Take-home Final

Anthony Várilly

Harvard University, Cambridge, MA 02138
Math 250b: Higher Algebra II, Spring 2003

1 Introduction

Let p be a rational prime number and let A be a commutative ring (in which p is not a zero-divisor), which is complete and separated with respect to the p-adic filtration

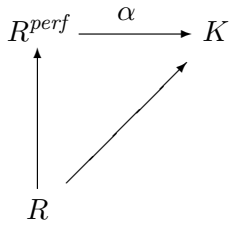
$$\cdots \subset p^n A \subset \cdots \subset p^2 A \subset pA \subset A.$$

We call $\tilde{K} := A/pA$ the *residue ring* of A. The goal of this note is to show that given a perfect ring $\tilde{K}$ of characteristic p there is a (unique) ring A, complete and separated with respect to the p-adic filtration, such that its residue ring is A. The first half of the paper contains a proof of the existence of such an A. We call this ring the ring of Witt vectors of $\tilde{K}$ and denote it $W(\tilde{K})$. The second half is devoted to a construction of $W(\tilde{K})$ due to Witt. The exposition is influenced by Serre [1].

We begin with some preliminary material on perfect closures of rings.

2 Perfect Closures

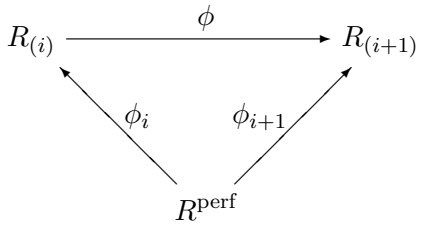
Theorem 1. *Let R be a ring of characteristic p. There exists a unique perfect ring R^{perf} of characteristic p together with an inclusion $R \to R^{perf}$ with the property that for any perfect ring K (with char $K = p$), together with an inclusion $R \to K$, there is a unique homomorphism α that makes the following diagram commute:*



Proof. There are many things to take care of. First, we will construct R^{perf} and prove it is perfect. Consider the p-power homomorphism $\phi : R \to R$. Let R^{perf} be the direct limit of the sequence of rings and homomorphisms:

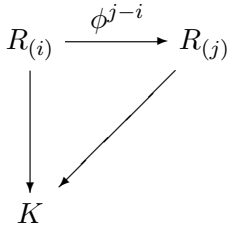
$$R \to R \to R \to R \to R \to \cdots,$$

where all the homomorphisms are equal to ϕ, and let $R \to R^{\text{perf}}$ be the natural inclusion. We claim R^{perf} is a perfect ring. Let $R_{(i)}$ denote the i-th copy of R in the above sequence. By the definition of direct limit we have homomorphisms $\phi_i : R_{(i)} \to R^{\text{perf}}$ which make the following diagram commute:



By a well-known property of the direct limit, any element $r \in R^{\text{perf}}$ can be written as $\phi_i(a)$, $a \in R_{(i)}$ for some i. But then by the commutativity of the above diagram we know that $\phi_i(a) = \phi_{i+1}(a^p) = \phi_{i+1}^p(a)$, whence r is a p-th power of an element in R^{perf}, which is to say that R^{perf} is perfect.

Next, we show that R^{perf} satisfies the desired universal property. If we can show that there are maps $R_{(i)} \to K$ such that the triangles



commute then by the defining universal property of the direct limit we will have a unique homomorphism $\alpha : R^{\text{perf}} \to K$. Let $\psi : K \to K$ denote the p-power map in K. It is a ring automorphism because K is perfect. We claim the maps $\psi^{-i+1} \circ \phi : R_{(i)} \to K$ do the trick. Indeed, for any $a \in R_{(i)}$ we have

$$\psi^{-j+1} \circ \phi \circ \phi^{j-i}(a) = \psi^{-j+1} \circ \phi^{j-i+1}(a) = \psi^{-i+1} \circ \phi(a),$$

because ϕ and ψ are both p-power maps. This means the required triangles are commutative.

It remains to show that R^{perf} is unique. Suppose there are two rings R^{perf} and $R^{\text{perf}'}$ that satisfy the universal property. Then we can play them against each other, i.e., we let both R^{perf} and $R^{\text{perf}'}$ take the role of K to obtain an isomorphism between R^{perf} and $R^{\text{perf}'}$. □

Example 1. Let $\{X_j\}_{j \in J}$ be a collection of indeterminates and set $R = \mathbb{F}_p[X_j; j \in J]$. We claim that the perfect closure of R is the union

$$\bigcup_{n=0}^{\infty} \mathbb{F}_p[X_j^{p^{-n}}; j \in J].$$

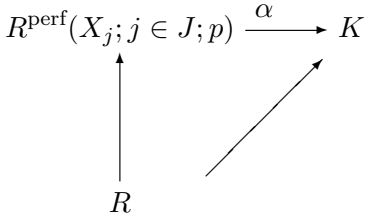
First, note this union is a ring since it is the direct limit of the sequence of rings and inclusions

$$\mathbb{F}_p[X_j; j \in J] \subset \mathbb{F}_p[X_j^{p^{-1}}; j \in J] \subset \mathbb{F}_p[X_j^{p^{-2}}; j \in J] \subset \cdots.$$

We will denote this ring by $R^{\text{perf}}(X_j; j \in J; p)$ or $\mathbb{F}_p[X_j^{p^{-n}}; j \in J, n \geq 0]$. To see that this is the perfect closure of R we will show it is the universal perfect ring for R. It is clear that $R^{\text{perf}}(X_j; j \in J; p)$

is perfect: the p-th root of a polynomial is obtained by extracting p-th roots of its indeterminates because we are working over characteristic p and because a p-th root of an element of $\mathbb{F}_p$ (i.e., a coefficient) is itself.

Now suppose we have any other perfect ring K that contains R. Let Y_i be the image in K of X_i under the inclusion $R \to K$. We must exhibit a map $\alpha : R^{\text{perf}}(X_j; j \in J; p) \to K$ such that the following diagram commutes:



We are forced to send $X_i \mapsto Y_i$ under α to ensure commutativity. Furthermore, if α is to be a homomorphism then we must send $X_i^{p^{-n}}$ to $Y_i^{p^{-n}}$. But then we have defined a map on the generators of $R^{\text{perf}}(X_j; j \in J; p)$ which is a homomorphism (the only relations between the $X_i^{p^{-n}}$ come from the p-power map, but we have taken care of these relations already). This establishes the existence and uniqueness of α. Hence $R^{\text{perf}}(X_j; j \in J; p)$ is the perfect closure of R as desired.

3 Existence of the Witt Ring

We now embark the proof of the existence of the ring of Witt vectors of a (characteristic p) perfect ring $\tilde{K}$. To begin, we discuss systems of multiplicative representatives in a slightly more general context than was presented in the introduction.

Theorem 2. *Let A be a commutative ring, separated and complete with respect to the sequence of ideals*

$$\cdots \subset I_{n+1} \subset I_n \subset \cdots \subset I_2 \subset I_1 \subset A$$

which have the property that

$$I_n \cdot I_m \subset I_{n+m}.$$

Let $\tilde{K} = A/I_1$ be the residue ring of A. Suppose $\tilde{K}$ is perfect of characteristic p. Then there is a unique system of representatives of $\tilde{K}$ in A, i.e., a map $\iota : \tilde{K} \to A$ such that

- $\iota(x^p) = \iota(x)^p$,
- *$a \in A$ is one of these representatives if and only if a is a p^n-th power for all $n \geq 0$,*
- *ι is multiplicative: $\iota(x \cdot y) = \iota(x) \cdot \iota(y)$,*
- *if A is of characteristic p then $\iota : \tilde{K} \to A$ is a ring homomorphism.*

First we have two useful lemmas:

Lemma 3. *Let $a, b \in A$ and suppose $a \equiv b \bmod I_n$. Then $a^p \equiv b^p \bmod I_{n+1}$.*

Proof. First consider the case when p is odd. Using the binomial expansion we see that

$$(a-b)^p = a^p - b^p + p\left[-a^{p-1}b + \cdots + ab^{p-1}\right].$$

Consider the sum inside the square brackets modulo I_n. Since $a \equiv b \bmod I_n$ each term in this sum is of the form $ma^{p-k}b^k \equiv ma^p \bmod I_n$. The sum of the *coefficients* inside the square brackets is zero (this is a consequence of the identity $\binom{n}{k} = \binom{n}{n-k}$). We conclude that $-a^{p-1}b + \cdots + ab^{p-1} \in I_n$. On the other hand $p \in I_1$ because $\tilde{K}$ has characteristic p, so

$$p\left[-a^{p-1}b + \cdots + ab^{p-1}\right] \in I_1 \cdot I_n \subset I_{n+1}.$$

Hence

$$0 \equiv (a-b)^p \equiv a^p - b^p \bmod I_{n+1},$$

as desired. If $p = 2$ then $(a-b)^2 \in I_n \cdot I_n \subset I_{2n} \subset I_{n+1}$. And since $ab \equiv b^2 \bmod I_n$ we have

$$(a-b)^2 = a^2 + b^2 - 2ab \equiv a^2 + b^2 - 2b^2 \equiv a^2 - b^2 \bmod I_{n+1}.$$

Therefore $a^2 \equiv b^2 \bmod I_{n+1}$. □

Lemma 4. *Let A be as above and suppose its residue ring has characteristic p. If $a^p \equiv b^p \bmod I_1$ for any elements $a, b \in A$, then $a \equiv b \bmod I_1$.*

Proof. We know $a^p - b^p \in I_1$, but $a^p - b^p \equiv (a-b)^p \bmod I_1$ because $\tilde{K}$ has charateristic p. Hence $(a-b)^p \in I_1$. Let $\overline{a-b}$ be the reduction of $a-b$ in $\tilde{K}$. Then $(\overline{a-b})^p = 0$ and since the p-power map is an automorphism of $\tilde{K}$ it follows that $\overline{a-b} = 0$, which is to say that $a - b \in I_1$, as desired. □

Proof of Theorem 2. We define the map $\iota : \tilde{K} \to A$ as follows. Since $\tilde{K}$ is perfect we have $x^{p^{-n}} \in \tilde{K}$ for every $x \in \tilde{K}$ and $n \geq 0$. Let $x_n \in A$ be a representative for $x^{p^{-n}}$, i.e., $x_n^{p^n}$ is in the equivalence class of x in $\tilde{K}$ for every nonnegative n. We claim that $(x_n^{p^n})_n$ is a Cauchy sequence. Indeed, since $x_{n+1}^{p^{n+1}} \equiv x_n^{p^n} \bmod I_1$, we conlude using Lemma 4 that

$$x_{n+1}^p \equiv x_n \bmod I_1.$$

After n applications of Lemma 3 we find that

$$x_{n+1}^{p^{n+1}} \equiv x_n^{p^n} \bmod I_{n+1},$$

which is to say that the sequence $(x_n^{p^n})_n$ is Cauchy with respect to the given filtration. Set

$$\iota(x) = \lim_{n\to\infty} x_n^{p^n},$$

and remark that $\iota(x) \in A$ by completeness of A. We claim that $\iota(x)$ depends only on x and not on the sequence $(x_n^{p^n})_n$. Indeed, take a different set $(x'_n)_n$ of elements of A such that x'_n is a representative of $x^{p^{-n}}$. Then by repeated application of Lemma 4 to the congruence $x_n'^{p^n} \equiv x_n^{p^n} \bmod I_1$ we see that $x'_n \equiv x_n \bmod I_1$ and so again by Lemma 3 we have

$$x_n'^{\,p^n} \equiv x_n^{p^n} \bmod I_{n+1},$$

which means that

$$\lim_{n\to\infty} {x'_n}^{p^n} = \lim_{n\to\infty} x_n^{p^n} = \iota(x).$$

Next, we show that ι commutes with the p-th power map. Suppose $x = y^p$. Then the p-th power map takes a representative y_n of $y^{p^{-n}}$ to y_n^p, and since

$$(y_n^p)^{p^n} = (y_n^{p^n})^p \in y^p = x,$$

it follows that y_n^p is a representative of $x^{p^{-n}}$. We have shown that ι is independent of the choice of representatives, so passing to the limit it follows that the p-power map takes $\iota(y)$ to $\iota(x)$, i.e.,

$$\iota(y)^p = \iota(x) = \iota(y^p),$$

as desired.

Since $\tilde{K}$ is perfect and ι commutes with the p-th power map an element $a \in A$ is a representative only if a is a p^n-th power for all $n \geq 0$. Indeed, if $a = \iota(x)$ then there is a $x_1 \in \tilde{K}$ such that $x = x_1^p$, which means $a = \iota(x_1^p) = \iota(x_1)^p$, etc. Conversely, if $a \in A$ is a p^n-th power for all $n \geq 0$, say $a = a_n^{p^n}$, then we can show a is a representative. Let x be the image of a under reduction. We show that $a = \iota(x)$. It would be enought to show that

$$a \equiv \iota(x) \bmod I_n \quad \text{for all } n \geq 1.$$

Since $\iota(x)$ is a p^n-th power for all n we may write $\iota(x) = x_n^{p^n}$. Since $a \equiv \iota(x) \bmod I_1$ we have

$$a_n^{p^n} \equiv x_n^{p^n} \bmod I_1.$$

Successive applications of Lemma 4 yield the congruence

$$a_n \equiv x_n \bmod I_1.$$

and then applying Lemma 3 we conclude that

$$\begin{aligned} a_n^{p^n} &\equiv x_n^{p^n} \bmod I_{n+1} \\ \implies a &\equiv \iota(x) \bmod I_{n+1}. \end{aligned}$$

To see that the system of representatives of $\tilde{K}$ in A is unique, suppose there is another system $\iota' : \tilde{K} \to A$ that commutes with the p-th power map. Then $\iota'(x)$ is a p^n-th power for all $n \geq 0$, which is to say $\iota'(x)$ is a representative for $x^{p^{-n}}$ for all n. These representatives form a Cauchy sequence converging to $\iota(x)$, hence $\iota'(x) = \iota(x)$.

To see that $\iota(xy) = \iota(x)\iota(y)$ we note that

$$\iota(xy) = \lim_{n\to\infty} (x_n \cdot y_n)^{p^n} = \lim_{n\to\infty} x_n^{p^n} \cdot \lim_{n\to\infty} y_n^{p^n} = \iota(x)\iota(y).$$

Finally, if A has characteristic p then

$$\iota(x+y) = \lim_{n\to\infty} (x_n + y_n)^{p^n} = \lim_{n\to\infty} (x_n^{p^n} + y_n^{p^n}) = \lim_{n\to\infty} x_n^{p^n} + \lim_{n\to\infty} y_n^{p^n} = \iota(x) + \iota(y),$$

so ι is a ring homomorphism in this case. □

We are interested in the particular case of Theorem 2 when p is not a zero-divisor in A and $I_n = p^n A$ for all $n \geq 0$ (the p-adic filtration). We claim that, in this case, for every sequence $(\alpha_0, \alpha_1, \dots, \alpha_n, \dots)$ of elements in $\tilde{K}$ there is an element α of A which is the limit of the Cauchy sequence of truncated sums in

$$\alpha = \iota(\alpha_0) + \iota(\alpha_1) \cdot p + \iota(\alpha_2) \cdot p^2 + \cdots + \iota(\alpha_n) \cdot p^n + \cdots \tag{1}$$

Indeed, let $S_n = \iota(\alpha_0) + \iota(\alpha_1) \cdot p + \iota(\alpha_2) \cdot p^2 + \cdots + \iota(\alpha_n) \cdot p^n$. Since $\iota(\alpha_j) \in A$ for every j we have $\iota(\alpha_j) \cdot p^j \in p^j A$. This means

$$S_{n+1} \equiv S_n \bmod p^{n+1} A,$$

which is to say that $(S_n)_n$ is a Cauchy sequence for the p-adic filtration. By completeness of A we have

$$\alpha = \lim_{n \to \infty} S_n \in A.$$

Conversely, every α in A has a unique such representation. Indeed, by definition of the system of representatives there is an $\iota(\alpha_0)$ such that $\alpha - \iota(\alpha_0) \in pA$. But then

$$\alpha = \iota(\alpha_0) + a_1 \cdot p, \quad a_1 \in A.$$

By the same reasoning there is an $\iota(\alpha_1)$ such that $a_1 - \iota(\alpha_1) \in pA$. This means $a_1 = \iota(\alpha_1) + a_2 \cdot p$ for some $a_2 \in A$, and hence

$$\alpha = \iota(\alpha_0) + \iota(\alpha_1) \cdot p + a_2 \cdot p^2, \quad a_2 \in A.$$

Continuing in this fashion we obtain a representation for α like that in (1). Furthermore, this representation is unique, for if

$$\begin{aligned} \alpha &= \iota(\alpha_0) + \iota(\alpha_1) \cdot p + \iota(\alpha_2) \cdot p^2 + \cdots + \iota(\alpha_n) \cdot p^n + \cdots \\ &= \iota(\beta_0) + \iota(\beta_1) \cdot p + \iota(\beta_2) \cdot p^2 + \cdots + \iota(\beta_n) \cdot p^n + \cdots , \end{aligned}$$

then $\iota(\alpha_0) \equiv \iota(\beta_0) \bmod p$, i.e., $\alpha_0 = \beta_0$ by definition of ι, and then a simple induction shows $\alpha_i = \beta_i$ for all i. We say that α has coordinates $(\alpha_0, \alpha_1 \dots)$.

We will show that if the ring of Witt vectors for $\tilde{K}$ exists, then it is unique up to isomorphism. We will need two lemmas to prove this result.

Lemma 5. *Let A and A' be rings that are separated and complete with respect to the p-adic filtration and have residue rings $\tilde{K}$ and $\tilde{K}'$, respectively. Every homomorphism $\phi : A \to A'$ commutes with multiplicative representatives.*

Proof. We are claiming the following diagram commutes:

$$\begin{array}{ccc} A & \xrightarrow{\phi} & A' \\ {\scriptstyle \iota_A}\uparrow & & \uparrow{\scriptstyle \iota_{A'}} \\ \tilde{K} & \xrightarrow{\overline{\phi}} & \tilde{K}' \end{array}$$

Let x be an element of $\tilde{K}$. Since $\iota(x) \in A$ is a multiplicative representative, it is a p^n-th power for all $n \geq 0$. We write $\iota(x) = x_n^{p^n}$. But ϕ is a homomorphism, and so

$$\phi(\iota(x)) = \phi(x_n^{p^n}) = \phi(x_n)^{p^n}.$$

This means $\phi(\iota(x)) \in A'$ is a p^n-th power for all n and is consequently a multiplicative representative for $\tilde{K}'$. In other words

$$\phi(\iota(x)) = \iota_{A'}(y) \tag{2}$$

for some $y \in \tilde{K}'$. Let $\pi : A \to \tilde{K}$ be the reduction mod p homomorphism, and similarly for $\pi' : A' \to \tilde{K}'$. We apply π' to (2) to obtain

$$\pi' \circ \phi \circ \iota(x) = \pi' \circ \iota_{A'}(y) = y.$$

By definition of reduction mod p we know $\overline{\phi} \circ \pi = \pi' \circ \phi$, hence

$$y = \pi' \circ \phi \circ \iota(x) = \overline{\phi} \circ \pi \circ \iota(x) = \overline{\phi}(x).$$

In view of (2) we conclude that $\phi \circ \iota(x) = \iota_{A'} \circ \overline{\phi}(x)$, as desired. □

Lemma 6. *Let A be a complete and separated ring with respect to the p-adic topology, with residue ring $\tilde{K}$. Let a, b be two elements of A with coordinates $(\alpha_0, \alpha_1, \dots)$ and $(\beta_0, \beta_1, \dots)$, respectively, and let $*$ denote one of the operations $+$ or $\times$. Then $a * b$ has coordinates $(\gamma_0, \gamma_1, \dots)$, with $\gamma_i = Q_i^*(\alpha_0, \alpha_1, \dots, \beta_0, \beta_1, \dots)$ for some $Q_i^* \in \mathbb{F}_p[X_i^{p^{-n}}, X_j^{p^{-n}};\ i, j, n \geq 0]$.*

We postpone the proof of this lemma until we have enough machinery at our disposal to tackle it.

Theorem 7. *Let A and A' be rings that are separated and complete with respect to the p-adic filtration and have residue rings $\tilde{K}$ and $\tilde{K}'$, respectively. Then any homomorphism of rings $\tilde{K} \to \tilde{K}'$ comes (by reduction mod p) from a* unique *homomorphism of rings $A \to A'$.*

Proof. Let $\alpha \in A$ have coordinates $(\alpha_0, \alpha_1, \dots, \alpha_n, \dots)$. Then a homomorphism $\phi : A \to A'$ that comes (via reduction mod p) from a *given* homomorphism $\overline{\phi} : \tilde{K} \to \tilde{K}'$ must satisfy

$$\phi(\alpha) = \sum_{i=0}^{\infty} \phi \circ \iota(\alpha_i) \cdot p^i = \sum_{i=0}^{\infty} \iota_{A'} \circ \overline{\phi}(\alpha_i) \cdot p^i, \tag{3}$$

(the second equality is a consequence of Lemma 5). This gives uniqueness of ϕ. To show existence, we take (3) as the definition for ϕ and show it is a ring homomorphism.

Let a, b be two elements of A with coordinates $(\alpha_0, \alpha_1, \dots)$ and $(\beta_0, \beta_1, \dots)$, respectively. Let $*$ denote one of the operations $+$ or $\times$. Since A is a ring $a * b$ has coordinates $(\gamma_0, \gamma_1, \dots)$, for some γ_i. In other words

$$\sum_{i=0}^{\infty} \iota(\alpha_i) \cdot p^i * \sum_{i=0}^{\infty} \iota(\beta_i) \cdot p^i = \sum_{i=0}^{\infty} \iota(\gamma_i) \cdot p^i, \tag{4}$$

By (3) we have

$$g(a * b) = \sum_{i=0}^{\infty} \phi \circ \iota(\gamma_i) \cdot p^i = \sum_{i=0}^{\infty} \iota_{A'} \circ \overline{\phi}(\gamma_i) \cdot p^i.$$

On the other hand, $\overline{\phi}(a * b) = \overline{\phi}(a) * \overline{\phi}(b)$ and hence

$$\begin{aligned} g(a) * g(b) &= \sum_{i=0}^{\infty} \phi \circ \iota(\alpha_i) \cdot p^i * \sum_{i=0}^{\infty} \phi \circ \iota(\beta_i) \cdot p^i \\ &= \sum_{i=0}^{\infty} \iota_{A'} \circ \overline{\phi}(\alpha_i) \cdot p^i * \sum_{i=0}^{\infty} \iota_{A'} \circ \overline{\phi}(\beta_i) \cdot p^i \\ &= \sum_{i=0}^{\infty} \iota_{A'} \circ (\delta_i) \cdot p^i, \end{aligned}$$

where, by Lemma 6 we have

$$\delta_i = Q_i^*(\overline{\phi}(\alpha_0), \dots, \overline{\phi}(\beta_0), \dots) = \overline{\phi}(Q_i^*(\alpha_0, \dots, \beta_0, \dots)) = \overline{\phi}(\gamma_i).$$

This shows that $g(a * b) = g(a) * g(b)$, as desired. □

Corollary 8. *Given a perfect ring $\tilde{K}$ of characteristic p there is at most one ring A complete and separated with respect to the p-adic filtration with residue ring equal to $\tilde{K}$.*

Proof. Let A and A' be two rings, complete and separated with respect to the p-adic filtration, both of which have residue ring equal to $\tilde{K}$. Consider the identity isomorphism $id : \tilde{K} \to \tilde{K}$. By Theore 7 this isomorphism comes from a unique homomorphism of rings $\phi : A \to A'$ that makes the following diagram commute:

$$\begin{array}{ccc} A & \xrightarrow{\phi} & A' \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi'} \\ \tilde{K} & \xrightarrow{id} & \tilde{K} \end{array}$$

By the same token, the inverse of id (which we also denote id for obvious reasons) comes from a ring homomorphism $\phi' : A' \to A$ that makes the following diagram commute:

$$\begin{array}{ccc} A & \xleftarrow{\phi'} & A' \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi'} \\ \tilde{K} & \xleftarrow{id} & \tilde{K} \end{array}$$

We know the maps ϕ and ϕ' are unique. The commutativity of the above diagrams shows that $\phi \circ \phi' = id_A$ and $\phi' \circ \phi = id_{A'}$; the uniqueness of ϕ and ϕ' afforded by our construction shows these isomorphims are canonical. □

We refer to the ring of Corollary 8 as $W(\tilde{K})$. It may or it may not exist for a given perfect ring $\tilde{K}$ of characteristice p. The ring $W(\mathbb{F}_p)$ does exist, for example. We may take $W(\mathbb{F}_p) = \mathbb{Z}_p$ because the p-adic integers form a complete separated ring with respect to the p-adic filtration and its residue ring is $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.

We remark that if $W(\tilde{K})$ does exist, then it is canonically a $\mathbb{Z}_p$-algebra. Let $W(\tilde{K}) = A$ for convenience. Since A is complete with respect to the p-adic topology we know that

$$A \cong \varprojlim_n A/p^n A. \tag{5}$$

We may consider the ring A as a $\mathbb{Z}$-algebra and extend the unique homomorphism $f : \mathbb{Z} \to A$ to a homomorphism $\mathbb{Z}_p \to A$ via the map

$$\varprojlim_n m_n \mapsto \varprojlim_n f(m_n),$$

This map is well-defined by (5); it shows A is canonically a $\mathbb{Z}_p$-algebra.

Recall our goal is to show that $W(\tilde{K})$ exists for every perfect ring $\tilde{K}$ of characteristic p. We begin with a particular case of great importance for our purposes.

Example 2. Given a collection of indeterminates $\{X_j\}_{j\in J}$ we have the ascending chain

$$\mathbb{Z}[X_j; j \in J] \subset \mathbb{Z}[X_j^{p^{-1}}; j \in J] \subset \mathbb{Z}[X_j^{p^{-2}}; j \in J] \subset \cdots .$$

We may take the direct limit of these rings under inclusions to form a ring

$$\mathcal{A} = \bigcup_{i=0}^{\infty} \mathbb{Z}[X_j^{p^{-n}}; j \in J] =: \mathbb{Z}[X_j^{p^{-n}}; j \in J, n \geq 0].$$

Let $\mathcal{W}(X_j; j \in J; p) := \varprojlim \mathcal{A}/p^n\mathcal{A}$ be the projective limit of the quotients $\mathcal{A}/p^n\mathcal{A}$ as $n \to \infty$. We claim that

$$\mathcal{W}(X_j; j \in J; p) = W(R^{\text{perf}}(X_j; j \in J; p)),$$

that is, the ring $\mathcal{W}(X_j; j \in J; p)$ is complete and separated in the p-adic topology and its residue ring is the perfect closure of $\mathbb{F}_p[X_j; j \in J]$. The ring $\mathcal{W}(X_j; j \in J; p)$ is complete with respect to the p-adic topology by its definition (completions are complete). To show it is separated we must prove that $\bigcap p^n\mathcal{A} = 0$, but this is clear because a polynomial will be in this intersection only if its coefficients are divisible by arbitrary powers of p and $\bigcap p^n\mathbb{Z} = 0$. Finally, we must show that $\mathcal{W}/p\mathcal{W} = R^{\text{perf}}(X_j; j \in J; p)$.

Note that

$$\mathcal{W} \cong \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})[X_j^{p^{-n}}; j \in J, n \geq 0] = \mathbb{Z}_p[X_j^{p^{-n}}; j \in J, n \geq 0]$$

and so

$$\begin{aligned} \mathcal{W}/p\mathcal{W} &\cong (\mathbb{Z}_p/p\mathbb{Z}_p)[X_j^{p^{-n}}; j \in J, n \geq 0] \\ &\cong \mathbb{F}_p[X_j^{p^{-n}}; j \in J, n \geq 0] = R^{\text{perf}}(X_j; j \in J; p). \end{aligned}$$

With this example in the bag, we can now prove Lemma 6 and thus finish the proof of Theorem 7.

Proof of Lemma 6. We want to show that

$$\sum_{i=0}^{\infty} \iota(\alpha_i) \cdot p^i * \sum_{i=0}^{\infty} \iota(\beta_i) \cdot p^i = \sum_{i=0}^{\infty} \iota(\gamma_i) \cdot p^i,$$

for γ_i as above.

We begin by noting that if x and y are elements of $\mathcal{W}(X_i, Y_j;\ i,j \geq 0; p)$ then

$$x * y = \sum_{i=0}^{\infty} f(Q_i^*)p^i \quad \text{for some } Q_i^* \in \mathbb{F}_p[X_i^{p^{-n}}, X_j^{p^{-n}};\ i,j,n \geq 0]$$

because $x * y$ is an element of the ring $\mathcal{W}(X_i, Y_j;\ i,j \geq 0; p)$. There is a homomorphism

$$f : \mathbb{Z}[X_i^{p^{-n}}, Y_j^{p^{-n}};\ i,j,n \geq 0] \to A$$

which maps X_i to $\iota(\alpha_i)$ and Y_i to $\iota(\beta_i)$. We may extend this homomorphism by continuity to the completion $\mathcal{W}(X_i, Y_j;\ i,j \geq 0; p)$ so that

$$x = \sum_{i=0}^{\infty} X_i p^i \mapsto \sum_{i=0}^{\infty} \iota(\alpha_i)p^i \quad \text{and} \quad y = \sum_{i=0}^{\infty} Y_i p^i \mapsto \sum_{i=0}^{\infty} \iota(\beta_i)p^i$$

We may reduce f to a homomorphism $\bar{f} : \mathbb{F}_p[X_i^{p^{-n}}, Y_j^{p^{-n}};\ i,j,n \geq 0] \to \tilde{K}$ that takes X_i to α_i and Y_i to β_i. Then

$$\begin{aligned} \sum \iota(\alpha_i)p^i * \sum \iota(\beta_i)p^i &= f(x) * f(y) = f(x * y) \\ &= \sum f(\iota(Q_i^*))p^i = \sum \iota(\bar{f}(Q_i^*))p^i. \end{aligned}$$

□

We are almost ready to show that $W(\tilde{K})$ exists. We need the following lemma.

Lemma 9. *If $f : \tilde{K} \to \tilde{K}'$ is a surjective homomorphism of perfect rings of characteristic p, and if $W(\tilde{K})$ exists, then $W(\tilde{K}')$ also exists and is a quotient ring of $W(\tilde{K})$.*

Proof. Suppose a and b are elements of $W(\tilde{K})$ with coordinates $(\alpha_0, \alpha_1, \dots)$ and $(\beta_0, \beta_1, \dots)$, respectively. We say that a and b are equivalent and write $a \cong b$ if $f(\alpha_i) = f(\beta_i)$ for all indices i.

Note that if $a \equiv a'$ and $b \equiv b'$ then $a * b \equiv a' * b'$ by virtue of (4). This means that the quotient of A under this equivalence relation is a ring, which we label A'. Let x be an element of A' and let a be a lift of x in A with coordinates α_i. Set $\zeta_i = f(\alpha_i)$ (note the ζ_i are independent of the chosen lift). By the definition of our equivalence relation, every sequence $(\zeta_0, \zeta_1, \dots)$ of elements in $\tilde{K}'$ gives coordinates for a uniquely determined element $x \in A'$. By the definition of 'coordinates', the multiplication by p map *shifts* the coordinates of an element in A':

$$(\zeta_0, \zeta_1, \dots) \xrightarrow{p} (0, \zeta_0, \zeta_1, \dots)$$

We readily infer that p is not a zero divisor in A' and $\bigcap p^n A' = 0$, which is to say that A' is separated under the p-adic topology. Since A' is a quotient ring of a complete ring it is itself complete. Finally, we claim the residue ring of A' is $\tilde{K}'$. We need only produce an isomorphism $A'/pA' \cong \tilde{K}$. The map $x \mapsto \zeta_0$ does the trick. It is clear it is a homomorphism and that its kernel is pA'. The only problem could be surjectivity. Let ζ_0 be an element of $\tilde{K}'$. Then there is an $\alpha_0 \in \tilde{K}$ such that $f(\alpha_0) = \zeta_0$ because f is surjective by hypothesis. Then the equivalence class $x \in A'$ of any element with coordinates $(\alpha_0, \dots)$ in $\tilde{K}$ will map to ζ_0. □

We are now in a position to prove our main result.

Theorem 10. *Given a perfect ring $\tilde{K}$ of characteristic p, there exists a ring $W(\tilde{K})$ complete and separated with respect to the p-adic topology whose residue ring is $\tilde{K}$.*

Proof. If $\tilde{K}$ is of the form $\mathbb{F}_p[X_j^{p^{-n}}; j \in J, n \geq 0]$ for a set of indeterminates $\{X_j\}_{j\in J}$ then Example 2 shows we may take $W(\tilde{K}) = \mathcal{W}(X_j; j \in J; p)$.

Any perfect ring $\tilde{K}$ of characteristic p admits a surjective homomorphism

$$\phi : \mathbb{F}_p[X_j^{p^{-n}}; j \in J, n \geq 0] \to \tilde{K}$$

for some set J. Just take $J = \tilde{K}$ and send $X_j \mapsto j$ and then extend by linearity to get the desired homomorphism. Since $W(\mathbb{F}_p[X_j^{p^{-n}}; j \in J, n \geq 0])$ exists, $W(\tilde{K})$ also exists by Lemma 9. □

4 Construction of the Witt Ring: Witt Vectors

In this second half of the paper we give a construction for $W(\tilde{K})$ for a perfect field $\tilde{K}$ of prime characteristic p.

Let p be a prime number, $(X_0, X_1, \dots, X_n, \dots)$ a sequence of indeterminates. The *Witt polynomials* $(W_0, W_1, \dots, W_n, \dots)$ in $\mathbb{Z}[X_0, X_1, \dots, X_n, \dots]$ are:

$$\begin{aligned} W_0 &= X_0, \\ W_1 &= X_0^p + pX_1, \\ &\vdots \\ W_n &= X_0^{p^n} + pX_1^{p^{n-1}} + \cdots + p^n X_n, \\ &\vdots \end{aligned}$$

We claim we can express X_n as a polynomial in $W_0, W_1, \dots, W_n$ if we invert p, i.e.,

$$\mathbb{Z}[1/p][W_0, W_1, \dots, W_n, \dots] = \mathbb{Z}[1/p][X_0, X_1, \dots, X_n, \dots] \quad \text{for all } n \geq 0.$$

To see this we use induction on n. Since $W_0 = X_0$ the claim is certainly true for $n = 0$. Suppose that $X_0, \dots, X_{n-1}$ can all be expressed as polynomial in $W_0, \dots, W_{n-1}$ with coefficients in $\mathbb{Z}[1/p]$, say

$$X_i = Q_i(W_0 \dots, W_i) \quad \text{for } 0 \leq i \leq n-1.$$

Then

$$\begin{aligned} X_n &= \frac{1}{p^n}(W_n - X_0^{p^n} - pX_1^{p^{n-1}} - \cdots - p^{n-1}X_{n-1}) \\ &= \frac{1}{p^n}(W_n - Q_0^{p^n} - pQ_1^{p^{n-1}} - \cdots - p^{n-1}Q_{n-1}) \end{aligned}$$

and it is clear by induction hypothesis that this last expression is a polynomial in $\mathbb{Z}[1/p][W_0, \dots, W_n]$.

For example,

$$
\begin{aligned}
X_0 &= W_0 \\
X_1 &= \frac{1}{p}(W_1 - W_0^p), \\
X_2 &= \frac{1}{p^2}\left(W_2 - p\left[\frac{1}{p}(W_1 - W_0^p)\right]^p - W_0^{p^2}\right), \\
X_3 &= \frac{1}{p^3}\left(W_3 - p^2\left[\frac{1}{p^2}\left(W_2 - p\left[\frac{1}{p}(W_1 - W_0^p)\right]^p - W_0^{p^2}\right)\right]^p - p\left[\frac{1}{p}(W_1 - W_0^p)\right]^{p^2} - W_0^{p^3}\right), \\
X_4 &= \frac{1}{p^4}\Bigg(W_4 - p^3\Bigg[\frac{1}{p^3}\left(W_3 - p^2\left[\frac{1}{p^2}\left(W_2 - p\left[\frac{1}{p}(W_1 - W_0^p)\right]^p - W_0^{p^2}\right)\right]^p\right. \\
&\quad \left. - p\left[\frac{1}{p}(W_1 - W_0^p)\right]^{p^2} - W_0^{p^3}\right]^{p^3} - p^2\left[\frac{1}{p^3}\left(W_3 - p^2\left[\frac{1}{p^2}\left(W_2 - p\left[\frac{1}{p}(W_1 - W_0^p)\right]^p - W_0^{p^2}\right)\right]^p\right]^{p^2} \\
&\quad - p\left[\frac{1}{p}(W_1 - W_0^p)\right]^p - W_0^{p^4}\Bigg)
\end{aligned}
$$

Theorem 11. *Let $(X_0, X_1, \dots, X_n, \dots)$ and $(Y_0, Y_1, \dots, Y_n, \dots)$ be two (different!) sequences of independent indeterminates, and let X, Y be two more of these. For every polynomial $F \in \mathbb{Z}[X, Y]$ there is a sequence of polynomials*

$$F_0, F_1, \dots \in \mathbb{Z}[X_0, X_1, \dots, X_n, \dots; Y_0, Y_1, \dots, Y_n, \dots]$$

such that

$$W_n(F_0, F_1, \dots) = F(W_n(X_0, X_1, \dots, X_n), W_n(Y_0, Y_1, \dots, Y_n))$$

for all $n \geq 0$.

Proof. We follow the ideas set out in Serre's *Local Fields* (§II.6, Thm. 6). To begin, we show the polynomials F_i exist if one allows them to have coefficients in $\mathbb{Z}[1/p]$. First set $n = 0$ to get

$$F_0 = W_0(F_0) = F(W_0(X_0), W_0(Y_0)) = F(X_0, Y_0);$$

we *define* F_0 to be $F(X_0, Y_0)$. Next put $n = 1$ to get

$$F_0^p + pF_1 = W(F_0, F_1) = F(X_0^p + pX_1, Y_0^p + pY_1).$$

Then define F_1 as

$$\frac{1}{p}(F(X_0^p + pX_1, Y_0^p + pY_1) - F_0^p).$$

Proceeding inductively it is clear that the F_i exist and are unique when we allow them to have coefficients in $\mathbb{Z}[1/p]$. The trick is to show that despite appearances the coefficients are integral.

Consider the ring $\mathcal{W}(X_i, Y_j; i, j \geq 0; p)$ (which we will abbreviate by $\mathcal{W}$ for clarity) and let

$$x' = \sum_{i=0}^{\infty} X_i^{p^{-i}} p^i \quad \text{and} \quad y' = \sum_{i=0}^{\infty} Y_i^{p^{-i}} p^i.$$

We may write

$$F(x',y') = \sum_{i=0}^{\infty} \iota(\overline{\phi_i})^{p^{-i}} p^i, \quad \overline{\phi_i} \in \mathbb{F}_p[X_i^{p^{-n}}, Y_j^{p^{-n}}; i,j \geq 0;\ n \geq 0] \tag{6}$$

because $F(x',y') \in \mathcal{W}$ and $\mathcal{W} = W(\mathbb{F}_p[X_i^{p^{-n}}, Y_j^{p^{-n}}; i,j \geq 0;\ n \geq 0])$ (see Example 2).

Let ϕ_i be a representative of $\overline{\phi_i}$ in $\mathcal{W}$. We show that $F_i \equiv \phi_i \bmod p$ and F_i has integral coefficients. Begin by noting that

$$F\left(\sum_{i\leq n} X_i^{p^{-i}} p^i, \sum_{i\leq n} Y_i^{p^{-i}} p^i\right) \equiv \sum_{i\leq n} \iota(\overline{\phi_i}(X,Y))^{p^{-i}} p^i \bmod p^{n+1}.$$

Now replace X_i by $X_i^{p^n}$ and Y_i by $Y_i^{p^n}$ to get

$$F(W_n(X_0,\dots,X_n), W_n(Y_0,\dots,Y_n)) \equiv \sum_{i\leq n} \iota(\overline{\phi_i}(X_0^{p^n},\dots,Y_0^{p^n},\dots))^{p^{-i}} p^i \bmod p^{n+1}.$$

Since the coefficients of $\overline{\phi_i}$ are elements of $\mathbb{F}_p$ we know that

$$\overline{\phi_i}(X_0^{p^n},\dots,Y_0^{p^n},\dots) = \overline{\phi_i}(X_0,\dots,Y_0,\dots)^{p^n}.$$

Also, recall that multiplicative representatives commute with the p-power map, so

$$W_n(F_0,\dots,F_n) = F(W_n(X_0,\dots,X_n), W_n(Y_0,\dots,Y_n)) \equiv \sum_{i\leq n} \iota(\overline{\phi_i})^{p^{n-i}} p^i \bmod p^{n+1}.$$

Since $\iota(\overline{\phi_i}) \equiv \phi_i \bmod p$ we have $\iota(\overline{\phi_i})^{p^{n-i}} \equiv \phi_i^{p^{n-i}} \bmod p^{n-i+1}$ (see Lemma 3), and so

$$W_n(F_0,\dots,F_n) \equiv \sum_{i\leq n} \iota(\overline{\phi_i})^{p^{n-i}} p^i \bmod p^{n+1} \equiv \sum_{i\leq n} \phi_i^{p^{n-i}} p^i \equiv W_n(\phi_0,\dots,\phi_n) \bmod p^{n+1}.$$

We may now use induction to show that the F_i have integral coefficients and are congruent to $\phi_i \bmod p$. This is certainly true for F_0 as we saw above, and if it is true for all F_i with $i < n$ then

$$\begin{aligned} & W_n(F_0,\dots,F_n) \equiv W_n(\phi_0,\dots,\phi_n) \bmod p^{n+1} \\ \implies\ & F_0^{p^n} + pF_1^{p^{n-1}} + \cdots + p^n F_n \equiv \phi_0^{p^n} + p\phi_1^{p^{n-1}} + \cdots + p^n\phi_n \bmod p^{n+1} \end{aligned}$$

By inductive hypothesis $F_i \equiv \phi_i \bmod p$ for all $i < n$. Hence $p^j F_i^{p^{n-j}} \equiv p^j \phi_i^{p^{n-j}} \bmod p^{n+1}$ for $i < n$ (see Lemma 3). We conclude that

$$p^n F_n \equiv p^n \phi_n \bmod p^{n+1}$$

and so F_n has integral coefficients and $F_n \equiv \phi_n \bmod p$, as desired.

Example 3. Let $F = S(X,Y) := X + Y$. There is a sequence of polynomials $S_n := F_n$ such that

$$W_n(S_0, S_1, \dots) = W_n(X_0, X_1, \dots, X_n) + W_n(Y_0, Y_1, \dots, Y_n)$$

for all $n \geq 0$. We compute S_0, S_1 and S_2. We have

$$\begin{aligned} & W_0(S_0) = W_0(X_0) + W_0(Y_0), \\ \implies & S_0 = X_0 + Y_0. \end{aligned}$$

Next,

$$\begin{aligned} & W_1(S_0, S_1) = W_1(X_0, X_1) + W_1(Y_0, Y_1), \\ \implies & S_0^p + pS_1 = X_0^p + pX_1 + Y_0^p + pY_1, \\ \implies & S_1 = X_1 + Y_1 + \frac{X_0^p + Y_0^p - (X_0 + Y_0)^p}{p}. \end{aligned}$$

Finally,

$$\begin{aligned} & W_2(S_0, S_1, S_2) = W_2(X_0, X_1, X_2) + W_2(Y_0, Y_1, Y_2), \\ \implies & S_0^{p^2} + pS_1^p + p^2 S_2 = X_0^{p^2} + pX_1^p + p^2 X_2 + Y_0^{p^2} + pY_1^p + p^2 Y_2, \\ \implies & S_2 = X_2 + Y_2 + \frac{1}{p}\left(X_1^p + Y_1^p - S_1^p\right) + \frac{1}{p^2}(X_0^{p^2} + Y_0^{p^2} - S_0^{p^2}). \\ \implies & S_2 = X_2 + Y_2 + \frac{1}{p}\left(X_1^p + Y_1^p - \left[X_1 + Y_1 + \frac{X_0^p + Y_0^p - (X_0 + Y_0)^p}{p}\right]^p\right) \\ & \qquad + \frac{1}{p^2}(X_0^{p^2} + Y_0^{p^2} - (X_0 + Y_0)^{p^2}). \end{aligned}$$

Note that, as expected, the coefficients of S_0, S_1 and S_2 are integers since any expression of the form $(A + B)^{p^n} - A^{p^n} - B^{p^n}$ has all its coefficients divisible by p^n.

Example 4. Let $F = P(X, Y) := X \cdot Y$. There is a sequence of polynomials $P_n := F_n$ such that

$$W_n(P_0, P_1, \dots) = W_n(X_0, X_1, \dots, X_n) \cdot W_n(Y_0, Y_1, \dots, Y_n)$$

for all $n \geq 0$. We compute P_0, P_1 and P_2. We have

$$\begin{aligned} & W_0(P_0) = W_0(X_0) \cdot W_0(Y_0), \\ \implies & P_0 = X_0 \cdot Y_0. \end{aligned}$$

Next,

$$\begin{aligned} & W_1(P_0, P_1) = W_1(X_0, X_1) \cdot W_1(Y_0, Y_1), \\ \implies & P_0^p + pP_1 = (X_0^p + pX_1) \cdot (Y_0^p + pY_1), \\ \implies & P_1 = X_0^p Y_1 + X_1 Y_0^p + pX_1 Y_1. \end{aligned}$$

Finally,

$$\begin{aligned} & W_2(P_0, P_1, P_2) = W_2(X_0, X_1, X_2) \cdot W_2(Y_0, Y_1, Y_2), \\ \implies & P_0^{p^2} + pP_1^p + p^2 P_2 = (X_0^{p^2} + pX_1^p + p^2 X_2) \cdot (Y_0^{p^2} + pY_1^p + p^2 Y_2), \\ \implies & P_2 = \frac{1}{p}(X_0^{p^2} Y_1^p + X_1^p Y_0^{p^2}) + (X_0^{p^2} Y_2 + X_1^p Y_1^p + X_2 Y_0^{p^2}) \\ & \qquad + p(X_1^p Y_2 + X_2 Y_1^p) + p^2 X_2 Y_2 - \frac{1}{p} P_1^p \end{aligned}$$

Note again that, as expected, the coefficients of P_0, P_1 and P_2 are integers (the only terms with non-integral coefficients in $(1/p)P_1^p$ are $X_0^{p^2}Y_1^p$ and $X_1^pY_0^{p^2}$, and they canceled in the above sum).

Let $\mathbb{N}$ denote the non-negative integers. Let $\tilde{K}$ be a perfect ring of characteristic p. Define sum and product operations, $+$ and $\times$ on $\tilde{K}^{\mathbb{N}}$ by positing, for $a = (a_0, a_1, \dots) \in \tilde{K}^{\mathbb{N}}$ and $b = (b_0, b_1, \dots) \in \tilde{K}^{\mathbb{N}}$,

$$\begin{aligned} a + b &= (S_0(a,b), S_1(a,b), \dots) \\ \text{and } a \times b &= (P_0(a,b), P_1(a,b), \dots). \end{aligned}$$

We will show this puts a commutative ring structure on $\tilde{K}^{\mathbb{N}}$ and that $\tilde{K}^{\mathbb{N}}$ is the ring of Witt vectors over $\tilde{K}$.

Lemma 12. *Let R be any commutative ring such that p is invertible in R. The map*

$$\begin{aligned} \tau : R^{\mathbb{N}} &\to R^{\mathbb{N}} \\ (a_0, a_1, \dots) &\mapsto (W_0(a_0), W_1(a_0, a_1), \dots) \end{aligned}$$

is a bijection.

Proof. First we show injectivity. Suppose $a, b \in R^{\mathbb{N}}$ are such that $\tau(a) = \tau(b)$, so certainly $a_0 = b_0$. Assume inductively that $a_i = b_i$ for all $0 \le i \le n-1$. Then by definition of τ we'd also have $p^n a_n = p^n b_n$ and since p is invertible in R this means $a_n = b_n$. Hence τ is injective.

Now we show surjectivity. Let $b \in R^{\mathbb{N}}$ be given. Set

$$\begin{aligned} a_0 &= b_0, \\ a_1 &= \frac{1}{p}(b_1 - a_0^p), \\ a_2 &= \frac{1}{p^2}(b_2 - pa_1 - a_0^{p^2}), \\ &\vdots \end{aligned}$$

Let $a = (a_0, a_1, \dots)$. Then it is easy to see that $\tau(a) = b$. □

Now we show that with the above structure $\tilde{K}^{\mathbb{N}}$ is a commutative ring. Put $R = \mathbb{Z}[X_j; j \in J]$ and let $R' = \bigcup_{n=1}^{\infty}(1/p^n)R$ so p is invertible in R. Denote (for clarity) by $(R'^{\mathbb{N}})$ the ring of Witt vectors over R'. Then by Lemma 12 $\tau : (R'^{\mathbb{N}}) \to R'^{\mathbb{N}}$ is a bijection and it preserves $+$ and $\times$ because

$$\begin{aligned} \tau(a+b) &= \tau((S_0(a,b), S_1(a,b), \dots)) = (W_0(S_0), W_1(S_0, S_1), \dots) \\ &= (W_0(a_0), W_1(a_0, a_1), \dots) + (W_0(b_0), W_1(b_0, b_1), \dots) = \tau(a) + \tau(b) \\ \text{and } \tau(a \times b) &= \tau((P_0(a,b), P_1(a,b), \dots)) = (W_0(P_0), W_1(P_0, P_1), \dots) \\ &= (W_0(a_0), W_1(a_0, a_1), \dots) \cdot (W_0(b_0), W_1(b_0, b_1), \dots) = \tau(a) \cdot \tau(b). \end{aligned}$$

Since $R'^{\mathbb{N}}$ is a commutative ring under component-wise addition and multiplication it follows that $(R')^{\mathbb{N}}$ is a commutative ring under Witt addition and multiplication. Furthermore, since the polynomials S_i and P_i have integral coefficients for all i, it follows that the subset $R^{\mathbb{N}}$ of $(R')^{\mathbb{N}}$ is closed under addition and multiplication and is therefore a *subring* of $(R')^{\mathbb{N}}$.

The ring $\tilde{K}$ is a quotient of R by some ideal. From the canonical surjective homomorphism $R \to \tilde{K}$ we obtain a surjective homomorphism of Witt rings $R^{\mathbb{N}} \to \tilde{K}^{\mathbb{N}}$ and so $K^{\mathbb{N}}$ is also a commutative ring under Witt addition and multiplication.

We now show that the ring $K^{\mathbb{N}}$ furnished with Witt addition and multiplication is the ring of Witt vectors $W(\tilde{K})$ of $\tilde{K}$.

Theorem 13. *Let $\tilde{K}$ be a perfect ring of characteristic p. The rings $W(\tilde{K})$ and $\tilde{K}^{\mathbb{N}}$ are isomorphic.*

Proof. Let $\iota : \tilde{K} \to W(\tilde{K})$ be a multiplicative system of representatives. Let $a = (\alpha_0, \alpha_1, \dots) \in \tilde{K}^{\mathbb{N}}$ and define the map

$$\begin{aligned} \phi : \tilde{K}^{\mathbb{N}} &\to W(\tilde{K}) \\ a &\mapsto \sum_{i=0}^{\infty} \iota(\alpha_i)^{p^{-i}} p^i. \end{aligned}$$

□

Consider the special case $\tilde{K} = \mathbb{F}_p[X_i^{p^{-n}}, Y_j^{p^{-n}}; i, j, n \geq 0]$, so that $W(\tilde{K}) = \mathcal{W}(X_i, Y_j; i, j \geq 0; p)$. We claim in this case the formulas

$$\phi(a+b) = \phi(a) + \phi(b) \quad \text{and} \quad \phi(a \times b) = \phi(a) \cdot \phi(b)$$

hold when $X_i = \iota(\alpha_1)$ and $Y_i = \iota(\beta_i)$. Indeed, let $F(\phi(a), \phi(b)) = \phi(a) + \phi(b)$; then applying (6) we see that

$$\phi(a) + \phi(b) = \sum_{i=0}^{\infty} \iota(\overline{\phi_i})^{p^{-i}} p^i, \quad \text{for some } \overline{\phi_i} \in \mathbb{F}_p[X_i^{p^{-n}}, Y_j^{p^{-n}}; i, j, n \geq 0]$$

Let ϕ_i be a representative for $\overline{\phi_i}$) in $\mathcal{W}(X_i, Y_j; i, j \geq 0; p)$. We saw in the course of the proof to Theorem 11 that $\phi_i \equiv S_i \bmod p$ (here the F_i of Theorem 11 are just S_i because $F(X, Y) = X + Y$). Hence

$$\phi(a) + \phi(b) = \sum_{i=0}^{\infty} \iota(\overline{S_i})^{p^{-i}} p^i.$$

Since $\overline{S_i}$ and S_i are equal *as functions* over $\mathbb{F}_p$ we obtain

$$\phi(a) + \phi(b) = \sum_{i=0}^{\infty} \iota(S_i(a, b))^{p^{-i}} p^i = \phi(a+b).$$

A similar argument shows that $\phi(a \times b) = \phi(a) \cdot \phi(b)$ in this special case. Since our argument works for the set of indeterminates in $\tilde{K}$, the result holds for every pair of elements $a, b \in \tilde{K}^{\mathbb{N}}$, i.e., the map

$$\phi : \mathbb{F}_p[X_i^{p^{-n}}, Y_j^{p^{-n}}; i, j, n \geq 0]^{\mathbb{N}} \to \mathcal{W}(X_i, Y_j; i, j \geq 0; p)$$

is a ring homomorphism. It is clear that it is a bijection, so it is an isomorphism. □

As an example, we consider the finite field $\tilde{K} = \mathbb{F}_q$, q a power of p. We claim the Frobenius map of $\mathbb{F}_q$ lifts to a unique automorphism of $\mathbb{F}_q^{\mathbb{N}} \cong W(\mathbb{F}_q)$. The unique lift is given by

$$\begin{aligned} \psi : \mathbb{F}_q^{\mathbb{N}} &\to \mathbb{F}_q^{\mathbb{N}} \\ a = (\alpha_0, \alpha_1, \dots) &\mapsto (\alpha_0^p, \alpha_1^p, \dots). \end{aligned}$$

To see why this map is even a ring homomorphism, let us agree that $a^p = (\alpha_0^p, \alpha_1^p, \dots)$, by abuse of notation. Then

$$\begin{aligned} \psi(a+b) &= \psi((S_0(a,b), S_1(a,b), \dots)) = (S_0(a,b)^p, S_1(a,b)^p, \dots) \\ &= (S_0(a^p, b^p), S_1(a^p, b^p), \dots) = \psi(a) + \psi(b) \\ \text{and } \psi(a \times b) &= \psi((P_0(a,b), P_1(a,b), \dots)) = (P_0(a,b)^p, P_1(a,b)^p, \dots) \\ &= (P_0(a^p, b^p), P_1(a^p, b^p), \dots) = \psi(a) \times \psi(b). \end{aligned}$$

It is quite clear that ψ is a bijection (because the Frobenius map of $\mathbb{F}_q$ is a bijection) and that ψ reduces to the Frobenius map of $\mathbb{F}_q$, so it gives the desired automorphism of $\mathbb{F}_q^{\mathbb{N}}$.

It is natural to ask if the lift of the Frobenius map and the multiplication by p map are related in $W(F_q)$. To see what the relation is we introduce the *shift* map $S : W(\tilde{K}) \to W(\tilde{K})$ defined by sending the vector $(\alpha_0^p, \alpha_1^p, \dots)$ to $(0, \alpha_0^p, \alpha_1^p, \dots)$. We claim that $\psi \circ S = p$. Indeed,

$$\begin{aligned} \phi \circ \psi \circ S(\alpha_0^p, \alpha_1^p, \dots) &= \phi \circ \psi((0, \alpha_0^p, \alpha_1^p, \dots)) \\ &= \sum_{i=0}^{\infty} \iota(\alpha_i^p)^{p^{-(i+1)}} p^{i+1} \\ &= \sum_{i=0}^{\infty} \iota(\alpha_i)^{p^{-i}} p^{i+1} = p\phi(a) = \phi(pa). \end{aligned}$$

References

[1] Serre, J.-P. *Local Fields* Springer, New York, 1979.