Münster J. of Math. **7** (2014), 105–114
urn:nbn:de:hbz:6-22359594300

Münster Journal of Mathematics

An alternative to Witt vectors

Joachim Cuntz and Christopher Deninger

(Communicated by Urs Hartl)

Dedicated to our friend and colleague Peter Schneider

Abstract. The ring of Witt vectors associated to a ring R is a classical tool in algebra. We introduce a ring $C(R)$ which is more easily constructed and which is isomorphic to the Witt ring $W(R)$ for a perfect $\mathbb{F}_p$-algebra R. It is obtained as the completion of the monoid ring $\mathbb{Z}R$, for the multiplicative monoid R, with respect to the powers of the kernel of the natural map $\mathbb{Z}R \to R$.

1. Introduction

Since the work of Witt on discretely valued fields with given perfect residue field in [9] the "vectors" that carry his name have become important in many branches of mathematics. In [6], [7] Lazard gave a new approach to Witt vectors generalizing the theory to the case of a perfect $\mathbb{F}_p$-residue algebra. This approach is the one used in Serre [8] for example. Addition and multiplication of Witt vectors are defined by certain universal polynomials. This description is cumbersome. While thinking about periodic cyclic cohomology for $\mathbb{F}_p$-algebras we found an alternative $C(R)$ to the p-typical Witt ring $W(R)$ of a perfect $\mathbb{F}_p$-algebra R. The rings $C(R)$ and $W(R)$ are canonically isomorphic but the construction of $C(R)$ as a completion (hence the name) of a monoid algebra $\mathbb{Z}R$ is much simpler. We have therefore made an effort to develop the properties of $C(R)$ independently of the theory of $W(R)$.

Using the approach in [3], [4] we can define periodic cyclic homology for a ring R using completed extensions by free (noncommutative) $\mathbb{Z}$-algebras. If one applies this procedure to an $\mathbb{F}_p$-algebra R, the completion $C(R)$ of the free $\mathbb{Z}$-module $\mathbb{Z}R$ appears as a natural intermediate step.

If the $\mathbb{F}_p$-algebra R is not perfect, $C(R)$ is still defined and different from $W(R)$. However a somewhat more involved construction in the same spirit does

Research supported by DFG through CRC 878 and by ERC through AdG 267079.

give $W(R)$ in general. We will address this in a subsequent paper together with applications.

In this note all rings are commutative with 1 and all ring homomorphisms map 1 to 1. The background reference is [8, II §4–§6].

2. Construction and properties of $C(R)$

A p-ring A is a commutative ring with unit which is Hausdorff and complete for the topology defined by a sequence of ideals $\mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \dots$ with the following properties:

1) $\mathfrak{a}_i \mathfrak{a}_j \subset \mathfrak{a}_{i+j}$ for $i, j \geq 1$,
2) $A/\mathfrak{a}_1 = R$ is a perfect $\mathbb{F}_p$-algebra, i.e. the Frobenius homomorphism $x \mapsto x^p$ is an isomorphism of R.

For a p-ring we have $p \in \mathfrak{a}_1$ and hence $\mathfrak{a}_i \supset p^i A$. A p-ring is called strict if $\mathfrak{a}_i = p^i A$ and if p is not a zero divisor in A. It is known that for every perfect $\mathbb{F}_p$-algebra R there is a strict p-ring $A = W(R)$ with $A/pA = R$. The pair $(W(R), W(R) \to R)$ is unique up to a unique isomorphism.

View R as a monoid under multiplication and let $\mathbb{Z}R$ be the monoid algebra of $(R, \cdot)$. Its elements are formal sums of the form $\sum_{r \in R} n_r [r]$ with almost all $n_r = 0$. Addition and multiplication are the obvious ones. Note that $[1] = 1$ but $[0] \neq 0$. Multiplicative maps $R \to B$ into commutative rings mapping 1 to 1 correspond to ring homomorphisms $\mathbb{Z}R \to B$. The identity map $R = R$ induces the surjective ring homomorphism $\pi : \mathbb{Z}R \to R$ which sends $\sum n_r[r]$ to $\sum n_r r$. Let I be its kernel, so that we have an exact sequence

$$0 \longrightarrow I \longrightarrow \mathbb{Z}R \xrightarrow{\pi} R \longrightarrow 0.$$

It is not difficult to see that as a $\mathbb{Z}$-module I is generated by elements of the form $[r] + [s] - [r + s]$ for $r, s \in R$. We will not use this fact in the sequel. The multiplicative isomorphism $r \mapsto r^p$ of R induces a ring isomorphism $F : \mathbb{Z}R \to \mathbb{Z}R$ mapping $\sum n_r[r]$ to $\sum n_r[r^p]$. It satisfies $F(I) = I$.

Let $C(R) = \varprojlim_\nu \mathbb{Z}R/I^\nu$ be the I-adic completion of $\mathbb{Z}R$. By construction $C(R)$ is Hausdorff and complete for the topology defined by the ideals $\mathfrak{a}_i = \widehat{I^i}$ where

$$\widehat{I^i} = \varprojlim_\nu I^i/I^\nu \subset C(R).$$

Note that at this stage we do not know that $\widehat{I^i} = \hat{I}^i$ since $\mathbb{Z}R$ is not noetherian in general. Condition 1) above is satisfied and 2) as well since

$$C(R)/\hat{I} = \mathbb{Z}R/I = R.$$

Hence $C(R)$ is a p-ring. The construction of $C(R)$ is functorial in R.

Theorem 1. *Let R be a perfect $\mathbb{F}_p$-algebra. Then $C(R)$ is a strict p-ring with $C(R)/pC(R) = R$.*

The result is an immediate consequence of the universal properties shared by $C(R)$ and any strict p-ring with residue algebra R, once one knows that such a strict p-ring exists; see remark 6 below. In the following we give a self-contained proof of Theorem 1 which does not use this information.

Consider the "arithmetic derivation" $\delta : \mathbb{Z}R \to \mathbb{Z}R$ defined by the formula

$$\delta(x) = \frac{1}{p}(F(x) - x^p).$$

It is well defined since $F(x) \equiv x^p \bmod p\mathbb{Z}R$ and since $\mathbb{Z}R$ being a free $\mathbb{Z}$-module has no $\mathbb{Z}$-torsion. The following formulas for $x, y \in \mathbb{Z}R$ are immediate

$$\delta(x+y) = \delta(x) + \delta(y) - \sum_{\nu=1}^{p-1} \frac{1}{p}\binom{p}{\nu} x^\nu y^{p-\nu} \tag{1}$$

and

$$\delta(xy) = \delta(x)F(y) + x^p \delta(y). \tag{2}$$

Applying (2) inductively gives the relation

$$\delta(x_1 \cdots x_n) = \sum_{\nu=1}^{n} x_1^p \cdots x_{\nu-1}^p \delta(x_\nu) F(x_{\nu+1}) \cdots F(x_n) \text{ for } x_i \in \mathbb{Z}R. \tag{3}$$

Equation (1) shows that we have

$$\delta(x+y) \equiv \delta(x) + \delta(y) \bmod I^n \text{ if } x \text{ or } y \text{ is in } I^n. \tag{4}$$

Together with (3) it follows that

$$\delta(I^n) \subset I^{n-1} \text{ for } n \geq 1. \tag{5}$$

Lemma 2. *Let R be a perfect $\mathbb{F}_p$-algebra and $n \geq 1$ an integer.*
a) If $pa \in I^n$ for some $a \in \mathbb{Z}R$ then $a \in I^{n-1}$.
b) $I^n = I^\nu + p^n\mathbb{Z}R$ for any $\nu \geq n$.

Proof. a) According to formula (5) we have $\delta(pa) \in I^{n-1}$. On the other hand, by definition:

$$\delta(pa) = F(a) - p^{p-1}a^p,$$

and therefore since $pa \in I^n$

$$\delta(pa) \equiv F(a) \bmod I^n.$$

It follows that $F(a) \in I^{n-1}$ and hence $a \in I^{n-1}$ since F is an automorphism with $F(I) = I$.

b) We prove the inclusion $I^n \subset I^\nu + p^n\mathbb{Z}R$ for $\nu \geq n$ by induction with respect to $n \geq 1$. The other inclusion is clear. For $y \in \mathbb{Z}R$ and $\nu \geq 1$ we have

$$F^\nu(y) \equiv y^{p^\nu} \bmod p\mathbb{Z}R.$$

Applying this to $y = F^{-\nu}(x)$, we get for all $x \in \mathbb{Z}R$

$$x \equiv F^{-\nu}(x)^{p^\nu} \bmod p\mathbb{Z}R.$$

For $x \in I$ this shows that $x \in I^\nu + p\mathbb{Z}R$ settling the case $n = 1$ of the assertion.

Now assume that $I^n \subset I^\nu + p^n\mathbb{Z}R$ has been shown for a given $n \geq 1$ and all $\nu \geq n$. Fix some $\nu \geq n+1$ and consider an element $x \in I^{n+1}$. By the induction assumption $x = y + p^n z$ with $y \in I^\nu$ and $z \in \mathbb{Z}R$. Hence

$p^n z = x - y \in I^{n+1}$. Using assertion a) of the lemma repeatedly shows that $z \in I$. Hence $z \in I^\nu + p\mathbb{Z}R$ by the case $n = 1$. Writing $z = a + pb$ with $a \in I^\nu$ and $b \in \mathbb{Z}R$ we find

$$x = (y + p^n a) + p^{n+1} b \in I^\nu + p^{n+1}\mathbb{Z}R.$$

Thus we have shown the induction step $I^{n+1} \subset I^\nu + p^{n+1}\mathbb{Z}R$. □

After these preparations the *proof of Theorem 1* follows easily: We have to show that $p^n C(R) = \widehat{I^n}$ for all $n \geq 1$ and that p is not a zero divisor in $C(R)$. Let $p^{-n}(I^\nu)$ be the inverse image of I^ν under p^n-multiplication on $\mathbb{Z}R$. Then for any $\nu \geq n \geq 1$ we have an exact sequence where the surjectivity on the right is due to part b) of Lemma 2:

$$0 \longrightarrow p^{-n}(I^\nu)/I^\nu \longrightarrow \mathbb{Z}R/I^\nu \xrightarrow{p^n} I^n/I^\nu \longrightarrow 0.$$

From this we get an exact sequence of projective systems whose transition maps for $\nu \geq n$ are the reduction maps. Set $N_\nu = p^{-n}(I^\nu)/I^\nu$. Then we have an exact sequence

$$0 \longrightarrow \varprojlim_{\nu} N_\nu \longrightarrow C(R) \xrightarrow{p^n} \widehat{I^n} \longrightarrow \varprojlim_{\nu}{}^{(1)} N_\nu.$$

The transition map $N_{\nu+n} \to N_\nu$ is the zero map since $a \in p^{-n}(I^{\nu+n})$ implies $p^n a \in I^{\nu+n}$ and hence $a \in I^\nu$ by part a) of Lemma 2. In particular (N_ν) is Mittag-Leffler, so that $\varprojlim_{\nu}^{(1)}(N_\nu) = 0$. It is also clear now that $\varprojlim_\nu N_\nu = 0$. It follows that p^n-multiplication on $C(R)$ is injective with image $\widehat{I^n}$. Hence p is not a zero divisor and $\widehat{I^n} = p^n C(R)$. □

Remarks.

1) If R is a perfect $\mathbb{F}_p$-algebra there is an isomorphism

$$R \xrightarrow{\sim} I^n/I^{n+1} \text{ given by } r \longmapsto p^n[r].$$

This follows because:

$$I^n/I^{n+1} = \widehat{I^n}/\widehat{I^{n+1}} = p^n C(R)/p^{n+1}C(R) \overset{p^{-n}}{=} C(R)/pC(R) = R.$$

2) The automorphism F of $\mathbb{Z}R$ satisfies $F(I) = I$. Hence it induces an automorphism F of $C(R)$ which lifts the Frobenius automorphism of the perfect $\mathbb{F}_p$-algebra R. The Verschiebung $V : C(R) \to C(R)$ is the additive homomorphism defined by $V(x) = pF^{-1}(x)$. By definition $\operatorname{Im} V^i = p^i C(R)$ and $V \circ F = F \circ V = p$. The projection $\pi : C(R) \to R$ has a multiplicative splitting defined as the composition $\omega : R \hookrightarrow \mathbb{Z}R \to C(R)$. Frobenius F, Verschiebung V and Teichmüller lift ω are well known extra structures on rings of Witt vectors.

Proposition 3. *If $R = K$ is a perfect field of characteristic p then $C(K)$ is a discrete valuation ring of mixed characteristic with residue field K.*

Proof. This is true for any strict p-ring W with residue field K. The well known argument is as follows. By assumption pW is a maximal ideal of W. For $x \in W \setminus pW$ choose $y \in W$ with $xy \equiv 1 \bmod p$. Then $(xy)^{p^\nu} \equiv 1 \bmod p^\nu$ by [8, II §4 Lemma 1]. Hence $x \bmod p^\nu$ is a unit in $W/p^\nu W$ and therefore $x = (x \bmod p^\nu)_{\nu \geq 0}$ is a unit in W. Hence the ring W is local with unique maximal ideal pW. Since W is separated i.e. $\bigcap_{\nu=1}^\infty p^\nu W = 0$ it follows that for every $0 \neq a \in W$ there is a unique integer $v(a) \geq 0$ with $a = p^{v(a)} x$ and $x \in W \setminus pW$ i.e. $x \in W^*$. Since multiplication with p is injective on W, it follows that W is an integral domain. The map $v : W \setminus \{0\} \to \mathbb{Z}$ satisfies $v(ab) = v(a) + v(b)$ by definition and $v(a+b) \geq \min(v(a), v(b))$ because as seen above, an element of W is a unit if and only if its reduction $\bmod p$ is nonzero. The valuation v extends uniquely to a discrete valuation on the quotient field Q of W with valuation ring W. □

Remark. In particular $C(K)$ is noetherian while in general $\mathbb{Z}K$ is very far from being noetherian.

As a topological additive group, $C(R)$ has another description which is sometimes useful. Let $\mathfrak{b}$ be a basis of the $\mathbb{F}_p$-algebra R and let $\mathbb{Z}\mathfrak{b}$ be the free $\mathbb{Z}$-module with basis $\mathfrak{b}$. The inclusion $\mathfrak{b} \subset R$ induces an additive homomorphism

$$\mathbb{Z}\mathfrak{b} \hookrightarrow \mathbb{Z}R \longrightarrow C(R)$$

and hence a map

$$\widehat{\mathbb{Z}\mathfrak{b}} = \varprojlim_n \mathbb{Z}\mathfrak{b}/p^n\mathbb{Z}\mathfrak{b} \longrightarrow C(R).$$

Proposition 4. *If R is a perfect $\mathbb{F}_p$-algebra, the map $\widehat{\mathbb{Z}\mathfrak{b}} \to C(R)$ is a topological isomorphism of additive groups. In particular any inclusion $R_1 \hookrightarrow R_2$ resp. surjection $R_1 \twoheadrightarrow R_2$ of perfect $\mathbb{F}_p$-algebras induces an inclusion $C(R_1) \hookrightarrow C(R_2)$ resp. surjection $C(R_1) \twoheadrightarrow C(R_2)$ with a continuous additive splitting.*

Proof. By Theorem 1 we have to show that for each $n \geq 1$ the additive map

$$\alpha_n : \mathbb{Z}\mathfrak{b}/p^n\mathbb{Z}\mathfrak{b} \longrightarrow C(R)/p^n C(R)$$

is an isomorphism. For $n = 1$ this is true because $\mathbb{F}_p\mathfrak{b} = R$ since $\mathfrak{b}$ is an $\mathbb{F}_p$-basis for R. Now assume that α_n is an isomorphism and consider the commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Z}\mathfrak{b}/p\mathbb{Z}\mathfrak{b} & \xrightarrow{p^n} & \mathbb{Z}\mathfrak{b}/p^{n+1}\mathbb{Z}\mathfrak{b} & \longrightarrow & \mathbb{Z}\mathfrak{b}/p^n\mathbb{Z}\mathfrak{b} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \alpha_1} & & \downarrow{\scriptstyle \alpha_{n+1}} & & \downarrow{\scriptstyle \alpha_n} & & \\
0 & \longrightarrow & C(R)/pC(R) & \xrightarrow{p^n} & C(R)/p^{n+1}C(R) & \longrightarrow & C(R)/p^nC(R) & \longrightarrow & 0
\end{array}$$

The upper sequence is exact and because of Theorem 1 the lower sequence is exact as well. Hence α_{n+1} is an isomorphism. The remaining assertions follow immediately. □

Remark. If the basis $\mathfrak{b}$ happens to be closed under multiplication then $\mathbb{Z}\mathfrak{b}$ is a ring and $\widehat{\mathbb{Z}\mathfrak{b}} \to C(R)$ an isomorphism of rings. This is the case in the following example. The perfect $\mathbb{F}_p$-algebra $R = \mathbb{F}_p[t_1^{p^{-\infty}}, \ldots, t_d^{p^{-\infty}}]$ has a basis $\mathfrak{b}$ consisting of monomials. This basis is multiplicatively closed and hence $C(R)$ is the p-adic completion of the monoid algebra $\mathbb{Z}\mathfrak{b}$ i.e. of the algebra $\mathbb{Z}[t_1^{p^{-\infty}}, \ldots, t_d^{p^{-\infty}}]$.

Proposition 5. *Let A be a p-ring with perfect residue algebra R as above. Then there is a unique homomorphism of rings $\hat{\alpha} : C(R) \to A$ such that the following diagram commutes:*

$$\begin{array}{ccc} C(R) & \xrightarrow{\hat{\alpha}} & A \\ & {\scriptstyle\pi}\searrow \quad \swarrow{\scriptstyle\pi_A} & \\ & R & \end{array} \tag{6}$$

Remark. This is true for any strict p-ring instead of $C(R)$, cp. [8, II §5 Prop. 10]. However in our case the argument is particularly simple and we do not even have to know that $C(R)$ is strict.

Proof. Since A is a p-ring, there is a unique multiplicative section $\alpha_0 : R \to A$ of π_A, cp. [8, II §4 Prop. 8]. Hence there is a unique ring homomorphism $\alpha : \mathbb{Z}R \to A$ such that the diagram

$$\begin{array}{ccc} \mathbb{Z}R & \xrightarrow{\alpha} & A \\ & {\scriptstyle\pi}\searrow \quad \swarrow{\scriptstyle\pi_A} & \\ & R & \end{array}$$

commutes. Since $\alpha(I) \subset \mathfrak{a}_1$ we have $\alpha(I^\nu) \subset \mathfrak{a}_1^\nu \subset \mathfrak{a}_\nu$ and therefore α extends to a unique and automatically continuous homomorphism $\hat{\alpha} : C(R) \to A$ such that (6) commutes. $\square$

Remark 6. As we saw above it is immediate that $C(R)$ is a p-ring with residue algebra R. Showing directly that $C(R)$ is a strict p-ring required some thought. If one already knows that there is a strict p-ring W with residue algebra R, then it is easy to see that $C(R)$ is isomorphic to W and hence strict. Here is the argument:

The universal property of strict p-rings [8, II §5 Prop. 10] gives us a unique homomorphism $\beta : W \to C(R)$ such that the diagram

$$\begin{array}{ccc} W & \xrightarrow{\beta} & C(R) \\ & \searrow \quad \swarrow{\scriptstyle\pi} & \\ & R & \end{array}$$

commutes. On the other hand by Proposition 5 there is a unique homomorphism $\hat{\alpha} : C(R) \to W$ such that

$$\begin{array}{ccc} C(R) & \xrightarrow{\hat{\alpha}} & W \\ & {\scriptstyle \pi}\searrow \quad \swarrow & \\ & R & \end{array}$$

commutes. The map $\alpha \circ \beta$ is the identity on W because of the universal property for the strict p-ring W. The map $\beta \circ \alpha$ is the identity on $C(R)$ by Proposition 5 because $C(R)$ is a p-ring. It follows that $C(R) \cong W$ is a strict p-ring. An equally simple proof may be given by using the characterization of the triple $(W(R), R \hookrightarrow W(R), \pi : W(R) \to R)$ in [2, Prop. 3.1] which is based on [5, Thm. 1.2.1].

From the preceding remark we get the following corollary:

Corollary 7. *Let $W_n(R)$ be the truncated (p-typical) Witt ring of the perfect $\mathbb{F}_p$-algebra R. There is a unique homomorphism of rings $\alpha_n : \mathbb{Z}R/I^n \to W_n(R)$ inducing the standard multiplicative embedding $R \hookrightarrow W_n(R)$ and making the following diagram commute*

$$\begin{array}{ccc} \mathbb{Z}R/I^n & \xrightarrow[\sim]{\alpha_n} & W_n(R) \\ & \searrow \quad \swarrow & \\ & R & \end{array}$$

Moreover, α_n is an isomorphism.

Proof. Let $W(R)$ be the p-typical Witt ring of R. According to Remark 6 there is a commutative diagram

$$\begin{array}{ccc} C(R) & \xrightarrow[\sim]{\hat{\alpha}} & W(R) \\ & \searrow \quad \swarrow & \\ & R & \end{array}$$

Reducing $\bmod p^n$ and noting that $W(R)/p^n W(R) = W_n(R)$ and

$$C(R)/p^n C(R) = C(R)/\widehat{I^n} = \mathbb{Z}R/I^n$$

we get an isomorphism α_n as desired. There is a unique ring homomorphism $\alpha : \mathbb{Z}R \to W_n(R)$ prolonging the multiplicative embedding $R \hookrightarrow W_n(R)$. Hence α_n is uniquely determined. $\square$

As a set $W_n(R)$ is R^n. Addition and multiplication are given by certain universal polynomials in $2n$ variables over $\mathbb{Z}$. We now describe the isomorphism α_2. Note that (4) and (5) imply that δ induces a (nonadditive) map

$$\overline{\delta} : \mathbb{Z}R/I^2 \longrightarrow \mathbb{Z}R/I = R.$$

We also have the ring homomorphism of reduction $\pi : \mathbb{Z}R/I^2 \to \mathbb{Z}R/I = R$.

Proposition 8. *The isomorphism*

$$\alpha_2 : \mathbb{Z}R/I^2 \xrightarrow{\sim} W_2(R) = R^2$$

is given by the map $(\pi, \overline{\delta})$.

Proof. The composition $R \to \mathbb{Z}R/I^2 \to W_2(R) = R^2$ is the standard multiplicative embedding. One checks that α_2 is a ring homomorphism using the formulas for addition and multiplication on $W_2(R) = R^2$:

$$(x, y) + (x', y') = \Big(x + x', y + y' - \frac{1}{p}\sum_{\nu=1}^{p-1}\binom{p}{\nu} x^{\nu} x'^{p-\nu}\Big)$$

and

$$(x, y) \cdot (x', y') = (xx', x'^p y + y' x^p + pyy').$$

Using Corollary 7 the assertion follows. □

Remark. With respect to the ordinary R-module structure on R^2 the map α_2 is nonlinear. Hence the simple addition and multiplication on $\mathbb{Z}R/I^2$ become something nonobvious on R^2. We have not tried to describe α_n for $n \geq 3$ by explicit formulas.

It is interesting to compare the I-adic completion $C(R)$ of $\mathbb{Z}R$ with its p-adic completion i.e. the completion with respect to powers of the ideal $p\mathbb{Z}R$. Lemma 2b) shows that the projective system $(I^n/p^n\mathbb{Z}R)_n$ satisfies the Mittag-Leffler condition. Therefore we obtain the following exact sequence

$$0 \to \varprojlim I^n/p^n\mathbb{Z}R \to \varprojlim \mathbb{Z}R/p^n\mathbb{Z}R \to \varprojlim \mathbb{Z}R/I^n \to 0 \tag{7}$$

which describes the kernel of the natural map from the p-adic completion to $C(R)$.

Now, if R is a finite perfect $\mathbb{F}_p$-algebra, then the p-adic completion of $\mathbb{Z}R$ is $\mathbb{Z}_pR$ the monoid algebra of R over $\mathbb{Z}_p$ and $C(R)$ has an instructive description as a complete subring of $\mathbb{Z}_pR$.

Proposition 9. *Assume that R is a finite perfect $\mathbb{F}_p$-algebra. Then there is an idempotent e in $\mathbb{Z}_pR$ such that $e(\mathbb{Z}_pR)$ is the kernel of the natural map $\mathbb{Z}_pR \to C(R)$ and such that $(1-e)\mathbb{Z}_pR$ is topologically isomorphic to $C(R)$.*

Proof. For each n, the quotient $\mathbb{Z}R/p^n\mathbb{Z}R$ is finite and in particular an Artin ring (descending chains of ideals become stationary). Using Lemma 2b), we see that the image A_n of I^n in $\mathbb{Z}R/p^n\mathbb{Z}R$ is an ideal such that $A_n^2 = A_n$.

According to the structure theorem for Artin rings (see e.g. [1, Thm. 8.7]), $\mathbb{Z}R/p^n\mathbb{Z}R$ is (uniquely) a finite direct product $\prod_i B_i$ of local Artin rings B_i. Any idempotent ideal in a local Artin ring B is either 0 or equal to B since the maximal ideal in B is nilpotent, [1, 8.2 and 8.4]. Therefore the projection of A_n to any of the components B_i is either 0 or B_i. If we let e_n denote the sum of the identity elements of the B_i in which the component of A_n is nonzero we get an idempotent e_n in $\mathbb{Z}R/p^n\mathbb{Z}R$ such that $e_n(\mathbb{Z}R/p^n\mathbb{Z}R) = A_n$ (e_n is a unit element for A_n and therefore uniquely determined).

Since, by Lemma 2b), the image of I^{n+1} in $\mathbb{Z}R/p^{n+1}\mathbb{Z}R$ maps surjectively to the image of I^n in $\mathbb{Z}R/p^n\mathbb{Z}R$ under the natural map, the sequence (e_n) defines an element e in $\mathbb{Z}_pR = \varprojlim \mathbb{Z}R/p^n\mathbb{Z}R$. By construction it is an idempotent in $A = \varprojlim A_n = \varprojlim I^n/p^n\mathbb{Z}R$ such that $ex = x$ for each x in A. It follows that $A = e(\mathbb{Z}_pR)$.

The exact sequence (7) then shows that the map $(1-e)\mathbb{Z}_pR \to C(R)$ is a continuous bijective homomorphism between compact rings and therefore a topological isomorphism. □

Remark. The proof shows that $A = e(\mathbb{Z}_pR)$ in the preceding proposition is a unital ring which is the projective limit of a system (A_n) of unital rings with unital transition maps. In the case $R = \mathbb{F}_p$ looking at the canonical decomposition of $\mathbb{Z}_pR$ under the action of $\mathbb{F}_p^\times$ we see that e has the following explicit description

$$1 - e = (p-1)^{-1} \sum_{r \in \mathbb{F}_p^\times} \omega(r)^{-1}[r] \text{ in } \mathbb{Z}_pR.$$

Here ω is the Teichmüller character $\omega : \mathbb{F}_p^\times \to \mathbb{Z}_p^\times$.

References

[1] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, MA, 1969. MR0242802 (39 #4129)

[2] A. Connes and C. Consani, Characteristic 1, entropy and the absolute point, in *Noncommutative geometry, arithmetic, and related topics*, 75–139, Johns Hopkins Univ. Press, Baltimore, MD. MR2907005

[3] J. Cuntz and D. Quillen, Cyclic homology and nonsingularity, J. Amer. Math. Soc. **8** (1995), no. 2, 373–442. MR1303030 (96e:19004)

[4] J. Cuntz and D. Quillen, Excision in bivariant periodic cyclic cohomology, Invent. Math. **127** (1997), no. 1, 67–98. MR1423026 (98g:19003)

[5] J.-M. Fontaine, Le corps des périodes p-adiques, Astérisque No. 223 (1994), 59–111. MR1293971 (95k:11086)

[6] M. Lazard, Détermination des anneaux p-adiques et π-adiques dont les anneaux des restes sont parfaits, in *Seminaire Krasner 1953/54*, Exp. 9, 16 pp, Fac. Sci. Paris, Paris. MR0115997 (22 #6794)

[7] M. Lazard, Bemerkungen zur Theorie der bewerteten Körper und Ringe, Math. Nachr. **12** (1954), 67–73. MR0066353 (16,561a)

[8] J.-P. Serre, *Local fields*, translated from the French by Marvin Jay Greenberg, Graduate Texts in Mathematics, 67. Springer-Verlag, New York-Berlin, 1979. MR0554237 (82e:12016)

[9] E. Witt, Zyklische Körper und Algebren der Charakteristik p vom Grad p^n. Struktur diskret bewerteter perfekter Körper mit vollkommenem Restklassenkörper der Charakteristik p, J. Reine Angew. Math. **176** (1936), 126–140.

Received November 12, 2013; accepted November 29, 2013

J. Cuntz
Westfälische Wilhelms-Universität Münster, Mathematisches Institut,
Einsteinstr. 62, 48149 Münster, Germany
E-mail: `cuntz@uni-muenster.de`

C. Deninger
Westfälische Wilhelms-Universität Münster, Mathematisches Institut,
Einsteinstr. 62, 48149 Münster, Germany
E-mail: `c.deninger@uni-muenster.de`