p-adic Galois representations of G_E with $\mathrm{Char}(E) = p > 0$ and the ring R

Gebhard Böckle

December 11, 2008

1 A short review

Let E be a field of characteristic $p > 0$ and denote by $\sigma\colon E \to E$ the absolute Frobenius endomorphism $x \mapsto x^p$. Based on the notion of étale φ-module, introduced in the last talk, the following theorem had been proved:

Theorem 1.1 *There are equivalences of categories*

$$\mathbf{Rep}_{\mathbb{F}_p}(G_E) \underset{\mathbb{M}}{\overset{\mathbb{V}}{\rightleftarrows}} \mathcal{M}_\varphi^{\mathrm{et}}(E),$$

where $\mathbb{V}$ assigns to $M \in \mathcal{M}_\varphi^{\mathrm{et}}(E)$ the mod p Galois representation $(E^s \otimes_E M)_{\varphi=\mathrm{id}}$ of G_E and $\mathbb{M}$ assigns to $V \in \mathbf{Rep}_{\mathbb{F}_p}(G_E)$ the étale φ-module $((E^s \otimes_{\mathbb{F}_p} V)^G, \sigma \otimes \mathrm{id})$ on E.

Recall that an étale φ-module is a finite dimensional E vector space, equipped with a σ-semi-linear endomorphism φ such that the linearization of φ is an isomorphism.

The first aim of this talk is to present a generalization to p-adic Galois representations of G_E. Recall from last time that

- $\mathcal{O}_\mathcal{E}$ is a Cohen ring of E.
- $\mathcal{E} := \mathrm{Frac}(\mathcal{O}_\mathcal{E})$.
- $\mathcal{O}_{\widehat{\mathcal{E}}^{\mathrm{unr}}}$ is the p-adic completion of $\varinjlim_{\mathcal{F}/\mathcal{E}} \mathcal{O}_\mathcal{F}$ where the limit is over all finite unramified extensions $\mathcal{F}/\mathcal{E}$, where unramified means that the extension F/E of residue fields is finite separable and that p is a uniformizer of $\mathcal{O}_\mathcal{F}$.
- $\widehat{\mathcal{E}}^{\mathrm{unr}} := \mathrm{Frac}(\mathcal{O}_{\widehat{\mathcal{E}}^{\mathrm{unr}}})$.

If E is perfect then $\mathcal{O}_\mathcal{E}$ is unique (up to unique isomorphism) and isomorphic to $W(E)$ and $\mathcal{O}_{\widehat{\mathcal{E}}^{\mathrm{unr}}} \cong W(E^s)$.

A Frobenius endomorphism: Using a basic property of Cohen rings, there exists a lift $\sigma\colon \mathcal{O}_\mathcal{E} \to \mathcal{O}_\mathcal{E}$ of $\sigma\colon E \to E$ and we fix one such. It has a unique extension

$$\sigma\colon \mathcal{O}_{\widehat{\mathcal{E}}^{\mathrm{unr}}} \longrightarrow \mathcal{O}_{\widehat{\mathcal{E}}^{\mathrm{unr}}}$$

which reduces to $\sigma\colon E^s \to E^s$ on residue fields. [For $\mathcal{F}$ over $\mathcal{E}$ finite, the residue field F of $\mathcal{F}$ contains $E\sigma(F)$, and hence by standard field theory there exists a unique extension of σ to $\mathcal{F}$. The extension from $\varinjlim_{\mathcal{F}/\mathcal{E}} \mathcal{F}$ to the p-adic completion is the unique continuous one.] Abbreviate

$$G := G_E \cong \mathrm{Gal}(\mathcal{E}^{\mathrm{unr}}/\mathcal{E}) \cong \mathrm{Aut}_{\mathrm{cont}}(\widehat{\mathcal{E}}^{\mathrm{unr}}/\mathcal{E}).$$

2 p-adic Galois representations of G_E

Theorem 2.1 *There are equivalences of categories*

$$\mathbf{Rep}_{\mathbb{Z}_p}(G_E) \underset{\mathbb{M}}{\overset{\mathbb{V}}{\rightleftarrows}} \mathcal{M}^{\mathrm{et}}_{\varphi}(\mathcal{O}_{\mathcal{E}}),$$

where $\mathbb{V}$ assigns to $M \in \mathcal{M}^{\mathrm{et}}_{\varphi}(\mathcal{O}_{\mathcal{E}})$ the Galois representation $\mathbb{V}(M) := (\mathcal{O}_{\widehat{\mathcal{E}}^{\mathrm{unr}}} \otimes_{\mathcal{O}_{\mathcal{E}}} M)_{\varphi=\mathrm{id}}$ of G_E and $\mathbb{M}$ assigns to $V \in \mathbf{Rep}_{\mathbb{Z}_p}(G_E)$ the étale φ-module $\mathbb{M}(V) := (\mathcal{O}_{\widehat{\mathcal{E}}^{\mathrm{unr}}} \otimes_{\mathbb{Z}_p} V)^G$ on $\mathcal{O}_{\mathcal{E}}$ with $\varphi = \sigma \otimes \mathrm{id}$ and where $\mathbb{V}$ and $\mathbb{M}$ are quasi-inverse to each other.

Example 2.2 Perhaps the simplest Cohen ring which is not a ring of Witt vectors is the following: Let k be a perfect field of characteristic p and $W := W(k)$ its ring of Witt vectors. Let $E := k((x))$. Then a Cohen ring of E is given by

$$\mathcal{O}_{\mathcal{E}} := \Big\{ \sum_{i \in \mathbb{Z}} a_i x^i \mid \forall i : \, a_i \in W \text{ and } \lim_{i \to \infty} a_{-i} = 0 \Big\}.$$

One can easily verify that $\mathcal{O}_{\mathcal{E}}$ is a complete discrete valuation ring with maximal ideal $p\,\mathcal{O}_{\mathcal{E}}$ and residue field E. A Frobenius lift is $\sigma \colon \mathcal{O}_{\mathcal{E}} \to \mathcal{O}_{\mathcal{E}}$ sending $\lambda \in W$ to $\sigma(\lambda)$, where $\sigma \colon W \to W$ is the unique lift of σ restricted to k, and sending x to x^p. Another possible choice for the image of x is $x^p + px$.

Proposition 2.3 *The following hold:*

(a) $(\mathcal{O}_{\widehat{\mathcal{E}}^{\mathrm{unr}}})^G = \mathcal{O}_{\mathcal{E}}$ *and* $(\widehat{\mathcal{E}}^{\mathrm{unr}})^G = \mathcal{E}$.

(b) $(\mathcal{O}_{\widehat{\mathcal{E}}^{\mathrm{unr}}})_{\sigma=\mathrm{id}} = \mathbb{Z}_p$ *and* $(\widehat{\mathcal{E}}^{\mathrm{unr}})_{\sigma=\mathrm{id}} = \mathbb{Q}_p$.

Proof: '$\supset$' is clear in all cases. (For (b) note that id is a lift to $\mathbb{Z}_p$ of σ on $\mathbb{F}_p$).
'$\subset$': For (b) note that $(\mathcal{O}_{\widehat{\mathcal{E}}^{\mathrm{unr}}})_{\sigma=\mathrm{id}} \subset (W(E^s))_{\sigma=\mathrm{id}} = W(\mathbb{F}_p)$ by direct inspection of φ on Witt vectors. The assertions of (a) are clear for the uncompleted rings $\mathcal{O}_{\mathcal{E}^{\mathrm{unr}}}$ and $\mathcal{E}^{\mathrm{unr}}$. To prove (a) one can either use a similar argument as for (b), or one can consider the following diagram

$$\begin{tikzcd}
0 \arrow[r] & p^n(\mathcal{O}_{\widehat{\mathcal{E}}^{\mathrm{unr}}})^G \arrow[r] & (\mathcal{O}_{\widehat{\mathcal{E}}^{\mathrm{unr}}})^G \arrow[r] & (\mathcal{O}_{\widehat{\mathcal{E}}^{\mathrm{unr}}}/p^n)^G \arrow[r] & H^1(\ldots) \\
0 \arrow[r] & p^n(\mathcal{O}_{\mathcal{E}^{\mathrm{unr}}})^G \arrow[r] \arrow[u, hook] & (\mathcal{O}_{\mathcal{E}^{\mathrm{unr}}})^G \arrow[r] \arrow[u, hook] & (\mathcal{O}_{\mathcal{E}^{\mathrm{unr}}}/p^n)^G \arrow[r] \arrow[u, equal] & H^1(G, \mathcal{O}_{\mathcal{E}^{\mathrm{unr}}}).
\end{tikzcd}$$

The term $H^1(G, \mathcal{O}_{\mathcal{E}^{\mathrm{unr}}})$ is zero by the additive Hilbert 90 theorem, and thus the second row is

$$0 \longrightarrow p^n\,\mathcal{O}_{\mathcal{E}} \longrightarrow \mathcal{O}_{\mathcal{E}} \longrightarrow \mathcal{O}_{\mathcal{E}}\,/p^n \longrightarrow 0.$$

So the diagram yields that the p-adic completion of $(\mathcal{O}_{\widehat{\mathcal{E}}^{\mathrm{unr}}})^G$ is a subring of $\mathcal{O}_{\mathcal{E}} = \varprojlim_n \mathcal{O}_{\mathcal{E}}\,/p^n$. By continuity of the action of G, the ring $(\mathcal{O}_{\widehat{\mathcal{E}}^{\mathrm{unr}}})^G$ is p-adically complete which completes the proof. ∎

For the proof of Theorem 2.1, we need the following

Key Lemma 2.4 *(a) Suppose $X \in \mathcal{M}_\varphi^{\mathrm{et}}(\mathcal{O}_{\widehat{\mathcal{E}}^{\mathrm{unr}}})$. Then*

$$\mathcal{O}_{\widehat{\mathcal{E}}^{\mathrm{unr}}} \otimes_{\mathbb{Z}_p} X_{\varphi=\mathrm{id}} \cong X. \quad \text{(Lang's Thm)}$$

(b) Suppose X is a continuous G-module, finitely generated over $\mathcal{O}_{\widehat{\mathcal{E}}^{\mathrm{unr}}}$. Then

$$\mathcal{O}_{\widehat{\mathcal{E}}^{\mathrm{unr}}} \otimes_{\mathcal{O}_{\mathcal{E}}} X^G \cong X. \quad \text{(Hilbert 90)}$$

Note that (b) (for all X ...) is equivalent to $H^1_{\mathrm{cont}}(G, \mathrm{Aut}(X)) = \{1\}$ (for all such X).

Proof: We first explain why it will suffice to prove both parts of the lemma for $\mathcal{O}_{\widehat{\mathcal{E}}^{\mathrm{unr}}}$-modules X of finite length. So suppose this is done and consider $X = \varprojlim_n X/p^nX$. Having the assertions of the lemma for all X/p^nX, one easily deduces that the inverse limit systems $(X/p^nX)_{\varphi=\mathrm{id}}$ or $(X/p^nX)^G$, respectively, have surjective transition maps. Since G and φ act continuously, it follows that the inverse limits of these agree with $X_{\varphi=\mathrm{id}}$ or X^G, respectively. The assertions for X in the lemma now directly follows from the assertions for all X/p^nX (of finite length) in the inverse limit system.
Suppose now that $\mathrm{len}(X) < \infty$. The aim is to reduce the proof to assertions proved in the last talk, i.e., to the case where X is a vector space over E^s. We induct over $n \in \mathbb{N}$ such that $p^nX = 0$. Define $X' := \{x \in X \mid px = 0\}$ and consider the short exact sequence

$$0 \longrightarrow X' \longrightarrow X \longrightarrow X'' \longrightarrow 0.$$

Taking φ-fixed points, or G invariants, respectively, yields the exact sequences

$$0 \longrightarrow (X')_{\varphi=\mathrm{id}} \longrightarrow (X)_{\varphi=\mathrm{id}} \longrightarrow (X'')_{\varphi=\mathrm{id}} \longrightarrow X'/(\varphi - \mathrm{id})X', \tag{1}$$

$$0 \longrightarrow (X')^G \longrightarrow (X)^G \longrightarrow (X'')^G \longrightarrow H^1_{\mathrm{cont}}(G, X'). \tag{2}$$

The module X' is p-torsion and hence a finite dimensional vector space over E^s. So to it we can apply the results of last time. In case (a) it will be an étale φ-sheaf over E^s. Any such is trivial, i.e., isomorphic to a finite sum of copies of (E^s, σ) (by Lang's Theorem). Since $\varphi - \mathrm{id}$ is surjective on E^s, the right-most term of (1) is zero. Similarly, in case (b) the results from last time imply that X' is a trivial G-module over E^s, i.e., isomorphic to a finite sum of copies of E^s with the canonical Galois action (by Hilbert 90). By the additive Hilbert 90, the right-most term of (2) is zero.
To finish the proof (say, only in case (b)), consider the following diagram:

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{O}_{\widehat{\mathcal{E}}^{\mathrm{unr}}} \otimes_{\mathcal{O}_{\mathcal{E}}} (X')^G \arrow[r] \arrow[d] & \mathcal{O}_{\widehat{\mathcal{E}}^{\mathrm{unr}}} \otimes_{\mathcal{O}_{\mathcal{E}}} X^G \arrow[r] \arrow[d] & \mathcal{O}_{\widehat{\mathcal{E}}^{\mathrm{unr}}} \otimes_{\mathcal{O}_{\mathcal{E}}} (X'')^G \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & X' \arrow[r] & X \arrow[r] & X'' \arrow[r] & 0.
\end{tikzcd}$$

By the result from last time, the vertical arrow on the left is an isomorphism, because X' is trivial. By our induction hypothesis, the vertical arrow on the right is an isomorphism. Hence by the Snake Lemma, then central vertical arrow is an isomorphism. ∎

Corollary 2.5 *The following natural maps are isomorphisms:*

(a) For $T \in \mathbf{Rep}_{\mathbb{Z}_p}(G)$ and $\mathbb{M}(T) = (\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{unr}}}} \otimes_{\mathbb{Z}_p} T)^G$ the map

$$\alpha_T \colon \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{unr}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} \mathbb{M}(T) \longrightarrow \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{unr}}}} \otimes_{\mathbb{Z}_p} T.$$

(b) For $M \in \mathcal{M}_{\varphi}^{\mathrm{et}}(\mathcal{O}_{\mathcal{E}})$ and $\mathbb{V}(M) = (\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{unr}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} M)_{\varphi=\mathrm{id}}$ the map

$$\alpha_M \colon \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{unr}}}} \otimes_{\mathbb{Z}_p} \mathbb{V}(M) \longrightarrow \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{unr}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} M.$$

The injectivity of the maps follows from the 'Artin trick' – note that the results of the last talk are not directly applicable to the d.v.r. $\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{unr}}}}$. By applying the previous lemma to $X = \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{unr}}}} \otimes_{\mathbb{Z}_p} T$ and $X = \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{unr}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} M$, respectively, it follows that the $\alpha_?$ are isomorphisms.

Proof of Theorem 2.1: By applying $\mathbb{V}$ to the isomorphism α_T and $\mathbb{M}$ to the isomorphism α_M, Proposition 2.3 yields that $\mathbb{V} \circ \mathbb{M}$ and $\mathbb{M} \circ \mathbb{V}$ are naturally isomorphic to the respective identity functors. ∎

3 The ring R

The aim of this part of the talk is to introduce a ring R which will be useful when describing p-adic Galois representations of the absolute Galois group G_K of a local field K. Before we come to its definition, we try to give a motivation.

3.1 A motivation

Let $\varepsilon^{(n)}$ denote a primitive p^n-th root of unity in $\overline{\mathbb{Q}_p}$. (Later we will assume that $(\varepsilon^{(n+1)})^p = \varepsilon^{(n)}$ for all n.) Define $K^{\mathrm{cyc}} := \bigcup_n K(\varepsilon^{(n)})$. Using that $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{cyc}}/\mathbb{Q}_p) \cong \mathbb{Z}_p^* \cong \mathbb{Z}_p \times \mathbb{F}_p^*$ (or $\cong \mathbb{Z}_2 \times \mathbb{Z}/(2)$ for $p = 2$) one deduces

$$\mathrm{Gal}(K^{\mathrm{cyc}}/K) \cong \mathbb{Z}_p \times \Delta_K$$

for a finite subgroup $\Delta_K \subset \mathbb{F}_p^*$ (or $\Delta_K \subset \mathbb{Z}/(2)$ for $p = 2$). One defines $K_\infty := (K^{\mathrm{cyc}})^{\Delta_K}$ and $\Gamma_K := \mathrm{Gal}(K_\infty/K)$. Consider

$$\begin{tikzcd}
\overline{K} \arrow[d, dash] \arrow[ddd, bend right=60, dash, "G_K"'] \arrow[dd, bend left=40, dash, "H_K"] \\
K^{\mathrm{cyc}} \arrow[d, dash, "\Delta_K"'] \\
K_\infty \arrow[d, dash, "\Gamma_K"] \\
K \arrow[d, dash, "\text{tot. ramif.}"'] \\
K_0 \arrow[d, dash, "\text{unr.}"'] \\
\mathbb{Q}_p.
\end{tikzcd}$$

An important observation by Fontaine-Wintenberger (?) is that there exists a field of characteristic p, the field $\mathbf{E}_K$ of norms of K such that

$$H_K \cong \mathrm{Gal}(\mathbf{E}_K^s/\mathbf{E}_K).$$

One has $\mathbf{E}_K \cong k_K((\pi_K))$ for k_K the residue field of K and π_K an indeterminate. We will not prove this, but only recall the definition of $\mathbf{E}_K$: Define $K_n = (K_\infty)^{p^n\Gamma_K}$ and

$$\mathbf{E}_K = \varprojlim(K_0 \xleftarrow{\mathrm{Norm}_{K_1/K_0}} K_1 \xleftarrow{\mathrm{Norm}_{K_2/K_1}} K_2 \longleftarrow \ldots)$$

One can prove that that $\mathbf{E}_K$ is also isomorphic to

$$\mathbf{E}_K = \varprojlim(K_\infty \xleftarrow{x\mapsto x^p} K_\infty \xleftarrow{x\mapsto x^p} K_\infty \longleftarrow \ldots)$$

We will bypass the theory of field of norms. But the second description of $\mathbf{E}_K$ is reminiscent of the defintion of R we are about to learn.

3.2 The ring $R(\bar{A})$

Let $\bar{A}$ be a ring of characteristic p and $\varphi\colon \bar{A} \to \bar{A} : x \to x^p$ be the Frobenius endomorphism of $\bar{A}$.

Definition 3.1

$$\begin{aligned} R(\bar{A}) &:= \varprojlim(\bar{A} \xleftarrow{\varphi} \bar{A} \xleftarrow{\varphi} \bar{A} \xleftarrow{\varphi} \ldots) \\ &= \{(x_n) \in \bar{A}^{\mathbb{N}} \mid \forall n : x_{n+1}^p = x_n\} \end{aligned}$$

The ring $R(\bar{A})$ is perfect and reduced, because $(x_n) = (x_{n+1})^p$ and if $(x_n)^{p^m} = 0$, then $(x_{n+m}) = (0)$. Let

$$\theta_m\colon R(\bar{A}) \longrightarrow \bar{A} : (x_n) \mapsto x_m.$$

The following lemma, may later be useful:

Lemma 3.2 *Suppose $\widetilde{R} \subset R(\bar{A})$ is a topologically closed subring such that $\theta_m(\widetilde{R}) = \theta_m(R(\bar{A}))$ for all m. Then $\widetilde{R} = R(\bar{A})$.*

PROOF:

$$\begin{aligned} R(\bar{A}) = \{(x_n) \mid \ldots\} &= \varprojlim \mathrm{Im}(\theta_1, \ldots, \theta_m) \\ &= \varprojlim(\theta_1, \ldots, \theta_m)(\widetilde{R}) = \widetilde{R}. \ \blacksquare \end{aligned}$$

Note that if φ is injective, then $R(\bar{A})$ is simply the intersection $\bigcup \bar{A}^{p^n}$. The cases we will be interested in are cases where $\bar{A}$ is highly non-reduced, such as $\mathcal{O}_{K_\infty}/p\mathcal{O}_{K_\infty}$.

Suppose A is a separated p-adically complete topological ring, i.e., $A \cong \varprojlim A/p^n$. Set $\bar{A} := A/p$.

Proposition 3.3 *The map*

$$S_A := \{(x^{(n)}) \in A^{\mathbb{N}} \mid \forall n : (x^{(n+1)})^p = x^{(n)}\} \longrightarrow R(\bar{A}) : (x^{(n)}) \mapsto (x^{(n)} \mod pA)_n$$

is a bijection. It is a ring isomorphism if on S_A one defines

$$(x^{(n)}) \cdot (y^{(n)}) = (x^{(n)} \cdot y^{(n)}) \quad \textit{and} \quad (x^{(n)}) + (y^{(n)}) = \Big(\lim_{m\to\infty} (x^{(n+m)} + y^{(n+m)})^{p^m}\Big)_n.$$

PROOF: Define $R(\bar{A}) \to S_A : (x_n) \to (x^{(n)})$ as follows: Lift $x_n \in \bar{A}$ to $\hat{x}_n \in A$ for all n. Then $\hat{x}_{n+1}^p - \hat{x}_n \in pA$ because mod p the element is $x_{n+1}^p - x_n = 0$. Using the binomial theorem for $(x+y)^p$, one deduces for all n:

$$\hat{x}_{n+1}^{p^{m+1}} - \hat{x}_n^{p^m} \in p^{m+1}A.$$

It follows that for all n the sequence $(\hat{x}_{n+m})^{p^m}$ is a Cauchy sequence in m. Defining $x^{(n)}$ as its limit, it follows that $(x^{(n)})$ is in S_A and it obviously reduces to (x_n) modulo pA. The $x^{(n)}$ are independent of the choice of the lifts $\hat{x}_n$. The sequence is also the unique sequence in S_A lifting $R(\bar{A})$. This shows that the map is a bijection.
It remains to see that for (x_n) and (y_n) in $R(\bar{A})$ with lifts $(x^{(n)})$ and $(y^{(n)})$ in S_A the given addition formula in S_A describes the lift of (x_n+y_n). But this is clear: $(x^{(n)}+y^{(n)})$ is a lift of x_n+y_n and by the formula which gives the canonical lifts from any sequence of lifts, we obtain the addition formula of the proposition. ∎

3.3 The ring R

Let $C := \widehat{\overline{K}}$.

Definition 3.4

$$R := R(\mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}}) = R(\mathcal{O}_C/p\mathcal{O}_C) = \{(x^{(n)}) \in \mathcal{O}_C^{\mathbb{N}} \mid \forall n : (x^{n+1})^p = x^n\}$$

$$v_R((x^{(n)})) := v_C(x^{(0)}) \quad \forall (x^{(n)}) \in R.$$

Theorem 3.5 *The following hold:*

(a) The ring R is perfect of characteristic p.

(b) (R, v) is a complete valuation ring with valuation $v = v_R$, with $v(R) = \mathbb{Q}_{\geq 0} \cup \{\infty\}$ with maximal ideal $\mathfrak{m}_R = \{x \in R \mid v(x) > 0\}$ and residue field $\bar{k} = \overline{\mathbb{F}_p}$.

(c) If the Teichmüller lift $\bar{k} \to \mathcal{O}_{K_0^{\mathrm{unr}}} \cong W(\bar{k})$ is denoted $a \mapsto \hat{a}$, then $\bar{k} \to R$ is the map $a \mapsto (\widehat{a^{p^{-n}}})_n$.

(d) $\mathrm{Frac}(R)$ is algebraically closed.

It follows that R is the completion of the algebraic closure of $\bar{k}((x))$ for any $x \in R$ with strict positive valuation. (Hence $R \cong \widehat{\mathbf{E}_K^s}$.) Also, note that one has the identification

$$\mathrm{Frac}(R) = \{(x^{(n)}) \in C^{\mathbb{N}} \mid \forall n : (x^{(n+1)})^p = x^{(n)}\}.$$

PROOF: Part (a) is clear. Part (c) is straightforward from the previous proposition. We first prove (b): Since C is algebraically closed it is closed under taking p-th roots and hence any $c \in C$ can occur as $c^{(0)}$ in a sequence $(c^{(n)})$ such that $(c^{(n+1)})^p = (c^{(n)})$ for all n. Hence $v_R(R) = v_C(\mathcal{O}_C)$ is as described. Also $v_R((x^{(n)})) = \infty$ if and only if $x^{(0)} = 0$ which is equivalent to all $x^{(n)}$ being zero.
The condition $v(x \cdot y) = v(x)+v(y)$ is straightforward from the definition of multiplication on sequences $x = (x^{(n)})$ and $y = (y^{(n)})$:

$$v_R((x^{(n)}) \cdot (y^{(n)})) = v_R((x^{(n)} \cdot y^{(n)})) = v_C(x^{(0)}y^{(0)}) = v_C(x^{(0)}) + v_C(y^{(0)}).$$

The ultrametric triangle inequality follows from

$$\begin{aligned} v_R(x+y) &= v_R((x^{(n)})+(y^{(n)})) = v_R\Big(\lim_{m\to\infty}(x^{(n+m)}+y^{(n+m)})^{p^m}\Big) \\ &= v_C\Big(\lim_{m\to\infty}(x^{(m)}+y^{(m)})^{p^m}\Big) = \lim_{m\to\infty} p^m \underbrace{v_C\Big((x^{(m)}+y^{(m)})\Big)}_{\geq \min\{v_C(x^{(m)}),v_C(y^{(m)})\}} \\ &\geq \liminf_{m\to\infty}\Big(\min\Big\{\underbrace{p^m v_C(x^{(m)})}_{=v_C(x^{(0)})},\underbrace{p^m v_C(y^{(m)})}_{=v_C(y^{(0)})}\Big\}\Big) = \min\{v_R(x),v_R(y)\}. \end{aligned}$$

For (b) it remains to show that v defines the topology on R given by the inverse limit topology (of the discrete sets $\mathcal{O}_C/p\mathcal{O}_C$) and that v is complete. For the topology, note that a neighborhood basis of R is given by the sets $(\mathrm{Ker}(\theta_m))_m$. Now for a sequence $(x^{(n)})$ we have

$$(x^{(n)}) \in \mathrm{Ker}(\theta_m) \Longleftrightarrow (x^{(m)} \mod p \equiv 0\mathcal{O}_C \Longleftrightarrow v_C(x^{(m)}) \geq 1 \Longleftrightarrow v_R((x^{(n)})) \geq p^m.$$

Thus the topologies agree. The completeness follows from the discreteness of $\mathcal{O}_C/p\mathcal{O}_C$: If in $\sum r_n$ the $r_n \in R$ tend to zero, then under any θ_m the sum becomes stationary and thus it converges.

We finally prove (d): Consider an irreducible polynomial

$$P(x) = x^d + a_{d-1}x^{d-1} + \ldots + a_1 x + a_0 \in R[x].$$

(It suffices to consider coefficients in R instead of $\mathrm{Frac}(R)$.) Because R is perfect, we may assume that P is separable, i.e., that it has no multiple roots.

Write $a_i = (a_i^{(n)}) \in S_{\mathcal{O}_C}$ and consider

$$P^{(n)}(x) = x^d + a_{d-1}^{(n)}x^{d-1} + \ldots + a_1^{(n)}x + a_0^{(n)} \in \mathcal{O}_C[x].$$

Because C is algebraically closed, the polynomial $P^{(n)}$ has roots $\alpha_1^{(n)}, \ldots, \alpha_d^{(n)}$ in C. We would like to see that for $n \gg 0$ these roots are pairwise distinct modulo $p\mathcal{O}_C$. For this we show that the discriminants of the $P^{(n)}$ have v_C valuations converging to 0, so that also the valuation of the difference of distinct roots has to converge to zero.

The discriminant of $P^{(n)}$ is the Resultant of $P^{(n)}$ and $(P^{(n)})'$. The latter can be computed from a determinant containing as its entries the coefficients of $P^{(n)}$ and of $(P^{(n)})'$. Determinants can be explicitly written in terms of sums and products of matrix entries. Based on this, one can verify the following: If $(a_{ij}) \in M_d(R)$ and $a_{ij} = (a_{ij}^{(n)})$, then $\det(a_{ij}^{(n+m)})^{p^m} \overset{m\to\infty}{\longrightarrow} (\det(a_{ij}))^{(n)}$. If one applies this to the above way of computing the discriminant of P, it follows that the sequence in C (in upper indexing) representing $\mathrm{discr}(P)$ is given by

$$\mathrm{discr}(P)^{(n)} = \lim_{m\to\infty} \mathrm{discr}(P^{(n+m)})^{p^m}.$$

Since P is has no multiple roots, $\mathrm{discr}(P)$ is non-zero, and so $v_C(\mathrm{discr}(P)^{(0)}) \geq 0$ is non-zero. Clearly $v_C(\mathrm{discr}(P)^{(n)}) = \frac{1}{p^n}v_C(\mathrm{discr}(P)^{(0)})$, and so it follows that

$$\mathrm{discr}(P^{(n)}) \overset{n\to\infty}{\longrightarrow} 0.$$

In particular, for all $n \gg 0$ we can order (for fixed n) the $\alpha_i^{(n)}$ in such a way that they form sequences in $\mathcal{O}_C$ satisfying

$$(\alpha_i^{(n+1)})^p = \alpha_i^{(n)}$$

(for all $n \gg 0$). It easily follows that these sequences define elements of R which are roots of P. ∎