APPENDIX 2. BASICS OF p-ADIC FIELDS

We collect in this appendix some basic facts about p-adic fields that are used in Lecture 9. In the first section we review the main properties of p-adic fields, in the second section we describe the unramified extensions of $\mathbf{Q}_p$, while in the third section we construct the field $\mathbf{C}_p$, the smallest complete algebraically closed extension of $\mathbf{Q}_p$. In §4 section we discuss convergent power series over p-adic fields, and in the last section we give some examples. The presentation in §2-§4 follows [Kob].

1. Finite extensions of $\mathbf{Q}_p$

We assume that the reader has some familiarity with I-adic topologies and completions, for which we refer to [Mat]. Recall that if $(R, \mathfrak{m})$ is a DVR with fraction field K, then there is a unique topology on K that is invariant under translations, and such that a basis of open neighborhoods of 0 is given by $\{\mathfrak{m}^i \mid i \geq 1\}$. This can be described as the topology corresponding to a metric on K, as follows. Associated to R there is a discrete valuation v on K, such that for every nonzero $u \in R$, we have $v(u) = \max\{i \mid u \not\in \mathfrak{m}^i\}$. If $0 < \alpha < 1$, then by putting $|u| = \alpha^{v(u)}$ for every nonzero $u \in K$, and $|0| = 0$, one gets a *non-Archimedean absolute value* on K. This means that $|\cdot|$ has the following properties:

i) $|u| \geq 0$, with equality if and only if $u = 0$.
ii) $|u + v| \leq \max\{|u|, |v|\}$ for every $u, v \in K$[1].
iii) $|uv| = |u| \cdot |v|$ for every $u, v \in K$.

In this case, by taking $d(x, y) = |x - y|$ we get a non-Archimedean[2] metric on K such that the corresponding topology is the unique topology mentioned above. Note that the topology is independent of the choice of α. It is clear that addition, multiplication, and taking the inverse of a nonzero element are all continuous.

The completion of R is defined algebraically as $\widehat{R} = \varprojlim_i R/\mathfrak{m}^i$. It is a general fact that R is local and Noetherian, and the canonical morphism $R \to \widehat{R}$ is injective. Furthermore, the maximal ideal in $\widehat{R}$ is $\mathfrak{m} \cdot R$, and for all $i \geq 1$ we have $R/\mathfrak{m}^i \simeq \widehat{R}/\mathfrak{m}^i\widehat{R}$. This implies that $\dim(\widehat{R}) = \dim(R) = 1$. Since the maximal ideal in $\widehat{R}$ is principal (being generated by a generator π of $\mathfrak{m}$), it is easy to see that $\widehat{R}$ is a DVR. Furthermore, we have $\widehat{K} := \mathrm{Frac}(\widehat{R}) = \widehat{R}[1/\pi] = K \otimes_R \widehat{R}$. In particular, we have a valuation and a non-Archimedean absolute value on $\widehat{K}$ that extend the corresponding ones on K. In fact, $\widehat{K}$ is the completion of K with respect to the topology defined by $|\cdot|$, and the absolute value on $\widehat{K}$ is the unique one extending the absolute value on K.

[1] A useful observation is that we automatically get that this is an equality if $|u| \neq |v|$.

[2] This means that we have the strong triangle inequality $d(x, y) \leq d(x, z) + d(y, z)$ for all x, y, and z.

Suppose now that p is a fixed prime integer. We apply the above discussion to $K = \mathbf{Q}$, where $R = \mathbf{Z}_{(p\mathbf{Z})}$ is the localization of $\mathbf{Z}$ at the maximal ideal $p\mathbf{Z}$. The corresponding topology on $\mathbf{Q}$ is the *p-adic topology*, and the corresponding absolute value, with $\alpha = \frac{1}{p}$ is denoted by $|\cdot|_p$. The field $\widehat{K}$ is the *field of p-adic rational numbers* $\mathbf{Q}_p$, and $\widehat{R}$ is the *ring of p-adic integers* $\mathbf{Z}_p$. The corresponding valuation and absolute value on $\mathbf{Q}_p$ are denoted by ord_p, and respectively, $|\cdot|_p$.

We now recall Hensel's Lemma, one of the basic results about complete local rings. For a proof, see [Mat, Theorem 8.3]. Let $(A, \mathfrak{m}, k)$ be a complete local ring. For a polynomial $g \in A[x]$, we denote by $\overline{g}$ its image in $k[x]$.

Proposition 1.1. *With the above notation, suppose that $f \in A[x]$ is a monic polynomial. If $u, v \in k[x]$ are relatively prime monic polynomials such that $\overline{f} = uv$, then there are monic polynomials $g, h \in A[x]$ such that*

i) $f = gh$
ii) $\overline{g} = u$ *and* $\overline{h} = v$.

A consequence of the above proposition is that if (keeping the notation) B is a finite A-algebra such that $B/\mathfrak{m}B$ splits as the product of two (nonzero) rings, then the same holds for B. Indeed, the hypothesis gives the existence of an idempotent $u \in B$ such that $u \neq 0, 1$. Applying Hensel's Lemma for the decomposition $x^2 - x = (x - u)(x - (1 - u))$ in $k[x]$, we get an idempotent in B different from 0 and 1. In particular, we see that if B is a domain, then the zero-dimensional ring $B/\mathfrak{m}_B$ is local, hence B is local, too.

A *p-adic field* is a finite field extension of $\mathbf{Q}_p$. If K is such a field, we denote by $\mathcal{O}_K$ the ring of integers in K (that is, the integral closure of $\mathbf{Z}_p$ in K). It is easy to see that since every element $u \in K$ is algebraic over $\mathbf{Q}_p$, there is $a \in \mathbf{Z}_p$ such that $au \in \mathcal{O}_K$. Therefore $\mathbf{Q}_p \otimes_{\mathbf{Z}_p} \mathcal{O}_K = K$ and K is the fraction field of $\mathcal{O}_K$.

Since $\mathbf{Z}_p$ is a DVR, it is well-known that $\mathcal{O}_K$ is a finite $\mathbf{Z}_p$-algebra (see [Lang, Precise]). Therefore the discussion after Proposition 1.1 implies that $\mathcal{O}_K$ is a local ring (and the inclusion $\mathbf{Z}_p \hookrightarrow \mathcal{O}_K$ is local, since $\mathcal{O}_K$ is finite over $\mathbf{Z}_p$). Furthermore, since $\dim(\mathcal{O}_K) = \dim(\mathbf{Z}_p) = 1$, and $\mathcal{O}_K$ is clearly normal, we conclude that $\mathcal{O}_K$ is again a DVR.

If v_K is the discrete valuation of K corresponding to $\mathcal{O}_K$, then $e_K := v_K(p)$ is the *ramification index* of K over $\mathbf{Q}_p$. We say that K is unramified over $\mathbf{Q}_p$ if $e_K = 1$. It is clear that for every $u \in \mathbf{Q}_p$, we have $v_K(u) = e_K \cdot \mathrm{ord}_p(u)$. The p-adic absolute value on K is defined by $|u|_p = \left(\frac{1}{p}\right)^{v_K(u)/e_K}$. Note that for $u \in \mathbf{Q}_p$, this agrees with the definition we gave before. We have $\mathcal{O}_K = \{u \in K, |u|_p \leq 1\}$, and the maximal ideal in $\mathcal{O}_K$ is $\mathfrak{m}_K = \{u \in K, |u| < 1\}$.

Since every ideal in $\mathbf{Z}_p$ is generated by some p^m, and $\mathcal{O}_K$ is clearly torsion-free, it follows that $\mathcal{O}_K$ is flat over $\mathbf{Z}_p$. We deduce that $\mathcal{O}_K$ is a free module over $\mathbf{Z}_p$, and its rank is clearly equal to $n = [K : \mathbf{Q}_p]$. Let π_K denote a generator of the maximal ideal $\mathfrak{m}_K$. The quotient $\mathcal{O}_K/p\mathcal{O}_K$ is free of rank n over $\mathbf{F}_p$; on the other hand, it has a filtration

$$(0) \subset \mathfrak{m}_K^{e_K-1}/\mathfrak{m}_K^{e_K} \subset \ldots \subset \mathfrak{m}_K/\mathfrak{m}_K^{e_K} \subset \mathcal{O}_K/\mathfrak{m}_K^{e_K},$$

with each successive quotient isomorphic to $\mathcal{O}_K/\mathfrak{m}_K$. We deduce that if $f = [\mathcal{O}_K/\mathfrak{m}_K : \mathbf{F}_p]$, then $n = ef$.

Exercise 1.2. *Let K be a p-adic field.*

i) *Show that a basis of open neighborhoods of 0 in $\mathcal{O}_K$ is given by $\{p^m\mathcal{O}_K \mid m \geq 1\}$.*
ii) *Deduce that if we choose an isomorphism of $\mathbf{Z}_p$-modules $\mathcal{O}_K \simeq \mathbf{Z}_p^n$, the topology on $\mathcal{O}_K$ corresponds to the product topology on $\mathbf{Z}_p^n$.*
iii) *Deduce that $\mathcal{O}_K$ is complete (and therefore so is K).*

Exercise 1.3. *Let $K \hookrightarrow L$ be two finite extensions of $\mathbf{Q}_p$.*

ii) *Show that if $e_{L/K}$ is defined by $\pi_K\mathcal{O}_L = (\pi_L^{e_{L/K}})$, and $f_{L/K} = [\mathcal{O}_L/\mathfrak{m}_L : \mathcal{O}_K/\mathfrak{m}_K]$, then $e_L = e_K \cdot e_{L/K}$ and $f_L = f_K \cdot f_{L/K}$. Deduce that $[L\colon K] = e_{L/K}f_{L/K}$.*
i) *Show that the two definitions of $|\cdot|_p$ on K and L are compatible.*

We say that L/K is unramified if $e_{L/K} = 1$, and that it is totally ramified if $e_{L/K} = [L\colon K]$.

Exercise 1.4. *Let K be a finite Galois extension of $\mathbf{Q}_p$. Show that if $\sigma \in G(K/\mathbf{Q}_p)$, then $|\sigma(u)|_p = |u|_p$ for every $u \in K$. Deduce that for every p-adic field K and every $u \in K$, we have $|u|_p = N_{K/\mathbf{Q}_p}(u)^{1/n}$, where $n = [K : \mathbf{Q}_p]$.*

Suppose now that $(K, |\cdot|)$ is an arbitrary field endowed with a non-Archimedean absolute value, and we consider on K the corresponding metric space structure. The following exercise gives some special features of the non-Archimedean setting.

Exercise 1.5. *With K as above, suppose that $(a_n)_{n\geq 1}$ is a sequence of elements of K.*

i) *Show that (a_n) is Cauchy if and only if $\lim_{n\to\infty}(a_n - a_{n+1}) = 0$.*
ii) *Show that if K is complete, then the series $\sum_{n\geq 1} a_n$ is convergent if and only if $\lim_{n\to\infty} a_n = 0$.*
iii) *Show that if the series $\sum_{n\geq 1} a_n$ is convergent, then for every permutation σ of $\mathbf{Z}_{>0}$, we have $\sum_{n\geq 1} a_{\sigma(n)} = \sum_{n\geq 1} a_n$.*

2. Unramified extensions of $\mathbf{Q}_p$ and Teichmüller lifts

Our main goal in this section is to describe the unramified extensions of $\mathbf{Q}_p$, and the morphisms between them. We will also take this opportunity to discuss Teichmüller lifts of elements in a finite field. In order to state the results, it is convenient to fix an algebraic closure $\overline{\mathbf{Q}_p}$ of $\mathbf{Q}_p$. The following is the main result of this section.

Theorem 2.1. *The unramified extensions of $\mathbf{Q}_p$ in $\overline{\mathbf{Q}_p}$ are described as follows.*

i) *For every n, there is a unique unramified extension of $\mathbf{Q}_p$ in $\overline{\mathbf{Q}_p}$ of degree n, denoted by $\mathbf{Q}_p^{(n)}$. This can be obtained by attaching to $\mathbf{Q}_p$ a primitive root of 1 of order $p^n - 1$.*

ii) *If $K \subseteq \overline{\mathbf{Q}_p}$ is a finite extension of $\mathbf{Q}_p$ and $f = f_K$, then $\mathbf{Q}_p^{(f)} \subseteq K$, and this extension is totally ramified.*

ii) *$\mathbf{Q}_p^{(n)}$ is a Galois extension of $\mathbf{Q}_p$, and we have an isomorphism of Galois groups $G(\mathbf{Q}_p^{(n)}/\mathbf{Q}_p) \to G(\mathbf{F}_{p^n}/\mathbf{F}_p)$, that associates to an automorphism of $\mathbf{Q}_p^{(n)}$ the induced automorphism of the residue field.*

Proof. We begin by showing that for every $n \geq 1$, there is an unramified extension of $\mathbf{Q}_p$ of degree n. Let $u \in \mathbf{F}_{p^n}^*$ be a multiplicative generator. Since $\mathbf{F}_{p^n} = \mathbf{F}_p(u)$, it follows that the minimal polynomial $P \in \mathbf{F}_p[x]$ of u over $\mathbf{F}_p$ has degree $[\mathbf{F}_{p^n} : \mathbf{F}_p] = n$. Let $\widetilde{P} \in \mathbf{Z}_p[x]$ be a monic polynomial lifting P. Since P is irreducible, it follows that $\widetilde{P}$ is irreducible. Let $w \in \overline{\mathbf{Q}_p}$ be a root of $\widetilde{P}$, and put $L = \mathbf{Q}_p(w)$. We have $[L : \mathbf{Q}_p] = \deg(\widetilde{P}) = n$, and since $\widetilde{P}$ is monic, we see that $w \in \mathcal{O}_L$. Let $\mathfrak{m}_L$ denote the maximal ideal in $\mathcal{O}_L$. The image $\overline{w} \in \mathcal{O}_L/\mathfrak{m}_L$ of w satisfies $P(\overline{w}) = 0$, hence w is a conjugate of u, so that $f_L \geq n$. Since $e_L f_L = n$, we conclude that $f_L = n$, and the extension $L/\mathbf{Q}_p$ is unramified. We thus have unramified extensions of $\mathbf{Q}_p$ of arbitrary degree.

Let us consider an arbitrary extension K of $\mathbf{Q}_p$ of degree d, contained in $\overline{\mathbf{Q}_p}$. We put $e = e_K$ and $f = f_K$. Let α be a multiplicative generator of $(\mathcal{O}_K/\mathfrak{m}_K)^*$. We claim that there is a lifting $\widetilde{\alpha} \in \mathcal{O}_K$ of α such that $\widetilde{\alpha}^{p^f-1} = 1$. We can write $x^{p^f-1} - 1 = (x - \alpha)G(x)$ for a monic polynomial $G \in \mathbf{F}_{p^f}[x]$. Since $G(\alpha) \neq 0$, it follows from Proposition 1.1 that we can write $x^{p^f-1} - 1 = (x - \widetilde{\alpha})\widetilde{G}(x)$ for some $\widetilde{G} \in \mathcal{O}_K[x]$, and some lift $\widetilde{\alpha} \in \mathcal{O}_K$ of α. This proves our claim. Note that $\widetilde{\alpha}$ is a primitive root of 1 of order $p^f - 1$: if $\widetilde{\alpha}^i = 1$ for some $0 < i < p^f - 1$, then $\alpha^i = 1$, a contradiction. It is clear that $f_{\mathbf{Q}_p(\widetilde{\alpha})} \geq [\mathbf{F}_p(\alpha) : \mathbf{F}_p] = f$, and since the reverse inequality follows from $\mathbf{Q}_p(\widetilde{\alpha}) \subseteq K$, we have $f_{\mathbf{Q}_p(\widetilde{\alpha})} = f$ and the extension $K/\mathbf{Q}_p(\widetilde{\alpha})$ is totally ramified.

Suppose now that K is unramified over $\mathbf{Q}_p$, hence $e = 1$. The above shows that $K = \mathbf{Q}_p(\alpha)$. Therefore every unramified degree n extension of $\mathbf{Q}_p$ is obtained by adjoining to $\mathbf{Q}_p$ a primitive root $\widetilde{\alpha}$ of 1 of order $p^n - 1$. Since such an extension is clearly independent of the choice of the primitive root, we get the assertion in i). We note that from the construction we also get that the image α of $\widetilde{\alpha}$ in the residue field of K is again a primitive root of 1 of order $p^n - 1$.

Returning to the case of an arbitrary K as above, we see that $\mathbf{Q}_p(\widetilde{\alpha}) = \mathbf{Q}_p^{(f)}$, hence the assertion in ii).

For every $\sigma \in G(\overline{\mathbf{Q}_p}/\mathbf{Q}_p)$, note that $\sigma(\mathbf{Q}_p^{(n)})$ is an unramified extension of $\mathbf{Q}_p$ of degree n, hence by the uniqueness statement in i), it is equal to $\mathbf{Q}_p^{(n)}$. This shows that the extension $\mathbf{Q}_p^{(n)}/\mathbf{Q}_p$ is Galois (it is separable since $\mathrm{char}(\mathbf{Q}_p) = 0$). It is clear that an automorphism σ of $L = \mathbf{Q}_p^{(n)}$ induces an automorphism of $\mathcal{O}_L$, hence an automorphism $\overline{\sigma}$ of the residue field $\mathcal{O}_L/\mathfrak{m}_L$. We thus get a group homomorphism $G := G(\mathbf{Q}_p^{(n)}/\mathbf{Q}_p) \to G(\mathbf{F}_{p^n}/\mathbf{F}_p)$. Since both groups have n elements, it is enough to show that this is an injective morphism. We have seen that $\mathbf{Q}_p^{(n)} = \mathbf{Q}_p(\widetilde{\alpha})$, where $\widetilde{\alpha} \in \overline{\mathbf{Q}_p}$ is a primitive root of 1 of order $p^n - 1$, and the image α of $\widetilde{\alpha}$ in the residue field is again a primitive root of 1 of order $p^n - 1$. Every σ in G satisfies $\sigma(\widetilde{\alpha}) = \widetilde{\alpha}^i$ for some i. If $\overline{\sigma} = \mathrm{id}$, then $\alpha = \overline{\sigma}(\alpha) = \alpha^i$, hence $\widetilde{\alpha} = \widetilde{\alpha}^i$, and we see that $\sigma = \mathrm{id}$. This completes the proof of iii), and thus the proof of the theorem. □

Corollary 2.2. *We have $\mathbf{Q}_p^{(m)} \subseteq \mathbf{Q}_p^{(n)}$ if and only if m divides n.*

Proof. If $\mathbf{Q}_p^{(m)} \subseteq \mathbf{Q}_p^{(n)}$, then $m = [\mathbf{Q}_p^{(m)} : \mathbf{Q}]$ divides $n = [\mathbf{Q}_p^{(n)} : \mathbf{Q}]$. Conversely, suppose that $m|n$, so that $r = \frac{p^n-1}{p^m-1}$ is an integer. If $\beta \in \overline{\mathbf{Q}_p}$ is a primitive root of 1 of order $p^n - 1$, then β^r is a primitive root of 1 of order $p^m - 1$, and $\mathbf{Q}_p^{(m)} = \mathbf{Q}_p(\beta^r) \subseteq \mathbf{Q}_p(\beta) = \mathbf{Q}_p^{(n)}$. □

We end this section by discussing the Teichmüller lift of an element in a finite field. For every $n \geq 1$, let $\mathbf{Z}_p^{(n)}$ denote the ring of integers of $\mathbf{Q}_p^{(n)}$.

Proposition 2.3. *For every $u \in \mathbf{F}_{p^n}$, there is a unique $\widetilde{u} \in \mathbf{Z}_p^{(n)}$ that is a lift of u, and such that $\widetilde{u}^{p^n} = u$.*

The element $\widetilde{u}$ in the above proposition is the *Teichmüller lift* of u. We start with a lemma.

Lemma 2.4. *If I is an ideal in a commutative ring A, and if $u, v \in A$ are such that $u \equiv v$ (mod pI), then $u^{p^i} \equiv v^{p^i}$ (mod $p^{i+1}I$) for every $i \geq 1$.*

Proof. Arguing by induction on i, we see that it is enough to prove the case $i = 1$. Write $u = v + a$, where $a \in pI$, hence

$$u^p - v^p = \sum_{j=1}^{p} \binom{p}{j} v^{p-j} a^j.$$

Since $a^j \in p^2 I^2$ for every $j \geq 2$, and $pa \in p^2 I$, we get the assertion in the lemma. □

Proof of Proposition 2.3. For the existence part, it is clear that if $u = 0$, then we may take $\widetilde{u} = 0$. Suppose now that u is nonzero. We have seen in the proof of Theorem 2.1 that $\mathbf{Q}_p^{(n)} = \mathbf{Q}_p(\widetilde{\alpha})$, where $\widetilde{\alpha} \in \overline{\mathbf{Q}_p}$ is a primitive root of 1 of order $p^n - 1$, and its image $\alpha \in \mathbf{F}_{p^n}$ is again a primitive root of 1 of order $p^n - 1$. Therefore α is a multiplicative generator of $\mathbf{F}_{p^n}^*$, hence there is m such that $u = \alpha^m$. Since $\widetilde{\alpha} \in \mathbf{Z}_p^{(n)}$, if we take $\widetilde{u} = \widetilde{\alpha}^m$, this has the required properties.

In order to prove uniqueness, suppose that $\widetilde{u}, \widetilde{v} \in \mathbf{Z}_p^{(n)}$ both satisfy the conditions in the proposition. In particular, we have $\widetilde{u} \equiv \widetilde{v}$ (mod $p\mathbf{Z}_p^{(n)}$), and the lemma implies $\widetilde{u}^{p^{ni}} \equiv \widetilde{v}^{p^{ni}}$ (mod $p^{ni+1}\mathbf{Z}_p^{(n)}$) for every $i \geq 1$. Since $\widetilde{u}^{p^{ni}} = \widetilde{u}$ and $\widetilde{v}^{p^{ni}} = \widetilde{v}$, we conclude that $\widetilde{u} - \widetilde{v} \in \bigcap_{i \geq 1} p^{ni}\mathbf{Z}_p^{(e)}$, hence $\widetilde{u} = \widetilde{v}$. □

Corollary 2.5. *Every element in $\mathbf{Z}_p^{(n)}$ has a unique expression as the sum of a series $\sum_{i \geq 0} a_i p^i$, where $a_i^{p^n} = a_i$ for every i.*

Proof. Given $u \in \mathbf{Z}_p^{(n)}$, let a_0 be the Teichmüller lift of the image of u in $\mathbf{F}_{p^n}$, so that $u - a_0 = pu_1$, for some $u_1 \in \mathbf{Z}_p^{(n)}$. Repeating this construction for u_1 etc., we see that we can write u as a sum as in the corollary. For uniqueness, note that if we have two expressions as in the statement

$$u = \sum_{i\geq 0} a_i p^i = \sum_{i\geq 0} b_i p^i,$$

then $a_0 = b_0$ by Proposition 2.3, and then $\sum_{i\geq 1} a_i p^{i-1} = \sum_{i\geq 1} b_i p^{i-1}$, and we repeat. □

Remark 2.6. Note that if m divides n, then $\mathbf{F}_{p^m} \subseteq \mathbf{F}_{p^n}$ and $\mathbf{Q}_p^{(m)} \subseteq \mathbf{Q}_p^{(n)}$. It follows from the uniqueness part in Proposition 2.3 that the Teichmüller lift $\widetilde{u}$ of an element $u \in \mathbf{F}_{p^m}$ is equal to the Techmüller lift of u when considered as an element in $\mathbf{F}_{p^n}$.

Remark 2.7. If $\widetilde{u}$ and $\widetilde{v}$ are the Teichmüller lifts of $u, v \in \mathbf{F}_{p^n}$, respectively, then $\widetilde{u}\widetilde{v}$ is the Teichmüller lift of uv. Indeed, it is clear that $\widetilde{u}\widetilde{v}$ satisfies both conditions in the definition of a Teichmüller lift.

3. The field $\mathbf{C}_p$

In this section we follow closely the presentation in [Kob, Chapter III.3]. Let $\overline{\mathbf{Q}_p}$ be an algebraic closure of $\mathbf{Q}_p$. We can write $\mathbf{Q}_p = \bigcup_K K$, where K varies over the finite extensions of $\mathbf{Q}_p$. By Exercise 1.3 the absolute values on the various K are compatible, hence we get a non-Archimedean absolute value $|\cdot|_p$ on $\overline{\mathbf{Q}_p}$, that restricts on each K to the one we have defined. As in §1, this gives a non-Archimedean metric on $\overline{\mathbf{Q}_p}$, and each finite extension K of $\mathbf{Q}_p$ is a metric subspace of $\overline{\mathbf{Q}_p}$. The *ring of integers* $\mathcal{O}_{\overline{\mathbf{Q}_p}}$ of $\overline{\mathbf{Q}_p}$ is the union $\bigcup_K \mathcal{O}_K$, hence it is the set of elements of $\overline{\mathbf{Q}_p}$ that are integral over $\mathbf{Z}_p$. We may also describe this as $\{u \in \overline{\mathbf{Q}_p}, |u|_p \leq 1\}$.

Exercise 3.1. *Show that $\mathcal{O}_{\overline{\mathbf{Q}_p}}$ is a local ring, with maximal ideal $\mathfrak{m} = \{u \in \overline{\mathbf{Q}_p}, |u|_p < 1\}$. Prove that there is an isomorphism $\mathcal{O}_{\overline{\mathbf{Q}_p}}/\mathfrak{m} \simeq \overline{\mathbf{F}_p}$.*

Proposition 3.2. *The field $\overline{\mathbf{Q}_p}$, with the metric described above, is not complete.*

Proof. We need to construct a Cauchy non-convergent sequence in $\overline{\mathbf{Q}_p}$. We start by choosing for every $i \geq 0$ a primitive root $b_i \in \overline{\mathbf{Q}_p}$ of 1 of order $p^{2^i} - 1$. Let $K_i = \mathbf{Q}_p(b_i)$. It follows from Theorem 2.1 that $[K_i : \mathbf{Q}_p] = 2^i$. If $i < j$, then $p^{2^i} - 1$ divides $p^{2^j} - 1$. This implies that b_i is a power of b_j, hence we have $K_i \subseteq K_j$.

We take $a_i = b_0 p^{N_0} + b_1 p^{N_1} + \ldots b_i p^{N_i}$, where $N_0 < N_1 < \ldots < N_i < \ldots$ will be chosen later. Note that since $|b_i|_p = 1$ for every i, we have $|a_i - a_{i+1}|_p = \frac{1}{p^{N_i}}$, hence the sequence $(a_i)_i$ is Cauchy by Exercise 1.5.

Suppose that $N_0, \ldots, N_i$ have been constructed, and a_i is defined as above. It is clear that we have $\mathbf{Q}_p(a_i) \subseteq K_i$. We claim that in fact this is an equality. Indeed, otherwise there is $\sigma\colon K_i \to \overline{\mathbf{Q}_p}$ that fixes $\mathbf{Q}_p(a_i)$, but such that $\sigma(b_i) \neq b_i$. We have

$$\sum_{j=0}^{i} \sigma(b_j)p^{N_j} = \sigma(a_i) = a_i = \sum_{j=0}^{i} b_j p^{N_j},$$

and the uniqueness part in Corollary 2.5 implies that $\sigma(b_i) = b_i$, a contradiction.

Assuming N_i chosen, we claim that there is $N_{i+1} > N_i$ such that a_i does not satisfy any congruence

$$(1) \qquad \alpha_n a_i^n + \alpha_{n-1}a_i^{n-1} + \ldots + \alpha_0 \equiv 0 \ (\mathrm{mod}\, p^{N_{i+1}})$$

for any $n < d := [\mathbf{Q}_p(a_i) : \mathbf{Q}_p] = 2^i$, with $\alpha_j \in \mathbf{Z}_p$, not all of them divisible by p. Indeed, for every $N \geq N_i$, consider the set A_N of all $(\alpha_0, \ldots, \alpha_{d-1}) \in \mathbf{Z}/p^{N+1}\mathbf{Z}$ with the property that $\sum_{j=0}^{d-1} \alpha_j a_i^j = 0$ in $\mathbf{Z}/p^{N+1}\mathbf{Z}$, and some α_j does not lie in $p\mathbf{Z}/p^{N+1}\mathbf{Z}$. Note that the projection $\mathbf{Z}/p^{N+2}\mathbf{Z} \to \mathbf{Z}/p^{N+1}\mathbf{Z}$ induces a map $A_{N+1} \to A_N$. If all A_N are nonempty, then $\varprojlim_N A_N$ is nonempty. Indeed, we may choose an element $c_{N_i} \in \bigcap_N \mathrm{Im}(A_N \to A_{N_i})$, then an element $c_{N_i+1} \in \bigcap_N \mathrm{Im}(A_N \to A_{N_i+1})$ that lies over c_{N_i}, etc. Since an element in $\varprojlim_N A_N$ determines a nontrivial equation of degree $< d$ with coefficients in $\mathbf{Q}_p$, we get a contradiction.

We choose the N_i inductively, such that the above condition is satisfied, and we claim that in this case the sequence $(a_i)_i$ is not convergent to an element of $\overline{\mathbf{Q}_p}$. Indeed, if the sequence converges to $a \in \overline{\mathbf{Q}_p}$, then let us consider a polynomial $f = \alpha_n x^n + \ldots + \alpha_0 \in \mathbf{Z}_p[x]$, with not all $\alpha_i \in p\mathbf{Z}_p$, such that $f(a) = 0$. Since $a \equiv a_\ell$ (mod $p^{N_{i+1}}\mathbf{Z}_p$) for $\ell \gg 0$, and $a_i \equiv a_\ell$ (mod $p^{N_{i+1}}\mathbf{Z}_p$) for $\ell \geq i$, it follows that $a \equiv a_i$ (mod $p^{N_{i+1}}\mathbf{Z}_p$). We get a contradiction if we take i such that $2^i > n$. This completes the proof of the proposition. □

Since $\overline{\mathbf{Q}_p}$ is a metric space, it is a general result that there is a *completion* of $\overline{\mathbf{Q}_p}$ that is denoted by $\mathbf{C}_p$. This means that we can embed $\overline{\mathbf{Q}_p}$ as a dense metric subspace in $\mathbf{C}_p$, which is complete. The field operations extend (uniquely) by continuity to $\mathbf{C}_p$, so this is a field. Furthermore, the absolute value on $\overline{\mathbf{Q}_p}$ extends uniquely to a non-Archimedean absolute value on $\mathbf{C}_p$, still denoted by $|\cdot|_p$, that induces the metric, hence the topology of $\mathbf{C}_p$. The miracle is that we do not have to repeat the process of taking algebraic closure and completion.

Theorem 3.3. *The field $\mathbf{C}_p$ is algebraically closed.*

Proof. Let $f = a_0x^n + a_1x^{n-1} + \ldots + a_n$ be a polynomial in $\mathbf{C}_p[x]$, with $a_0 \neq 0$. We need to show that f has a root in $\mathbf{C}_p$. Since $\overline{\mathbf{Q}_p}$ is dense in $\mathbf{C}_p$, we can find $a_{m,i} \in \overline{\mathbf{Q}_p}$ with $a_{m,0} \neq 0$ and $|a_{m,i} - a_i|_p < \varepsilon_m < 1$, where (ε_m) is a strictly decreasing sequence, converging to 0. Let $f_m = \sum_{i=0}^{n} a_{m,i}x^{n-i} \in \overline{\mathbf{Q}_p}[x]$. Since $\overline{\mathbf{Q}_p}$ is algebraically closed, we can factor each f_m as

$$f_m = a_{m,0}(x - \alpha_{m,1}) \cdots (x - \alpha_{m,n}),$$

for suitable $\alpha_{m,i} \in \overline{\mathbf{Q}_p}$.

We first show that there is $C \geq 1$ such that $|\alpha_{m,i}|_p \leq C$ for all i and m. Indeed, let us fix m, and suppose after reordering the $(\alpha_{m,j})_j$ that

$$\alpha_{m,1} = \ldots = \alpha_{m,r} > \alpha_{m,j} \text{ for all } j > r.$$

If s_r is the r^{th} elementary symmetric function of the $\alpha_{m,j}$, then

$$|\alpha_{m,1}|^r = |s_r|_p = |a_{m,r}/a_{m,0}|_p.$$

We conclude that

$$\alpha_{m,i} \leq \max_{1 \leq j \leq n} \frac{|a_{m,j}|_p^{1/j}}{|a_{m,0}|_p^{1/j}},$$

and since each $a_{m,j}$ is close to a_j, we see that we can find C as desired.

We now show that we can reorder $(\alpha_{m,i})_i$ for all m, such that $|\alpha_{m,1} - \alpha_{m+1,1}| \leq C' \varepsilon_m^{1/n}$ for all m, where C' is a constant independent of m. Note that this implies by Exercise 1.5 that the sequence $(\alpha_{m,1})_m$ is Cauchy. Let us suppose that we did this up to m. We have

$$f_{m+1}(\alpha_{m,1}) = a_{m,0} \prod_{j=1}^{n} (\alpha_{m,1} - \alpha_{m+1,j}),$$

and on the other hand

$$f_{m+1}(\alpha_{m,1}) = f_{m+1}(\alpha_{m,1}) - f_m(\alpha_{m,1}) = \sum_{i=0}^{n} (a_{m+1,i} - a_{m,i}) \alpha_{m,1}^{n-i}.$$

Therefore we get

$$|a_{m,0}|_p \cdot \prod_{j=1}^{n} |\alpha_{m,1} - \alpha_{m+1,j}|_p \leq \varepsilon_m C^{n-1},$$

and after reordering the $\alpha_{m+1,j}$ we may assume that

$$|\alpha_{m,1} - \alpha_{m+1,1}|_p \leq C' \varepsilon_m^{1/n},$$

where C' is a constant that only depends on C, n, and $\min_m |a_{m,0}|_p > 0$.

Therefore we may assume that $(\alpha_{m,1})_m$ is a Cauchy sequence, hence is convergent to some $\alpha \in \mathbf{C}_p$. Since $f_m(\alpha_{m,1}) = 0$ for every m, and $\lim_{m \to \infty} a_{m,i} = a_i$ for every i, we have $f(\alpha) = 0$. This completes the proof. □

Remark 3.4. Note that $\mathbf{C}_p$ is obtained from $\mathbf{Q}$ in a similar way that with how $\mathbf{C}$ is obtained from $\mathbf{Q}$, with the respect to the usual Archimedean absolute value on $\mathbf{Q}$ (however, in the case of $\mathbf{C}_p$ we had to complete twice).

Remark 3.5. Note that the algebraic closure and the completion are unique up to a canonical isomorphism. Therefore the field $\mathbf{C}_p$ is unique up to a canonical isomorphism (of fields equipped with an absolute value).

The field $\mathbf{C}_p$ therefore is algebraically closed and complete with respect to the non-Archimedean absolute value $|\cdot|_p$. This provides the right setting for doing p-adic analysis.

4. Convergent power series over complete non-Archimedean fields

In this section we review some basic facts about convergent power series and analytic functions in the non-Archimedean setting. The principle is that the familiar results over $\mathbf{R}$ or $\mathbf{C}$ carry over to this framework, sometimes in a slightly improved version.

Let $(K, |\cdot|)$ be a field endowed with a nontrivial[3] non-Archimedean absolute value, which is complete with respect to the induced metric space structure. For applications we will be interested in the case when $K = \mathbf{C}_p$, or K is a p-adic field. For every point $a \in K$ and every $r > 0$, we put

$$D_r(a) = \{u \in K, |u-a| \leq r\}, \;\; D_r^{\circ}(a) = \{u \in K, |u-a| < r\}.$$

It is clear that $D_r^{\circ}(a)$ is an open neighborhood of a. A special feature of the non-Archimedean setting is that $D_r(a)$ is both open and closed[4].

Proposition 4.1. *Given a formal power series $f = \sum_{n\geq 0} a_n t^n \in K[\![t]\!]$ be a over K, let $r(f) := 1/\mathrm{limsup}_n |a_n|^{1/n}$*[5]*, and consider $u \in K$.*

i) *If $|u| < r(f)$, then $\sum_{n\geq 0} a_n u^n$ is convergent.*
ii) *If $|u| > r(f)$, then $\sum_{n\geq 0} a_n u^n$ is divergent.*
iii) *If $v \in K$ is such that $|u| = |v| = r(f)$, then $\sum_{n\geq 0} a_n u^n$ is convergent if and only if $\sum_{n\geq 0} a_n v^n$ is.*

The *radius of convergence* of f is $r(f)$.

Proof. If $|u| < r(f)$, then $\inf_m \sup_{n\geq m} |a_n|^{1/n} < \frac{1}{|u|}$, hence there is n_0 and $\rho < 1$ such that $|a_n|^{1/n} < \frac{\rho}{|u|}$ for all $n \geq n_0$. Therefore $|a_n u^n| < \rho^n$ for $n \geq n_0$, hence $\lim_{n\to\infty} a_n u^n = 0$, and we deduce from Exercise 1.5 that $\sum_{n\geq 0} a_n u^n$ is convergent.

Suppose now that $|u| > r(f)$, hence $\inf_m \sup_{n\geq m} |a_n|^{1/n} > \frac{1}{|u|}$. It follows that we can find $\rho > \frac{1}{|u|}$ such that for every m, there is $n \geq m$ with $|a_n u^n| > (\rho|u|)^n$. Therefore $\sum_{n\geq 0} a_n u^n$ is divergent. The assertion in iii) follows from the fact that if $|u| = r(f)$, then $\sum_{n\geq 0} a_n u^n$ is convergent if and only if $\lim_{n\to\infty} |a_n| r(f)^n = 0$. □

If $U \subseteq K$ is open, a function $\varphi\colon U \to K$ is *analytic* if for every $a \in U$, there is $r > 0$ with $D_r^{\circ}(a) \subseteq U$, and a formal power series $f \in K[\![t]\!]$ with radius of convergence $r(f) \geq r$ such that $\varphi(u) = f(u-a)$ for every $u \in D_r^{\circ}(a)$.

Lemma 4.2. *If $f = \sum_{n\geq 0} a_n t^n \in K[\![t]\!]$ and $|b| < r(f)$, then there is $g \in K[\![t]\!]$ with $r(g) \geq r(f)$ such that $f(u) = g(u-b)$ for every $u \in K$ with $|u| < r(f)$.*

[3] An absolute value is trivial if it only takes the values 0 and 1.

[4] This shows that K is *totally disconnected*, that is, every point has a basis of neighborhoods that are both open and closed. This is a fact of life in the non-Archimedean setting, and the need to correct this led to the theory of rigid analytic spaces, see [Con].

[5] We make the convention that if $\limsup_n |a_n|^{1/n}$ is zero or infinite, then $r(f) = \infty$ or $r(f) = 0$, respectively.

Proof. For every $u \in K$ we have $|u-b| < r(f)$ if and only if $|u| < r(f)$, and in this case

$$f(u) = \sum_{n\geq 0} a_n((u-b)+b)^n = \sum_{n\geq 0} a_n \sum_{i=0}^{n} \binom{n}{i}(u-b)^i b^{n-i} = \sum_{i\geq 0}\left(\sum_{j\geq 0}\binom{i+j}{i} a_{i+j} b^j\right)(u-b)^i.$$

In particular, $\beta_i := \sum_{j\geq 0}\binom{i+j}{i}a_{i+j}b^j$ is well-defined, the series $g = \sum_{i\geq 0}\beta_i t^i$ has radius of convergence $\geq r(f)$, and $f(u) = g(u-b)$ whenever $|u-b| < r(f)$. □

Corollary 4.3. *If $f \in K[\![t]\!]$ has radius of convergence $r(f) > 0$, then the function*

$$\{u \in K, |u| < r(f)\} \ni u \to f(u) \in K$$

is an analytic function.

Analytic functions on open subsets of K satisfy properties entirely analogous to the ones of real or complex analytic functions. We list some of these properties, but leave as an exercise for the reader the task of checking that the familiar proofs also work in the non-Archimedean setting.

• Every analytic function is continuous. This is a consequence of the fact that for every $f = \sum_{n\geq 0} a_n t^n \in K[\![t]\!]$, if we put $f_m = \sum_{n=0}^{m} a_n t^n$, then the convergence of $f_m(u)$ to $f(u)$ is uniform on every subset $D_R(0)$, with $R < r(f)$. Indeed, we have

$$|f(u) - f_m(u)| \leq \sup_{n\geq m} |a_n| R^n \to 0 \text{ when } m \to \infty.$$

• The set of analytic functions on an open subset $U \subseteq K$ is a ring. Furthermore, if φ is analytic and nonzero at every point of U, then $1/\varphi$ is analytic.

More precisely, suppose that φ and ψ are analytic on U, and they are given on $D_r^\circ(a) \subseteq U$ as $\varphi(u) = f(u-a)$ and $\psi(u) = g(u-a)$, for some $f, g \in K[\![t]\!]$ $r(f), r(g) \geq r$. In this case the radii of convergence of $f+g$ and fg are both $\geq r$, and $\varphi(u) + \psi(u) = (f+g)(u-a)$ and $\varphi(u)\psi(u) = fg(u-a)$ for $u \in D_r^\circ(a)$. Furthermore, if $\varphi(u) \neq 0$ for every $u \in D_r^\circ(a)$, then in particular $f(0) \neq 0$, hence f is invertible. The radius of convergence of f^{-1} is $\geq r$, and $1/\varphi(u) = f^{-1}(u-a)$ for every $u \in D_r^\circ(a)$.

• If $\varphi\colon U \to V$ and $\psi\colon V \to K$ are analytic functions, then the composition $\psi \circ \varphi$ is analytic. More precisely, given $a \in U$, suppose that $D_r^\circ(a) \subseteq U$ and $D_{r'}^\circ(\varphi(a)) \subseteq V$ are such that $\varphi(u) = f(u-a)$ and $\psi(v) = g(v - \varphi(a))$ for suitable $f, g \in K[\![t]\!]$, such that the radii of convergence of f and g are $\geq r, r'$, respectively. Note that $f(0) = \varphi(a)$, and let $\widetilde{f} = f - f(0)$, and $h = g \circ \widetilde{f} \in K[\![t]\!]$. After possibly replacing r by a smaller value, we may assume that $\varphi(D_r^\circ(a)) \subseteq D_{r'}^\circ(\varphi(a))$. In this case the radius of convergence of h is $\geq r$, and we have $\varphi(\psi(u)) = h(u-a)$ for $u \in D_r^\circ(a)$.

• If $f, g \in K[\![t]\!]$ have radii of convergence $\geq R > 0$, and $f(u) = g(u)$ for every u with $0 < |u| < R$, then $f = g$

One can differentiate analytic functions, and the result is again analytic. One can also consider, more generally, analytic functions of several variables. However, while such functions show up in Lecture 9, we do not need to develop any theory in this setting.

We end this section with the following result that is needed in Lecture 9. For simplicity, we assume that $|K^*|$ is dense in $\mathbf{R}_0$. For example, this always holds if K is algebraically closed. Indeed, if $u \in K$ is such that $|u| > 1$, then $|u|^q \in |K^*|$ for every $q \in \mathbf{Q}$, hence $|K^*|$ is dense in $\mathbf{R}_{>0}$.

Proposition 4.4. *Suppose that $|K^*|$ is dense in $\mathbf{R}_{>0}$, and let $R > 0$ and $f \in K[\![t]\!]$ be such that $r(f) > R$. In this case, there is a polynomial $P \in K[t]$ and an invertible power series $g \in K[\![t]\!]$ such that both g and g^{-1} are convergent on $D_R(0)$, and $f = Pg$.*

Before giving the proof of the proposition, we introduce some notation. Let $A_K = \{u \in R, |u| \leq 1\}$ and $\mathfrak{m}_K = \{u \in A_K, |u| < 1\}$. It is clear that A_K is a subring of K, $\mathfrak{m}_K$ is an ideal in A_K, and the quotient $A_K/\mathfrak{m}_K$ is a field, that we denote by k. If $f \in A[\![t]\!]$, we denote by $\overline{f}$ its image in $k[\![t]\!]$.

Let T denote the set of formal power series in $K[\![t]\!]$ that are convergent on $D_1(0)$. If $f = \sum_{n \geq 0} a_n t^n$, then $f \in T$ if and only if $\lim_{n \to \infty} a_n = 0$. It follows that if we put $\| f \| := \max_n |a_n|$, then this maximum is well-defined, and it is attained for only finitely many n. Note that if $f \in R[\![t]\!] \cap T$, then $\overline{f}$ is a polynomial.

Exercise 4.5. *Show that if $f, g \in T$, then $\| f \cdot g \| = \| f \| \cdot \| g \|$.*

Proof of Proposition 4.4. The assertion holds trivially if $f = 0$, hence from now on we assume $f \neq 0$. Since $|K^*|$ is dense in $\mathbf{R}_{>0}$, after possibly replacing R by a larger value, we may assume that $R \in |K^*|$. We first note that if $\alpha \in D^{\circ}_{r(f)}(0)$ is such that $f(\alpha) = 0$, then $f = (t - \alpha) f_1$ for some $f_1 \in K[\![t]\!]$ with $r(f_1) \geq r(f)$. Indeed, by Lemma 4.2 there is $g \in K[\![t]\!]$ with $r(g) \geq r(f)$ such that $f(u) = g(u - \alpha)$ for $|u| < r(f)$. Since $f(\alpha) = 0$, it follows that $g = t g_1$ for some $g_1 \in K[\![t]\!]$, and we clearly have $r(g_1) = r(g)$. Another application of Lemma 4.2 gives $f_1 \in K[\![t]\!]$ with $r(f_1) \geq r(g_1) \geq r(f)$ such that $g_1(u) = f_1(u + \alpha)$ whenever $|u| < r(f)$. Therefore

$$f(u) = g(u - \alpha) = (u - \alpha) g_1(u - \alpha) = (u - \alpha) f_1(u)$$

for all u with $|u| < r(f)$, hence $f = (t - \alpha) f_1$.

We now show that there are $\alpha_1, \ldots, \alpha_r \in D_R(0)$ (possibly not distinct) such that

$$f = (t - \alpha_1) \cdots (t - \alpha_r) g \tag{2}$$

for some $g \in K[\![t]\!]$ with $r(g) \geq r(f)$, and such that $g(\alpha) \neq 0$ for every $\alpha \in D_R(0)$. If $\lambda \in K$ is such that $|\lambda| = R$, then after replacing f by $f(\lambda t)$, we may assume that $R = 1$. Let us write $f = \sum_{n \geq 0} a_n t^n$. By assumption, we have $f \in T$, and let N be the largest n with $|a_n| = \| f \|$. After replacing f by $a_N^{-1} f$, we may assume that $a_N = 1$. Therefore $f \in A_K[\![t]\!]$, and $\overline{f}$ is a monic polynomial of degree N. By what we have already proved, it is enough to show that given any expression as in (2), we have $r \leq N$. Since $\| t - \alpha_i \| = 1$ for all i, it follows from Exercise 4.5 that $\| g \| = 1$. In particular, we have $g \in A_K[\![t]\!]$, and if we take the image in $k[\![t]\!]$, we get $\overline{f} = \overline{g} \cdot \prod_{i=1}^{r} (t - \overline{\alpha_i})$. Since $\overline{f}$ is a polynomial of degree N, we deduce that $r \leq N$.

In order to complete the proof of the proposition, it is enough to show that if we write f as in (2), with g not vanishing anywhere on $D_R(0)$, then g^{-1} converges on $D_R(0)$:

indeed, we then take $P=\prod_{i=1}^r(t-\alpha_i)$. Since $|K^*|$ is dense in $\mathbf{R}_{>0}$, there is $R'\in|K^*|$ with $R<R'<r(f)$. Applying what we have already proved for g and $D_{R'}(0)$, we see that there are only finitely many $\alpha\in D_{R'}(0)$ with $g(\alpha)=0$. It follows that after replacing R' by a smaller one, we may assume that g does not vanish on $D_{R'}(0)$, and in this case the radius of convergence of g^{-1} is $\geq R'>R$. This completes the proof of the proposition. □

5. Examples of analytic functions

In this section we discuss the p-adic version of some familiar complex analytic functions Let us start with the exponential function. In this section we assume that $K=\mathbf{C}_p$.

Consider $f=\sum_{n\geq 0}\frac{t^n}{n!}\in\mathbf{C}_p[\![t]\!]$, and let us determine the radius of convergence of f. Note that unlike in the complex case, the large denominators make the radius of convergence small. For every n we have

$$\mathrm{ord}_p(n!)=\sum_{i\geq 1}\lfloor n/p^i\rfloor\leq\sum_{i\geq 1}\frac{n}{p^i}=\frac{n}{p-1},$$

hence $(|1/n!|_p)^{1/n}\leq\left(\frac{1}{p}\right)^{-1/(p-1)}$. On the other hand, if $n=p^m$, then

$$\mathrm{ord}_p(n!)=p^{m-1}+\ldots+p+1=\frac{p^m-1}{p-1},$$

hence $\mathrm{ord}_p(p^m!)/p^m$ converges to $\frac{1}{p-1}$. We thus conclude that $\mathrm{limsup}_n(|1/n!|_p)^{1/n}=\left(\frac{1}{p}\right)^{-1/(p-1)}$, hence by Proposition 4.1 the radius of convergence of f is $\left(\frac{1}{p}\right)^{1/(p-1)}<1$. This implies that the *p-adic exponential function* $\exp_p$ given by $\exp_p(u)=f(u)$ is not defined, for example, on all $\mathbf{Z}_p$.

Let us consider also the *p-adic logarithm function* $\log_p(1+u)=g(u)$, where $g(t)=\sum_{n\geq 1}(-1)^{n-1}\frac{t^n}{n}$. We now are in better shape: if $\mathrm{ord}_p(n)=i$, then $n\geq p^i$, hence $\frac{i}{n}\leq\frac{\log(n)}{n\cdot\log(p)}$, which converges to zero when n goes to infinity. It then follows from Proposition 4.1 that the radius of convergence of g is 1, hence $\log_p(1+u)$ is defined in $D_1^\circ(0)$, precisely as in the complex case.

We now consider the *p-adic binomial series*. Let us recall first the formula for the binomial series in the case of complex functions. If $a\in\mathbf{C}$, then we may consider the analytic function $\varphi(u)=(1+u)^a$. More precisely, we have $\varphi(u)=\exp(a\cdot\log(1+u))$, which is defined and analytic for $|u|<1$. The Taylor expansion at 0 is given by

$$\varphi(u)=\sum_{m\geq 0}\frac{\varphi^{(m)}(0)}{m!}u^m.$$

Since we have $\varphi'(u)=a(1+u)^{a-1}$, one sees immediately by induction on m that $\varphi^{(m)}(0)=a(a-1)\cdots(a-m+1)$.

We will now use the same formal power series in the p-adic setting, by allowing the exponent to lie in $\mathbf{C}_p$. More precisely, for $a \in \mathbf{C}_p$, consider the formal power series

$$B_{a,p}(y) = \sum_{m \geq 0} \frac{a(a-1)\cdots(a-m+1)}{m!} y^m \in \mathbf{C}_p[\![y]\!].$$

For obvious reasons, we also write $(1+y)^a$ for $B_{a,p}(y)$, and $(1+u)^a$ for $B_{a,p}(u)$, when $u \in \mathbf{C}_p$ is such that $|u|$ is smaller than the radius of convergence of $B_{a,p}$. Let us first discuss the radius of convergence of $B_{a,p}$.

Lemma 5.1. *Let $a \in \mathbf{C}_p$, and denote by R the radius of convergence of $B_{a,p}$.*

- i) *If $|a|_p > 1$, then $R = \frac{1}{|a|_p} \left(\frac{1}{p}\right)^{1/(p-1)}$.*
- ii) *If $|a|_p \leq 1$, then $R \geq \left(\frac{1}{p}\right)^{1/(p-1)}$.*
- iii) *If $a \in \mathbf{Z}_p$, then $R \geq 1$.*

Proof. Suppose first that $|a|_p > 1$. In this case $|a-i|_p = |a|_p$ for every $i \in \mathbf{Z}$. Therefore

$$\left(\frac{|a(a-1)\cdots(a-m+1)|_p}{|m!|_p}\right)^{1/m} = \frac{|a|_p}{|m!|_p^{1/m}},$$

and the computation that we have done for $\exp_p$ shows that in this case the radius of convergence of $B_{a,p}(x)$ is $\frac{1}{|a|_p} \left(\frac{1}{p}\right)^{1/(p-1)}$.

If $|a|_p \leq 1$, then $|a-i|_p \leq 1$ for every $i \in \mathbf{Z}$, and we deduce from Proposition 4.1 and the computation in the case of the exponential function that $R \geq \left(\frac{1}{p}\right)^{1/(p-1)}$. For the assertion in iii), it is enough to show that if $a \in \mathbf{Z}_p$, then $\frac{a(a-1)\cdots(a-m+1)}{m!} \in \mathbf{Z}_p$. This is clear when $a \in \mathbf{Z}$, and the general case follows since $\mathbf{Z}$ is dense in $\mathbf{Z}_p$ (recall that $\mathbf{Z}_p$ consists of those $u \in \mathbf{Q}_p$ with $|u|_p \leq 1$). □

Remark 5.2. It is clear from definition that if m is a nonnegative integer, then $B_{m,p}(1+y)$ is, as expected, the m^{th} power of $1+y$.

The binomial series satisfies the following "expected" properties.

Proposition 5.3. *If $a, b \in \mathbf{C}_p$, then the following hold.*

- i) $(1+y)^a \cdot (1+y)^b = (1+y)^{a+b}$.
- ii) $((1+y)^a)^b = (1+y)^{ab}$.

Regarding ii), note that $(1+y)^a = 1 + v(y)$ for some $v \in y\mathbf{C}_p[\![y]\!]$, hence $(1+v(y))^b$ is well-defined in $\mathbf{C}_p[\![y]\!]$. We will prove the assertions in the proposition by reducing them to the corresponding ones over $\mathbf{C}$. However, it is more convenient to first introduce a formal series over $\mathbf{Q}$ in two variables, by letting a become a formal variable. More precisely, we consider

$$(1+y)^x := \sum_{m \geq 0} \frac{x(x-1)\cdots(x-m+1)}{m!} y^m \in \mathbf{Q}[\![x,y]\!].$$

Proposition 5.4. *We have the following equalities in* $\mathbf{Q}[\![x_1, x_2, y]\!]$.

i) $(1+y)^{x_1} \cdot (1+y)^{x_2} = (1+y)^{x_1+x_2}$.
ii) $((1+y)^{x_1})^{x_2} = (1+y)^{x_1 x_2}$.

Proof. Let us prove i). Let f and g denote the left-hand side (respectively, the right-hand side) in i). In order to show that $f = g$, it is enough to show that they are equal in $\mathbf{C}[\![x_1, x_2, y]\!]$, hence it is enough to show that if $u_1, u_2, v \in \mathbf{C}$ are such that $|v| < 1$, then $f(u_1, u_2, v) = g(u_1, u_2, v)$ in $\mathbf{C}$ (note that under the condition on v, both sides are well-defined. As we have seen,

$$\begin{aligned}(1+v)^{u_1} \cdot (1+v)^{u_2} &= \exp(u_1 \log(1+v)) \cdot \exp(u_2 \log(1+v)) \\ &= \exp((u_1+u_2)\log(1+v)) = (1+v)^{u_1+u_1}.\end{aligned}$$

This completes the proof of i), and the proof of ii) is entirely similar. □

Proof of Proposition 5.3. If $g \in \mathbf{C}_p[\![x_1, x_2, y]\!]$ is such that the coefficient of every y^m is in $\mathbf{C}_p[x_1, x_2]$, for every $a, b \in \mathbf{C}_p$ we may consider $g(a, b, y) \in \mathbf{C}_p[\![y]\!]$. By letting $x_1 = a$ and $x_2 = b$ in Proposition 5.4, we get the assertions in Proposition 5.3. □

Example 5.5. Suppose that m is a positive integer not divisible by p, hence $\frac{1}{m} \in \mathbf{Z}_p$. It follows from Proposition 5.1 that for every $u \in \mathbf{C}_p$ with $|u|_p < 1$ (for example, for every $u \in p\mathbf{Z}_p$) $v = (1+u)^{1/m}$ is well-defined, and by Proposition 5.3 we have $v^m = 1 + u$.

References

[Con] B. Conrad, Several approaches to non-Archimedean geometry, in *p-adic geometry*, 963, Univ. Lecture Ser., 45, Amer. Math. Soc., Providence, RI, 2008. 9

[Kob] N. Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, Second edition, Graduate Texts in Mathematics, 58, Springer-Verlag, New York, 1984. 1, 6

[Lang] S. Lang, *Algebraic number theory*, Graduate Texts in Mathematics, 110, Springer-Verlag, New York, 1994. 2

[Mat] H. Matsumura, *Commutative ring theory*, translated from the Japanese by M. Reid, Second edition, Cambridge Studies in Advanced Mathematics 8, Cambridge University Press, Cambridge, 1989. 1, 2