D-MATH Number Theory II FS 2024
Prof. Richard Pink

Solutions 16

Absolute Values, Completion, Power series

1. *(Product formula)* A non-archimedean absolute value $|\ |$ on a field K, whose valuation ring $\mathcal{O}_K$ is discrete with finite residue field $\mathcal{O}_K/\mathfrak{m}$, is called *normalized* if $|\pi| = |\mathcal{O}_K/\mathfrak{m}|^{-1}$ for any element π with $(\pi) = \mathfrak{m}$. Consider a finite field k.

   (a) Write down all normalized absolute values $|\ |_v$ on $k(t)$.

   (b) For any $a \in k(t)^\times$ prove that $\prod_v |a|_v = 1$.

   (*Hint:* Compare Examples 8.2.6 (a–b) and Theorem 8.4.15 of Ostrowski.)

   Solution:

   (a) For any monic irreducible polynomial $p \in k[t]$ and any $f \in k(t)$ we define $|f|_p := |k[t]/(p)|^{-\operatorname{ord}_p(f)}$. This defines a non-archimedean absolute value with $\mathcal{O}_{k(t)} = k[t]_{(p)}$, which is normalized because $|p|_p = |k[t]/(p)|^{-1} = |\mathcal{O}_{k(t)}/(p)|^{-1}$. Varying p, this yields all the normalized absolute values on $k(t)$ associated to maximal ideals of $k[t]$.

   An additional normalized absolute value $|\ |_\infty$ is obtained in the same way from the maximal ideal $(s) \subset k[s]$ after the substitution $s = \frac{1}{t}$. For any non-zero polynomial $f \in k[t]$ of degree $n \in \mathbb{Z}$ the substitution yields $f(t) = s^n \cdot f(\frac{1}{s}) \cdot s^{-n}$ with $|s^n \cdot f(\frac{1}{s})|_\infty = 1$ and hence $|f|_\infty = |s|_\infty^{-n} = |k|^{\deg(f)}$. For arbitrary non-zero $f, g \in k[t]$ we therefore have $|\frac{f}{g}|_\infty = |k|^{\deg(f)-\deg(g)}$.

   Clearly every absolute value on $k(t)$ is equivalent to a unique normalized one. Thus by Theorem 4.1 in the following notes by Brian Conrad the above list of normalized absolute values on $k(t)$ is complete:

   `http://math.stanford.edu/~conrad/676Page/handouts/ostrowski.pdf`

   (b) By multiplicativity it suffices to prove this for generators of the group $k(t)^\times$, namely for any monic irreducible polynomial $p \in k[t]$ and any element $\alpha \in k^\times$. The latter has finite order and hence satisfies $|\alpha|_v = 1$ for all absolute values $|\ |_v$, and therefore also $\prod_v |a|_v = 1$. The former satisfies $|p|_p = |k[t]/(p)|^{-1} = |k|^{-\deg(p)}$ and $|p|_\infty = |k|^{\deg(p)}$, while $|p|_{p'} = 1$ for all monic irreducible polynomials $p' \in k[t]$ that are distinct from p. Thus the product is again 1.

2. Work out the details of the proof of Proposition 8.5.5 of the lecture: Every metric space possesses a completion.

   Solution: See for example [Marco Manetti: Topology (2015) Theorem 6.47].

3. Let K be a complete ultrametric field. Show that a convergent series with summands in K can be arbitrarily rearranged and subdivided without changing convergence or the limit.

(*Hint:* Test your analysis skills by trying to give a complete formal proof.)

Solution: Consider a convergent series $\sum_{n=0}^{\infty} a_n$ in K. In the lecture we showed that $\lim_{n\to\infty} a_n = 0$. Thus for any $\varepsilon > 0$ there exists an $n_\varepsilon \geqslant 0$ such that $|a_n| \leqslant \varepsilon$ for all $n > n_\varepsilon$.

First consider an arbitrary bijection $\sigma\colon \mathbb{Z}^{\geqslant 0} \to \mathbb{Z}^{\geqslant 0}$. For any $\varepsilon > 0$ set $m_\varepsilon := \max\{n, \sigma n \mid 0 \leqslant n \leqslant n_\varepsilon\}$. Then for any $m > m_\varepsilon$ the partial sum of differences $\sum_{n=0}^{m}(a_n - a_{\sigma n})$ is a finite sum of terms of the form $\pm a_n$ with $n > n_\varepsilon$. By the construction of n_ε all these satisfy $|\pm a_n| = |a_n| \leqslant \varepsilon$; hence the strict triangle inequality implies that $\left|\sum_{n=0}^{m}(a_n - a_{\sigma n})\right| \leqslant \varepsilon$. Thus the series $\sum_{n\geqslant 0}(a_n - a_{\sigma n})$ converges to 0; hence the series $\sum_{n\geqslant 0} a_{\sigma n}$ converges to the same limit as the series $\sum_{n\geqslant 0} a_n$.

Now consider a bjiection $\tau\colon (\mathbb{Z}^{\geqslant 0})^2 \to \mathbb{Z}^{\geqslant 0}$. Then for each $i \geqslant 0$ the subsequence $(a_{\tau(i,j)})_j$ of the original sequence $(a_n)_n$ also converges to 0; hence the series $\sum_{j\geqslant 0} a_{\tau(i,j)}$ converges, say to $x_i \in K$. Moreover, for any $\varepsilon > 0$ set

$$m_\varepsilon \;:=\; \max\{n_\varepsilon\} \cup \{j \geqslant 0 \mid \exists i \geqslant 0\colon \tau(i,j) \leqslant n_\varepsilon\} \cup \{i \geqslant 0 \mid \exists j \geqslant 0\colon \tau(i,j) \leqslant n_\varepsilon\}.$$

Then for any $i \geqslant 0$ the partial sums $\sum_{j=0}^{m} a_{\tau(i,j)}$ for all $m \geqslant m_\varepsilon$ differ only by terms a_n with $n > n_\varepsilon$ and hence with $|a_n| \leqslant \varepsilon$. By the strict triangle inequality the difference of any such partial sums thus also has norm $\leqslant \varepsilon$. Passing to the limit we deduce that $\left|\sum_{j=0}^{m} a_{\tau(i,j)} - x_i\right| \leqslant \varepsilon$ for all $i \geqslant 0$ and $m \geqslant m_\varepsilon$. Using the strict triangle inequality again we deduce that $\left|\sum_{i=0}^{m}\sum_{j=0}^{m} a_{\tau(i,j)} - \sum_{i=0}^{m} x_i\right| \leqslant \varepsilon$ for all $m \geqslant m_\varepsilon$.

On the other hand, the definition of m_ε implies that for any $m > m_\varepsilon$, the difference $\sum_{i=0}^{m}\sum_{j=0}^{m} a_{\tau(i,j)} - \sum_{n=0}^{m} a_n$ is a finite sum of terms of the form $\pm a_n$ with $n > n_\varepsilon$. By the construction of n_ε all these satisfy $|\pm a_n| = |a_n| \leqslant \varepsilon$; hence the strict triangle inequality implies that $\left|\sum_{i=0}^{m}\sum_{j=0}^{m} a_{\tau(i,j)} - \sum_{n=0}^{m} a_n\right| \leqslant \varepsilon$. Using the strict triangle inequality again we find that $\left|\sum_{i=0}^{m} x_i - \sum_{n=0}^{m} a_n\right| \leqslant \varepsilon$ as well. Thus the series $\sum_{i\geqslant 0} x_i$ converges to the same limit as the series $\sum_{n\geqslant 0} a_n$, as desired.

4. Let K be a field with a complete absolute value $|\ |$. The *radius of convergence* of a power series $f(X) = \sum_{n=0}^{\infty} a_n X^n \in K[[X]]$ is defined as

$$r_f \;:=\; \sup\bigl\{r \in \mathbb{R}^{\geqslant 0} : |a_n| r^n \to 0 \text{ for } n \to \infty\bigr\} \;\in\; \mathbb{R} \cup \{\infty\}.$$

   (a) Show that

$$r_f \;=\; \frac{1}{\limsup_{n\to\infty} |a_n|^{1/n}}.$$

(b) Show that for any $x \in K$ the series $f(x) := \sum_{n=0}^{\infty} a_n x^n$ diverges if $|x| > r_f$ and converges if $|x| < r_f$.

(c) What happens for $|x| = r_f$?

Solution:

(a) Set

$$r'_f \; := \; \frac{1}{\limsup_{n\to\infty} |a_n|^{1/n}}.$$

First consider any real number $r > r'_f$. Then there exist infinitely many $n \in \mathbb{N}$ such that $r > \frac{1}{|a_n|^{1/n}}$. For these n we have $|a_n|r^n > 1$, so the sequence $(|a_n|r^n)_n$ does not converge to 0 for $n \to \infty$; hence $r \geqslant r_f$. Varying r this shows that $r'_f \geqslant r_f$.

Now consider any real number $r < r'_f$. Choose another real number r' such that $r < r' < r'_f$. Then

$$\limsup_{n\to\infty} r' \, |a_n|^{\frac{1}{n}} \;=\; r' \limsup_{n\to\infty} |a_n|^{\frac{1}{n}} \;=\; \frac{r'}{r'_f} < 1.$$

Hence there exists an $N \geqslant 1$ such that

$$\sup_{n \geqslant N} r' \, |a_n|^{\frac{1}{n}} < 1.$$

For any $n > N$ we therefore have $|a_n| \, (r')^n < 1$ and so

$$|a_n| \, r^n \;=\; |a_n| \, (r')^n \left(\frac{r}{r'}\right)^n \;<\; \left(\frac{r}{r'}\right)^n,$$

which tends to 0 for $n \to \infty$. This shows that $r \leqslant r_f$, and varying r it implies that $r'_f \leqslant r_f$.

(b) Suppose first that $|x| > r_f$. Then the definition of r_f implies that $|a_n x^n| = |a_n| \cdot |x|^n$ does not converge to zero; hence the series diverges.

Now suppose that $|x| < r_f$. Then by the definition of r_f there exists $r \in \mathbb{R}$ such that $|x| < r$ and that $|a_n|r^n \to 0$ for $n \to \infty$. This r in particular satisfies $C := \sup\{|a_n|r^n : n \geqslant 0\} < \infty$ and $\big||x|/r\big| < 1$. Therefore

$$\sum_{n\geqslant 0} |a_n x^n| \;=\; \sum_{n\geqslant 0} |a_n| r^n \cdot (|x|/r)^n \;\leqslant\; \sum_{n\geqslant 0} C \cdot (|x|/r)^n \;=\; \frac{C}{1 - |x|/r} \;<\; \infty.$$

Hence the series converges.

(c) For $|x| = r_f$ the series may or may not converge, as in real analysis.

For example take $f(X) := \sum_{n=0}^{\infty} X^n$. Then $r_f = 1$, but for any $x \in K$ with $|x| = 1$ we have $|x|^n \not\to 0$ for $n \to \infty$; hence the series does not converge.

By contrast, fix any element $\pi \in K$ with $0 < |\pi| < 1$, and for any $n \geqslant 1$ set $k_n := \lceil -\frac{\log n^2}{\log |\pi|} \rceil$. Then we have $\log|\pi| < 0$ and hence

$$\begin{aligned} & -\tfrac{\log n^2}{\log|\pi|} \leqslant k_n \leqslant -\tfrac{\log n^2}{\log|\pi|} + 1 \\ \Rightarrow\ & -\log n^2 \geqslant k_n \cdot \log|\pi| \geqslant -\log n^2 + \log|\pi| \\ \Rightarrow\ & \tfrac{1}{n^2} \geqslant |\pi^{k_n}| \geqslant \tfrac{|\pi|}{n^2}. \end{aligned}$$

By real analysis we thus know that for any $r \in \mathbb{R}^{\geqslant 0}$ we have $|\pi^{k_n}|r^n \to 0$ if $r < 1$ and $|\pi^{k_n}|r^n \to \infty$ if $r > 1$. Thus the power series $f(X) := \sum_{n=0}^{\infty} \pi^{k_n} X^n$ has radius of convergence $r_f = 1$. But for any $x \in K$ with $|x| = 1$ we have

$$\sum_{n\geqslant 1} |\pi^{k_n} x^n| = \sum_{n\geqslant 1} |\pi|^{k_n} \leqslant \sum_{n\geqslant 0} \tfrac{1}{n^2} < \infty;$$

hence the series converges.

5. Let K be a field that is complete with respect to a p-adic absolute value. Consider $\alpha, \beta \in \mathbb{Z}_p$ and $m, n \in \mathbb{Z}$ with $n \geqslant 0$. Prove:

   (a) The binomial coefficient $\binom{\alpha}{n} := \frac{\alpha(\alpha-1)\cdots(\alpha-n+1)}{n!}$ lies in $\mathbb{Z}_p$.

   (b) The power series $F_\alpha(X) := \sum_{n\geqslant 0} \binom{\alpha}{n} X^n \in K[[X]]$ has convergence radius $\geqslant 1$. Moreover, for $x \in K$ with $|x| < 1$ we have $|F_\alpha(x) - 1| < 1$.

   (c) $F_{\alpha+\beta}(x) = F_\alpha(x) \cdot F_\beta(x)$.

   (d) $F_{m\alpha}(x) = F_\alpha(x)^m$.

   (e) $F_m(x) = (1+x)^m$.

   (f) $y := F_{m/n}(x)$ is the only solution of the equation $y^n = (1+x)^m$ with $|y-1| < 1$, if $p \nmid n$.

   This therefore justifies writing $F_\alpha(x) = (1+x)^\alpha$.

   *(g) Do we then also have $((1+x)^\alpha)^\beta = (1+x)^{\alpha\beta}$?

   (h) Find a closed form of $\sqrt{7}$ in $\mathbb{Q}_3$.

   Solution:

   (a) Since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, we can find a sequence of non-negative integers $(a_k)_{k\in\mathbb{Z}^{\geqslant 1}}$ such that $\lim_{k\to\infty} a_k = \alpha$ in $\mathbb{Z}_p$. It follows that $\lim_{k\to\infty} \binom{a_k}{n} = \binom{\alpha}{n}$, because $\binom{X}{n} \in \mathbb{Z}_p[X]$ is a polynomial and it follows from exercise 4 of sheet 15 that polynomial functions are continuous. As $\binom{a_k}{n} \in \mathbb{Z} \subset \mathbb{Z}_p$ for all k and $\mathbb{Z}_p$ is closed in $\mathbb{Q}_p$ it follows that the limit $\binom{\alpha}{n}$ also lies in $\mathbb{Z}_p$.

(b) By (a), we have $\binom{\alpha}{n} \in \mathbb{Z}_p$ and hence $|\binom{\alpha}{n}| \leqslant 1$. Thus by exercise 4 the radius of convergence is at least 1. In particular it converges whenever $|x| < 1$. In that case the multiplicativity of the norm implies that $\left|\binom{\alpha}{n}x^n\right| \leqslant |x|^n \leqslant |x|$ for all $n \geqslant 1$. Thus

$$|F_\alpha(x) - 1| \;=\; \left|\sum_{n\geqslant 1}\binom{\alpha}{n}x^n\right| \;\leqslant\; \sup\left\{\left|\binom{\alpha}{n}x^n\right| : n \geqslant 1\right\} \;\leqslant\; |x| \;<\; 1.$$

(c) We will use the fact that for convergent series $\sum_{n\geqslant 0} a_n$ and $\sum_{n\geqslant 0} b_n$ in a non-archimedean complete field K the product can be calculated as the Cauchy product $\sum_{k\geqslant 0}\sum_{n+m=k} a_m b_n$. A reference for this fact and many other useful statements about infinite series can be found for example in the following expository text by Keith Conrad:

`https://kconrad.math.uconn.edu/blurbs/gradnumthy/infseriespadic.pdf`

We calculate

$$F_\alpha(x)\cdot F_\beta(x) = \sum_{n\geqslant 0} x^n \sum_{k=0}^{n} \binom{\alpha}{k}\binom{\beta}{n-k},$$

and hence the desired equality follows from the following

Claim: We have $\sum_{k=0}^{n}\binom{\alpha}{k}\binom{\beta}{n-k} = \binom{\alpha+\beta}{n}$.

Proof. In the case when $\alpha, \beta \in \mathbb{Z}^{\geqslant 0}$, this is just the Vandermonde identity. For the general case note that the polynomials $\sum_{k=0}^{n}\binom{X}{k}\binom{Y}{n-k}$ and $\binom{X+Y}{n}$ in $\mathbb{Z}_p[X,Y]$ agree on the set $(\mathbb{Z}^{\geqslant 0})^2$ which is dense in $(\mathbb{Z}_p)^2$. Because polynomial functions are continuous it follows that they agree everywhere. □

(d) For $m = 0$ this is clear from the definition. For $m > 0$ it follows by induction from (c). For $m < 0$ just observe that by (c) we have $F_{m\alpha}(x)\cdot F_{-m\alpha}(x) = F_0(x) = 1$ and therefore $F_{m\alpha}(x) = F_{-m\alpha}(x)^{-1} = (F_\alpha(x)^{-m})^{-1} = F_\alpha(x)^m$.

(e) For $m \geqslant 0$ this follows immediately from the binomial theorem. For $m < 0$ we deduce from (d) that $F_m(x) = F_{-m}(x)^{-1} = ((1+x)^{-m})^{-1} = (1+x)^m$.

(f) We calculate

$$y^n = F_{m/n}(x)^n \overset{(d)}{=} F_m(x) \overset{(e)}{=} (1+x)^m.$$

Moreover $|y-1| < 1$ by (a), which is equivalent to saying that $y \in \mathcal{O}_K$ and $y \equiv 1 \bmod (p)$. It remains to show that y is the only root of $f(X) := X^n - (1+x)^m \in \mathcal{O}_K[X]$ that is $\equiv 1 \bmod (p)$. But since $n \not\equiv 0 \bmod (p)$, we have $f'(y) = ny^{n-1} \not\equiv 0 \bmod (p)$. Thus $y \bmod (p)$ is a simple root of $f \bmod (p)$; so by Hensel's lemma f has precisely one root in $\mathcal{O}_K$ that is $\equiv 1 \bmod (p)$, as desired.

*(g) Yes, by a similar, though somewhat more elaborate, reasoning as in (c). Likewise we have $((1+x)(1+y))^\alpha = (1+x)^\alpha(1+y)^\alpha$ whenever $|x|, |y| < 1$.

(h) We have $F_{1/2}(6)^2 = 1+6 = 7$. Thus $\sqrt{7} = F_{1/2}(6)$.

*6. *(Newton method for finding zeros of a polynomial)* Let p be a prime number, let $f \in \mathbb{Z}_p[X]$ and let $\alpha \in \mathbb{Z}_p$ be a root of f such that $f'(\alpha) \neq 0$. Set

$$U \; := \; \big\{a \in \mathbb{Z}_p \, : \, |f(a)| < |f'(a)|^2 \text{ and } |\alpha - a| < |f'(a)|\big\},$$

which is an open neighborhood of α in $\mathbb{Z}_p$. Take $a_1 \in U$ and recursively define $a_{n+1} := a_n - \frac{f(a_n)}{f'(a_n)}$ for $n \geqslant 1$. Show that for all n:

(a) $a_n \in U$,

(b) $|f'(a_n)| = |f'(a_1)|$,

(c) $|f(a_n)| \leqslant |f'(a_1)|^2 t^{2^{n-1}}$ for $t = |f(a_1)/f'(a_1)| < 1$.

Moreover, show that $\lim_{n \to \infty} a_n = \alpha$ and $|f'(\alpha)| = |f'(a_1)|$.

Solution: See the proof of Theorem 4.1 in Section 5 of the following notes by Keith Conrad:

`https://kconrad.math.uconn.edu/blurbs/gradnumthy/hensel.pdf`