Lecture 8

December 9, 2004
Notes by Egon Rütsche

§20 The ring of Witt vectors over $\mathbb{Z}$

In this section we show that the group scheme structure on $\mathrm{W}_{\mathbb{Z}}$ from Proposition 19.4 is the addition for a certain ring scheme structure on $\mathrm{W}_{\mathbb{Z}}$. Set

$$\Phi_\ell(\underline{x}) \;:=\; \sum_{n=0}^{\ell} p^n x_n^{p^{\ell-n}} \;=\; x_0^{p^\ell} + p x_1^{p^{\ell-1}} + \ldots + p^\ell x_\ell. \tag{20.1}$$

Then using Lemma 19.1 we can rewrite

$$\begin{aligned} E(\underline{x}, t) &= \prod_{n \geq 0} \exp\Big(-\sum_{m \geq 0} \frac{(x_n t^{p^n})^{p^m}}{p^m}\Big) \\ &= \exp\Big(-\sum_{n,m \geq 0} p^n x_n^{p^m} \cdot \frac{t^{p^{n+m}}}{p^{n+m}}\Big) \;=\; \exp\Big(-\sum_{\ell \geq 0} \Phi_\ell(\underline{x}) \cdot \frac{t^{p^\ell}}{p^\ell}\Big). \end{aligned}$$

The relation in Proposition 19.4 becomes

$$\log E(\underline{x}, t) + \log E(\underline{y}, t) = \log E(\underline{s}(\underline{x}, \underline{y}), t),$$

which is equivalent to

$$-\sum_{\ell \geq 0} \Phi_\ell(\underline{x}) \frac{t^{p^\ell}}{p^\ell} - \sum_{\ell \geq 0} \Phi_\ell(\underline{y}) \frac{t^{p^\ell}}{p^\ell} = -\sum_{\ell \geq 0} \Phi_\ell\big(\underline{s}(\underline{x}, \underline{y})\big) \frac{t^{p^\ell}}{p^\ell}.$$

By equating coefficients, we deduce that Proposition 19.4 is equivalent to

Proposition 20.2. The above group law on $\mathrm{W}_{\mathbb{Z}}$ is the unique one for which each $\Phi_\ell : \mathrm{W}_{\mathbb{Z}} \longrightarrow \big(\mathbb{A}^1_{\mathbb{Z}}, +\big)$ is a homomorphism.

Remark. We write this group law additively, i.e. $\underline{s}(\underline{x}, \underline{y}) =: \underline{x} + \underline{y}$.

Terminology. An element $\underline{x} = (x_0, x_1, \ldots) \in \mathrm{W}(R)$ is called a *Witt vector*, and the $x_0, x_1, \ldots$ its *components*. The expressions $\Phi_\ell(\underline{x})$ are called *phantom components*. The reason for this is that over $\mathbb{Z}[\frac{1}{p}]$, giving the x_ℓ is equivalent to giving the $\Phi_\ell(\underline{x})$, because we have an isomorphism

$$\mathrm{W}_{\mathbb{Z}[\frac{1}{p}]} \longrightarrow \prod_{\ell=0}^{\infty} \mathbb{A}^1_{\mathbb{Z}[\frac{1}{p}]}, \; \underline{x} \mapsto \big(\Phi_\ell(\underline{x})\big)_\ell. \tag{20.3}$$

But the expressions reduce to $\Phi_\ell(\underline{x}) \equiv x_0^{p^\ell} \mod p$, so only a "phantom" of what was there remains.

Proposition 20.2 also generalizes as follows, with an independent proof:

Theorem 20.4. There are unique morphisms $+, \cdot : \mathrm{W}_\mathbb{Z} \times \mathrm{W}_\mathbb{Z} \longrightarrow W_\mathbb{Z}$ defining a unitary ring structure, such that each $\Phi_\ell : \mathrm{W}_\mathbb{Z} \longrightarrow \mathbb{A}^1_\mathbb{Z}$ is a unitary ring homomorphism (and $+$ coincides with that from Propositions 19.4 and 20.2).

Remark. On Witt vectors $+$ and $\cdot$ will always denote the above morphisms, not the componentwise addition and multiplication.

Proof. The isomorphism (20.3) shows that the theorem holds over $\mathbb{Z}[\frac{1}{p}]$. To prove it over $\mathbb{Z}$ we must show that $+$ and $\cdot$, as well as the respective identity sections and the additive inverse, are morphisms defined over $\mathbb{Z}$. For $+$ and $\cdot$ this is achieved conveniently by Lemma 20.5 below. One easily checks that $\underline{0} = (0, 0, \ldots)$ and $\underline{1} = (1, 0, 0, \ldots)$ are the additive and multiplicative identity sections. For the additive inverse the reader is invited to adapt Lemma 20.5. Finally, once all morphisms are defined over $\mathbb{Z}$, the ring and homomorphism axioms over $\mathbb{Z}$ follow directly from those over $\mathbb{Z}[\frac{1}{p}]$. □

Lemma 20.5. For every morphism $u : \mathbb{A}^1_\mathbb{Z} \times \mathbb{A}^1_\mathbb{Z} \longrightarrow \mathbb{A}^1_\mathbb{Z}$ there exists a unique morphism $\underline{v} : \mathrm{W}_\mathbb{Z} \times \mathrm{W}_\mathbb{Z} \longrightarrow \mathrm{W}_\mathbb{Z}$ such that for all $\ell \geq 0 :\ \Phi_\ell \circ \underline{v} = u \circ (\Phi_\ell \times \Phi_\ell)$.

Proof. By the isomorphism (20.3) there exist unique $\underline{v} = (v_0, v_1, \ldots)$ with $v_n \in \mathbb{Z}[\frac{1}{p}][x_0, \ldots, x_n, y_0, \ldots, y_n]$ satisfying the desired relations. It remains to show that $v_n \in A := \mathbb{Z}[x_0, \ldots, y_0, \ldots]$. Since $\Phi_0(\underline{x}) = x_0$, this is clear for $v_0 = u(x_0, y_0)$. So fix $n \geq 0$ and assume that $v_i \in A$ for all $i \leq n$. For any sequence $\underline{x} = (x_0, x_1, \ldots)$ we will abbreviate $\underline{x}^p = (x_0^p, x_1^p, \ldots)$. Then the definition (20.1) of Φ_ℓ implies that

$$\Phi_{n+1}(\underline{x}) \;=\; \Phi_n(\underline{x}^p) + p^{n+1} x_{n+1}.$$

Using this and the relation defining $\underline{v}$ we deduce that

$$\begin{aligned} \Phi_n(\underline{v}^p) + p^{n+1} v_{n+1} &= \Phi_{n+1}(\underline{v}) \\ &\stackrel{\text{def}}{=} u\big(\Phi_{n+1}(\underline{x}), \Phi_{n+1}(\underline{y})\big) \\ &= u\big(\Phi_n(\underline{x}^p) + p^{n+1} x_{n+1}, \Phi_n(\underline{y}^p) + p^{n+1} y_{n+1}\big). \end{aligned}$$

Here note that the right hand side and $\Phi_n(\underline{v}^p)$ are already in A. Thus we have $p^{n+1} v_{n+1} \in A$ and

$$\begin{aligned} p^{n+1} v_{n+1} &\equiv u\big(\Phi_n(\underline{x}^p), \Phi_n(\underline{y}^p)\big) - \Phi_n(\underline{v}^p) \mod p^{n+1} A \\ &\stackrel{\text{def}}{=} \Phi_n\big(\underline{v}(\underline{x}^p, \underline{y}^p)\big) - \Phi_n(\underline{v}^p). \end{aligned} \tag{20.6}$$

To evaluate this further recall that $v_i \in A$ for all $0 \leq i \leq n$; hence

$$v_i(\underline{x}^p, \underline{y}^p) \equiv v_i(\underline{x}, \underline{y})^p \mod pA.$$

This implies that

$$\begin{aligned}
v_i(\underline{x}^p, \underline{y}^p)^{p^{n-i}} &\equiv \big(v_i(\underline{x}, \underline{y})^p\big)^{p^{n-i}} \mod p^{n-i+1}A, \text{ hence} \\
p^i v_i(\underline{x}^p, \underline{y}^p)^{p^{n-i}} &\equiv p^i\big(v_i(\underline{x}, \underline{y})^p\big)^{p^{n-i}} \mod p^{n+1}A, \text{ and therefore} \\
\Phi_n\big(\underline{v}(\underline{x}^p, \underline{y}^p)\big) &\equiv \Phi_n(\underline{v}^p) \mod p^{n+1}A.
\end{aligned}$$

Together with (20.6) we deduce that $p^{n+1}v_{n+1} \in p^{n+1}A$, and hence $v_{n+1} \in A$. The lemma follows by induction on n. □

Examples. We write $\underline{s} = (s_0, s_1, \ldots)$ for the morphism $+$, and $\underline{p} = (p_0, p_1, \ldots)$ for the morphism $\cdot$. Using the relations $\Phi_0(\underline{x}) = x_0$ and $\Phi_1(\underline{x}) = x_0^p + px_1$, elementary calculation shows that

$$\begin{aligned}
s_0(\underline{x}, \underline{y}) &= x_0 + y_0, \\
p_0(\underline{x}, \underline{y}) &= x_0 \cdot y_0, \\
s_1(\underline{x}, \underline{y}) &= x_1 + y_1 + \frac{1}{p}\big(x_0^p + y_0^p - (x_0 + y_0)^p\big) \\
&= x_1 + y_1 - \sum_{i=0}^{p-1} \frac{1}{p}\binom{p}{i} x_0^i y_0^{p-i}, \\
p_1(\underline{x}, \underline{y}) &= x_0^p y_1 + x_1 y_0^p + px_1y_1.
\end{aligned}$$

As one can see, the formulas are quickly becoming very complicated. One should not use them directly, but think conceptually.

For use in the next section we note:

Proposition 20.7. The morphism $\tau : \mathbb{A}^1_{\mathbb{Z}} \longrightarrow \mathrm{W}_{\mathbb{Z}},\ x \mapsto (x, 0, \ldots)$ is multiplicative, i.e., it satisfies $\tau(xy) = \tau(x) \cdot \tau(y)$.

Proof. It is enough to check this over $\mathbb{Z}[\frac{1}{p}]$, i.e., after applying each Φ_ℓ. But $\Phi_\ell\big(\tau(x)\big) = x^{p^\ell}$ is obviously multiplicative. □

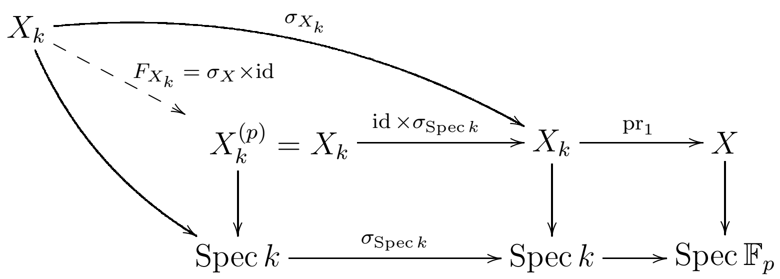
Finally, we introduce *Witt vectors of finite length* $n \geq 1$. For this recall that the m-th components of $\underline{x} + \underline{y}$ and $\underline{x} \cdot \underline{y}$ and $-\underline{x}$ depend only on the first m components of $\underline{x}$ and $\underline{y}$. Thus the same formulas define a ring structure on $W_{n,R} := \prod_{m=0}^{n-1} \mathbb{A}^1_R$ for any ring R, such that the truncation map

(20.8) $$W_R \longrightarrow W_{n,R},\ \underline{x} \mapsto (x_0, \ldots, x_{n-1})$$

is a ring homomorphism.

§21 Witt vectors in characteristic p

From now on let k be a perfect field of characteristic $p > 0$. For any scheme X over $\mathbb{F}_p$ we abbreviate $X_k := X \times_{\operatorname{Spec}\mathbb{F}_p} \operatorname{Spec} k$. Then there is a natural isomorphism $X_k^{(p)} \cong X_k$ which turns the relative Frobenius of X_k into the endomorphism $\sigma_X \times \mathrm{id}$ of X_k, where σ_X denotes the absolute Frobenius of X. Indeed, this follows from the definition of Frobenius from §14 and the fact that the two rectangles in the following commutative diagram are cartesian:



In particular we can apply this to $W_k = W_{\mathbb{F}_p} \times_{\operatorname{Spec}\mathbb{F}_p} \operatorname{Spec} k$. Thus the Frobenius and Verschiebung for the additive group of W_k become *endomorphisms* satisfying $F \circ V = V \circ F = p \cdot \mathrm{id}$. The following proposition collects some of their properties.

Proposition 21.1. (a) $F\big((x_0, x_1, \ldots)\big) = (x_0^p, x_1^p, \ldots)$.

(b) $V\big((x_0, x_1, \ldots)\big) = (0, x_0, x_1, \ldots)$.

(c) $p \cdot (x_0, x_1, \ldots) = (0, x_0^p, x_1^p, \ldots)$.

(d) $F(\underline{x} + \underline{y}) = (F\underline{x}) + (F\underline{y})$.

(e) $F(\underline{x} \cdot \underline{y}) = (F\underline{x}) \cdot (F\underline{y})$.

(f) $\underline{x} \cdot (V\underline{y}) = V\big((F\underline{x}) \cdot \underline{y}\big)$.

(g) $E\big(\underline{x} \cdot (V\underline{y}), t\big) = E\big((F\underline{x}) \cdot \underline{y}, t^p\big)$.

Remark. Part (b) is probably the reason why V is called Verschiebung.

Proof. (a), (d), and (e) are clear from the definition and functoriality of F. (b) is equivalent to (c) by the relation $p \cdot \underline{x} = VF\underline{x}$, because $F : \mathrm{W}_k \to \mathrm{W}_k$ is an epimorphism. For (c) we cannot use the phantom components, because we are in characteristic $p > 0$. Instead we use the Artin-Hasse exponential

$E(\underline{x}, t) = \prod_{n=0}^{\infty} F(x_n t^{p^n})$. Recall that it defines a homomorphism and a closed embedding $W_{\mathbb{Z}_{(p)}} \to \Lambda_{\mathbb{Z}_{(p)}}$, and hence also $W_k \to \Lambda_k$. Therefore

$$\begin{aligned} E(p \cdot \underline{x}, t) \;=\; E(\underline{x}, t)^p \;&=\; \prod_{n=0}^{\infty} F(x_n t^{p^n})^p \;\overset{(*)}{=}\; \prod_{n=0}^{\infty} F(x_n^p t^{p^{n+1}}) \\ &=\; \prod_{n=1}^{\infty} F(x_{n-1}^p t^{p^n}) \;=\; E\big((0, x_0^p, x_1^p, \ldots), t\big), \end{aligned}$$

where $(*)$ follows from the fact that we are working over k and that F has coefficients in $\mathbb{Z}_{(p)}$. This shows (c). Next, since F is an epimorphism, it suffices to prove (f) for $\underline{y} = F\underline{z}$. But for this it follows from the calculation

$$\begin{aligned} \underline{x} \cdot (V\underline{y}) \;&=\; \underline{x} \cdot (VF\underline{z}) \;=\; \underline{x} \cdot (p \cdot \underline{z}) \;=\; p \cdot (\underline{x} \cdot \underline{z}) \\ &=\; VF(\underline{x} \cdot \underline{z}) \;\overset{\text{(e)}}{=}\; V\big((F\underline{x}) \cdot (F\underline{z})\big) \;=\; V\big((F\underline{x}) \cdot \underline{y}\big). \end{aligned}$$

Finally, (g) results from

$$E\big(\underline{x} \cdot (V\underline{y}), t\big) \;\overset{\text{(f)}}{=}\; E\big(V\big((F\underline{x}) \cdot \underline{y}\big), t\big) \;\overset{\text{def. of } E}{=}\; E\big((F\underline{x}) \cdot \underline{y}, t^p\big). \qquad \square$$

Theorem 21.2. $\mathrm{W}(k)$ is a complete discrete valuation ring with uniformizer p and residue field k.

Proof. Since k is perfect, we have $p^n\,\mathrm{W}(k) = V^n\big(\mathrm{W}(k)\big)$ for all $n \geq 1$. By iterating Proposition 21.1 (b) this is also the kernel of the truncation homomorphism $W(k) \to W_n(k)$ from (20.8). Thus $W(k)/p^n W(k) \cong W_n(k)$ and $W(k)/pW(k) \cong W_1(k) \cong k$. Using this, by induction on n one shows that $W_n(k)$ is a $W(k)$-module of length n. Since clearly $W(k) \cong \varprojlim_n W_n(k)$, the theorem follows. $\square$

Theorem 21.3 (Witt). Let R be a complete noetherian local ring with residue field k.

(a) There exists a unique ring homomorphism $u : \mathrm{W}(k) \longrightarrow R$ such that the following diagram commutes:

$$\begin{array}{ccc} \mathrm{W}(k) & \xrightarrow{\;u\;} & R \\ & \searrow \quad \swarrow & \\ & k. & \end{array}$$

(b) If R is a complete discrete valuation ring with uniformizer p, then u is an isomorphism.

Proof. Recall that by Proposition 18.1 there are unique multiplicative sections

$$\mathrm{W}(k) \xleftarrow{\ \tau\ } k \xrightarrow{\ i\ } R.$$

Since u is also multiplicative, it must therefore satisfy the equation $i = u \circ \tau$. By Proposition 20.7 we have $\tau(x) = (x, 0, \ldots)$. In view of Proposition 21.1 (c) this implies that any element $\underline{x} = (x_0, x_1, \ldots) \in \mathrm{W}(k)$ has the power series expansion

$$\underline{x} \;=\; \tau(x_0) + p \cdot \tau(x_1^{1/p}) + p^2 \cdot \tau(x_2^{1/p^2}) + \ldots .$$

So the ring homomorphism u must be given by

$$u(\underline{x}) \;=\; i(x_0) + p \cdot i(x_1^{1/p}) + p^2 \cdot i(x_2^{1/p^2}) + \ldots .$$

In particular u is unique, but we must verify that this formula does define a ring homomorphism. For this, let $\mathfrak{m}$ be the maximal ideal of R, which contains p, and calculate:

$$\begin{aligned} u(\underline{x}) &\equiv i(x_0) + p \cdot i(x_1^{1/p}) + \ldots + p^n \cdot i(x_n^{1/p^n}) \quad \bmod \mathfrak{m}^{n+1}, \\ &= i(x_0^{p^{-n}})^{p^n} + p \cdot i(x_1^{p^{-n}})^{p^{n-1}} + \ldots + p^n \cdot i(x_n^{p^{-n}}) \\ &= \Phi_n\big(i(x_0^{p^{-n}}), \ldots, i(x_n^{p^{-n}})\big). \end{aligned}$$

It is enough to show that this defines a ring homomorphism $W(k) \to R/\mathfrak{m}^{n+1}$ for any n, because R is complete noetherian and hence $R = \varprojlim R/\mathfrak{m}^{n+1}$. Since Frobenius defines a ring automorphism of $W(k)$, this is equivalent to showing that $\Phi_n\big(i(x_0), \ldots, i(x_n)\big)$ defines a ring homomorphism $W(k) \to R/\mathfrak{m}^{n+1}$. But $\Phi_n : \mathrm{W}(R) \to R$ is a ring homomorphism by the construction of Witt vectors. Moreover, we have $\Phi_n(x_0, \ldots, x_n) \in \mathfrak{m}^{n+1}$ if all $x_i \in \mathfrak{m}$, by the definition of Φ_n. Thus the composite homomorphism in the diagram

$$\begin{array}{ccc} \mathrm{W}(R) & \xrightarrow{\ \Phi_n\ } & R \\ \downarrow & & \downarrow \\ \mathrm{W}(k) & \dashrightarrow & R/\mathfrak{m}^{n+1} \end{array}$$

vanishes on the kernel of the left vertical map; hence it factors through a ring homomorphism along the lower edge. The lower arrow is then given explicitly by $\Phi_n\big(i(x_0), \ldots, i(x_n)\big) \bmod \mathfrak{m}^{n+1}$ for any section i, in particular for the canonical one. Therefore this defines a ring homomorphism, proving (a).

(b) follows from the fact that any homomorphism of complete discrete valuation rings with the same uniformizer and the same residue field is an isomorphism. □