The Theory of Witt Vectors
Joseph Rabinoff
version of 7 May 2009 (posted on arXiv as arXiv:1409.7445v1)
Errata and addenda by Darij Grinberg

I will refer to the results appearing in the note "The Theory of Witt Vectors" by the numbers under which they appear in this note (specifically, in its version of May 7th, 2009[1]).

10. Errata

- **Page 2, proof of Lemma 1.4:** Replace "$y^{p^i(p-n)}$" by "$y^{p^{i-1}(p-n)}$" (in the displayed equation, just after the binomial coefficient).
- **Page 4:** "Letting $X_1, Y_1, X_2, Y_2, \ldots$ be indeterminates" should be "Letting $X_0, X_1, X_1, Y_1, X_2, Y_2, \ldots$ be indeterminates".
- **Page 4, proof of Theorem 1.5:** Throughout the proof, the indexing of the S_i is wrong: Every "S_{p^i}" should be replaced by "S_i"; also, "S_1", "S_p" and "S_{p^n}" should be "S_0", "S_1" and "S_n", respectively.

  That said, of course, the notation you are using from §2 on is different. Maybe it is worth pointing this out, that the S_k introduced in §1 are the S_{p^k} (and not the S_k) in §2 and later.
- **Page 4, proof of Theorem 1.5:** In the last displayed equation of the proof, replace "$\tau(x_1) + p\tau(x_1)$" by "$\tau(x_0) + p\tau(x_1)$". Similarly, replace "$\tau(y_1) + p\tau(y_1)$" by "$\tau(y_0) + p\tau(y_1)$", and replace "$\tau(\widetilde{s}_1) + p\tau(\widetilde{s}_1)$" by "$\tau(\widetilde{s}_0) + p\tau(\widetilde{s}_1)$".
- **Page 7:** In the displayed equation "$w_n\left((S_n)_{n\in P}\right) = w_n\left((X_n)_{n\in P}\right) + w_n\left((Y_n)_{n\in P}\right)$", you are using the letter "n" in two different meanings (as an index and as a variable). I suggest replacing it by "$w_m\left((S_n)_{n\in P}\right) = w_m\left((X_n)_{n\in P}\right) + w_m\left((Y_n)_{n\in P}\right)$".
- **Page 7, Example 2.12:** Replace "$\sum_{i=0}^{n} p^i X_i^{p^{n-i}}$" by "$\sum_{i=0}^{n} p^i X_{p^i}^{p^{n-i}}$".
- **Page 8, Theorem 2.13:** "reprsentatives" $\to$ "representatives".
- **Page 8, proof of Theorem 2.13:** Replace "$\widetilde{x}_{p^i}$" and "$\widetilde{y}_{p^i}$" by "$\widetilde{x}_i$" and "$\widetilde{y}_i$", respectively (in the third displayed equation of this proof).

[1] This version is exactly the version that is available on the arXiv under the identifier arXiv:1409.7445v1; it also is exactly the version that used to be available at `http://www.math.harvard.edu/~rabinoff/misc/witt.pdf`.

- **Page 10, proof of Lemma 3.2:** Replace "$y_n \in \mathbf{Z}[X_1, \ldots, X_n]$" by "$y_n \in \mathbf{Z}[x_1, \ldots, x_n]$".
- **Page 10, proof of Lemma 3.2:** Replace "for some choice of $x_n \in A$" by "for some choice of $x_n \in B$".
- **Page 12, proof of Theorem 2.6:** When you say "The unicity of the ring structure on $W(A)$", it might be helpful to clarify that you are talking about the unicity of the whole functor W, not of a single ring structure $W(A)$ considered in isolation. (I don't think the latter would be unique, without the functoriality requirement.)
- **Page 12, proof of Theorem 2.6:** I think your proof is missing a part: the proof of the fact that every element of $W(A)$ has an additive inverse (one of the ring axioms). To prove this, I would again argue by functoriality (first constructing the additive inverse of the Witt vector $X = (X_1, X_2, X_3, \ldots)$ in $W(\mathbf{Q}[X_1, X_2, X_3, \ldots])$, then showing (using Lemma3.2) that its Witt coordinates belong to $\mathbf{Z}[X_1, X_2, X_3, \ldots]$, then projecting it onto $W(A)$ for any A).
- **Page 12, §3:** I think it is worth explicitly stating (as a proposition?) the fact that the bijection $x \mapsto f_x : W(A) \to \Lambda(A)$ introduced in Corollary 3.3 is a ring homomorphism. This is easy to prove[2], and used a few times in the rest of your paper.
- **Page 13, Proposition 4.5:** Replace "$s_n = \begin{cases} x_n & \text{if } x_n \neq 0 \\ y_n & \text{if } y_n \neq 0 \end{cases}$" by "$s_n = \begin{cases} x_n, & \text{if } y_n = 0; \\ y_n, & \text{if } x_n = 0 \end{cases}$". (Otherwise, you are making no claim about the case when both x_n and y_n are 0.)
- **Page 13, proof of Proposition 4.5:** "the equality of polynomial equations" → "the equality of polynomials" maybe?
- **Page 14, §5:** "Verchiebung" → "Verschiebung".
- **Page 15, Lemma 5.2:** "two natural transformations" → "two natural transformations between group-valued functors". (This is to clarify that the natural transformations have to preserve the groups' addition.)
- **Page 15, proof of Lemma 5.2:** "Let $A_n = A[X_1, X_2, \ldots, X_n]$" should be "Let $A_n = K[X_1, X_2, \ldots, X_n]$".

[2]It requires showing that $f_{xy} = f_x \widehat{\cdot} f_y$ and $f_{x+y} = f_x \widehat{+} f_y$ for any $x, y \in W(A)$ (where $\widehat{\cdot}$ and $\widehat{+}$ are the multiplication and the addition in the ring $\Lambda(A)$), and that $f_1 = 1 - t$ and $f_0 = 1$. Proving that $f_{xy} = f_x \widehat{\cdot} f_y$ for any $x, y \in W(A)$ is easy: it follows (by functoriality) from $f_{XY} = f_X \widehat{\cdot} f_Y$ (where X and Y are as in the proof of Theorem 2.6), which was proven in the proof of Theorem 2.6. Similarly, the other properties can be shown.

- **Page 15, proof of Lemma 5.2:** The notation A_n (for $K[X_1, X_2, \ldots, X_n]$) conflicts with the notation A_0 (for $K[x]$). I would suggest changing one of the two notations.
- **Page 15, proof of Lemma 5.2:** "commutivity" $\to$ "commutativity".
- **Page 19, proof of Proposition 5.10:** Remove the sentence "By Proposition 5.9, we may assume that n and m are prime" (nothing wrong about it, but it is unnecessary). Replace "Since m and n are distinct primes" by "Since m and n are relatively prime".
- **Page 19, proof of Proposition 5.12:** The letter "N" should be replaced by a (operatorname, or mathrm-shaped) "N" several times (whenever it stands for the norm map).
- **Page 19, proof of Proposition 5.12:** Replace "Now let $n > 1$" by "Now let $n \geq 1$".
- **Page 20, Theorem 5.14:** "reprsentatives" $\to$ "representatives".
- **Page 21, proof of Theorem 5.14:** Replace all three summation signs by "$\sum_{n=0}^{\infty}$".
- **Page 22, proof of Theorem 6.1:** Replace "$\sigma_m(y)$" by "$\sigma_m(x)$" (after "so by induction").
- **Page 22, proof of Theorem 6.1:** Replace "$\sigma_n(y) = \sigma_{p_i}(y) \circ \sigma_m(y)$" by "$\sigma_n(x) = \sigma_{p_i}(\sigma_m(x))$".
- **Page 22, proof of Theorem 6.1:** Replace "$\sigma_n(y) \equiv$" by "$\sigma_n(x) \equiv$" (twice).
- **Page 22, proof of Theorem 6.1:** Replace "$\sigma_n(y) -$" by "$\sigma_n(x) -$".
- **Page 24, §7:** Replace "since is difficult" by "since it is difficult".
- **Page 25, proof of Lemma 7.3:** In the first displayed equation of this proof, add a "x" addend on the left hand side (the sum should start with x, not with $\frac{x^p}{p}$).
- **Page 25, proof of Lemma 7.3:** Replace "x^{p^n} coefficient" by "x^{p^n}-coefficient".
- **Page 25, proof of Lemma 7.3:** After "$p \nmid s$", add "and $s > 1$".
- **Page 26, proof of Lemma 7.4:** Replace "a pth power" by "a power of p" (twice).
- **Page 26, Lemma 7.5:** Replace "$\prod_{r \geq 1}$" by "$\prod_{r \geq 0}$".

- **Page 26, Lemma 7.5:** I would suggest clarifying that the product $\prod\limits_{r\geq 0} \operatorname{hexp}\left(x_{p^r} t^{p^r}\right)$ is taken in $A\left[\left[t\right]\right]$, not in $\Lambda\left(A\right)$.
- **Page 26, proof of Lemma 7.5:** Replace every appearance of "$\prod\limits_{r\geq 1}$", "$\prod\limits_{n\geq 1}$" or "$\prod\limits_{m\geq 1}$" by "$\prod\limits_{r\geq 0}$", "$\prod\limits_{n\geq 0}$" or "$\prod\limits_{m\geq 0}$", respectively.
- **Page 27, Theorem 7.6:** Replace "$\prod\limits_{r\geq 1}$" by "$\prod\limits_{r\geq 0}$".
- **Page 27, Theorem 7.6:** I would suggest clarifying that the product $\prod\limits_{r\geq 0} \operatorname{hexp}\left(x_{p^r} t^{p^r}\right)$ is taken in $A\left[\left[t\right]\right]$, not in $\Lambda\left(A\right)$.
- **Page 27:** In "every element of $\widehat{\Lambda}\left(\mathcal{N}\right) := 1 + \mathcal{N}\left[t\right]$ can be written uniquely as a finite product $\prod\left(1 - a_n t^n\right)$", I would replace the product sign "$\prod$" by "$\prod\limits_{n=0}^{\infty}$" (as the reader would otherwise expect $\prod\limits_{n=1}^{\infty}$ instead). (Alternatively, you can replace it by "$\prod\limits_{n=1}^{\infty}$", but then you'd need to replace "$\widehat{\Lambda}\left(\mathcal{N}\right) := 1 + \mathcal{N}\left[t\right]$" by "$\widehat{\Lambda}\left(\mathcal{N}\right) := 1 + t\mathcal{N}\left[t\right]$".)

11. Addenda

Let me now add some further properties of Witt vectors.

I shall use the notations of §2–§7 of your notes. In particular, the Witt polynomials w_n will be defined as in Definition 2.4 (not as in §1): namely, by

$$w_n = \sum_{d\mid n} d X_d^{n/d} \in \mathbf{Z}\left[\left\{X_d : d \mid n\right\}\right].$$

Thus, if p is a prime and if n is a nonnegative integer, then the definition of w_{p^n} yields

$$w_{p^n} = \sum_{d\mid p^n} d X_d^{p^n/d} = \sum_{i=0}^{n} p^i X_{p^i}^{p^{n-i}} \tag{1}$$

(since the positive divisors of p^n are $p^0, p^1, \ldots, p^n$).

Sam Raskin has pointed out to me that Theorem 6.6 can be generalized: namely, the condition that L be perfect can be dropped from the definition of a p-ring. In other words, the following holds:

Theorem 11.1. Let p be a prime. Let R be a ring equipped with a decreasing sequence $R = \mathfrak{a}_0 \supset \mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \mathfrak{a}_3 \supset \cdots$ of ideals such that ($\mathfrak{a}_n \cdot \mathfrak{a}_m \subset \mathfrak{a}_{n+m}$ for all $n \geq 0$ and $m \geq 0$). Equip R with the topology defined by this sequence of ideals. Assume that R is Hausdorff and complete for this

topology. Assume that the residue ring $L = R/\mathfrak{a}_1$ has $p \cdot 1_L = 0$. Let π denote the canonical projection $R \to R/\mathfrak{a}_1 = L$.

Let K be a perfect ring of characteristic p. Let $f : K \to L$ be a ring homomorphism.

There exists a unique continuous ring homomorphism $\theta : W_p(K) \to R$ making the square

$$\begin{array}{ccc} W_p(K) & \xrightarrow{\theta} & R \\ {\scriptstyle w_1}\downarrow & & \downarrow{\scriptstyle \pi} \\ K & \xrightarrow{f} & L \end{array} \tag{2}$$

commute.

Theorem 11.1 generalizes your Theorem 6.6.

The proof of Theorem 11.1 given below is (at least on a superficial level) quite different from your proof of Theorem 6.6; it is inspired by the proof of [BriCon09, Lemma 4.4.1] (thanks again to Sam Raskin for the reference).[3]

Before I prove Theorem 11.1, let me derive various facts that will be used in its proof and (some of which) are of independent interest:

Proposition 11.2. Let R be a ring equipped with a decreasing sequence $R = \mathfrak{a}_0 \supset \mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \mathfrak{a}_3 \supset \cdots$ of ideals such that ($\mathfrak{a}_n \cdot \mathfrak{a}_m \subset \mathfrak{a}_{n+m}$ for all $n \geq 0$ and $m \geq 0$). Equip R with the topology defined by this sequence of ideals. Assume that R is Hausdorff for this topology.

(a) We have $\bigcap\limits_{n \geq 0} \mathfrak{a}_n = 0$.

(b) If u and v are two elements of R such that every $i \geq 0$ satisfies $u \equiv v \bmod \mathfrak{a}_i$, then $u = v$.

(c) For every $n \geq 0$, let π_n be the canonical projection $R \to R/\mathfrak{a}_n$.

Let A be a set, and let $\varphi : A \to R$ and $\psi : A \to R$ be two maps. Assume that $\pi_n \circ \varphi = \pi_n \circ \psi$ for every $n \geq 0$. Then, $\varphi = \psi$.

Proof of Proposition 11.2. Recall the definition of the topology on R: A subset S of R is said to be open if and only if for every $s \in S$, there exists an $n \geq 0$ satisfying $s + \mathfrak{a}_n \subset S$.

(a) Let $u \in \bigcap\limits_{n \geq 0} \mathfrak{a}_n$. We shall show that $u = 0$.

Let P be an open subset of R containing u. Let Q be an open subset of R containing 0. (We shall not use the fact that Q is open.)

The subset P of R is open. In other words, for every $s \in P$, there exists an $n \geq 0$ satisfying $s + \mathfrak{a}_n \subset P$ (by the definition of the topology on R). Applying this to $s = u$, we conclude that there exists an $n \geq 0$ satisfying $u + \mathfrak{a}_n \subset P$. Let p be this n. Thus, $p \geq 0$ satisfies $u + \mathfrak{a}_p \subset P$.

[3] As far as I recall, I devised this proof based on discussions with Sam Raskin at MIT in 2016. Sam seems to have a cleaner and shorter proof, which I unfortunately have never had the time to fully comprehend. Sorry, Sam, for making a mess of your ideas!

On the other hand, $0 \in Q$ (since Q contains 0).

But $u \in \bigcap_{n \geq 0} \mathfrak{a}_n \subset \mathfrak{a}_p$ and thus $u \equiv 0 \bmod \mathfrak{a}_p$. Hence, $0 \equiv u \bmod \mathfrak{a}_p$. In other words, $0 \in u + \mathfrak{a}_p \subset P$. Combining this with $0 \in Q$, we obtain $0 \in P \cap Q$. Hence, the set $P \cap Q$ contains at least one element (namely, 0). Thus, $P \cap Q \neq \varnothing$.

Now, forget that we fixed P and Q. We thus have shown that if P is an open subset of R containing u, and if Q is an open subset of R containing 0, then $P \cap Q \neq \varnothing$. Since the topological space R is Hausdorff, this shows that $u = 0$.

Now, forget that we fixed u. We thus have proven that every $u \in \bigcap_{n \geq 0} \mathfrak{a}_n$ satisfies $u = 0$. In other words, $\bigcap_{n \geq 0} \mathfrak{a}_n = 0$. This proves Proposition 11.2 **(a)**.

(b) Let u and v be two elements of R such that every $i \geq 0$ satisfies $u \equiv v \bmod \mathfrak{a}_i$. Hence, every $i \geq 0$ satisfies $u - v \in \mathfrak{a}_i$ (since $u \equiv v \bmod \mathfrak{a}_i$). In other words, $u - v \in \bigcap_{i \geq 0} \mathfrak{a}_i = \bigcap_{n \geq 0} \mathfrak{a}_n = 0$ (by Proposition 11.2 **(a)**). In other words, $u - v = 0$, so that $u = v$. This proves Proposition 11.2 **(b)**.

(c) Let $a \in A$. Let $n \geq 0$. Then, $\pi_n(\varphi(a)) = \underbrace{(\pi_n \circ \varphi)}_{=\pi_n \circ \psi}(a) = (\pi_n \circ \psi)(a) = \pi_n(\psi(a))$. Since π_n is the canonical projection $R \to R/\mathfrak{a}_n$, this rewrites as $\varphi(a) \equiv \psi(a) \bmod \mathfrak{a}_n$. In other words, $\varphi(a) - \psi(a) \in \mathfrak{a}_n$.

Now, forget that we fixed n. We thus have proven that $\varphi(a) - \psi(a) \in \mathfrak{a}_n$ for each $n \geq 0$. Hence, $\varphi(a) - \psi(a) \in \bigcap_{n \geq 0} \mathfrak{a}_n = 0$ (by Proposition 11.2 **(a)**), so that $\varphi(a) - \psi(a) = 0$ and thus $\varphi(a) = \psi(a)$.

Now, forget that we fixed a. We have now shown that $\varphi(a) = \psi(a)$ for each $a \in A$. In other words, $\varphi = \psi$. This proves Proposition 11.2 **(c)**. □

Proposition 11.3. Let R be a ring equipped with a decreasing sequence $R = \mathfrak{a}_0 \supset \mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \mathfrak{a}_3 \supset \cdots$ of ideals such that ($\mathfrak{a}_n \cdot \mathfrak{a}_m \subset \mathfrak{a}_{n+m}$ for all $n \geq 0$ and $m \geq 0$). Equip R with the topology defined by this sequence of ideals. Assume that R is Hausdorff for this topology. For every $n \geq 0$, let π_n be the canonical projection $R \to R/\mathfrak{a}_n$.

Let A be a ring. Let $\gamma : A \to R$ be a map. Assume that the map $\pi_n \circ \gamma : A \to R/\mathfrak{a}_n$ is a ring homomorphism for each $n \geq 0$. Then, the map γ is a ring homomorphism.

Proof of Proposition 11.3. We need to show the following four claims:

Claim 1: We have $\gamma(0_A) = 0_R$.

Claim 2: We have $\gamma(a) + \gamma(b) = \gamma(a + b)$ for any $a \in A$ and $b \in A$.

Claim 3: We have $\gamma(1_A) = 1_R$.

Claim 4: We have $\gamma(a)\gamma(b) = \gamma(ab)$ for any $a \in A$ and $b \in A$.

We shall only prove Claim 4; all the other three claims can be proven in the same vein.

Proof of Claim 4: Let $a \in A$ and $b \in A$. Let n be a nonnegative integer. Then, the map $\pi_n \circ \gamma : A \to R/\mathfrak{a}_n$ is a ring homomorphism (by our assumption). Thus, $(\pi_n \circ \gamma)(a) \cdot (\pi_n \circ \gamma)(b) = (\pi_n \circ \gamma)(ab)$.

Now, recall that π_n is the canonical projection $R \to R/\mathfrak{a}_n$, and thus a ring homomorphism. Hence,

$$\begin{aligned}\pi_n\left(\gamma\left(a\right)\gamma\left(b\right)\right) &= \underbrace{\pi_n\left(\gamma\left(a\right)\right)}_{=(\pi_n\circ\gamma)(a)} \cdot \underbrace{\pi_n\left(\gamma\left(b\right)\right)}_{=(\pi_n\circ\gamma)(b)} = \left(\pi_n\circ\gamma\right)\left(a\right)\cdot\left(\pi_n\circ\gamma\right)\left(b\right) \\ &= \left(\pi_n\circ\gamma\right)\left(ab\right) = \pi_n\left(\gamma\left(ab\right)\right).\end{aligned}$$

In other words, $\gamma\left(a\right)\gamma\left(b\right) \equiv \gamma\left(ab\right) \bmod \mathfrak{a}_n$ (since π_n is the canonical projection $R \to R/\mathfrak{a}_n$). In other words, $\gamma\left(a\right)\gamma\left(b\right) - \gamma\left(ab\right) \in \mathfrak{a}_n$.

Now, forget that we fixed n. We thus have shown that $\gamma\left(a\right)\gamma\left(b\right) - \gamma\left(ab\right) \in \mathfrak{a}_n$ for every $n \geq 0$. Thus, $\gamma\left(a\right)\gamma\left(b\right) - \gamma\left(ab\right) \in \bigcap\limits_{n\geq 0} \mathfrak{a}_n = 0$ (by Proposition 11.2 **(a)**). In other words, $\gamma\left(a\right)\gamma\left(b\right) - \gamma\left(ab\right) = 0$, so that $\gamma\left(a\right)\gamma\left(b\right) = \gamma\left(ab\right)$. This proves Claim 4.

As we have said, the Claims 1, 2 and 3 can be shown by analogous arguments. Thus, all four claims are proven, and the proof of Proposition 11.3 is complete. □

Proposition 11.4. Let R be a ring equipped with a decreasing sequence $R = \mathfrak{a}_0 \supset \mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \mathfrak{a}_3 \supset \cdots$ of ideals such that ($\mathfrak{a}_n \cdot \mathfrak{a}_m \subset \mathfrak{a}_{n+m}$ for all $n \geq 0$ and $m \geq 0$). Equip R with the topology defined by this sequence of ideals. For every $n \geq 0$, let π_n be the canonical projection $R \to R/\mathfrak{a}_n$.

Let A be a topological space. Let $\varphi : A \to R$ be a map. Assume that for each $n \geq 0$, the map $\pi_n \circ \varphi : A \to R/\mathfrak{a}_n$ is continuous (where $R/\mathfrak{a}_n$ is equipped with the discrete topology). Then, the map $\varphi : A \to R$ is continuous.

Proof of Proposition 11.4. Recall the definition of the topology on R: A subset S of R is said to be open if and only if for every $s \in S$, there exists an $n \geq 0$ satisfying $s + \mathfrak{a}_n \subset S$.

Let U be an open subset of R. We shall show that the subset $\varphi^{-1}\left(U\right)$ of A is open.

Indeed, let $t \in \varphi^{-1}\left(U\right)$ be arbitrary. Thus, $\varphi\left(t\right) \in U$.

The subset U of R is open. In other words, for every $s \in U$, there exists an $n \geq 0$ satisfying $s + \mathfrak{a}_n \subset U$ (by the definition of the topology on R). Applying this to $s = \varphi\left(t\right)$, we conclude that there exists an $n \geq 0$ satisfying $\varphi\left(t\right) + \mathfrak{a}_n \subset U$. Consider this n.

Consider the set $R/\mathfrak{a}_n$ as a topological space, equipped with the discrete topology. Then, each subset of $R/\mathfrak{a}_n$ is open. In particular, the subset $\left\{\pi_n\left(\varphi\left(t\right)\right)\right\}$ of $R/\mathfrak{a}_n$ is open.

By our assumption, the map $\pi_n \circ \varphi : A \to R/\mathfrak{a}_n$ is continuous. Thus, for each open subset Q of $R/\mathfrak{a}_n$, the subset $\left(\pi_n \circ \varphi\right)^{-1}\left(Q\right)$ of A is open. Applying this to $Q = \left\{\pi_n\left(\varphi\left(t\right)\right)\right\}$, we conclude that the subset $\left(\pi_n \circ \varphi\right)^{-1}\left(\left\{\pi_n\left(\varphi\left(t\right)\right)\right\}\right)$ of A is open (since the subset $\left\{\pi_n\left(\varphi\left(t\right)\right)\right\}$ of $R/\mathfrak{a}_n$ is open). Denote this subset

$(\pi_n \circ \varphi)^{-1}(\{\pi_n(\varphi(t))\})$ by G. Thus, $G = (\pi_n \circ \varphi)^{-1}(\{\pi_n(\varphi(t))\})$ is an open subset of A.

Furthermore, $G \subset \varphi^{-1}(U)$ [4] and $t \in G$ [5]. Hence, G is an open neighborhood of t (since G is open and satisfies $t \in G$) and is a subset of $\varphi^{-1}(U)$ (since $G \subset \varphi^{-1}(U)$). We thus have shown that there exists some open neighborhood of t that is a subset of $\varphi^{-1}(U)$ (namely, G).

Now, forget that we fixed t. We have now proven that for each $t \in \varphi^{-1}(U)$, there exists some open neighborhood of t that is a subset of $\varphi^{-1}(U)$. This means that the subset $\varphi^{-1}(U)$ of A is open (by one of the criteria for openness).

Now, forget that we fixed U. We thus have shown that if U is an open subset of R, then the subset $\varphi^{-1}(U)$ of A is open. In other words, the map $\varphi : A \to R$ is continuous. This proves Proposition 11.4. □

Proposition 11.5. Let p be a positive integer. Let R be a ring equipped with a decreasing sequence $R = \mathfrak{a}_0 \supset \mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \mathfrak{a}_3 \supset \cdots$ of ideals such that

$$(\mathfrak{a}_n \cdot \mathfrak{a}_m \subset \mathfrak{a}_{n+m} \text{ for all } n \geq 0 \text{ and } m \geq 0). \tag{3}$$

Assume that the residue ring $L = R/\mathfrak{a}_1$ has $p \cdot 1_L = 0$.

(a) We have $\mathfrak{a}_1^n \subset \mathfrak{a}_n$ for every $n \geq 0$.

(b) We have $p \cdot 1_R \in \mathfrak{a}_1$ and $pR \subset \mathfrak{a}_1$.

(c) We have $p^n \cdot 1_R \in \mathfrak{a}_n$ for every $n \geq 0$.

(d) If x and y are two elements of R satisfying $x \equiv y \bmod \mathfrak{a}_1$, then

$$x^{p^i} \equiv y^{p^i} \bmod \mathfrak{a}_{i+1} \qquad \text{for every } i \geq 0.$$

(e) Every $u \in \mathfrak{a}_1$, every $n \geq 0$ and every $i \in \{0, 1, \ldots, n\}$ satisfy $p^i u^{p^{n-i}} \in \mathfrak{a}_n$.

(f) If a and b are two elements of R and i is a positive integer satisfying $a \equiv b \bmod \mathfrak{a}_i$, then

$$a^p \equiv b^p \bmod \mathfrak{a}_{i+1}.$$

(g) We have $p\mathfrak{a}_{n-1} \subset \mathfrak{a}_n$ for every positive integer n.

Proof of Proposition 11.5. **(a)** Using (3), we can easily prove Proposition 11.5 **(a)** (by induction on n). (The induction base follows from $\mathfrak{a}_1^0 \subset R = \mathfrak{a}_0$.)

(b) We have $p \cdot 1_R \in \mathfrak{a}_1$ (since the projection of $p \cdot 1_R$ onto $R/\mathfrak{a}_1 = L$ is $p \cdot 1_L = 0$) and thus $pR = \underbrace{(p \cdot 1_R)}_{\in \mathfrak{a}_1} R \subset \mathfrak{a}_1 R \subset \mathfrak{a}_1$ (since $\mathfrak{a}_1$ is an ideal of R). This proves

[4] *Proof.* Let $g \in G$. Thus, $g \in G = (\pi_n \circ \varphi)^{-1}(\{\pi_n(\varphi(t))\})$. Hence, $(\pi_n \circ \varphi)(g) \in \{\pi_n(\varphi(t))\}$, so that $(\pi_n \circ \varphi)(g) = \pi_n(\varphi(t))$. Hence, $\pi_n(\varphi(t)) = (\pi_n \circ \varphi)(g) = \pi_n(\varphi(g))$. In other words, $\varphi(t) \equiv \varphi(g) \bmod \mathfrak{a}_n$ (since π_n is the canonical projection $R \to R/\mathfrak{a}_n$). Thus, $\varphi(g) \in \varphi(t) + \mathfrak{a}_n \subset U$. Hence, $g \in \varphi^{-1}(U)$.

Now, forget that we fixed g. We thus have proven that $g \in \varphi^{-1}(U)$ for each $g \in G$. In other words, $G \subset \varphi^{-1}(U)$.

[5] *Proof.* We have $(\pi_n \circ \varphi)(t) = \pi_n(\varphi(t)) \in \{\pi_n(\varphi(t))\}$ and thus $t \in (\pi_n \circ \varphi)^{-1}(\{\pi_n(\varphi(t))\}) = G$.

Proposition 11.5 **(b)**.

(c) We have $p^n \cdot 1_R = \left(\underbrace{p \cdot 1_R}_{\in \mathfrak{a}_1} \right)^n \in \mathfrak{a}_1^n \subset \mathfrak{a}_n$ (by Proposition 11.5 **(a)**) for every $n \geq 0$. This proves Proposition 11.5 **(c)**.

(g) Let n be a positive integer. Proposition 11.5 **(b)** yields $pR \subset \mathfrak{a}_1$. Now, $p \underbrace{\mathfrak{a}_{n-1}}_{\subset R\mathfrak{a}_{n-1}} \subset \underbrace{pR}_{\subset \mathfrak{a}_1} \mathfrak{a}_{n-1} \subset \mathfrak{a}_1 \cdot \mathfrak{a}_{n-1} \subset \mathfrak{a}_n$ (by (3), applied to 1 and $n-1$ instead of n and m). This proves Proposition 11.5 **(g)**.

(f) Let a and b be two elements of R, and let i be a positive integer satisfying $a \equiv b \bmod \mathfrak{a}_i$.

Since i is a positive integer, we have $i \geq 1$. Thus, $\mathfrak{a}_i \subset \mathfrak{a}_1$ (since $\mathfrak{a}_0 \supset \mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \mathfrak{a}_3 \supset \cdots$).

Proposition 11.5 **(b)** yields $p \cdot 1_R \in \mathfrak{a}_1$ and $pR \subset \mathfrak{a}_1$.

It is well-known that every $u \in R$ and $v \in R$ and $g \geq 0$ satisfy

$$u^g - v^g = (u - v) \left(\sum_{k=0}^{g-1} u^k v^{g-1-k} \right). \tag{4}$$

But $a \equiv b \bmod \mathfrak{a}_i$. Hence, $a - b \in \mathfrak{a}_i \subset \mathfrak{a}_1$, so that $a \equiv b \bmod \mathfrak{a}_1$. Also,

$$\sum_{k=0}^{p-1} \underbrace{a^k}_{\substack{\equiv b^k \bmod \mathfrak{a}_1 \\ (\text{since } a \equiv b \bmod \mathfrak{a}_1)}} b^{p-1-k} \equiv \sum_{k=0}^{p-1} \underbrace{b^k b^{p-1-k}}_{=b^{p-1}} = \sum_{k=0}^{p-1} b^{p-1} = p b^{p-1}$$

$$= \underbrace{p \cdot 1_R}_{\substack{\equiv 0 \bmod \mathfrak{a}_1 \\ (\text{since } p \cdot 1_R \in \mathfrak{a}_1)}} \quad b^{p-1} \equiv 0 \bmod \mathfrak{a}_1;$$

thus, $\sum_{k=0}^{p-1} a^k b^{p-1-k} \in \mathfrak{a}_1$. Now, (4) (applied to $a = u$, $b = v$ and $g = p$) yields

$$a^p - b^p = \underbrace{(a-b)}_{\in \mathfrak{a}_i} \underbrace{\left(\sum_{k=0}^{p-1} a^k b^{p-1-k} \right)}_{\in \mathfrak{a}_1} \in \mathfrak{a}_i \mathfrak{a}_1 \subset \mathfrak{a}_{i+1}$$

(by (3), applied to $n = i$ and $m = 1$). In other words, $a^p \equiv b^p \bmod \mathfrak{a}_{i+1}$. This proves Proposition 11.5 **(f)**.

(d) Proposition 11.5 **(d)** can be proven by induction over i, similarly to the proof of Lemma 1.4. However, let me sketch a slightly different proof, for the sake of diversity. We proceed by induction over i. The case of $i = 0$ is obvious. The induction step proceeds as follows: Let $i \geq 1$, and assume that $x^{p^{i-1}} \equiv y^{p^{i-1}} \bmod \mathfrak{a}_i$. We must show that $x^{p^i} \equiv y^{p^i} \bmod \mathfrak{a}_{i+1}$.

Set $a = x^{p^{i-1}}$ and $b = y^{p^{i-1}}$. Then, $a = x^{p^{i-1}} \equiv y^{p^{i-1}} = b \bmod \mathfrak{a}_i$. Hence, Proposition 11.5 **(f)** yields $a^p \equiv b^p \bmod \mathfrak{a}_{i+1}$. Since $a = x^{p^{i-1}}$, we have $a^p = \left(x^{p^{i-1}}\right)^p = x^{p^i}$. Similarly, $b^p = y^{p^i}$. Thus, $x^{p^i} = a^p \equiv b^p = y^{p^i} \bmod \mathfrak{a}_{i+1}$. This completes the induction step; thus, Proposition 11.5 **(d)** is proven.

(e) Let $u \in \mathfrak{a}_1$, $n \geq 0$ and $i \in \{0, 1, \ldots, n\}$. We have $u \in \mathfrak{a}_1$, so that $u \equiv 0 \bmod \mathfrak{a}_1$. Thus, Proposition 11.5 **(d)** (applied to u, 0 and $n-i$ instead of x, y and i) yields $u^{p^{n-i}} \equiv 0^{p^{n-i}} = 0 \bmod \mathfrak{a}_{(n-i)+1}$ (since p^{n-i} is a positive integer). Thus, $u^{p^{n-i}} \in \mathfrak{a}_{(n-i)+1} \subset \mathfrak{a}_{n-i}$. Now,

$$p^i \underbrace{u^{p^{n-i}}}_{\in \mathfrak{a}_{n-i} \subset R\mathfrak{a}_{n-i}} \in \underbrace{p^i R}_{= p^i \cdot 1_R R} \mathfrak{a}_{n-i} = \underbrace{p^i \cdot 1_R}_{\substack{\in \mathfrak{a}_i \\ \text{(by Proposition 11.5 (c),} \\ \text{applied to } i \text{ instead of } n\text{)}}} R\mathfrak{a}_{n-i}$$

$$\subset \mathfrak{a}_i \underbrace{R\mathfrak{a}_{n-i}}_{\substack{\subset \mathfrak{a}_{n-i} \\ \text{(since } \mathfrak{a}_{n-i} \text{ is an} \\ \text{ideal of } R\text{)}}} \subset \mathfrak{a}_i \mathfrak{a}_{n-i} \subset \mathfrak{a}_n$$

(by (3), applied to i and $n-i$ instead of n and m). This proves Proposition 11.5 **(e)**. □

The following proposition is just the fundamental theorem on homomorphisms (in a slight disguise):

Proposition 11.6. Let A, B and C be three rings. Let $\varphi : A \to B$ be a surjective ring homomorphism. Let $\psi : A \to C$ be a ring homomorphism such that $\psi(\operatorname{Ker} \varphi) = 0$. Then, there exists a unique ring homomorphism $\zeta : B \to C$ such that $\zeta \circ \varphi = \psi$.

Proof of Proposition 11.6. The surjective ring homomorphism $\varphi : A \to B$ induces a canonical ring isomorphism $B \cong A / \operatorname{Ker} \varphi$. Thus, the ring B and the ring homomorphism $\varphi : A \to B$ satisfy the universal property of the quotient $A / \operatorname{Ker} \varphi$. But this is precisely the statement of Proposition 11.6. □

Proposition 11.7. Let p be a prime. Let R be a ring equipped with a decreasing sequence $R = \mathfrak{a}_0 \supset \mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \mathfrak{a}_3 \supset \cdots$ of ideals such that ($\mathfrak{a}_n \cdot \mathfrak{a}_m \subset \mathfrak{a}_{n+m}$ for all $n \geq 0$ and $m \geq 0$). Assume that the residue ring $L = R/\mathfrak{a}_1$ has $p \cdot 1_L = 0$. Let π denote the canonical projection $R \to R/\mathfrak{a}_1 = L$. For every $n \geq 0$, let π_n be the canonical projection $R \to R/\mathfrak{a}_n$.

Let $n \geq 0$. There exists a unique ring homomorphism $\widetilde{w}_{p^n} : W_p(L) \to R/\mathfrak{a}_n$ such that the diagram

$$\begin{array}{ccc} W_p(R) & \xrightarrow{w_{p^n}} & R \\ {\scriptstyle W_p(\pi)}\downarrow & & \downarrow{\scriptstyle \pi_n} \\ W_p(L) & \xrightarrow[\widetilde{w}_{p^n}]{} & R/\mathfrak{a}_n \end{array} \tag{5}$$

commutes.

Proof of Proposition 11.7. The map $\pi : R \to L$ is surjective (being a projection). Hence, the map $W_p(\pi) : W_p(R) \to W_p(L)$ is also surjective[6]. Furthermore, this map $W_p(\pi)$ is a ring homomorphism (since π is a ring homomorphism).

Now, let $x \in \operatorname{Ker}\left(W_p(\pi)\right)$. We are going to show that $w_{p^n}(x) \in \mathfrak{a}_n$.

Indeed, the definition of $W_p(\pi)$ yields

$$\left(W_p(\pi)\right)(x) = \left(\pi\left(x_m\right)\right)_{m \in P_p}.$$

Hence, $\left(\pi\left(x_m\right)\right)_{m \in P_p} = \left(W_p(\pi)\right)(x) = 0$ (since $x \in \operatorname{Ker}\left(W_p(\pi)\right)$). In other words, $\pi\left(x_m\right) = 0$ for every $m \in P_p$. In other words,

$$x_m \in \mathfrak{a}_1 \qquad \text{for every } m \in P_p \tag{6}$$

(because π is the canonical projection $R \to R/\mathfrak{a}_1$, and therefore the equality $\pi\left(x_m\right) = 0$ means that $x_m \in \mathfrak{a}_1$).

Every $i \in \{0, 1, \ldots, n\}$ satisfies $p^i \in P_p$ and thus $x_{p^i} \in \mathfrak{a}_1$ (by (6), applied to $m = p^i$), so that

$$p^i x_{p^i}^{p^{n-i}} \in \mathfrak{a}_n \tag{7}$$

(by Proposition 11.5 **(e)**, applied to $u = x_{p^i}$).

From (1), we obtain

$$w_{p^n}(x) = \sum_{i=0}^{n} \underbrace{p^i x_{p^i}^{p^{n-i}}}_{\substack{\in \mathfrak{a}_n \\ \text{(by (7))}}} \in \sum_{i=0}^{n} \mathfrak{a}_n \subset \mathfrak{a}_n.$$

Thus, $\pi_n\left(w_{p^n}(x)\right) = 0$ (since π_n is the canonical projection $R \to R/\mathfrak{a}_n$). Hence, $\left(\pi_n \circ w_{p^n}\right)(x) = \pi_n\left(w_{p^n}(x)\right) = 0$.

Now, forget that we fixed x. We thus have shown that

$$\left(\pi_n \circ w_{p^n}\right)(x) = 0 \qquad \text{for every } x \in \operatorname{Ker}\left(W_p(\pi)\right).$$

In other words,

$$\left(\pi_n \circ w_{p^n}\right)\left(\operatorname{Ker}\left(W_p(\pi)\right)\right) = 0.$$

[6] *Proof.* Recall that $W_p(R) = R^{P_p}$ (as sets) and $W_p(L) = L^{P_p}$ (as sets). The map $W_p(\pi)$ is defined by

$$W_p(\pi)\left(\left(a_n\right)_{n \in P_p}\right) = \left(\pi\left(a_n\right)\right)_{n \in P_p} \qquad \text{for every } \left(a_n\right)_{n \in P_p} \in W_p(R).$$

In other words, the map $W_p(\pi) : W_p(R) \to W_p(L)$ is identical with the map $\prod_{q \in P_p} \pi : R^{P_p} \to L^{P_p}$. But the latter map is clearly surjective (since the map π is surjective). Hence, the former map is surjective. Qed.

On the other hand, $w_{p^n} : W_p(R) \to R$ is a ring homomorphism (by Theorem 2.6 **(ii)**, applied to R, P_p and p^n instead of A, P and n). The map $\pi_n : R \to R/\mathfrak{a}_n$ also is a ring homomorphism (being the canonical projection). Hence, the map $\pi_n \circ w_{p^n} : W_p(R) \to R/\mathfrak{a}_n$ is a ring homomorphism (being the composition of two ring homomorphisms).

Thus, Proposition 11.6 (applied to $A = W_p(R)$, $B = W_p(L)$, $C = R/\mathfrak{a}_n$, $\varphi = W_p(\pi)$ and $\psi = \pi_n \circ w_{p^n}$) yields that there exists a unique ring homomorphism $\zeta : W_p(L) \to R/\mathfrak{a}_n$ such that $\zeta \circ W_p(\pi) = \pi_n \circ w_{p^n}$. Renaming ζ as $\widetilde{w}_{p^n}$ in this statement, we obtain the following: There exists a unique ring homomorphism $\widetilde{w}_{p^n} : W_p(L) \to R/\mathfrak{a}_n$ such that $\widetilde{w}_{p^n} \circ W_p(\pi) = \pi_n \circ w_{p^n}$. In other words, there exists a unique ring homomorphism $\widetilde{w}_{p^n} : W_p(L) \to R/\mathfrak{a}_n$ such that the diagram (5) commutes. This proves Proposition 11.7. □

Definition 11.8. Let K and R be two rings. A map $\varphi : K \to R$ is said to be *multiplicative* if and only if it satisfies $\varphi(1) = 1$ and $(\varphi(ab) = \varphi(a)\varphi(b)$ for every $a \in K$ and $b \in K)$.

Proposition 11.9. Let K and R be two rings. Let $\varphi : K \to R$ be a multiplicative map. Let $v \in K$ and $i \geq 0$. Then, $\varphi\left(v^i\right) = (\varphi(v))^i$.

Proof of Proposition 11.9. This follows by straightforward induction on i. □

Proposition 11.10. Let p be a prime. Let R be a ring equipped with a decreasing sequence $R = \mathfrak{a}_0 \supset \mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \mathfrak{a}_3 \supset \cdots$ of ideals such that $(\mathfrak{a}_n \cdot \mathfrak{a}_m \subset \mathfrak{a}_{n+m}$ for all $n \geq 0$ and $m \geq 0)$. Equip R with the topology defined by this sequence of ideals. Assume that R is Hausdorff for this topology.

Assume that the residue ring $L = R/\mathfrak{a}_1$ has $p \cdot 1_L = 0$. Let π denote the canonical projection $R \to R/\mathfrak{a}_1 = L$.

Let K be a perfect ring of characteristic p. Let $f : K \to L$ be any map. Then, there exists at most one multiplicative map $r : K \to R$ satisfying

$$(\pi(r(a)) = f(a) \qquad \text{for every } a \in K). \tag{8}$$

Proof of Proposition 11.10. We need to show that if r_1 and r_2 are two multiplicative maps $r : K \to R$ satisfying (8), then $r_1 = r_2$.

So let r_1 and r_2 be two multiplicative maps $r : K \to R$ satisfying (8). We must show that $r_1 = r_2$.

Let $u \in K$. Let $n \geq 0$. Then, the element u^{1/p^n} of K is well-defined (since K is a perfect ring of characteristic p). Moreover, r_1 is multiplicative; thus, Proposition 11.9 (applied to $\varphi = r_1$, $v = u^{1/p^n}$ and $i = p^n$) yields $r_1\left(\left(u^{1/p^n}\right)^{p^n}\right) = \left(r_1\left(u^{1/p^n}\right)\right)^{p^n}$. Since $\left(u^{1/p^n}\right)^{p^n} = u$, this rewrites as $r_1(u) = \left(r_1\left(u^{1/p^n}\right)\right)^{p^n}$. Similarly, $r_2(u) = \left(r_2\left(u^{1/p^n}\right)\right)^{p^n}$.

But the map r_1 satisfies (8). Hence, (8) (applied to $r = r_1$ and $a = u^{1/p^n}$) yields $\pi\left(r_1\left(u^{1/p^n}\right)\right) = f\left(u^{1/p^n}\right)$. Similarly, $\pi\left(r_2\left(u^{1/p^n}\right)\right) = f\left(u^{1/p^n}\right)$. Hence, $\pi\left(r_1\left(u^{1/p^n}\right)\right) = f\left(u^{1/p^n}\right) = \pi\left(r_2\left(u^{1/p^n}\right)\right)$. In other words, $r_1\left(u^{1/p^n}\right) \equiv r_2\left(u^{1/p^n}\right) \bmod \mathfrak{a}_1$ (since π is the canonical projection $R \to R/\mathfrak{a}_1$). Hence, Proposition 11.5 **(d)** (applied to $x = r_1\left(u^{1/p^n}\right)$, $y = r_2\left(u^{1/p^n}\right)$ and $i = n$) yields $\left(r_1\left(u^{1/p^n}\right)\right)^{p^n} \equiv \left(r_2\left(u^{1/p^n}\right)\right)^{p^n} \bmod \mathfrak{a}_{n+1}$. Thus,

$$r_1(u) = \left(r_1\left(u^{1/p^n}\right)\right)^{p^n} \equiv \left(r_2\left(u^{1/p^n}\right)\right)^{p^n} = r_2(u) \bmod \mathfrak{a}_{n+1}.$$

Thus, $r_1(u) - r_2(u) \in \mathfrak{a}_{n+1} \subset \mathfrak{a}_n$.

Now, forget that we fixed n. We thus have shown that $r_1(u) - r_2(u) \in \mathfrak{a}_n$ for every $n \geq 0$. In other words, $r_1(u) - r_2(u) \in \bigcap_{n \geq 0} \mathfrak{a}_n = 0$ (by Proposition 11.2 **(a)**). In other words, $r_1(u) - r_2(u) = 0$, so that $r_1(u) = r_2(u)$.

Now, forget that we fixed u. We thus have shown that $r_1(u) = r_2(u)$ for every $u \in K$. In other words, $r_1 = r_2$. This completes the proof of Proposition 11.10. □

Theorem 11.11. Let p be a prime. Let R be a ring equipped with a decreasing sequence $R = \mathfrak{a}_0 \supset \mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \mathfrak{a}_3 \supset \cdots$ of ideals such that ($\mathfrak{a}_n \cdot \mathfrak{a}_m \subset \mathfrak{a}_{n+m}$ for all $n \geq 0$ and $m \geq 0$). Equip R with the topology defined by this sequence of ideals. Assume that R is Hausdorff and complete for this topology. Assume that the residue ring $L = R/\mathfrak{a}_1$ has $p \cdot 1_L = 0$. Let π denote the canonical projection $R \to R/\mathfrak{a}_1 = L$.

Let K be a perfect ring of characteristic p. Let $f : K \to L$ be a ring homomorphism.

There exists a unique multiplicative map $r : K \to R$ satisfying

$$(\pi(r(a)) = f(a) \qquad \text{for every } a \in K). \tag{9}$$

Theorem 11.11 is a generalization of the existence of a Teichmüller system of representatives for a perfect ring[7].

Proof of Theorem 11.11. Proposition 11.5 **(b)** shows that $p \cdot 1_R \in \mathfrak{a}_1$ and $pR \subset \mathfrak{a}_1$.

The map π is surjective (since it is the canonical projection $R \to R/\mathfrak{a}_1$).

Proposition 11.10 shows that there exists **at most one** multiplicative map $r : K \to R$ satisfying (9). It thus remains to prove that there exists **at least one** such map. In other words, it remains to construct such a map.

[7]More precisely: If we apply it to $L = K$ and $f = \mathrm{id}_K$, where R is a p-ring with residue ring K, then we recover the classical result that there exists a unique Teichmüller system of representatives $K \to R$.

Let $a \in K$. Then, the element a^{1/p^i} of K is defined for every $i \in \{0,1,2,\ldots\}$ (since K is a perfect ring of characteristic p).

For every $i \in \{0,1,2,\ldots\}$, choose some $g_i \in R$ such that $\pi(g_i) = f\left(a^{1/p^i}\right)$. (This is well-defined, since π is surjective.) Thus, a sequence $(g_0, g_1, g_2, \ldots) \in R^\infty$ of elements of R is defined. We have

$$g_i^{p^i} \equiv g_{i+1}^{p^{i+1}} \bmod \mathfrak{a}_{i+1} \qquad \text{for every } i \geq 0. \tag{10}$$

[8] Thus, the sequence $\left(g_0^{p^0}, g_1^{p^1}, g_2^{p^2}, \ldots\right)$ is Cauchy with respect to the topology on R. Hence, the limit $\lim\limits_{n\to\infty} g_n^{p^n}$ is defined. Denote this limit by g'. Thus, $g' = \lim\limits_{n\to\infty} g_n^{p^n}$. From (10), we obtain

$$g' \equiv g_i^{p^i} \bmod \mathfrak{a}_{i+1} \qquad \text{for every } i \geq 0. \tag{11}$$

We notice the following fact: If $u \in R$ and $i \in \{0,1,2,\ldots\}$ are such that $\pi(u) = f\left(a^{1/p^i}\right)$, then

$$g' \equiv u^{p^i} \bmod \mathfrak{a}_{i+1}. \tag{12}$$

[9]

The value of g' does not depend on the choice of the elements g_i [10]. We denote this value of g' by $r(a)$ (to stress its dependence on a). It has the property

[8] *Proof of (10):* Let $i \geq 0$. The definition of g_i yields $\pi(g_i) = f\left(a^{1/p^i}\right)$. The definition of g_{i+1} yields $\pi(g_{i+1}) = f\left(a^{1/p^{i+1}}\right)$. Hence,

$$\pi\left(g_{i+1}^p\right) = \left(\underbrace{\pi(g_{i+1})}_{=f\left(a^{1/p^{i+1}}\right)}\right)^p = \left(f\left(a^{1/p^{i+1}}\right)\right)^p = f\left(\underbrace{\left(a^{1/p^{i+1}}\right)^p}_{=a^{1/p^i}}\right)$$
$$\text{(since } f \text{ is a ring homomorphism)}$$
$$= f\left(a^{1/p^i}\right) = \pi(g_i).$$

In other words, $g_{i+1}^p \equiv g_i \bmod \mathfrak{a}_1$. Hence, Proposition 11.5 **(d)** (applied to $x = g_{i+1}^p$ and $y = g_i$) yields $\left(g_{i+1}^p\right)^{p^i} \equiv g_i^{p^i} \bmod \mathfrak{a}_{i+1}$. Now, $g_{i+1}^{p^{i+1}} = \left(g_{i+1}^p\right)^{p^i} \equiv g_i^{p^i} \bmod \mathfrak{a}_{i+1}$. This proves (10).

[9] *Proof of (12):* Let $u \in R$ and $i \in \{0,1,2,\ldots\}$ be such that $\pi(u) = f\left(a^{1/p^i}\right)$. From $\pi(u) = f\left(a^{1/p^i}\right) = \pi(g_i)$, we obtain $u \equiv g_i \bmod \mathfrak{a}_1$. Hence, Proposition 11.5 **(d)** (applied to $x = u$ and $y = g_i$) yields $u^{p^i} \equiv g_i^{p^i} \bmod \mathfrak{a}_{i+1}$. Now, $u^{p^i} \equiv g_i^{p^i} \equiv g' \bmod \mathfrak{a}_{i+1}$ (by (11)). This proves (12).

[10] *Proof.* We need to show that if g_1' and g_2' are two possible values of g', then $g_1' = g_2'$.

Indeed, let g_1' and g_2' be two possible values of g'. Let $i \in \{0,1,2,\ldots\}$. Pick any $u \in R$ satisfying $\pi(u) = f\left(a^{1/p^i}\right)$ (such a u exists, since π is surjective). Then, (12) (applied to

that if $u \in R$ and $i \in \{0,1,2,\ldots\}$ are such that $\pi(u) = f\left(a^{1/p^i}\right)$, then

$$r(a) \equiv u^{p^i} \bmod \mathfrak{a}_{i+1} \tag{13}$$

(indeed, this is just a restatement of (12) using the new notation $r(a)$ for g').

Now, forget that we fixed a. We thus have defined an element $r(a) \in R$ for each $a \in K$, and noticed that this element satisfies (13). Thus, we have defined a map $r : K \to R$ such that every $a \in K$ satisfies (13). In order to prove Theorem 11.11, it remains to prove that this map r is multiplicative and satisfies (9).

Proof that r is multiplicative: We have $r(1) = 1$ [11]. Also, $r(ab) = r(a)\, r(b)$ for every $a \in K$ and $b \in K$ [12]. Hence, the map r is multiplicative.

---

g'_1 instead of g') yields $g'_1 \equiv u^{p^i} \bmod \mathfrak{a}_{i+1}$ (since g'_1 is one possible value of g'). Similarly, $g'_2 \equiv u^{p^i} \bmod \mathfrak{a}_{i+1}$. Thus, $g'_1 \equiv u^{p^i} \equiv g'_2 \bmod \mathfrak{a}_{i+1}$. In other words, $g'_1 - g'_2 \in \mathfrak{a}_{i+1} \subset \mathfrak{a}_i$, so that $g'_1 \equiv g'_2 \bmod \mathfrak{a}_i$.

Now, forget that we fixed i. We thus have proven that $g'_1 \equiv g'_2 \bmod \mathfrak{a}_i$ for each $i \in \{0,1,2,\ldots\}$. Hence, $g'_1 = g'_2$ (by Proposition 11.2 **(b)**, applied to $u = g'_1$ and $v = g'_2$), qed.

[11] *Proof.* Let $i \in \{0,1,2,\ldots\}$. Then, $f\left(\underbrace{1^{1/p^i}}_{=1}\right) = f(1) = 1$ (since f is a ring homomorphism), and thus $\pi(1) = 1 = f\left(1^{1/p^i}\right)$. Hence, (13) (applied to $a = 1$ and $u = 1$) yields $r(1) \equiv 1^{p^i} = 1 \bmod \mathfrak{a}_{i+1}$. Thus, $r(1) - 1 \in \mathfrak{a}_{i+1} \subset \mathfrak{a}_i$, so that $r(1) \equiv 1 \bmod \mathfrak{a}_i$.

Now, forget that we fixed i. We thus have shown that $r(1) \equiv 1 \bmod \mathfrak{a}_i$ for every $i \in \{0,1,2,\ldots\}$. Hence, $r(1) = 1$ (by Proposition 11.2 **(b)**, applied to $u = r(1)$ and $v = 1$), qed.

[12] *Proof.* Let $a \in K$ and $b \in K$. Let $i \in \{0,1,2,\ldots\}$.

Pick some $u \in R$ such that $\pi(u) = f\left(a^{1/p^i}\right)$. (Such a u exists, since π is surjective.) Hence, (13) yields $r(a) \equiv u^{p^i} \bmod \mathfrak{a}_{i+1}$.

Pick some $v \in R$ such that $\pi(v) = f\left(b^{1/p^i}\right)$. (Such a v exists, since π is surjective.) Hence, (13) (applied to b and v instead of a and u) yields $r(b) \equiv v^{p^i} \bmod \mathfrak{a}_{i+1}$.

Now,

$$\begin{aligned}
\pi(uv) &= \underbrace{\pi(u)}_{=f\left(a^{1/p^i}\right)} \underbrace{\pi(v)}_{=f\left(b^{1/p^i}\right)} = f\left(a^{1/p^i}\right) f\left(b^{1/p^i}\right) \\
&= f\left(\underbrace{a^{1/p^i} b^{1/p^i}}_{=(ab)^{1/p^i}}\right) \qquad \text{(since } f \text{ is a ring homomorphism)} \\
&= f\left((ab)^{1/p^i}\right).
\end{aligned}$$

Thus, (13) (applied to ab and uv instead of a and u) yields $r(ab) \equiv (uv)^{p^i} = \underbrace{u^{p^i}}_{\equiv r(a) \bmod \mathfrak{a}_{i+1}} \underbrace{v^{p^i}}_{\equiv r(b) \bmod \mathfrak{a}_{i+1}} \equiv r(a)\, r(b) \bmod \mathfrak{a}_{i+1}$. Thus, $r(ab) - r(a)\, r(b) \in \mathfrak{a}_{i+1} \subset \mathfrak{a}_i$, so that $r(ab) \equiv r(a)\, r(b) \bmod \mathfrak{a}_i$.

Now, forget that we fixed i. We thus have shown that $r(ab) \equiv r(a)\, r(b) \bmod \mathfrak{a}_i$ for all $i \in \{0,1,2,\ldots\}$. Thus, $r(ab) = r(a)\, r(b)$ (by Proposition 11.2 **(b)**, applied to $u = r(ab)$ and $v = r(a)\, r(b)$), qed.

Proof that r satisfies (9): Let $a \in K$. Pick some $u \in R$ such that $\pi(u) = f(a)$. (Such a u exists, since π is surjective.) Now, $\pi(u) = f\left(\underbrace{a}_{=a^1=a^{1/p^0}}\right) = f\left(a^{1/p^0}\right)$. Hence, (13) (applied to $i = 0$) yields $r(a) \equiv u^{p^0} = u^1 = u \bmod \mathfrak{a}_1$. Hence, $\pi(r(a)) = \pi(u) = f(a)$. Thus, (9) is proven.

So we have defined a map $r : K \to R$, and showed that this map r is multiplicative and satisfies (9). Thus, we have constructed the map r whose existence was alleged in Theorem 11.11. This proves Theorem 11.11. □

Lemma 11.12. Let p be a prime. Let K be a perfect ring of characteristic p. Let $x \in W_p(K)$. Then, there exist two elements y and z of $W_p(K)$ such that $x = y^p + pz$.

Proof of Lemma 11.12. The ring K is a perfect ring of characteristic p. Hence, an element $x_m^{1/p}$ of K is well-defined for every $m \in P_p$. Now, define $a \in W_p(K)$ by $a = \left(x_m^{1/p}\right)_{m \in P_p}$. Then, $a_m = x_m^{1/p}$ for every $m \in P_p$. In other words, $a_m^p = x_m$ for every $m \in P_p$.

Let $b = F_p(a)$. Then, Proposition 5.12 (applied to P_p, K, a and b instead of P, A, x and y) yields the following:

1. We have $b_m \equiv a_m^p \bmod pK$ for every $m \in P_p$.
2. We have $F_p(a) \equiv a^p \bmod pW_p(K)$.

We have $F_p(a) \equiv a^p \bmod pW_p(K)$. In other words, there exists some $c \in W_p(K)$ such that $F_p(a) = a^p + pc$. Consider this c.

We have $pK = 0$ (since K has characteristic p). Now, for every $m \in P_p$, we have $b_m \equiv a_m^p \bmod pK$, thus $b_m = a_m^p$ (since $pK = 0$), hence $b_m = a_m^p = x_m$ (since $a_m^p = x_m$). Therefore, $b = x$. Comparing this with $b = F_p(a)$, we obtain $F_p(a) = x$. Thus, $x = F_p(a) = a^p + pc$. Hence, there exist two elements y and z of $W_p(K)$ such that $x = y^p + pz$ (namely, $y = a$ and $z = c$). This proves Lemma 11.12. □

Proposition 11.13. Let p be a prime. Let R be a ring equipped with a decreasing sequence $R = \mathfrak{a}_0 \supset \mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \mathfrak{a}_3 \supset \cdots$ of ideals such that ($\mathfrak{a}_n \cdot \mathfrak{a}_m \subset \mathfrak{a}_{n+m}$ for all $n \geq 0$ and $m \geq 0$). Equip R with the topology defined by this sequence of ideals. Assume that R is Hausdorff for this topology.

Assume that the residue ring $L = R/\mathfrak{a}_1$ has $p \cdot 1_L = 0$. Let π denote the canonical projection $R \to R/\mathfrak{a}_1 = L$.

Let K be a perfect ring of characteristic p. Let $G : W_p(K) \to L$ be any map.

Then, there exists at most one ring homomorphism $\theta : W_p(K) \to R$ such that $\pi \circ \theta = G$.

Proof of Proposition 11.13. We need to show that if θ_1 and θ_2 are two ring homomorphisms $\theta : W_p(K) \to R$ such that $\pi \circ \theta = G$, then $\theta_1 = \theta_2$.

So let θ_1 and θ_2 be two ring homomorphisms $\theta : W_p(K) \to R$ such that $\pi \circ \theta = G$. We must show that $\theta_1 = \theta_2$.

Define the maps π_n for all $n \geq 0$ as in Proposition 11.2 **(c)**.

We first observe that

$$\pi_1 \circ \theta_1 = \pi_1 \circ \theta_2. \tag{14}$$

[13]

We shall show that

$$\pi_n \circ \theta_1 = \pi_n \circ \theta_2 \qquad \text{for every } n \geq 0. \tag{15}$$

Proof of (15): We shall prove (15) by induction on n:

Induction base: The map π_0 is the canonical projection $R \to R/\mathfrak{a}_0 = 0$ (since $\mathfrak{a}_0 = R$). Hence, any two maps become equal when composed with π_0. In particular, we thus have $\pi_0 \circ \theta_1 = \pi_0 \circ \theta_2$. In other words, (15) holds for $n = 0$. This completes the induction base.

Induction step: Let N be a positive integer. Assume that (15) holds for $n = N - 1$. We must show that (15) holds for $n = N$. In other words, we need to prove that $\pi_N \circ \theta_1 = \pi_N \circ \theta_2$.

If $N = 1$, then this follows immediately from (14). Hence, we WLOG assume that $N \neq 1$. Hence, $N \geq 2$ (since N is a positive integer). Thus, $N - 1$ is a positive integer.

We have assumed that (15) holds for $n = N - 1$. In other words, $\pi_{N-1} \circ \theta_1 = \pi_{N-1} \circ \theta_2$. For every $a \in W_p(K)$, we have

$$\theta_1(a) \equiv \theta_2(a) \bmod \mathfrak{a}_{N-1} \tag{16}$$

[14] and

$$(\theta_1(a))^p \equiv (\theta_2(a))^p \bmod \mathfrak{a}_N \tag{17}$$

[15] and

$$p\theta_1(a) \equiv p\theta_2(a) \bmod \mathfrak{a}_N \tag{18}$$

[13] *Proof of (14):* Both maps π_1 and π are defined as the canonical projection $R \to R/\mathfrak{a}_1$. Hence, these two maps are equal. In other words, $\pi_1 = \pi$.

We know that θ_1 is a ring homomorphism $\theta : W_p(K) \to R$ such that $\pi \circ \theta = G$. Hence, $\pi \circ \theta_1 = G$. The same argument (applied to θ_2 instead of θ_1) shows that $\pi \circ \theta_2 = G$. Hence, $\pi \circ \theta_1 = G = \pi \circ \theta_2$. In light of $\pi_1 = \pi$, this rewrites as $\pi_1 \circ \theta_1 = \pi_1 \circ \theta_2$. This proves (14).

[14] *Proof of (16):* Let $a \in W_p(K)$. Then,

$$\pi_{N-1}(\theta_1(a)) = \underbrace{(\pi_{N-1} \circ \theta_1)}_{=\pi_{N-1} \circ \theta_2}(a) = (\pi_{N-1} \circ \theta_2)(a) = \pi_{N-1}(\theta_2(a)).$$

In other words, $\theta_1(a) \equiv \theta_2(a) \bmod \mathfrak{a}_{N-1}$ (since π_{N-1} is the canonical projection $R \to R/\mathfrak{a}_{N-1}$). This proves (16).

[15] *Proof of (17):* Let $a \in W_p(K)$. From (16), we have $\theta_1(a) \equiv \theta_2(a) \bmod \mathfrak{a}_{N-1}$. Thus, Proposition 11.5 **(f)** (applied to $\theta_1(a)$, $\theta_2(a)$ and $N - 1$ instead of a, b and i) yields $(\theta_1(a))^p \equiv (\theta_2(a))^p \bmod \mathfrak{a}_{(N-1)+1}$. In other words, $(\theta_1(a))^p \equiv (\theta_2(a))^p \bmod \mathfrak{a}_N$. This proves (17).

[16].

Proposition 11.5 **(b)** yields $pR \subset \mathfrak{a}_1$.

Let $x \in W_p(K)$. Lemma 11.12 shows that there exist two elements y and z of $W_p(K)$ such that $x = y^p + pz$. Consider these y and z. Applying the map θ_1 to the equality $x = y^p + pz$, we find

$$\theta_1(x) = \theta_1(y^p + pz) = (\theta_1(y))^p + p\theta_1(z) \tag{19}$$

(since θ_1 is a ring homomorphism). The same argument (applied to θ_2 instead of θ_1) shows that

$$\theta_2(x) = (\theta_2(y))^p + p\theta_2(z). \tag{20}$$

Now, (19) becomes

$$\begin{aligned}\theta_1(x) = &\underbrace{(\theta_1(y))^p}_{\substack{\equiv(\theta_2(y))^p \bmod \mathfrak{a}_N \\ \text{(by (17), applied to } a=y\text{)}}} + \underbrace{p\theta_1(z)}_{\substack{\equiv p\theta_2(z) \bmod \mathfrak{a}_N \\ \text{(by (18), applied to } a=z\text{)}}} \\ &\equiv (\theta_2(y))^p + p\theta_2(z) = \theta_2(x) \bmod \mathfrak{a}_N\end{aligned}$$

(by (20)). In other words, $\pi_N(\theta_1(x)) = \pi_N(\theta_2(x))$. Thus, $(\pi_N \circ \theta_1)(x) = \pi_N(\theta_1(x)) = \pi_N(\theta_2(x)) = (\pi_N \circ \theta_2)(x)$.

Now, forget that we fixed x. We thus have proven that $(\pi_N \circ \theta_1)(x) = (\pi_N \circ \theta_2)(x)$ for every $x \in W_p(K)$. In other words, $\pi_N \circ \theta_1 = \pi_N \circ \theta_2$. This completes the induction step. The induction proof of (15) is thus complete.

Proposition 11.2 **(c)** (applied to $A = W_p(K)$, $\varphi = \theta_1$ and $\psi = \theta_2$) thus yields $\theta_1 = \theta_2$. This completes the proof of Proposition 11.13. □

Proof of Theorem 11.1. Proposition 11.5 **(b)** shows that $p \cdot 1_R \in \mathfrak{a}_1$ and $pR \subset \mathfrak{a}_1$.

The map π is surjective (since it is the canonical projection $R \to R/\mathfrak{a}_1$).

Theorem 11.11 shows that there exists a unique multiplicative map $r : K \to R$ satisfying (9). Consider this r.

The ring K is perfect of characteristic p. Hence, an element v^{1/p^n} of K is well-defined for each $v \in K$ and each $n \geq 0$. In particular, an element $x_{p^n}^{1/p^n}$ of K is well-defined for each $x \in W_p(K)$ and each $n \geq 0$.

Define a map $\Theta : W_p(K) \to R$ by

$$\left(\Theta(x) = \sum_{n \geq 0} r\left(x_{p^n}^{1/p^n}\right) p^n \qquad \text{for every } x \in W_p(K)\right).$$

[16] *Proof of (18):* Let $a \in W_p(K)$. From (16), we have $\theta_1(a) \equiv \theta_2(a) \bmod \mathfrak{a}_{N-1}$. In other words, $\theta_1(a) - \theta_2(a) \in \mathfrak{a}_{N-1}$. Now,

$$p\theta_1(a) - p\theta_2(a) = p\underbrace{(\theta_1(a) - \theta_2(a))}_{\in \mathfrak{a}_{N-1}} \in p\mathfrak{a}_{N-1} \subset \mathfrak{a}_N$$

(by Proposition 11.5 **(g)**, applied to $n = N$). Thus, $p\theta_1(a) \equiv p\theta_2(a) \bmod \mathfrak{a}_N$. This proves (18).

This is well-defined (because the infinite sum $\sum_{n\geq 0} r\left(x_{p^n}^{1/p^n}\right) p^n$ converges[17]). Moreover, the square (2) commutes for $\theta = \Theta$. [18]

Notice that every $x \in W_p(K)$ satisfies

$$\Theta(x) \equiv \sum_{k=0}^{i} r\left(x_{p^k}^{1/p^k}\right) p^k \bmod \mathfrak{a}_{i+1} \qquad \text{for every } i \geq -1. \tag{22}$$

[19]

For every $n \geq 0$, let π_n be the canonical projection $R \to R/\mathfrak{a}_n$. Then, every

[17] since $r\left(x_{p^n}^{1/p^n}\right) p^n = r\left(x_{p^n}^{1/p^n}\right) \underbrace{p^n \cdot 1_R}_{\in \mathfrak{a}_n \text{ (by Proposition 11.5 (c))}} \in \mathfrak{a}_n$ for every $n \geq 0$

[18] *Proof.* Let $x \in W_p(K)$. Every $n \geq 1$ satisfies

$$r\left(x_{p^n}^{1/p^n}\right) p^n = \underbrace{p^n}_{=pp^{n-1}} r\left(x_{p^n}^{1/p^n}\right) = p \underbrace{p^{n-1} r\left(x_{p^n}^{1/p^n}\right)}_{\in R} \in pR \subset \mathfrak{a}_1$$

and thus

$$\pi\left(r\left(x_{p^n}^{1/p^n}\right) p^n\right) = 0 \tag{21}$$

(since π is the canonical projection $R \to R/\mathfrak{a}_1$). Now,

$$\begin{aligned}
(\pi \circ \Theta)(x) &= \pi\left(\underbrace{\Theta(x)}_{=\sum_{n\geq 0} r\left(x_{p^n}^{1/p^n}\right) p^n}\right) = \pi\left(\sum_{n\geq 0} r\left(x_{p^n}^{1/p^n}\right) p^n\right) = \sum_{n\geq 0} \pi\left(r\left(x_{p^n}^{1/p^n}\right) p^n\right) \\
&= \pi\left(\underbrace{r\left(x_{p^0}^{1/p^0}\right) p^0}_{=r(x_1)1=r(x_1)}\right) + \sum_{n\geq 1} \underbrace{\pi\left(r\left(x_{p^n}^{1/p^n}\right) p^n\right)}_{\substack{=0 \\ \text{(by (21))}}} \\
&= \pi(r(x_1)) + \underbrace{\sum_{n\geq 1} 0}_{=0} = \pi(r(x_1)) = f(x_1)
\end{aligned}$$

(by (9), applied to $a = x_1$). Comparing this with

$$(f \circ w_1)(x) = f\left(\underbrace{w_1(x)}_{=x_1}\right) = f(x_1),$$

we obtain $(\pi \circ \Theta)(x) = (f \circ w_1)(x)$. Since we have proven this for every $x \in W_p(K)$, we thus conclude that $\pi \circ \Theta = f \circ w_1$. In other words, $\pi \circ \theta = f \circ w_1$ for $\theta = \Theta$. In other words, the square (2) commutes for $\theta = \Theta$.

[19] *Proof of (22):* Let $x \in W_p(K)$ and $i \geq -1$. Then, Proposition 11.5 **(c)** yields that $p^n \cdot 1_R \in \mathfrak{a}_n$ for

$x \in W_p(K)$ and $n \geq 0$ satisfy

$$(\pi_n \circ \Theta)(x) = \pi_n\left(\sum_{i=0}^{n} p^i \left(r\left(x_{p^i}^{1/p^n}\right)\right)^{p^{n-i}}\right). \tag{23}$$

[20] Hence, for every $n \geq 0$, the map $\pi_n \circ \Theta : W_p(K) \to R/\mathfrak{a}_n$ is continuous

---

every $n \geq 0$. Now,

$$\begin{aligned}
\Theta(x) &= \sum_{n\geq 0} r\left(x_{p^n}^{1/p^n}\right) p^n = \sum_{n=0}^{i} r\left(x_{p^n}^{1/p^n}\right) p^n + \sum_{n\geq i+1} \underbrace{r\left(x_{p^n}^{1/p^n}\right) p^n}_{= r\left(x_{p^n}^{1/p^n}\right) p^n \cdot 1_R} \\
&= \sum_{n=0}^{i} r\left(x_{p^n}^{1/p^n}\right) p^n + \sum_{n\geq i+1} r\left(x_{p^n}^{1/p^n}\right) \underbrace{p^n \cdot 1_R}_{\substack{\in \mathfrak{a}_n \subset \mathfrak{a}_{i+1} \\ (\text{since } n \geq i+1)}} \in \sum_{n=0}^{i} r\left(x_{p^n}^{1/p^n}\right) p^n + \underbrace{\sum_{n\geq i+1} r\left(x_{p^n}^{1/p^n}\right) \mathfrak{a}_{i+1}}_{\subset \mathfrak{a}_{i+1}} \\
&\subset \sum_{n=0}^{i} r\left(x_{p^n}^{1/p^n}\right) p^n + \mathfrak{a}_{i+1}.
\end{aligned}$$

In other words, $\Theta(x) \equiv \sum_{n=0}^{i} r\left(x_{p^n}^{1/p^n}\right) p^n \bmod \mathfrak{a}_{i+1}$. Renaming the summation index n as k in this congruence, we obtain $\Theta(x) \equiv \sum_{k=0}^{i} r\left(x_{p^k}^{1/p^k}\right) p^k \bmod \mathfrak{a}_{i+1}$, qed.

[20] *Proof of (23):* Let $x \in W_p(K)$ and $n \geq 0$. Applying (22) to $i = n$, we obtain

$$\Theta(x) \equiv \sum_{k=0}^{n} r\left(x_{p^k}^{1/p^k}\right) p^k = \sum_{k=0}^{n} p^k r\left(x_{p^k}^{1/p^k}\right) = \sum_{i=0}^{n} p^i r\left(x_{p^i}^{1/p^i}\right) \bmod \mathfrak{a}_{n+1}.$$

In other words, $\Theta(x) - \sum_{i=0}^{n} p^i r\left(x_{p^i}^{1/p^i}\right) \in \mathfrak{a}_{n+1} \subset \mathfrak{a}_n$, so that

$$\Theta(x) \equiv \sum_{i=0}^{n} p^i r\left(x_{p^i}^{1/p^i}\right) \bmod \mathfrak{a}_n. \tag{24}$$

Now, fix $i \in \{0, 1, \ldots, n\}$. Recall that the map r is multiplicative. Thus, Proposition 11.9 (applied to r, $x_{p^i}^{1/p^n}$ and p^{n-i} instead of φ, v and i) yields $r\left(\left(x_{p^i}^{1/p^n}\right)^{p^{n-i}}\right) = \left(r\left(x_{p^i}^{1/p^n}\right)\right)^{p^{n-i}}$. Hence,

$$\left(r\left(x_{p^i}^{1/p^n}\right)\right)^{p^{n-i}} = r\left(\underbrace{\left(x_{p^i}^{1/p^n}\right)^{p^{n-i}}}_{= x_{p^i}^{p^{n-i}/p^n} = x_{p^i}^{1/p^i}}\right) = r\left(x_{p^i}^{1/p^i}\right). \tag{25}$$

Now, forget that we fixed i. Thus, we have shown that (25) holds for each $i \in \{0, 1, \ldots, n\}$.

(where $R/\mathfrak{a}_n$ is equipped with the discrete topology)[21]. Therefore, Proposition 11.4 (applied to $A = W_p(K)$ and $\varphi = \Theta$) shows that the map $\Theta : W_p(K) \to R$ is continuous.

Now, fix a nonnegative integer n.

Let ω denote the map $K \to K,\ u \mapsto u^p$. Thus, ω is the Frobenius homomorphism of the ring K, and is a ring homomorphism (since the ring K has characteristic p) and invertible (since the ring K is perfect). Hence, its inverse map ω^{-1} is also a ring homomorphism. Thus, the map ω^{-n} is also a ring homomorphism. It is easy to see that

$$\omega^{-i}(v) = v^{1/p^i} \qquad \text{for every } v \in K \text{ and } i \geq 0. \tag{26}$$

[22] We have

$$\left(f \circ \omega^{-n}\right)(v) = \pi\left(r\left(v^{1/p^n}\right)\right) \tag{27}$$

for each $v \in K$. [23]

Now, (24) becomes

$$\Theta(x) \equiv \sum_{i=0}^{n} p^i \underbrace{r\left(x_{p^i}^{1/p^i}\right)}_{=\left(r\left(x_{p^i}^{1/p^n}\right)\right)^{p^{n-i}} \text{ (by (25))}} = \sum_{i=0}^{n} p^i \left(r\left(x_{p^i}^{1/p^n}\right)\right)^{p^{n-i}} \bmod \mathfrak{a}_n.$$

In other words, $\pi_n(\Theta(x)) = \pi_n\left(\sum_{i=0}^{n} p^i \left(r\left(x_{p^i}^{1/p^n}\right)\right)^{p^{n-i}}\right)$ (since π_n is the canonical projection $R \to R/\mathfrak{a}_n$). Thus,

$$\left(\pi_n \circ \Theta\right)(x) = \pi_n(\Theta(x)) = \pi_n\left(\sum_{i=0}^{n} p^i \left(r\left(x_{p^i}^{1/p^n}\right)\right)^{p^{n-i}}\right),$$

and so (23) is proven.

[21] *Proof.* Let $n \geq 0$. Then, for every $x \in W_p(K)$, the formula (23) expresses $\left(\pi_n \circ \Theta\right)(x)$ through the first $N+1$ coordinates $x_{p^0}, x_{p^1}, \ldots, x_{p^N}$ of x. Hence, $\left(\pi_n \circ \Theta\right)(x)$ depends only on the first $N+1$ coordinates $x_{p^0}, x_{p^1}, \ldots, x_{p^N}$ of x. Thus, the map $\pi_n \circ \Theta : W_p(K) \to R/\mathfrak{a}_n$ is continuous (by the definition of the topology on $W_p(K)$). Qed.

[22] *Proof of (26):* We have $\omega(v) = v^p$ for every $v \in K$. Thus, $\omega^{-1}(v) = v^{1/p}$ for every $v \in K$. Thus, we can easily see (by a straightforward induction over i) that $\omega^{-i}(v) = v^{1/p^i}$ for every $v \in K$ and $i \geq 0$. Thus, (26) is proven.

[23] *Proof of (27):* Let $v \in K$. Then,

$$\left(f \circ \omega^{-n}\right)(v) = f\left(\underbrace{\omega^{-n}(v)}_{\substack{=v^{1/p^n} \\ \text{(by (26), applied to } i=n\text{)}}}\right) = f\left(v^{1/p^n}\right) = \pi\left(r\left(v^{1/p^n}\right)\right)$$

(because (9) (applied to $a = v^{1/p^n}$) yields $\pi\left(r\left(v^{1/p^n}\right)\right) = f\left(v^{1/p^n}\right)$). This proves (27).

Proposition 11.7 shows that there exists a unique ring homomorphism $\widetilde{w}_{p^n} : W_p(L) \to R/\mathfrak{a}_n$ such that the diagram (5) commutes. Consider this $\widetilde{w}_{p^n}$.

But $f \circ \omega^{-n} : K \to L$ is a ring homomorphism (since both f and ω^{-n} are ring homomorphisms). Thus, $W_p(f \circ \omega^{-n}) : W_p(K) \to W_p(L)$ is a ring homomorphism as well. Now, we shall show that

$$\widetilde{w}_{p^n} \circ W_p\left(f \circ \omega^{-n}\right) = \pi_n \circ \Theta. \tag{28}$$

Proof of (28): Let $x \in W_p(K)$. The definition of $W_p(f \circ \omega^{-n})$ yields

$$\left(W_p\left(f \circ \omega^{-n}\right)\right)(x) = \left(\underbrace{\left(f \circ \omega^{-n}\right)(x_m)}_{\substack{=\pi\left(r\left(x_m^{1/p^n}\right)\right) \\ \text{(by (27), applied} \\ \text{to } v=x_m\text{)}}} \right)_{m \in P_p} = \left(\pi\left(r\left(x_m^{1/p^n}\right)\right)\right)_{m \in P_p}. \tag{29}$$

On the other hand, define $y \in W_p(R)$ by $y = \left(r\left(x_m^{1/p^n}\right)\right)_{m \in P_p}$. Then, the definition of $W_p(\pi)$ yields

$$\left(W_p(\pi)\right)(y) = \left(\pi\left(r\left(x_m^{1/p^n}\right)\right)\right)_{m \in P_p} = \left(W_p\left(f \circ \omega^{-n}\right)\right)(x) \qquad \text{(by (29))}.$$

Applying the map $\widetilde{w}_{p^n} : W_p(L) \to R/\mathfrak{a}_n$ to both sides of this equality, we obtain

$$\widetilde{w}_{p^n}\left(\left(W_p(\pi)\right)(y)\right) = \widetilde{w}_{p^n}\left(\left(W_p\left(f \circ \omega^{-n}\right)\right)(x)\right) = \left(\widetilde{w}_{p^n} \circ W_p\left(f \circ \omega^{-n}\right)\right)(x).$$

Thus,

$$\begin{aligned}\left(\widetilde{w}_{p^n} \circ W_p\left(f \circ \omega^{-n}\right)\right)(x) = \widetilde{w}_{p^n}\left(\left(W_p(\pi)\right)(y)\right) &= \underbrace{\left(\widetilde{w}_{p^n} \circ W_p(\pi)\right)}_{\substack{=\pi_n \circ w_{p^n} \\ \text{(since the diagram (5)} \\ \text{commutes)}}}(y) \\ &= \left(\pi_n \circ w_{p^n}\right)(y) = \pi_n\left(w_{p^n}(y)\right). \end{aligned} \tag{30}$$

On the other hand, (1) yields

$$w_{p^n}(y) = \sum_{i=0}^{n} p^i \left(r\left(x_{p^i}^{1/p^n}\right)\right)^{p^{n-i}} \qquad \left(\text{since } y = \left(r\left(x_m^{1/p^n}\right)\right)_{m \in P_p}\right).$$

Applying the map π_n to both sides of this equality, we obtain

$$\pi_n\left(w_{p^n}(y)\right) = \pi_n\left(\sum_{i=0}^{n} p^i \left(r\left(x_{p^i}^{1/p^n}\right)\right)^{p^{n-i}}\right) = \left(\pi_n \circ \Theta\right)(x)$$

(by (23)). Hence, (30) becomes

$$\left(\widetilde{w}_{p^n} \circ W_p\left(f \circ \omega^{-n}\right)\right)(x) = \pi_n\left(w_{p^n}(y)\right) = (\pi_n \circ \Theta)(x). \tag{31}$$

Now, forget that we fixed x. We thus have proven (31) for each $x \in W_p(K)$. In other words, we have $\widetilde{w}_{p^n} \circ W_p\left(f \circ \omega^{-n}\right) = \pi_n \circ \Theta$. Thus, (28) is proven.

Now, the map $\widetilde{w}_{p^n} \circ W_p\left(f \circ \omega^{-n}\right)$ is a ring homomorphism (since it is the composition of the two ring homomorphisms $\widetilde{w}_{p^n}$ and $W_p\left(f \circ \omega^{-n}\right)$). In view of (28), this rewrites as follows: The map $\pi_n \circ \Theta$ is a ring homomorphism.

Now, forget that we fixed n. We thus have shown that the map $\pi_n \circ \Theta$ is a ring homomorphism for each $n \geq 0$. Hence, Proposition 11.3 (applied to $A = W_p(K)$ and $\gamma = \Theta$) shows that $\Theta : W_p(K) \to R$ is a ring homomorphism. Hence, there exists a continuous ring homomorphism $\theta : W_p(K) \to R$ making the square (2) commute (namely, $\theta = \Theta$).

It thus only remains to show that there exists **at most** one such homomorphism. It will clearly be enough to prove that there exists at most one ring homomorphism $\theta : W_p(K) \to R$ making the square (2) commute. In other words, it will be enough to prove that there exists at most one ring homomorphism $\theta : W_p(K) \to R$ such that $\pi \circ \theta = f \circ w_1$. But this follows from Proposition 11.13 (applied to $G = f \circ w_1$). Thus, the proof of Theorem 11.1 is complete. □

References

[BriCon09] Olivier Brinon, Brian Conrad, *CMI Summer School notes on p-adic Hodge theory (preliminary version)*, 24 June 2009.
`http://math.stanford.edu/~conrad/papers/notes.pdf`