On generic C_{p^n}-extensions

by

Cornelius Greither

Max-Planck-Institut für Mathematik
Gottfried-Claren-Str. 26
D-5300 Bonn 3, FRG

Mathematisches Institut
der Universität München
Theresienstr. 39
D-8000 München 2, FRG

MPI/89- 59

0. Introduction

The purpose of this note is to bring together several approaches which lead to information on p-power cyclic Galois extensions of commutative rings A, and hence on p-power cyclic unramified extensions of p-adic fields K (here one uses the well-known principle: L/K is Galois and unramified iff O_L/O_K is Galois). One idea is to construct a "generic" C_{p^n}-extension, as set forth by Saltman [**Sa**], the major difference being that Saltman uses a base field but our interest is in mixed characteristic cases. We cannot construct extensions which are generic for the whole category of commutative rings A, so we restrict A to range over the category of p-adically complete and separated rings (call such rings *p-complete* for short). For a discussion how the C_{p^n}-extensions of A relate to those of its p-adic completion, see §2 in [**Gr2**]. Another method is Ullom's approach [**Ul**] (Ullom credits Iwasawa for the idea): Describe unramified C_{p^n}-extensions of $K_n = \mathbf{Q}_n(\zeta_{p^n})$ by exhibiting them in the form $E = K_n(\beta^{p^{-n}})$ with suitable conditions on β. It turns out that one may take β of the form y^ξ, where $\xi \in \mathbf{Z}[\mathrm{Aut}(K_n/\mathbf{Q}_p)]$ is a sort of Stickelberger element. This leads us to the third approach: There is a technique of Galois descent which allows one to descend certain C_{p^n}-extensions from $K(\zeta_{p^n})$ to K (K a suitable ring and $p \neq 2$). The element ξ plays an important role in that theory, which was first expounded by Miki [**Mi**]; see also [**Gr1**] and [**Ch**]. Note here that for $K = \mathbf{Q}_p$ *all* unramified extensions of $K(\zeta_{p^n})$ descend to extensions of K. Last, there is Hasse's elegant description of unramified C_{p^n}-extensions of p-adic fields which contain ζ_{p^n} (see [**Ha**]), which uses what I call Artin-Hasse exponentials. In the given form, this theory is unsuitable for calculations. In [**Gr2**] we have given a modified version which seems to be more explicit.

The results in this note draw on all this, to some part only implicitly.

Let us describe the main result. Let $R = \mathbf{Z}[t]^{\wedge_p}$ be the p-adic completion of $\mathbf{Z}[t]$, t a variable, p a prime. One may think of R as the subring of $\mathbf{Z}_p[[t]]$ which consists of all $\sum a_i t^i$ where the a_i are a null sequence in $\mathbf{Z}_p$. Let $1 \leq n \in \mathbf{N}$. Then there exists a C_{p^n}-Galois extension $R^{(n)}/R$ such that:

a) $R^{(n)}/R$ is "generic" for p-complete rings: For any C_{p^n}-Galois extension B/A of p-complete rings, there is a ring homomorphism $\phi : R \to A$ realizing

B/A, i.e. such that $B \cong A \otimes_\phi R^{(n)}$, up to twist with a smaller p-extension (we will shortly explain what this phrase means).

b) One has a quite explicit description of $R^{(n)}$. Here we will only give the description of $R_n^{(n)} = R^{(n)}[\zeta_{p^n}]$, and defer the description of $R^{(n)}$ proper to §4. To wit, $R_n^{(n)}$ is the integral closure of $R[\zeta_{p^n}]\big[B_n(t)^{p^{-n}}\big]$, and

$$B_n(t) = \exp\big(p^n\eta\, t + (p^n\eta + p^{n-1}\eta^p)t^p + (p^n\eta + p^{n-1}\eta^p + p^{n-2}\eta^{p^2})t^{p^2} + \ldots\big),$$

where η is a parameter of the DVR $\mathbf{Z}_p[\zeta_{p^n}]$, defined by the formula

$$\prod_{(p,m)=1} (1-\eta^m)^{\mu(m)/m} = \zeta_{p^n}.$$

The main point in the description of $R^{(n)}$ is that one has an explicit solution of the equation $B_n(t) = Y_n(t)^\xi$ in R_n.

Remarks. 1) The *existence* of $R^{(n)}/R$ as in a) , even without the encumbering phrase "up to twist..", is a rather easy consequence of the following: whenever A is p-adically complete, reduction mod p defines an equivalence of categories between the C_{p^n}-extensions of A and those of $\bar{A} = A/pA$. This, and how to prove the existence result from it, will be explained in §1. In the rest of the paper, it is the actual *description* of $R^{(n)}$ that matters.

2) The definition of $B_n(t)$ is complicated and seems to properly involve infinite expressions. Observe, however, that for actual calculations only a good p-adic approximation to η and $B_n(t)$ is needed, since all elements of $R[\zeta_{p^n}]$ sufficiently close to 1 are p^n-th powers.

3) The term "generic" is only used informally in §§1-4: whenever we attach this label to some Galois extension we say explicitly what we mean by it in the given case. However, in §5 we offer a suggestion how one might formalize the notion "generic for a certain category of rings" for C_{p^n}-extensions.

At the end of this introduction we explain the imprecise phrase "up to twist .." in a) above, and how to do away with it.

Given any $C_{p^{n-1}}$-extension D/A, one associates to it a C_{p^n}-extension called $\mathrm{Ind}_{n-1}^n(D)/A$. The definition is precisely the definition of induction in representation theory; we always fix a generator σ_n of C_{p^n} and think of $C_{p^{n-1}}$ as a subgroup of C_{p^n} by $\sigma_{n-1} = \sigma_n^p$. Moreover, the set $\mathrm{Gal}(A, C_{p^n})$

of all (isomorphism classes of) C_{p^n}-extensions is an abelian group (the so-called Harrison group), and we now declare the phrase "up to twist with a smaller p-extension" to mean: "up to multiplication with a factor of the form $\mathrm{Ind}_{n-1}^n(D)$", D as above. One can get rid of these factors by an inductive procedure, we sketch the argument. Let $S = n$-fold tensor product of R with itself. Let $S_{(i)}$ $(i = 0, \ldots, n-1)$ be the $C_{p^{n-i}}$-extension obtained by base-extending the "generic" extension $R^{(i)}$ along the $i+1$-st injection $R \to S$. Let $S^{(n)}$ be the Harrison product

$$S_{(0)} \cdot \mathrm{Ind}_{n-1}^n(S_{(1)}) \cdot \mathrm{Ind}_{n-2}^n(S_{(2)}) \cdot \ldots \cdot \mathrm{Ind}_1^n(S_{n-1})$$

in $\mathrm{Gal}(S, C_{p^n})$. One can then easily show (amended version of a) above) that every C_{p^n}-extension B/A of p-complete rings can be obtained from $S^{(n)}/S$ by base change $\phi : S \to A$. We won't use this in the sequel.

At this point, I would like to thank S. Ullom for a stimulating letter. This is also a good opportunity to express my gratitude to the MPI in Bonn for its hospitality.

Conventions and Notations:

All rings are commutative. C_{p^n} stands for the cyclic group of order p^n, we fix a generator $\sigma = \sigma_n$. For any finite abelian group G and any ring A, $\mathrm{Gal}(A, G)$ is the group of isomorphism classes of G-Galois extensions of A (we will not distinguish isomorphism classes and their representatives). Good references on Galois theory of rings are [**CHR**], [**DeI**], and also Section 0 of [**Sa**] for a review of facts.

Our main notational problem is that there are too many rings involved. We adopt therefore two standing rules: If ? is a ring, then $?_n$ denotes that ring with ζ_{p^n} adjoined. If ? is a ring, then anything denoted $?^{(n)}$ will be a C_{p^n} extension of ? (of course, this is not a definition, just a mnemotechnic aid). The rings we use for generic constructions in char. zero have letters R, S, T, V (possibly adorned); rings of char. p are $\Lambda, \Sigma, \mathsf{F}$, maybe adorned. There is a list of rings at the end of the paper. If A is a ring, we let $\bar{A} = A/pA$. Lastly, recall A is p-complete iff $A \cong \varprojlim A/p^n A$.

1. Reduction mod p

Proposition 1.1. *If A is p-complete, then the map $r_A : \mathrm{Gal}(A, C_{p^n}) \to \mathrm{Gal}(\bar{A}, C_{p^n})$ which sends B to $\bar{B} = B/pB$, is an isomorphism. For $B_1, B_2 \in \mathrm{Gal}(A, C_{p^n})$, the canonical map $\mathrm{Hom}(B_1, B_2) \to \mathrm{Hom}(\overline{B_1}, \overline{B_2})$ is also an isomorphism. (The Hom's mean C_{p^n}-invariant A-(resp. $\bar{A}$-)algebra homomorphisms.) The same holds if we reduce not mod p but mod any $\lambda \in A$ a power of which is associated to p (main example: $\lambda = 1 - \zeta_{p^n}$).*

PROOF: See 2.1 and 2.2 of [**GH**]. One can also deduce the proposition from EGA IV, 18.1.2, using a passage to the limit. QED.

As mentioned earlier, we get from this an existence theorem for generic extensions almost for free. We shall give this argument, even though we shall later more or less duplicate the existence proof by our explicit construction. One reason for doing so is that it gives us an opportunity to review Artin-Schreier theory (cf. [**Gr2**],§3):

Let Σ be a ring of char. p. Then every C_{p^n}-extension Λ/Σ is obtained as follows:

$$\Lambda = \Sigma[\theta^{(n)}]/(\theta^{(n)^{\mathrm{Fr}}} \dot{-} \theta^{(n)} \dot{-} a^{(n)}), \qquad a^{(n)} \in W_n(\Sigma),$$

$$\sigma(\theta^{(n)}) = \theta^{(n)} \dot{+} \mathbf{1}.$$

Explanation of symbols used: $a^{(n)}$ is a Witt vector of length n over Σ; $\theta^{(n)}$ is a vector of n indeterminates $\theta_1, \ldots, \theta_n$; the symbols $\dot{+}, \dot{-}$ denote addition resp. subtraction in the ring of n-Witt vectors over $\Sigma[\theta_1, \ldots, \theta_n]$; Fr is Frobenius, acting on the components of Witt vectors; $\mathbf{1}$ is the unit element of the ring of Witt vectors. All relations and equations are actually n-tuples of relations or equations: this is a shorthand notation. In the case $n = 1$ where one can forget about Witt vectors, all this is widely known.

From this description, it is rather clear that there exists a generic C_{p^n}-extension $\Sigma^{(n)}/\Sigma$ *for rings of char.* p, and one can take $\Sigma = \mathbf{F}_p[t_1, \ldots, t_n]$ and $\Sigma^{(n)} = \Lambda$ as above with $a^{(n)} = (t_1, \ldots, t_n)$. One can find a more general result on p-groups in §4 of [**Sa**]. We can now prove

Theorem 1.2. *There is a C_{p^n}-extension $S'^{(n)}/S'$ of p-complete rings such that for any C_{p^n}-extension B/A of p-complete rings there exists $\phi : S' \to A$ with $A \otimes_\phi S'^{(n)} = B$.*

PROOF. Let S' be the p-completion of $\mathbf{Z}[t_1, \ldots, t_n]$, and note that $\overline{S'} = \Sigma$. By 1.1 there is a C_{p^n}-extension $S'^{(n)}$ (say) of S' with $\overline{S'^{(n)}} = \Sigma^{(n)}$. If B/A is now given, find $\psi : \Sigma \to \bar{A}$ with $\bar{B} = \bar{A} \otimes_\phi \Sigma^{(n)}$. There exists $\phi : S' \to A$ with $\bar{\phi} = \psi$, because S' is free on the elements $t_1, \ldots, t_n$ in the category of p-complete rings. We have a commutative diagram (where the argument C_{p^n} is omitted from Gal, and where the horizontal maps are base change along ϕ and ψ respectively):

$$\begin{array}{ccc} \mathrm{Gal}(S') & \longrightarrow & \mathrm{Gal}(A) \\ r_{S'} \downarrow & & r_A \downarrow \\ \mathrm{Gal}(\Sigma) & \longrightarrow & \mathrm{Gal}(\bar{A}) \end{array}$$

with injective vertical arrows. Then $A \otimes_\phi S'^{(n)} \cong B$, since this becomes true after applying r_A to both sides. QED.

This proof is very inconstructive, since one has no real handle on preimages under the reduction map mod p. There is, however, a special case where one knows more (and we will use this knowledge):

Definitions.

A ring Σ is perfect if Fr: $x \mapsto x^p$ *is bijective. (Surjectivity is not enough!)*

A ring R is a Witt ring for the perfect ring Σ if: p does not divide zero in R, R is p-adically complete, and $R/pR \cong \Sigma$.

Proposition 1.3. *If Σ is perfect, then a Witt ring for Σ exists; it may be obtained as the ring of infinite Witt vectors, as in Witt's original construction, and it is unique up to unique isomorphism and functorial in Σ. One denotes it by $W(\Sigma)$. In particular,* Fr: $\Sigma \to \Sigma$ *lifts to* Fr $\in Aut(W(\Sigma))$. *There is a unique multiplicative section $j : \Sigma^\times \to R = W(\Sigma)$, and one has*

$j(\alpha) = \lim a_n^{p^n}$ *where* a_n *is a preimage of* $\alpha^{p^{-n}} \in \Sigma$. *Finally, every* $x \in R$ *has a unique representation in the form*

$$x = \sum_{\nu=0}^{\infty} j(x_\nu)\, p^\nu, \qquad x_\nu \in \Sigma.$$

PROOF. All of this is well-known. For precise references and indications of proofs, see [**Gr2**], p.278.

Lemma 1.4. *Suppose* $p \in R$ *is a nonzerodivisor,* R *is* p*-complete, and* $\bar{R}$ *is perfect. Then the inverse to*

$$r_R : \mathrm{Gal}(R, C_{p^n}) \to \mathrm{Gal}(\bar{R}, C_{p^n})$$

is given by the Witt ring functor: $\Lambda \mapsto W(\Lambda)$.

PROOF. We may identify R with $W(\bar{R})$. Since $\overline{W(\Lambda)} = \Lambda$ for all perfect Λ, it suffices to show that for all $\Lambda \in \mathrm{Gal}(\bar{R}, C_{p^n})$, Λ is again perfect and its Witt ring is in fact a C_{p^n}-extension of $W(\bar{R})$. The first statement is an easy lemma, see [**Gr2**], Lemma 5.2. As to the second: if $R^{(n)} \in \mathrm{Gal}(R, C_{p^n})$ is any lifting of Λ, then $R^{(n)}$ is automatically p-complete and p does not divide zero in it, hence $R^{(n)}$ is a Witt ring for Λ. (One might also work with Witt vectors explicitly and show $W(\Lambda)/W(\Sigma)$ Galois by brute force.) QED.

To obtain a generic C_{p^n}-extension $R^{(n)}/R$, the obvious idea is now to take the generic extension $\Sigma^{(n)}/\Sigma$ in characteristic p and apply the Witt ring functor to it. The main objection is, of course, that $\Sigma = \mathsf{F}_p[t_1, \ldots, t_n]$ is not perfect. A minor point is that we would like to deal with one variable t at a time. The generic base ring R which we are about to construct will reduce to $\mathsf{F}_p[t]$ mod p (and not to Σ), but under way we will have to consider also F, the perfect closure of $\mathsf{F}_p[t]$, and worse things.

2. The formalism of Artin-Hasse powers

This section is expository and proofs can be found in [**Gr2**] or Hasse's original paper [**Ha**].

For each p-complete ring A let $m(A) = \{a \in A : \exists s \in \mathbf{N}[a^s \in pA]\}$. Suppose $\bar{A}$ is perfect, and $A \subset A_1$ is another p-complete ring. (In important applications, $\overline{A_1}$ will not be perfect.) Then one has a power

$$(1-b)^a, \qquad a \in A,\ b \in m(A_1),$$

satisfying the following rules:

Proposition 2.1. [Hasse]

(0) If $a \in \mathbf{Z}_p \subset A$, then $(1-b)^a$ is the same as if evaluated via the binomial series (which converges in A_1). In particular, for $n \in \mathbf{Z}$, $(1-b)^n$ is what it should be.

(1) $(1-b)^a \equiv (1-ab) \bmod b^2 A_1$.

(2) $(1-b)^a \cdot (1-b)^c = (1-b)^{a+c}$ $(a, c \in A)$.

(3) $(1-b)^{ar} = \left((1-b)^a\right)^r$ $(a \in A, r \in \mathbf{Z}_p)$.

Remark to (3): (3) can be deduced from (2) by continuity arguments. The other equation $(1-b)^{ar} = ((1-b)^r)^a$ fails badly. We shall see cases with $1-b = \zeta_{p^n}$ where $(1-b)^{ap^n}$ is different from 1.

We now put the definition of $(1-b)^a$ on record for future reference:

$$(1-b)^a = \prod_{\nu=0}^{\infty} P\left(1 - j(a_\nu) \cdot \eta(b)\right)^{p^\nu}$$

with

$$a = \sum_{\nu=0}^{\infty} j(a_\nu) p^\nu, a_\nu \in \bar{A},$$

$$P(1-X) = \prod_{(p,m)=1} (1-X^m)^{\mu(m)/m},$$

and

$$\eta(X) \in \mathbf{Z}_p[\zeta_{p^n}][[X]] \text{ is defined by } P(1-\eta(X)) = 1 - X.$$

We prove also for later use

Lemma 2.2. *Let A, A_1 be p-complete, $A = W(\bar{A})$, $\bar{A}$ perfect, $\zeta_{p^n} \in A_1$. Then*

a) *If $p^{2n} \mid a \in A$, then $\zeta_{p^n}^a \equiv 1 \bmod p^n$. (The exponent $2n$ is bigger than actually necessary here.)*

b) *Suppose that we have $A_1 = A[\zeta_{p^n}]$. Let $B \in \mathrm{Gal}(A, C_{p^n})$, hence $B = W(\bar{B})$ with $\bar{B} \in \mathrm{Gal}(\bar{A}, C_{p^n})$. Put $B_n = B[\zeta_{p^n}]$ and extend $\sigma \in C_{p^n}$ to B_n by putting $\sigma(\zeta_{p^n}) = \zeta_{p^n}$. Suppose finally we have $\theta \in B$ with $\sigma(\theta) \equiv \theta + 1 \bmod p^{2n}$. Then the element $z := \zeta_{p^n}^\theta$ satisfies $\sigma(z) \equiv \zeta_{p^n} z \bmod p^n$.*

PROOF. a) We have $\zeta_{p^n} = 1 - \lambda$ with $\lambda^{(p-1)p^{n-1}}$ associated to p in A_1. Moreover, $\eta(\lambda)$ is associated to λ. One now uses the definition of $\zeta_{p^n}^a$, the fact that $a_\nu = 0$ for $\nu < 2n$, and some trivial estimate like $p^n \geq 2n$ to obtain the result.

b) Using the functoriality of the Witt ring construction, one obtains the Galois action formula

$$\sigma((1-b)^a) = (1-\sigma(b))^{\sigma(a)}$$

for $a \in B, b \in m(B_n)$. Here σ can be any automorphism of B_1 leaving B invariant. In our special case $1 - b = \zeta_{p^n}$ we get

$$\sigma(\zeta_{p^n}^\theta) = \zeta_{p^n}^{\sigma(\theta)}.$$

From this, and part a), and the rules 2.1 (1), (2), the conclusion follows. QED.

Lemma 2.2 b) gives an impression of the fundamental idea, which goes back to Hasse and Witt: If θ is an "Artin-Schreier element", then $\zeta_{p^n}^\theta$ is a Kummer element.

3. Construction of the generic extension $R_n^{(n)}/R_n$

Recall R = p-adic completion of $\mathbf{Z}[t]$. We let $R_n = R[\zeta_{p^n}]$. Here we construct a "generic" C_{p^n}-extension $R_n^{(n)}/R_n$, which will later be descended to an extension $R^{(n)}/R$ with analogous properties. Since the base ring R_n is in a sense still too small, there is another descent implicit in the proof of theorem 3.1, which we will now state after defining some notation.

Let $T = W(\mathsf{F})$ with $\mathsf{F} = \mathsf{F}_p[t^{p^{-\infty}}]$.

Let $V = W(\hat{\mathsf{F}})$ with $\hat{\mathsf{F}}$ = t-adic completion of F. Note that F and $\hat{\mathsf{F}}$ are perfect. As usual let T_n and V_n arise from T and V by adjunction of ζ_{p^n}. We denote the image of t under the multiplicative section $j : \mathsf{F} \to T$ again by t. Let

$$\Theta = -t - t^p - t^{p^2} - t^{p^3} - \dots$$

Remark: This is indeed a well-defined element of V. This is not entirely trivial, since Θ is not j of the analogously defined element of $\hat{\mathsf{F}}$. What one needs is that V is t-adically complete, and this can be shown either by inspection of Witt polynomials or by noting that the t-adic completion of V is again a Witt ring for $\hat{\mathsf{F}}$ and invoking uniqueness.

Obviously we have $\Theta^{\mathrm{Fr}} - \Theta = t$. (This formula motivated the definition of Θ.)

Theorem 3.1. *Let $Z_n = Z_n(t) \in V_n$ be the Artin-Hasse power $\zeta_{p^n}^{\Theta}$.*

a) $Z_n^{p^n} \in R_n$ (R_n embeds into V_n by $t \mapsto t$).

b) $R_n^{(n)}$:= integral closure of $R_n[Z_n]$ in $R_n[Z_n, \frac{1}{p}]$ is a C_{p^n}-Galois extension with $\sigma(Z_n) = \zeta_{p^n} \cdot Z_n$.

c) If we reduce modulo $\lambda = 1 - \zeta_{p^n}$, then we obtain $R_n/(\lambda) = \mathsf{F}_p[t]$ and

$$R_n^{(n)}/(\lambda) \cong \mathsf{F}_p[t]\big[\theta^{(n)}\big]\big/\big(\theta^{(n)^{\mathrm{Fr}}} \dot{-} \theta^{(n)} \dot{-} (t, 0, ..., 0)\big),$$

an Artin-Schreier extension as explained in §1.

PROOF. First we construct a $\mathbf{Z}_p$-extension

$$\mathsf{F} = \mathsf{F}^{(0)} \subset \mathsf{F}^{(1)} \subset \dots \subset \mathsf{F}^{(N)} \subset \dots \subset \hat{\mathsf{F}},$$

and a corresponding $\mathbf{Z}_p$-extension

$$T = T^{(0)} \subset T^{(1)} \subset \ldots \subset T^{(N)} \subset \ldots \subset V,$$

and the usual variant of the latter with ζ_{p^n} adjoined (denoted by a subscript n), with the following property:

$$\mathsf{F}^{(N)} \cong \mathsf{F}[\theta^{(N)}]/(\theta^{(N)^{\mathrm{Fr}}} \dot{-} \theta^{(N)} \dot{-} (t, 0, \ldots, 0)),$$

and the (topological) generator σ of $\mathbf{Z}_p = \varprojlim C_{p^n}$ acts by $\sigma(\theta^{(N)}) = \theta^{(N)} \dot{+} 1$ for all $N \in \mathbf{N}$. This goes by "approximating Θ":

Let $\Theta = \sum_{\nu=0}^{\infty} j(a_\nu^{p^{-\nu}})p^\nu$ with $a_\nu \in \hat{\mathsf{F}}$. If we identify V with the ring of infinite length Witt vectors over $\hat{\mathsf{F}}$, Θ becomes identified with the vector $(a_0, a_1, \ldots)$. Let $\theta^{(N)}$ be the vector $(a_0, \ldots, a_{N-1})$. We get from the equation $\Theta^{\mathrm{Fr}} - \Theta = t = j(t) = j(t) \cdot p^0$ that

$$\theta^{(N)^{\mathrm{Fr}}} \dot{-} \theta^{(N)} = (t, 0, \ldots, 0) \in W_N(\hat{\mathsf{F}}).$$

Hence $\mathsf{F}^{(N)} := \mathsf{F}[a_0, \ldots, a_{N-1}]$ is C_{p^N}-Galois with σ acting by the rule $\sigma(\theta^{(N)}) = \theta^{(N)} \dot{+} 1$, and the chain $(\mathsf{F}^{(N)})_{N \in \mathbf{N}}$ forms a $\mathbf{Z}_p$-extension. Let $T^{(N)} \subset V$ be the Witt ring of $\mathsf{F}^{(N)}$ and $T_n^{(N)} := T^{(N)}[\zeta_{p^n}]$. Then the $T^{(N)}$ and $T_n^{(N)}$ form a $\mathbf{Z}_p$-extension of T and T_n respectively. Let $T_n^{(\infty)}$ be the p-adic closure of $\bigcup_{N \in \mathbf{N}} T_n^{(N)}$. The automorphism σ can be uniquely extended to $T_n^{(\infty)}$.

CLAIM: $Z_n \in T_n^{(\infty)}$ and $\sigma(Z_n) = \zeta_{p^n} Z_n$.

Proof of Claim: Let $\zeta = \zeta_{p^n}$. Let $\Theta_N = \sum_{\nu=0}^{N-1} j(a_\nu^{p^{-\nu}})p^\nu$. Then the Artin-Hasse power ζ^{Θ_N} is in $W(\mathsf{F}^{(N)})[\zeta] = T_n^{(N)}$, and p^N divides $\Theta - \Theta_N$. From Lemma 2.2 a) we infer that $\zeta^\Theta \in$ closure $(\bigcap_N T_n^{(N)})$. Similarly, $\sigma(\Theta_N) \equiv \Theta_N + 1$ modulo p^N. Applying 2.2 a) again we get $\sigma(\Theta) = \Theta + 1$ and (by 2.1)

$$\sigma(Z_n) = \sigma(\zeta^\Theta) = \zeta^{\sigma(\Theta)} = \zeta^{\Theta+1} = \zeta \cdot Z_n.$$

This proves the Claim.

By the claim, σ fixes $Z_n^{p^n}$. From this one gets that $Z_n^{p^n} \in T_n$. (There is a slight technical problem here: if $Z_n^{p^n}$ were in any of the $T_n^{(N)}$, one would be done immediately, but we only know it is in the closure of their union. We

leave this harmless technical point to the reader.) By the same reasoning, Z_n itself lies in $T_n^{(n)}$, the n-th layer of the Zp-extension. Hence Z_n is a Kummer element for the C_{p^n}-extension $T_n^{(n)}/T_n$, in particular it is a unit. From this we get by Kummer theory (noting that T_n is integrally closed): $T_n^{(n)}$ is the integral closure of $T_n[Z_n]$ in its quotient field. This is what we want to prove, except that the base ring is T_n, not R_n.

Definition: $B_n = Z_n^{p^n} \in T_n$.

We now try to replace T_n by R_n. Note first that $T_n^{(N)}$ reduces mod λ to $\mathsf{F}^{(N)}$. Let $\mathsf{F}_p[t]^{(N)}$ be defined as the Artin-Schreier extension of $\mathsf{F}_p[t]$ given by

$$\mathsf{F}_p[t]^{(N)} = \mathsf{F}_p[t]\big[\theta^{(N)}\big] \big/ \big(\theta^{(N)^{\mathrm{Fr}}} \dot{-} \theta^{(N)} \dot{-} (t, 0, \ldots, 0)\big).$$

Let $\tilde{R}_n^{(N)}/R_n$ be a lifting of the C_{p^n}-extension $\mathsf{F}_p[t]^{(N)}/\mathsf{F}_p[t]$. Then $T_n \otimes_{R_n} \tilde{R}_n^{(N)}$ induces the same thing mod λ as does $T_n^{(N)}$, so these two extensions are isomorphic themselves by Prop. 1.1. Moreover one finds by Kummer theory a unit $\tilde{B}_n \in R_n$ such that $\tilde{R}_n^{(N)}$ is the integral closure of $R_n[\tilde{B}_n^{p^{-n}}]$. (Use $\mathrm{Pic}(R_n) = 0$ and R_n integrally closed.) It follows that the quotient $\tilde{B}_n B_n^{-1}$ is a p^n-th power in T_n. We know $\tilde{B}_n \in R_n$, and we shall prove $B_n \in R_n$ in Theorem 3.3 (no circularity involved). Hence the quotient just mentioned is a unit of R_n. By a somewhat technical but straightforward result (see [**Gr2**] Thm. B), the quotient has to be a p^n-th power in R_n already. (Idea of proof of that result: The "only" elements of R_n which become p-th powers in T^n are powers of t, but these are non-units.) Hence $R_n^{(N)}$ (as defined in the statement of 3.1) and $\tilde{R}_n^{(N)}$ coincide, and 3.1 is proved modulo 3.3. QED.

Proposition 3.2. a) *With $\eta \in \mathbf{Z}_p[\zeta_{p^n}]$ defined by setting X equal to $\lambda = 1 - \zeta_{p^n}$ in $\eta(X)$, we have*

$$-\log Z_n = \eta t + (\eta + \frac{\eta^p}{p})t^p + (\eta + \frac{\eta^p}{p} + \frac{\eta^{p^2}}{p^2})t^{p^2} + \ldots$$

in $V[\frac{1}{p}]$.

b) $\log Z_n \in R_n[\frac{1}{p}]$.

PROOF. a) We compute:

$$\begin{aligned}\log Z_n &= \log(\zeta^{\Theta}) \\ &= -\sum_{\nu=0}^{\infty} \log \zeta^{t^{p^\nu}} \ \text{(def. of } \Theta\text{; 2.1 (2))} \\ &= -\sum_{\nu} \log P(1-\eta\, t^{p^\nu}) \ \ \text{(use } j(t^{p^\nu}) = t^{p^\nu}\text{)} \\ &= \sum L(1-\eta\, t^{p^\nu})\end{aligned}$$

(where $L(1-X) = X + X^p/p + X^{p^2}/p^2 + \ldots$; the claimed equality results from the definition of P and Möbius inversion, see 4.10 [**Gr2**])

$$\begin{aligned}= -\eta\, t - \frac{\eta^p}{p} t^p - \frac{\eta^{p^2}}{p^2} t^{p^2} - \ldots \\ - \eta\, t^p - \frac{\eta^p}{p} t^{p^2} \ldots \\ - \eta\, t^{p^2} - \ldots \\ \ddots\end{aligned}$$

QED.

b) The terms η^{p^ν}/p^ν converge to zero p-adically (and rapidly so, once $\nu > n$). Furthermore, from

$$0 = \log(1-\lambda) = \log P(1-\eta) = -L(1-\eta) = \eta + \frac{\eta^p}{p} + \frac{\eta^{p^2}}{p^2} + \ldots$$

one sees that also the partial sums $\sum_{i \le \nu} \frac{\eta^{p^\nu}}{p^\nu}$, i.e. the coefficients of t^{p^ν} in $-\log Z_n$, go to zero for $\nu \to \infty$. QED.

As a corollary we obtain

Theorem 3.3.

$$B_n^{-1} = \exp\bigl(p^n \eta t + (p^n \eta + p^{n-1}\eta^p) t^p + (p^n \eta + p^{n-1}\eta^p + p^{n-2}\eta^{p^2}) t^{p^2} + \ldots\bigr),$$

and this is in R_n.

PROOF. Since $Z_n \equiv 1$ modulo η, we have $B_n \equiv 1$ modulo η^{p^n}. The latter is associated with $p(1-\zeta_p)$. Hence B_n certainly is equal to exp of its log,

and the result follows from 3.2. (One should check that there are indeed no denominators left, i.e. the p^{n-i} are always made integral by the η^{p^i}.) QED.

We conclude this section by formulating and proving the genericity property of the extension $R_n^{(n)}/R_n$:

Theorem 3.4. *For each C_{p^n}-extension B/A of p-complete rings containing ζ_{p^n}, there exists $\phi : R_n \to A$ with*

$$B \cong (A \otimes_\phi R_n^{(n)}) \text{ times } B',$$

where B' is induced from a $C_{p^{n-1}}$-extension.

PROOF. Recall $\lambda = 1 - \zeta_{p^n}$. We know that $R_n^{(n)}$ reduces modulo λ to

$$\bar{R}[\theta^{(n)}]/(\theta^{(n)^{\mathrm{Fr}}} \dot{-} \theta^{(n)} \dot{-} (t, 0, \ldots, 0)).$$

By Artin-Schreier theory there exist $a_0, \ldots, a_{n-1} \in \bar{A}$ with

$$B/\lambda B \cong (A/\lambda A)[X^{(n)}]/(X^{(n)^{\mathrm{Fr}}} \dot{-} X^{(n)} \dot{-} (a_0, \ldots, a_{n-1}),$$

where $X^{(n)}$ is a fresh vector of n indeterminates. Define $\phi : R_n \to A$ by sending t to any preimage of a_0. We now assert that B differs from $A \otimes_\phi R_n^{(n)}$ only by an induced extension B' as in the theorem. By Prop. 1.1 we may check this after going modulo λ. Then $A \otimes_\phi R_n^{(n)}$ becomes

$$(A/(\lambda))[X^{(n)}]/(X^{(n)^{\mathrm{Fr}}} \dot{-} X^{(n)} \dot{-} (a_0, 0, \ldots, 0)),$$

and our assertion is reduced to (easy) facts from Artin-Schreier theory: addition of Witt vectors $a^{(n)}$ corresponds to the Harrison product of corresponding Artin-Schreier extensions, and extending vectors of length $n-1$ by a zero on the left essentially corresponds to induction of $C_{p^{n-1}}$-extensions to C_{p^n}-extensions.

For p-adic fields, we get the following:

Corollary 3.5. *Suppose K is a p-adic field containing ζ_{p^n}, and suppose its residue class field k has degree prime to p over F_p. Then "the" unramified C_{p^n}-extension L/K is obtained by adjoining a p^n-th root of $B_n(1)$ to K.*

PROOF. The Artin-Schreier extension of k belonging to the Witt vector $(1, 0, \ldots, 0)$ of length n is nondegenerate in the sense that it is not induced

from a $C_{p^{n-1}}$-extension (reason: its lowest layer $k[\theta_1]/(\theta_1^p - \theta_1 - 1)$ is a field). Moreover, K has essentially (i.e. up to changing the C_{p^n}-action) only one unramified C_{p^n}-extension. Hence this one must be the extension $D := O_K \otimes_\phi R_n^{(n)}$, with $\phi : R_n \to O_K, t \mapsto 1$. D is an integrally closed domain, Galois over O_K, hence we may write it $D = O_L$ with L/K an unramified C_{p^n}-extension. From the definition of D, it is clear that $L = K(B_n(1)^{p^{-n}})$. QED.

4. Cyclotomic descent

In this section we assume $p \neq 2$. Let $n \in \mathbf{N}, n \geq 1$.

Let K be any domain containing $\frac{1}{p}$ such that ζ_{p^n} has the maximal possible degree $s := \varphi(p^n) = (p-1)p^{n-1}$ over $\mathrm{Quot}(K)$, so $K_n = K[\zeta_{p^n}]$ is Galois over K with group Γ, where Γ comes with a canonical isomorphism $\omega : \Gamma \to (\mathbf{Z}/p^n\mathbf{Z})^\times$ which satisfies $\zeta^\delta = \zeta^{\omega(\delta)}$ for all $\zeta \in \mu_{p^n}(K_n), \delta \in \Gamma$. (The above degree assumption is unnecessary but it simplifies matters.) Let $g \in \mathbf{Z}$ be a primitive root mod p^2. As is well-known, g is then also primitive mod p^n (we excluded $p = 2$). Let $\gamma \in \Gamma$ be $\omega^{-1}(\bar{g})$, whence $\Gamma = \langle\gamma\rangle$. We will use two particular elements of $\mathbf{Z}\Gamma$, a sort of cyclotomically twisted conorm and norm:

$$\gamma - g,$$

and

$$\xi := \sum_{i=0}^{s-1} \gamma^i g^{s-i}$$

(recall $s = \varphi(p^n) = |\Gamma|$). ξ is similar to a Stickelberger element. In the following, we use for $\beta \in K_n^\times$ the notation $K_n\{z^{p^n} = \beta\}$ for the C_{p^n}-Galois extension $K_n[Z]/(Z^{p^n} - \beta), \sigma(\beta) = \zeta_{p^n}\beta$.

The following theorem was first proved by Miki [**Mi**] (he assumed K to be a field, but everything goes through in our situation. See also [**Gr1**] §2 and [**Ch**]): Let $\beta \in K_n^\times$.

Theorem 4.1.

a) *The extension $K_n\{z^{p^n} = \beta\}$ is abelian over K iff $\beta^{\gamma - g}$ is a p^n-th power in K_n.*

b) *The extension $K_n\{z^{p^n} = \beta\}$ can be written as $K_n \otimes_K L$, $L \in \mathrm{Gal}(K, C_{p^n})$ iff there exists $y \in K_n^\times$ with $\beta \equiv y^\xi$ modulo $K_n^{\times p^n}$.*

PROOF. See [**Mi**] Prop. 2 and 3 or [**Sa**] Thm.2.3.

Remarks: 1) If $L_n := K_n\{z^{p^n} = \beta\}$ is not a domain, it is not quite clear what "abelian" means (since "the" Galois group of L_n over K is not well-defined), so we had better explain what we mean. We mean the following: L_n/K is G-Galois, where G is abelian, and appears in a short exact sequence

$$1 \to C_{p^n} \to G \to \Gamma \to 1,$$

where we also demand that this sequence induce the given actions of C_{p^n} on L_n/K_n, and of Γ on K_n/K.

2) Of course, the left hand side of b) in the theorem implies the left hand side of a) (with $G = C_{p^n} \times \Gamma$, i.e. the sequence mentioned in 1) splits). The same implication for the right hand sides can be quickly seen as follows: We have $(\gamma - g)\xi = \gamma^s - g^s = 1 - g^s = up^n$ with $u \in \mathbf{Z}$. (Later we will even use that u is not divisible by p, because g is also a primitive root modulo p^{n+1}.) Hence $\beta \equiv y^\xi$ implies $\beta^{\gamma - g} \equiv y^{up^n} \equiv 1$ (congruences modulo $K_n^{\times p^n}$).

3) In [**Gr1**] §2 and also in [**Ch**] it is shown that the group of extensions L_n satisfying b) has index p^{n-1} in the group of extensions satisfying the weaker condition a). In fact, let $U = K_n^\times / K_n^{\times p^n}$ and note that $\gamma - g$ as well as ξ pass on to endomorphisms $(\gamma - g)_U$ and ξ_U of U. Then $\mathrm{Ker}((\gamma - g)_U)/\mathrm{Im}(\xi_U)$ is cyclic of order p^{n-1}, generated by $\overline{\zeta_{p^n}}$. In verifying this, note that $\gamma - g$ kills ζ_{p^n} and $\zeta_{p^n}^\xi = \zeta_{p^n}^{-p^{n-1}}$ is a p-th primitive root of unity.

4) If $K = \mathbf{Q}_p$ and L/K is "the" nondegenerate unramified C_{p^n}-extension of K, then LK_n is "the" unramified C_{p^n}-extension of K_n and it is of the form $K_n\{Z^{p^n} = \beta\}$ for some $\beta = y^\xi, y \in K_n^\times$ by b). Ullom [**Ul**] has determined possible choices for y: for $n > 1$, all y with

$$y \in U_{2p-1}(K_n), y \notin U_{2p}(K_n)$$

will give "the" nondegenerate unramified C_{p^n}-extension of K_n.

Now we come back to generic extensions.

Theorem 4.2.

a) *The C_{p^n}-extension $R_n^{(n)}/R_n$ can be descended to a C_{p^n}-Galois extension $R^{(n)}/R$ which has the analogous generic property for C_{p^n}-extensions B/A as $R_n^{(n)}/R_n$ has for extensions B/A with the extra condition $\zeta_{p^n} \in A$ (Thm. 3.4).*

b) *$R^{(n)}$ can be constructed explicitly as follows: $B_n = Y_n^\xi$ with $Y_n = Y_n(t) \in R_n$ explicitly given, and $R^{(n)} \subset R_n^{(n)}$ is the fixed ring of the automorphism $\tilde{\gamma}$ defined by: $\tilde{\gamma} \mid R_n = \gamma$ (i.e. $\tilde{\gamma} \mid R = \mathrm{id}_R, \tilde{\gamma}(\zeta_{p^n}) = \zeta_{p^n}^g$), and $\tilde{\gamma}(B_n^{p^{-n}}) = B_n^{g \cdot p^{-n}} \cdot Y_n^{-u}$.*

PROOF. a) Again, existence is easy and is proved as before. Let $R^{(n)}/R$ be the extension inducing the Artin-Schreier extension

$$\bar{R}[\theta^{(n)}]/(\theta^{(n)^{\mathrm{Fr}}} \dot{-} \theta^{(n)} \dot{-} (t, 0, \ldots, 0))$$

on reduction modulo p. By Thm. 3.1 c) and Prop. 1.1 one obtains that indeed $R_n \otimes_R R^{(n)} \cong R_n^{(n)}$. The generic property is shown as in 3.4. QED.

b) We know from a) and 4.1 b) that the equation $B_n = Y_n^{\xi}$ is solvable at least up to a p^n-th power in $R_n[1/p]$. It is a good test for the whole theory to ask for an explicit solution, and this turns out to work quite well: we find such a solution for the equation (not only the congruence modulo p^n-th powers), and even in $R_n^{\times}$. Before entering the details, recall $(\gamma - g)\xi = up^n$ with $u \in \mathbf{Z}, u \notin p\mathbf{Z}$ (cf. Remark 2)). Recall also that

$$Z_n = \zeta^{\Theta} = \prod_{\nu=0}^{\infty} P(1 - \eta\, t^{p^{\nu}}) \in \mathbf{Z}_p[\zeta][[t]]$$

(but not in R_n), and $B_n = Z_n^{p^n} \in R_n^{\times}$.

Let $Y_n = Y_n(t) := Z_n^{(\gamma-g)/u}$. (The p-adic exponent $1/u$ is no problem since $Z_n \equiv 1 \bmod \lambda$.) The element Y_n is a priori in $\mathbf{Z}_p[\zeta_{p^n}][[t]]$, and it is also in $R_n^{(n)}$ because that ring is γ-stable. We want to show it is in R_n. For this, it suffices by Galois theory to show that Y_n is fixed under σ. For the following calculation, note that γ and σ commute, γ fixes $\Theta \in \mathbf{Z}_p[[t]]$, and σ fixes ζ_{p^n}. We find

$$\begin{aligned}
(Z_n^{\gamma})^{\sigma} &= \left((\zeta_{p^n}^{\Theta})^{\gamma}\right)^{\sigma} \\
&= \left(\gamma(\zeta)^{\Theta}\right)^{\sigma} \\
&= \gamma(\zeta)^{\sigma(\Theta)} \\
&= \gamma(\zeta)^{\Theta+1} \\
&= \gamma(\zeta) \cdot \gamma(\zeta)^{\Theta} \\
&= \zeta^{\gamma} \cdot Z_n^{\gamma}.
\end{aligned}$$

On the other hand:

$$\begin{aligned}(Z_n^g)^\sigma &= \left((\zeta^\Theta)^g\right)^\sigma \\ &= \left(\zeta^{g\Theta}\right)^\sigma \quad \text{by 2.1 (3)} \\ &= \zeta^{\sigma(g\Theta)} \\ &= \zeta^{g\Theta+g} \\ &= \zeta^g \cdot Z_n^g.\end{aligned}$$

By dividing and using $\zeta^\gamma = \zeta^g$ we obtain that $Y_n = Z_n^{\gamma-g}$ is fixed under σ, as we wanted.

The only question left is now to describe $R^{(n)}$ "physically" as a subset of $R_n^{(n)}$ = integral closure of $R_n[B_n^{p^{-n}}]$. We begin with some general remarks about so-called descent data: Suppose K is as at the beginning of this § and L/K is C_{p^n}-Galois. Assume $K_n \otimes_K L = K_n\{z^{p^n} = \beta\}$, $\beta \in K_n^\times$ ($K_n = K[\zeta_{p^n}]$ as always). Then L =Fix($\tilde{\gamma}$) where $\tilde{\gamma}$ is a Γ-descent datum, i.e. an automorphism of order $|\Gamma|$ of L_n/K which restricts to γ on K_n and commutes with the C_{p^n}-action. (We are implicitly using here that Γ is cyclic.) Of necessity, we will then have

$$\tilde{\gamma}(z) = z^g \cdot a, \quad a \in K_n^\times.$$

If so *defined*, $\tilde{\gamma}$ will give a descent datum if and only if $z^{g^s-1} \cdot a^\xi = 1$, i.e. $\beta^u \cdot a^\xi = 1$. (See **[Gr1]** §2, **[Sa]** p.258.) If we have a representation $\beta = y^\xi$ to begin with, we can rewrite $\beta^u a^\xi = 1$ as $(y^u \cdot a)^\xi = 1$. Hence the possible values of a are just $y^{-u} \cdot \epsilon$, with $\epsilon^\xi = 1$.

Lemma 4.3. *The group $\{\epsilon \in K_n^\times \mid \epsilon^\xi = 1\}$ is finite, and its p-component is precisely the group of p^{n-1}-st roots of unity, hence cyclic of order p^{n-1} (remember that K_n is a domain containing $1/p$).*

PROOF. If $\epsilon^\xi = 1$, then $\epsilon^{p^n u} = \epsilon^{\xi\cdot(\gamma-g)} = 1$, hence ϵ is a $p^n u$-th root of unity. If $\epsilon^{p^n} = 1 = \epsilon^\xi$ then ϵ cannot be a primitive p^n-th root of unity (we said before that $\zeta_{p^n}^\xi$ is not 1), but for any p^{n-1}-st root ϵ of unity, $\epsilon^\xi = 1$. QED.

We go back to the special situation $R_n^{(n)}/R_n$ which we want to descend explicitly. Let $K = R[1/p], K_n = R_n[1/p], L = R^{(n)}[1/p]$, to be in tune with

the notation used in the preceding discussion. By general descent theory, $R^{(n)}[1/p] = \mathrm{Fix}(\tilde{\gamma})$ for some Γ-descent datum $\tilde{\gamma}$ on $LK_n = R_n^{(n)}[1/p]$. We also have (because $R^{(n)}$ is integrally closed) that $R^{(n)} = \mathrm{Fix}(\tilde{\gamma}|R_n^{(n)})$. By construction of Y_n, we have $B_n = Z_n^{p^n} = Y_n^{\xi}$. Hence we have by the general discussion above and Lemma 4.3:

$$\tilde{\gamma}(Z_n) = Z_n^g \cdot Y_n^{-u} \cdot \epsilon,$$

where ϵ is some root of unity.

Theorem 4.4. $\epsilon = 1$.

PROOF. Note first we haven't made any statement as to the unicity of $\tilde{\gamma}$ and ϵ so far. We observe that $\epsilon \equiv 1$ modulo $\lambda = 1 - \zeta_{p^n}$. Reason: Z_n and Y_n are $\equiv 1$ modulo λ by construction, and $\tilde{\gamma}$ is $\equiv$ identity mod λ on $R[\zeta_{p^n}]$, hence $\equiv$ identity on $R_n^{(n)} = R_n R^{(n)}$ (note $\tilde{\gamma}$ fixes the elements of $R^{(n)}$). Hence $\epsilon \equiv 1$. By 4.3, ϵ must be a p-power root of unity and even a p^{n-1}-st root of unity. If we let ϵ *range* over all these, we get all *possible* descent data. But there are p^{n-1} nonisomorphic possibilities to descend LK_n/K_n to K. This is because the natural map $\mathrm{Gal}(K, C_{p^n}) \to \mathrm{Gal}(K_n, C_{p^n})$ has a kernel of order p^{n-1}; it is generated by Ind_{n-1}^n of the p-primary part of the Γ-extension K_n/K, or in more number-theoretic terms, by the same Ind of the $n-1$-st layer of the cyclotomic $\mathbf{Z}_p$-extension of K. Hence there exists only one ϵ which possibly can show up, and one suspects of course it has to be the distinguished choice $\epsilon = 1$. To prove this, we go modulo t and note that our uniqueness argument for ϵ is still valid. ($R/(t)$ is just $\mathbf{Z}_p$.) But by construction of $R^{(n)}/R$, this extension becomes trivial modulo t (look modulo p: you get the Artin-Schreier extension with Witt vector $(0, \ldots, 0)$). Note also $B_n \equiv 1$ modulo t. It is then elementary to verify that $\epsilon = 1$ defines a descent datum descending the trivial extension $R_n^{(n)}/(t)$ = integral closure of $\mathbf{Z}_p[\zeta_{p^n}]\{z^{p^n} = 1\}$ to the trivial C_{p^n}-extension of $R/(t) = \mathbf{Z}_p$, hence $\epsilon = 1$ is the only possibility modulo (t), and we are done. (Actually, if one tries to descend mod t with the wrong ϵ, one gets ramification.)

5. Final remarks

We never defined what a generic extension (for a certain range of rings) actually is (the genericity properties of our constructions were spelled out each time) . The following definition is to be regarded as tentative.

Let $\underline{C}$ be any full subcategory of the category of commutative rings which has pushouts (= tensor products). A C_{p^n}-extension S/R ($S, R \in \underline{C}$) is called $\underline{C}$-generic, if:

a) every C_{p^n}-extension B/A, $B, A \in \underline{C}$, can be deduced from S/R by a base change $\phi : R \to A$ in $\underline{C}$;

b) $R = R_0[1/r]$ with R_0 free in $\underline{C}$ over some finite set and $r \in R_0$.

Examples: We showed the existence of a generic C_{p^n}-extension for $\underline{C} = \{p$-complete rings$\}$ (Thm. 3.4 plus the discussion in the introduction). Here $R = p$-adic completion of $\mathbf{Z}[t]$ and r can be taken 1. Saltman [Sa] has shown the existence of a generic C_{p^n}-extension for all categories $F - \underline{Alg}$, F any field.

Saltman's proof (loc.cit. Thm. 5.3) shows: If there is a generic C_{p^n}-extension for $\underline{C}$, then for each semilocal $A \in \underline{C}$ with $A/\mathrm{rad}(A) \in \underline{C}$, we have the "lifting property":

$$\mathrm{Gal}(A, C_{p^n}) \to \mathrm{Gal}(A/\mathrm{rad}(A), C_{p^n}) \quad \text{is surjective.}$$

For $\underline{C} = \{p$-complete rings$\}$, this lifting property is, again, a direct consequence of the reduction mod p technique and Artin-Schreier theory. It seems, however, to be possible to construct a generic C_{p^n}-extension for the category of commutative rings A with: $\mathrm{Pic}(A) = 0$, $p \in A$ not a zero divisor, and $\zeta_{p^n} \in a$. The condition on p is more convenient than necessary. The condition on $\mathrm{Pic}(A)$ is necessary, since in its absence the lifting property may fail. It is not yet clear whether one can get rid of ζ_{p^n}. Another approach to get rid of the Pic condition is to only consider extensions with normal basis. A lifting property for these has been obtained by Kersten and Michaličeк [KM] for rings containing $1/p$ but not (necessarily) ζ_{p^n}. The question might be put as follows: What is the best (i.e. largest) category of rings for which one finds generic cyclic Galois extensions (working either with normal bases

or imposing Pic conditions to get around possible failures of the lifting property)? Note in this context that for p-complete A, all C_{p^n}-extension B/A have normal bases.

List of rings used:

A, B	mostly range over p-complete rings
R	$= p$-adic completion of $\mathbf{Z}[t]$
R_n	$= R[\zeta_{p^n}]$
$R^{(n)}/R$	$=$ a C_{p^n}-extension lifting a certain A.S. extension of $\mathbf{F}_p[t]$
$R_n^{(n)}$	$= R^{(n)}[\zeta_{p^n}]$

From now on, wo only list the "without subscript n" version of each ring. Cf. Conventions and Notations.

S	$= R^{\otimes n}$
$S^{(n)}$	$=$ a C_{p^n}-extension of S built from extensions of the tensor factors
S'	$= p$-adic completion of $\mathbf{Z}[t_1, \ldots, t_n]$
$S'^{(n)}$	$=$ a C_{p^n}-extension of S' lifting a certain A.S. extension
$\mathbf{F}$	$= \mathbf{F}_p[t^{p^{-\infty}}]$
$\hat{\mathbf{F}}$	$=t$-adic completion of $\mathbf{F}_p[t^{p^{-\infty}}]$
T	$=$ Witt ring of $\mathbf{F} = \mathbf{F}_p[t^{p^{-\infty}}]$
V	$=$ Witt ring of $\hat{\mathbf{F}}$
$\mathbf{F}^{(N)}$	$=$ a certain A.S. extension of $\mathbf{F}$
$\mathbf{F}_p[t]^{(N)}$	$=$ a certain A.S. extension of $\mathbf{F}_p[t]$
$T^{(N)}$	$=$ Witt ring of the former ring
$T^{(\infty)}$	$= p$-adic completion of $\bigcup T^{(N)}$
$\tilde{R}^{(N)}$	$= C_{p^n}$-extension of R lifting $\mathbf{F}_p[t]^{(N)}$.

References

[CHR] S.U. Chase, D. K. Harrison, A. Rosenberg: Galois theory and Galois cohomology of commutative rings, Memoirs AMS 52 (1965, reprinted with corrections 1968), 1-19

[Ch] L. Childs: Cyclic Stickelberger cohomology and descent of Kummer extensions, Proc. AMS 90 (1984), 505-510

[DeI] F. DeMeyer, E. Ingraham: Separable algebras over commutative rings, Springer Lecture Notes 181, Berlin 1971

[EGA IV] A. Grothendieck: Eléments de géometrie algèbrique, Publ. IHES 32

[Gr1] C. Greither: Galois extensions and normal bases, to appear in Trans. Amer. Math. Soc.

[Gr2] C. Greither: Unramified Kummer extensions of prime power degree, manuscripta math. 64 (1989), 261-290

[GH] C. Greither, R. Haggenmüller: Abelsche Galoiserweiterungen von $R[X]$, manuscr. math. 38 (1982), 239-256

[Ha] H. Hasse: Die Gruppe der p^n-primären Zahlen für einen Primteiler $\wp$ von p, Crelle 174 (1936), 174-183

[KM] I. Kersten, J. Michaliček: Kummer theory without roots of unity, J. Pure Appl. Algebra 50 (1988), 21-72

[Mi] H. Miki: On $\mathbf{Z}_p$-extensions of complete p-adic power series fields and function fields, J. Fac. Sci. Tokyo (I) 21 (1974), 377-393

[Sa] D. Saltman: Generic Galois extensins and problems in field theory, Adv. Math. 43 (1982), 250-283

[Ul] S. Ullom: Integral representations afforded by ambiguous ideals in some abelian extensions, J. Number Th. 6 (1974), 32-49