_n}) - g'(x_{s'_1}, \dots, x_{s'_n})$$

is in the kernel. When multiplying by p, it is in I^2, showing that the inverse is well defined. We should explain the last line of the lemma. This follows from the below exact sequence, using that the right term is a free R-module by Lemma 1.5

$$0 \to R \xrightarrow{\cdot p} I/I^2 \to J/J^2 \to 0.$$

Note that $(p \cdot R)$ denotes the R-module inside I/I^2 which is generated by $p \in I$. We may write it as $R \cdot (p)/(p^2)$ to be more precise to be closer to our notation in the base $\mathbb{F}_p$-case. □

Example 2.4. We are now ready to treat more generally deformations of perfect rings in characteristic p. Let R be a perfect ring in characteristic p. Let N be a R-module. Let $S \subset R$ be a subset of generators. Let I be the kernel of $\mathbb{Z}/p^2\mathbb{Z}[S] \to R$. Because $L_{R|\mathbb{Z}} = R[1]$ isomorphism classes of square zero extensions

$$0 \to N \to R' \to R \to 0$$

are classified by elements $n \in N$. With the previous Lemma 2.3 and Lemma 1.3 we see that the derivations may be entirely described by sending $p \in J/J^2$ to $n \in N$. Therefore we can describe the associated square zero extension as the quotient

$$\frac{\mathbb{Z}/p^2\mathbb{Z}[S]/I^2 \oplus_0 N}{((-p, n), (x^p_{s^{1/p}} - x_s, 0))}$$

In particular take $R = N$ and $n = 1 \in R$. Then using the injection of Lemma 2.3, we can describe the above as

$$W' = \frac{\mathbb{Z}/p^2\mathbb{Z}[S]}{(I^2, x_s - x^p_{s^{1/p}})}.$$

Note that the image of I/I^2 in this quotient is just isomorphic to R and is spanned by p as an R-module because we precisely quotiented out by the direct summand of $p \cdot R$ in I/I^2, see Lemma 2.3. This says that

$$1 \to \underbrace{pW'}_{\cong R} \to W' \to R \to 0$$

where the second map is the evaluation: the kernel is the image of I which we just argued that is the ideal generated by p.

Our goal is now to show that $W_2(R)$ is isomorphic to the above W'. Note that for the proof we take $S = R$ in order to carry canonical construction, but all set of generators will give an isomorphic ring by deformation theory. We would like to locate naturally the Teichmüller lifts, which should define a multiplicative section of $W' \to R$.

Lemma 2.5. *The ring W' admits a canonical Frobenius lift ϕ, which comes from the map $\mathbb{Z}[R] \to \mathbb{Z}[R]$ sending $x_r \mapsto x_r^p$ which passes to the quotient. Furthermore, ϕ is bijective.*

Proof. Note that this map preserves I, because R is supposed perfect. Therefore the map preserves I^2. We now study for any $r \in R$ the image of $x_r - x^p_{r^{1/p}}$ along the map. But using the relation $x_r = x^p_{r^{1/p}}$ for any $r \in R$ valid in W' we get in particular that

$$x_r^p - x^{p^2}_{r^{1/p}} = x_{r^p} - x_r^p$$

in W' showing indeed that the ideal $(I^2, x_r - x^p_{r^{1/p}})_{r\in R}$ is preserved.

To show that ϕ is bijective, we construct an inverse map. We send $x_r \mapsto x_{r^{1/p}}$. This is even more straightforward that the previous calculation to show that it is well defined. □

Lemma 2.6 (Teichmüller lifts)**.** *There is a multiplicative section $R \to W'$, with image determined by elements satisfying $f^p = \phi(f)$.*

Proof. We say that $f \in W'$ is a *Teichmüller lift* of $\mathrm{ev}(f)$ if $f^p = \phi(f)$. For example $x_r \in W'$ is a Teichmüler lift of $r \in R$. It is clear that Tecihmüller lifts are closed under multiplication. We now argue that Teichmüller lifts are unique in W', in the sense that if f and g are Teichmüller lifts with the same image by ev, then they are actually equal in W'. It suffices to show that if for any $f, g \in W'$ we have $\mathrm{ev}(f^p) = \mathrm{ev}(g^p)$, then in fact, $f^p = g^p$, so $\phi(f) = \phi(g)$ if they are both Teichmüller lifts of $\mathrm{ev}(f) = \mathrm{ev}(g)$. We can then conclude by the bijetivity of ϕ. We can write by the above

$$f = x_{\mathrm{ev}(f)} + pf_1 \quad g = x_{\mathrm{ev}(g)} + pg_1$$

where f_1, g_1 are some elements. Because $p^2 = 0$, we see that

$$f^p = x^p_{\mathrm{ev}(f)} \quad g^p = x^p_{\mathrm{ev}(g)}$$

showing the claim. □

Note also that because $pf = px_{\mathrm{ev}(f)}$ (because their difference is in I^2) we can write any element as

$$f = x_{\mathrm{ev}(f)} + px_{r_f}$$

for some unique $r_f \in R$. In other words we can write any element as a Teichmüller lift plus p time a Tecihmüller lift, in an unique way.

Corollary 2.7. *There is a set theoretic bijection given by sending $f = x_{\mathrm{ev}(f)} + px_{r_f} \in W'$ to $(\mathrm{ev}(f), r_f^p) \in R \times R$.*

In this notation we have

$$\phi(f) = x_{\mathrm{ev}(f)^p} + px_{r_f^p}.$$

Therefore $\phi(f) - f^p = px_{r_f^p}$. Note that for any $r, s \in R$

$$(x_r + x_s)^p - \phi(x_r + x_s) = (x_r + x_s)^p - x_s^p - x_s^p = p\left(\sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} x_r^i x_s^{p-i}\right) = px_{\left(\sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} r^i s^{p-i}\right)}$$

This implies the following rule for sum of Teichmüller lifts.

$$x_r + x_s = x_{r+s} + px_{\left(-\sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} r^i s^{p-i}\right)^{1/p}}$$

We now inspect the multiplication of two elements. Say take two elements $f = x_{r_1} + px_{s_1^{1/p}}$ and $g = x_{r_2} + px_{s_2^{1/p}}$. As $p^2 = 0$, we get using multiplicativity of Teichmüller lifts that,

$$fg = x_{r_1 r_2} + p(x_{r_1} x_{s_2^{1/p}} + x_{r_2} x_{s_1^{1/p}}).$$

So by Corollary 2.7, we can express the multplication as

$$(r_1, s_1)(r_2, s_2) = (r_1 r_2, r_1^p s_2 + r_2^p s_1).$$

The formula of the sum of Teichmüller lifts and this observation leads to see that W' is indeed isomorphic as $W_2(R)$.

We gather the information in the following corollary.

Corollary 2.8. *Let R be a perfect ring of characteristic p, and I the kernel of $\mathbb{Z}/p^2\mathbb{Z}[R] \to R$. The set of isomorphism classes of square zero extensions with kernel isomorphic to R canonically identifies to*

$$R/R^\times.$$

Therefore, there is a canonical deformation corresponding to the class of 1. This can be expressed as the quotient

$$\frac{\mathbb{Z}/p^2\mathbb{Z}[R]}{(I^2, (x_r - x^p_{r^{1/p}})_{r\in R})}.$$

This ring is $W_2(R)$. The square zero extension corresponding is

$$0 \longrightarrow R \xrightarrow{r \mapsto p x_r} \frac{\mathbb{Z}/p^2\mathbb{Z}[R]}{(I^2, x_r - x^p_{r^{1/p}})} \xrightarrow{\text{ev}} R \longrightarrow 0$$

We note that we rediscovered the Witt addition and multiplication by purely deformation theoretic arguments.

Corollary 2.9. *Let k be a perfect field in characteristic p. Then there is a unique square zero extension not in characteristic p with kernel k, namely $W_2(k)$.*

Proof. By the previous example, we learned that there is only two square extensions with kernel k, and $W_2(k)$ is one which is not isomorphic to $k[\epsilon]$. □