1. Witt Vectors

Recall the following result.

Lemma 1.0.1. Let $\Phi(X,Y) \in \mathbb{Z}[X,Y]$. There exists a unique sequence $(\Phi_n)_{n\in\mathbb{Z}}$ of polynomials

$$\Phi_n \in \mathbb{Z}[X_0, X_1, \ldots, X_n, Y_0, \ldots, Y_n]$$

such that

$$\Phi(W_n(\underline{X}), W_n(\underline{Y})) = W_n(\Phi_0, \ldots, \Phi_n).$$

Definition 1.0.2. The polynomials

$$S_n, P_n \in \mathbb{Z}[X_0, \ldots, X_n, Y_0, \ldots, Y_n]$$

are obtained by applying the previous lemma with $\Phi = X + Y$ and $\Phi = XY$. In other words, they are defined inductively by

$$W_n(\underline{X}) + W_n(\underline{Y}) = W_n(S_0, \ldots, S_n)$$
$$W_n(\underline{X}) \cdot W_n(\underline{Y}) = W_n(P_0, \ldots, P_n)$$

We have a similar definition for scalar multiplication. Let $\lambda \in \mathbb{Z}_p$. The polynomials

$$M(\lambda)_n \in \mathbb{Z}_p[X_0, \ldots, X_n]$$

are obtained with $\Phi(X) = \lambda X$, i.e. inductively defined by

$$\lambda W_n(\underline{X}) = W_n(M(\lambda)_0, \ldots, M(\lambda)_n).$$

Example 1.0.3. Explicit computations.

(1) $S_0 = X_0 + Y_0$, $P_0 = X_0Y_0$, and $M(\lambda)_0 = \lambda X_0$.

(2) S_1 is determined via

$$(X_0^p + pX_1) + (Y_0^p + pY_1) = S_0^p + pS_1 = (X_0 + Y_0)^p + pS_1.$$

Hence

$$S_1 = X_1 + Y_1 - \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} X_0^i Y_0^{p-i}.$$

(3) P_1 is determined via

$$(X_0^p + pX_1)(Y_0^p + pY_1) = P_0^p + pP_1 = (X_0Y_0)^p + pP_1.$$

Hence

$$P_1 = pX_1Y_1 + X_1Y_0^p + Y_1X_0^p.$$

2. Prisms

All the rings are $\mathbb{Z}_{(p)}$-algebras. The Jacobson radical of a ring R is denoted by $\mathrm{jrad}(A)$.

Definition 2.0.1. Let A be a ring. Let $I \subset A$ be an ideal. The localization of A along $V(I)$ is $S^{-1}A$ where

$$S = A \backslash \cup_{\mathfrak{p}\in V(I)} \mathfrak{p} = \overline{1+I}.$$

Here, the last equality requires the axiom of choice, where $\overline{1+I}$ denotes the saturation of the multiplicative set $1+I$, i.e. $x \in \overline{1+I}$ if and only if there exists $y \in A$ such that $xy \in 1+I$.

Lemma 2.0.2. Let $I \subset A$ be an ideal.

(1) $IS^{-1}A$ is contained in $\mathrm{jrad}(S^{-1}A)$.

Proof. Proof of (1). We need to prove that every maximal ideal of $S^{-1}A$ contains $IS^{-1}A$. A prime ideal of $S^{-1}A$ corresponds to a prime ideal of A not intersecting with S, i.e. a prime ideal $\mathfrak{p} \subset A$ contained in $\cup_{\mathfrak{p}\in V(I)}\mathfrak{p}$. For such a prime $\mathfrak{p}$, we have

$$\mathfrak{p} + I \subset \cup_{I\subset\mathfrak{q}}\mathfrak{q}.$$

Hence $\mathfrak{p} + I$ is a proper ideal, and thus is contained in some maximal ideal $\mathfrak{m}$. □

Lemma 2.0.3. Let $A \to B$ be a flat ring map. The following are equivalent.

(1) $A \to B$ is faithfully flat.
(2) $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is surjective.
(3) The image of $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ contains every closed point.

Lemma 2.0.4. Let $R \to S$ be a flat ring map. Then it satisfies going down. In other words, if $\mathfrak{p} \subset \mathfrak{p}' \subset R$ and $\mathfrak{q}' \subset S$ are primes with $\mathfrak{q}'$ mapping to $\mathfrak{p}'$, then there exists a prime $\mathfrak{q} \subset \mathfrak{q}'$ mapping to $\mathfrak{p}$.

Lemma 2.0.5. Let A be a δ-ring. Let $d \in A$. Suppose $(d, p) \subset \mathrm{jrad}(A)$. Then d is distinguished if and only if $p \in (d, \phi(d))$.

Lemma 2.0.6. Let A be a ring. Let $I \subset A$ be an ideal. Let A' be the localization of A along $V(I)$. Then the image of $\mathrm{Spec}(A') \to \mathrm{Spec}(A)$ contains $V(I)$.

Lemma 2.0.7. Let A be a δ-ring. Let $I \subset A$ be a locally principal ideal. Assume that $(p, I) \subset \mathrm{jrad}(A)$. The following are equivalent.
(1) $p \in I^p + \phi(I)A$.
(2) $p \in I + \phi(I)A$.
(3) There exists a faithfully flat map $A \to A'$ of δ-rings that is an ind Zariski localization such that IA' is generated by a distinguished element d and $d, p \in \mathrm{jrad}(A')$.

Proof. Proof of (1) $\Rightarrow$ (2). We have $I^p \subset I$.

Proof of (2) $\Rightarrow$ (3). Let $g_1, \ldots, g_n \in A$ be elements generating the unit ideal of A such that every $IA[1/g_i]$ is principal. Define

$$A' = \prod_{i=1}^{n} A_i,$$

where A_i is the Zariski localization of $A[1/g_i]$ along $V(p, I)$. So

$$(p, I)A_i \subset \mathrm{jrad}(A_i).$$

Then

$$(p, I)A' \subset \mathrm{jrad}(A').$$

The map $A \to A'$ is flat because
(1) The localizations $A \to A[1/g_i] \to A_i$ are flat.
(2) Product of flat A-algebras is flat.

Next we show that $A \to A'$ is faithfully flat. It sufficies to prove that the map $\mathrm{Spec}(A') \to \mathrm{Spec}(A)$ is surjective, which follows from
(1) The image of $\mathrm{Spec}(A') \to \mathrm{Spec}(A)$ is stable under generalization (i.e. going down) by flatness.
(2) The image contains $V(p, I) \subset \mathrm{Spec}(A)$, as

$$\mathrm{Spec}(A') \simeq \sqcup_{i=1}^{n} \mathrm{Spec}(A_i) \to \mathrm{Spec}(A),$$

and the image of $\mathrm{Spec}(A_i) \to \mathrm{Spec}(A)$ contains $V(p, I) \cap \mathrm{Spec}(A[1/g_i])$.
(3) $(p, I) \subset \mathrm{jrad}(A)$, i.e. $V(p, I)$ contains all the closed points of $\mathrm{Spec}(A)$.

By construction, we have $IA' = (d)$ for some $d \in A'$. It remains to prove
(1) A' admits a unique δ-A-algebra structure.
(2) The element d is distinguished.

For the second assertion, we need to show

$$p \in (d, \phi(d)),$$

which follows from $p \in I + \phi(I)A$ and that the associated Frobenius $\phi : A \to A$ is functorial in A. For the first assersion, we use the general result on localizations of δ-rings.

Proof of (3) $\Rightarrow$ (1). The goal is to check $p = 0$ in the quotient

$$A/(I^p + \phi(I)A).$$

As $A \to A'$ is faithfully flat, the base change

$$A/(I^p + \phi(I)A) \to A'/(d^p, \phi(d))$$

is also faithfully flat, and thus injective. So it sufficies to check $p = 0$ in $A'/(d^p, \phi(d))$. Recall that $\phi(d) = d^p + p\delta(d)$, and that d is distinguished means $\phi(d)$ is a unit. Hence the result is clear. $\square$

Lemma 2.0.8. Let A be a δ-ring. Let $S \subset A$ be a multiplicative subset with $\phi(S) \subset S$. Then the localization $S^{-1}A$ admits a unique δ-structure compatible with $A \to S^{-1}A$.

Lemma 2.0.9. Let $A \to B$ be a faithfully flat ring map. Then it is injective.

Proof. Let $r \in \ker(A \to B)$. The sequence

$$rA \to A \to A$$

is exact since

$$0 = rB \to B \to B$$

is exact. Hence $rA = 0$, and thus $r = 0$. □

Definition 2.0.10. A prism is a pair (A, I) where A is a δ-ring and $I \subset A$ is an ideal defining a Cartier divisor on $\mathrm{Spec}(A)$ (i.e. I is an invertible A-module) such that A is derived (p, I)-complete, and $p \in I + \phi(I)A$.

Remark 2.0.11. The ring A is derived (p, I)-complete implies that $(p, I) \subset \mathrm{jrad}(A)$, and hence also $\phi(I) \subset \mathrm{jrad}(A)$.