J. Math. Kyoto Univ.
8-2 (1968) 279-283

On the Witt vectors over nonperfect rings

By

T. KAMBAYASHI

(Communicated by Professor Nagata, May 21, 1968)

In this note we offer a theorem which purports to characterizing the ring of Witt vectors built over a nonperfect ring of prime characteristic p provided that the extraction of p-th root is possible within the latter ring.

The formulation of the theorem as well as essential ideas for its proof were made known to the writer in 1966 by M. Nagata while both of us were in Pisa, Italy. The writer now undertakes to publish the result by furnishing details.

1. Throughout let K denote a commutative ring with 1 having prime characteristic p. Let $W(K)$ denote the Witt vector ring of infinite length over K.

Theorem 1. *Let A be a commutative ring with* 1, *complete and separated with respect to the topology defined by the ideals $\{p^\nu A;\ \nu=1,2,\cdots\}$; suppose that p is not a zero-divisor and that $A/pA\simeq K$. Then the following are equivalent*:

a) *The Frobenius morphism $x\to x^p$ is bijective from K to K* (i. e. *K is perfect*);

b) *A is canonically isomorphic with $W(K)$.*

The implication a)$\Rightarrow$b) is rather classical; an interesting version of proof due to M. Lazard is found in Serre's *Corps Locaux*, Chap.

II, §5, pp. 45–49 (Hermann, Paris: 1962).

The part b)⇒ a) was remarked to the writer by M. Poletti, and it can be readily verified.

2. Before proceeding to the main result of the paper, we fix notations as follows: If x is an element of a commutative ring then $\bar{x}$ will invariably denote the residue class of x modulo p. Another note: For typographical reasons, the p^ν-th power of an entity X will always be denoted by $X^{p(\nu)}$.

Theorem 2. *Let R be a commutative ring with* 1, *complete and separated with respect to the topology defined by the ideals $\{p^\nu R;\ \nu=1, 2, \cdots\}$; suppose that $R/pR \simeq K$ and that the Frobenius morphism $x \to x^p$ of K is surjective* (i.e. $K^p=K$). *Then*:

A) *There is a (canonical) surjective ring homomorphism φ: $W(K)\to R$ if and only if*

$$(*)\quad \begin{cases} \text{for every } \bar{a}\in K \text{ with } \bar{a}^{p(n)}=0 \text{ for a positive integer } n, \text{ there} \\ \text{is a } b\in R \text{ with } \bar{b}=\bar{a} \text{ such that } p^s b^{p(n-s)}\equiv 0 \pmod{p^n} \text{ for all} \\ 0\leq s\leq n-1. \end{cases}$$

B) *In case the condition of* A) *is satisfied, the homomorphism φ: $W(K)\to R$ is an isomorphism if and only if $p^n c=0$ for a positive integer n and for a $c\in R$ implies $\bar{c}^{p(n)}=0$ in K.*

The next lemma is the key to all.

Lemma. *Let R, K be as in* Th. 2 *and assume the condition* (*) *to hold. Let x, y be elements of K, and let $\{x_\nu;\ \nu=0, 1, 2, \cdots\}$, $\{y_\nu;\ \nu=0, 1, 2, \cdots\}$ be sequences of elements in R such that $(\overline{x_\nu})^{p(\nu)}=\bar{x}$, $(\overline{y_\nu})^{p(\nu)}=\bar{y}$ for all $0\leq\nu<\infty$. Then, the limits $\lim_{\nu\to\infty} x^{p(\nu)}$, $\lim_{\nu\to\infty} y^{p(\nu)}$ exist; if $\bar{x}^{p(n)}=\bar{y}^{p(n)}$, then $p^n \lim_{\nu\to\infty} x^{p(\nu)}=p^n \lim_{\nu\to\infty} y^{p(\nu)}$.*

Proof of the lemma. Let $\bar{z}_\nu=\bar{x}_\nu-\bar{y}_\nu$; by assumption, we have $(\bar{z}_\nu)^{p(n+\nu)}=\bar{x}^{p(n)}-\bar{y}^{p(n)}=0$, whence there exists $z_\nu\in R$ for each ν with $\bar{z}_\nu=\bar{z}_\nu$ such that $p^s z_\nu^{p(n+\nu-s)}\equiv 0 \pmod{p^{n+\nu}}$ for $0\leq s\leq n+\nu-1$. Now

start out with the relation $x_\nu \equiv y_\nu + z_\nu \pmod{p}$, and take the p^ν-th powers of both sides to obtain

$$x_\nu^{p(\nu)} \equiv y_\nu^{p(\nu)} + \sum_{i=1}^{p^\nu-1} \binom{p^\nu}{i} y_\nu^{p(\nu)-i} z_\nu^i \quad (p^{\nu+1}).$$

But, if $p^k \leq i < p^{k+1} \leq p^\nu$, then it is easily verified that $\binom{p^\nu}{i} \equiv 0 \ (p^{\nu-k})$. It follows that

$$p^n \binom{p^\nu}{i} z_\nu^i = p^{n+\nu-k} \times (\text{an integer}) \times z_\nu^{p(k)} z_\nu^{i-p(k)} \equiv 0 \quad (p^{n+\nu})$$

and, consequently, $p^n x_\nu^{p(\nu)} \equiv p^n y_\nu^{p(\nu)} \pmod{p^{n+\nu}}$, which would prove $p^n \lim x_\nu^{p(\nu)} = p^n \lim y_\nu^{p(\nu)}$ provided that the limits exist. But the existence of $\lim x_\nu^{p(\nu)}$, say, can be easily seen if one takes an obviously convergent sequence $w_0 = x, w_1, \cdots, w_\nu, \cdots$ in R with $(\overline{w_{\nu+1}})^p = \overline{w_\nu}$ $(0 \leq \nu < \infty)$ and apply the foregoing to the sequences $\{x_\nu\}$, $\{w_\nu\}$ to get $x_\nu^{p(\nu)} \equiv w_\nu^{p(\nu)} \ (p^\nu)$ for all ν. This proves the lemma.

Proof of Theorem 2. A) Assume the condition (*) to be true. Let $\bar{x} \in K$ be given, and find a sequence $\{x_\nu;\ \nu = 0, 1, 2, \cdots\}$ in R with $(\overline{x_\nu})^{p(\nu)} = \bar{x}$ for all ν. Define a mapping μ: $K \to R$ by $\mu(\bar{x}) = \lim_{\nu\to\infty} x_\nu^{p(\nu)}$. By the lemma, $\mu(x)$ is well-defined. Clearly μ is multiplicative: $\mu(\bar{x}\bar{y}) = \mu(\bar{x})\mu(\bar{y})$ for all $\bar{x}, \bar{y} \in K$. Also, evidently, $\overline{\mu(\bar{x})} = \bar{x}$. Further, if λ: $K \to R$ is a mapping with the last two properties, then $\lambda(\bar{a}) = \lambda(\bar{a}_\nu)^{p(\nu)}$ for every choice of a sequence $\{a_\nu\}$ with $(\bar{a}_\nu)^{p(\nu)} = \bar{a}$ for all ν, whence $\lambda(\bar{a}) = \lim_{\nu\to\infty} \lambda(a_\nu)^{p(\nu)} = \mu(\bar{a})$. We have thus established that μ is the unique multiplicative cross section of $R \to R/pR$ (*viz.* a generalized Teichmüller lifting).

We now define φ: For each Witt vector $(\bar{x}_0, \bar{x}_1, \cdots, \bar{x}_n, \cdots) \in W(K)$, let $\varphi(\bar{x}_0, \bar{x}_1, \cdots, \bar{x}_n, \cdots) = \mu(\bar{x}_0) + \mu(\bar{x}_1^{p(-1)})p + \cdots + \mu(\bar{x}_n^{p(-n)})p^n + \cdots$. Here, for each $1 \leq n < \infty$, $\bar{x}_n^{p(-n)}$ denotes any one of possibly many p^n-th roots of $\bar{x}_n$ in K. By virtue of the lemma, the choice of p^n-th root does not affect $\mu(\bar{x}_n^{p(-n)})p^n$, and we find φ well-defined. Proof that φ is a ring-homomorphism may be carried out exactly

the same way as in the standard Witt theory. We omit the proof, referring the reader to Serre (*loc. cit.*). Finally, for a given $y=\sum_{\nu=0}^{\infty}\mu(\bar{y}_\nu)p^\nu$, we find $\varphi(\bar{y}_0, \bar{y}_1^{p}, \cdots, \bar{y}_n^{p^{(n)}}, \cdots)=y$. This shows the surjectiveness of φ. We have thus derived the existence of the desired φ from the condition (*). The converse being obvious, the proof of A) is done.

B) Let φ be as above, and suppose that $\varphi(\bar{x}_0, \bar{x}_1, \cdots, \bar{x}_n, \cdots)=\mu(\bar{x}_0)+\mu(\bar{x}_1^{p^{(-1)}})p+\cdots+\mu(\bar{x}_n^{p^{(-n)}})p^n+\cdots=0$. Then $\overline{\mu(\bar{x}_0)}=\bar{x}_0=0$; if $\bar{x}_0=\cdots=\bar{x}_{n-1}=0$, then $p^n[\mu(\bar{x}_n^{p^{(-n)}})+\mu(\bar{x}_{n+1}^{p^{(-n-1)}})p+\cdots]=0$, and the hypothesis gives $(\bar{x}_n^{p^{(-n)}})^{p^{(n)}}=\bar{x}_n=\bar{0}$. Conversely, if φ is an isomorphism, $p^nc=0$ for $c\in R=W(K)$ clearly implies $\bar{c}^{p^{(n)}}=\bar{0}$. This concludes the proof of Theorem 2.

Remark. In the statement of Theorem 2, the modulus p^n appearing in (*) may be replaced by $p^{\alpha(n)}$ where α is an arbitrary, integer-valued, monotone increasing function of n.

3. In connection with the essential assumption, $K^p=K$, of Theorem 2, we observe the following fact:

Proposition. *Let K be a commutative ring with 1 having prime characteristic p. One can then build a commutative ring $\widetilde{K}$ with 1 which is closed under the p-th root operation ($\widetilde{K}^p=\widetilde{K}$) and an injective ring-homomorphism $K\subseteq\widetilde{K}$.*

Proof. For each $\alpha\in K$ let X_α be an indeterminate. To the finite field F_p of p elements adjoin the family $\{X_\alpha;\ \alpha\in K\}$ of indeterminates to obtain the polynomial ring $F_p[X]=F_p[X_\alpha;\ \alpha\in K]$. Next adjoin to the last ring all the formal p^ν-th roots $X^{p^{(-\nu)}}$ of the X_α's and form the ring $F_p[X_\alpha X^{p^{(-\infty)}}]=F_p[X_\alpha^{p^{(-1)}}, \cdots, X_\alpha^{p^{(-n)}}, \cdots;\ \alpha\in K]$. Now consider the surjective ring-homomorphism $F_p[X]\to R$ defined by $X_\alpha\to\alpha$, and call J its kernel. Let $\widetilde{J}$ be the extension of J to $F_p[X^{p^{(-\infty)}}]$, *viz.* $\widetilde{J}=JF_p[X^{p^{(-\infty)}}]$. We then obtain a diagram

$$\begin{array}{ccccc} \widetilde{J} & \overset{\subset}{\to} & F_p[X^{p^{(-\infty)}}] & \overset{\text{onto}}{\longrightarrow} & \widetilde{K}=F_p[X^{p^{(-\infty)}}]/\widetilde{J} \\ \uparrow\cup & & \uparrow\cup & & \uparrow \\ J & \overset{\subset}{\to} & F_p[X] & \overset{\text{onto}}{\longrightarrow} & K. \end{array}$$

At this point we remark that the ring $F_p[X^{p^{(-\infty)}}]$ viewed as F_p-vector space has a basis consisting of monomials in the X_α's with each X_α having an exponent of type

$$\frac{m_{-\lambda}}{p^\lambda}+\cdots+\frac{m_{-1}}{p}+m_0+\cdots+m_\nu p^\nu$$

with $0\leq m_i\leq p-1$ for all i. Let $F_p[X]^*$ represent the set of all F_p-linear combinations of the monomials $X_\alpha^a\cdots X_\sigma^s$ for which at least one of the $a,\cdots,s$ is *not* a p-adic integer. Evidently, $F_p[X]^*$ is an $F_p[X]$-module and, furthermore, it gives a direct sum decomposition

$$F_p[X^{p^{(-\infty)}}]=F_p[X]\dot{+}F_p[X]^*$$

as $F_p[X]$-modules. That having been said, one can now prove that $\widetilde{J}\cap F_p[X]=J$. Indeed, if $f_1b_1+\cdots+f_mb_m\in F_p[X]$ with $f_i\in F_p[X^{p^{(-\infty)}}]$ and $b_i\in J$ for all $1\leq i\leq m$, then for each i make a decomposition $f_i=f_{i1}+f_{i2}$, $f_{i1}\in F_p[X]$, $f_{i2}\in F[X]^*$ so as to get $f_1b_1+\cdots+f_mb_m=(f_{11}b_1+\cdots+f_{m1}b_m)+(f_{12}b_1+\cdots+f_{m2}b_m)$; evidently $f_{12}b_1+\cdots+f_{m2}b_m=0$ since $f_1b_1+\cdots+f_mb_m\in F_p[X]$, which yields the result $\widetilde{J}\cap F_p[X]=J$. As a consequence the ring-homomorphism $K\to\widetilde{K}$ is injective. q.e.d.

In conclusion let us observe that the $\widetilde{K}$ we have constructed is noncanonical and possesses no uniqueness property.

NORTHERN ILLINOIS UNIVERSITY