D-MATH Algebraic Number Theory FS 2018
Prof. Richard Pink

Solutions 10

p-adic Numbers, Absolute Values, Completion

1. Let p be a prime number.

   (a) Show that the sequence $\frac{1}{10}, \frac{1}{10^2}, \frac{1}{10^3}, \ldots$ does not converge in $\mathbb{Q}_p$.

   (b) For any $a \in \mathbb{Z}$ coprime to p show that the sequence $(a^{p^n})_{n\geqslant 1}$ converges in $\mathbb{Q}_p$.

   (c) Determine this limit.

   Solution:

   (a) Note that $10^{-n} - 10^{-n-1} = 9 \cdot 10^{-n-1}$ and the latter does not converge to 0 because no prime factor appears with increasing positive multiplicity. Therefore the sequence $\frac{1}{10}, \frac{1}{10^2}, \frac{1}{10^3}, \ldots$ is not a Cauchy sequence in $\mathbb{Q}_p$ and thus does not converge.

   (b) Let n be a positive integer. Then $a^{p^{n+k}-p^{n+k-1}} \equiv 1 \bmod p^n$ for $k \geqslant 0$, because a is a unit $\bmod p^n$ and $|(\mathbb{Z}/p^n\mathbb{Z})^\times| = p^n - p^{n-1}$ divides $p^{n+k} - p^{n+k-1}$. Hence $a^{p^{n+k}} \equiv a^{p^{n+k-1}} \bmod p^n$ and inductively, we obtain $a^{p^{n+k}} \equiv a^{p^{n-1}} \bmod p^n$. It follows that $|a^{p^{n-1}} - a^{p^{n+k}}| \leqslant p^{-n}$ and we deduce that $\{a^{p^n}\}_{n\in\mathbb{Z}^{\geqslant 1}}$ is a Cauchy sequence. As $\mathbb{Q}_p$ is complete, the sequence converges to some element $\alpha \in \mathbb{Q}_p$.

   (c) The above congruences include the fact that $a^{p^n} \in a + p\mathbb{Z} \subset a + p\mathbb{Z}_p$ for all n. In the limit we therefore find that $\alpha \in a + p\mathbb{Z}_p$. On the other hand the Cauchy sequence also means that $(a^{p^n})^p - a^{p^n} = a^{p^{n+1}} - a^{p^n}$ goes to 0 for $n \to \infty$. In the limit we therefore find that $\alpha^p - \alpha = 0$. Thus α is either 0 or a $(p-1)^{\text{st}}$ root of unity. As this leaves at most p different possibilities for α, and we already know that $\alpha \equiv a \bmod p$ runs through p distinct residue classes, we deduce that this residue class alone determines α. In conclusion we find that α is zero if $p|a$, and otherwise it is the unique $(p-1)^{\text{st}}$ root of unity in $\mathbb{Z}_p^\times$ which is congruent to a modulo (p).

   Note: This $\alpha \in \mathbb{Z}_p$ is called the *Teichmüller representative* of the residue class $a \bmod p$.

2. Here we consider $\mathbb{Q}_p$ as an abstract field and include $\mathbb{Q}_\infty := \mathbb{R}$.

   (a) Show that $\mathbb{Q}_p$ and $\mathbb{Q}_q$ are not isomorphic for any $p \neq q$.

   (b) Prove that every automorphism of $\mathbb{Q}_p$ is trivial.

   Hint: Look at which integers are squares in the respective field.

   Solution: (a) For any prime number p, the equation $x^2 = p$ has a solution in $\mathbb{R}$, but not in $\mathbb{Q}_p$, because every element of $\mathbb{Q}_p^\times$ has the form $x = p^n u$ for some $n \in \mathbb{Z}$ and $u \in \mathbb{Z}_p^\times$ and hence $x^2 = p^2 u^2$ with $u^2 \in \mathbb{Z}_p^\times$. Thus $\mathbb{Q}_p \not\cong \mathbb{R}$.

   For any two prime numbers $p \neq q$, without loss of generality we can assume that q is odd. Choose an integer a with $pa \equiv 1 \bmod (q)$. After replacing a by $a + q$ if necessary, we can assume that in addition $p \nmid a$. Then the equation $x^2 = pa$ does not have a solution in $\mathbb{Q}_p$ for the same reason as above. But we claim that it has a solution in $\mathbb{Q}_q$. Indeed, for every $n \geqslant 1$ the residue class $pa + q^n\mathbb{Z}$ lies in the subgroup $1 + q\mathbb{Z}/q^n\mathbb{Z}$ of odd order q^{n-1}. Thus the equation $x^2 = pa$ has a solution in $1 + q\mathbb{Z}/q^n\mathbb{Z}$, namely $(pa)^k + q^n\mathbb{Z}$ for the integer $k := \frac{q^{n-1}+1}{2}$. Varying n, by §9 Prop. 4 of the lecture course it follows that $x^2 = pa$ has a solution in $\mathbb{Z}_q$, as claimed. (*Aliter:* Use Exercise 6 below.) As the same equation has a solution in $\mathbb{Q}_p$ but not in $\mathbb{Q}_q$, the fields are not isomorphic.

   (b) Let σ be any automorphism of $\mathbb{Q}_p$. In each case we exploit the fact that σ maps the set of squares in $\mathbb{Q}_p$ bijectively to itself.

   In $\mathbb{Q}_p = \mathbb{R}$ the squares are precisely the non-negative real numbers. Thus σ preserves the sign. Applying this to the difference $x - y$ of two real numbers it follows that σ preserves the order relation '$<$'. Being order preserving and the identity on the dense subset $\mathbb{Q}$ it must therefore be the identity.

   For $\mathbb{Q}_p$ with $p < \infty$ we follow Lahtonen:
   `https://math.stackexchange.com/q/449465` .

   For p odd we first prove that an element $a \in \mathbb{Q}_p$ lies in $\mathbb{Z}_p$ if and only if $1 + pa^2$ is a square in $\mathbb{Q}_p$. Indeed, if $a \in \mathbb{Z}_p$, we have $X^2 - 1 - pa^2 \equiv (X-1)(X+1) \bmod (p)$ with coprime factors $X-1$, $X+1 \in \mathbb{F}_p[X]$; so by Hensel's lemma the left hand side factors in $\mathbb{Z}_p[X]$ and hence $1 + pa^2$ is a square in $\mathbb{Q}_p$. Conversely, if $a \in \mathbb{Q}_p \smallsetminus \mathbb{Z}_p$, then $0 > \operatorname{ord}_p(pa^2) = \operatorname{ord}_p(1+pa^2)$ is odd and so $1+pa^2$ cannot be a square in $\mathbb{Q}_p$.

   For $p = 2$ we show that an element $a \in \mathbb{Q}_2$ lies in $\mathbb{Z}_2$ if and only if $1 + 8a^2$ is a square in $\mathbb{Q}_2$. Suppose first that $a \in \mathbb{Z}_2$. Then $1 + 8a^2$ is a square in $\mathbb{Q}_2$ if and only if $X^2 - 1 - 8a^2 = 0$ has a solution in $\mathbb{Q}_2$. Substituting X by $2Y + 1$ and dividing by 4, we obtain the equivalent equation $Y^2 + Y - 2a^2 = 0$. Since $Y^2 + Y - 2a^2 \equiv Y(Y+1) \bmod (2)$ with coprime factors Y, $Y + 1 \in \mathbb{F}_2[X]$, we can apply Hensel's lemma and deduce that $1 + 8a^2$ is a square in $\mathbb{Q}_2$. Conversely, suppose that $a \in \mathbb{Q}_2 \smallsetminus \mathbb{Z}_2$, that is $\operatorname{ord}_2(a) < 0$. If $\operatorname{ord}_2(a) \leqslant -2$, analogously to the case when p is odd, it follows that $\operatorname{ord}_2(1 + 8a^2)$ is odd and hence $1 + 8a^2$ is not a square in $\mathbb{Q}_2$. By contrast, if $\mathrm{ord}_2(a) = -1$, then $2a \in \mathbb{Z}_2^\times = 1 + 2\mathbb{Z}_2$ and hence $1+8a^2 \equiv 3 \bmod (4)$. In particular $\mathrm{ord}_2(1+8a^2) = 0$, so if $1+8a^2$ is a square in $\mathbb{Q}_2$, it is already the square of an element in $\mathbb{Z}_2^\times = 1+2\mathbb{Z}_2$. But for every $b \in \mathbb{Z}_2$ we have $(1+2b)^2 = 1+4b+4b^2 \equiv 1 \bmod (4)$. Thus $1+8a^2 \equiv 3 \bmod (4)$ implies that $1+8a^2$ is not a square in $\mathbb{Q}_2$.

In all cases we have thus proved that an element $a \in \mathbb{Q}_p$ lies in $\mathbb{Z}_p$ if and only if $1+qa^2$ is a square in $\mathbb{Q}_p$ for $q := p$ or 8. Since $\sigma(1+qa^2) = 1+q\sigma(a)^2$ and the set of squares is preserved by σ, it follows that $\sigma(\mathbb{Z}_p) = \mathbb{Z}_p$. As σ is the identity on $\mathbb{Q}$, for all $\alpha \in \mathbb{Q}$ and all $k \in \mathbb{Z}$ it follows that $\sigma(\alpha + p^k\mathbb{Z}_p) = \alpha + p^k\mathbb{Z}_p$.

Now consider an arbitrary $a \in \mathbb{Q}_p$. Since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, for any $k \in \mathbb{Z}$ there exists an $\alpha \in \mathbb{Q} \cap (a + p^k\mathbb{Z}_p)$. The strict triangle inequality then implies that $a + p^k\mathbb{Z}_p = \alpha + p^k\mathbb{Z}_p$. Thus it follows that $\sigma(a + p^k\mathbb{Z}_p) = a + p^k\mathbb{Z}_p$. Since $\bigcap_{k\geqslant 0}(\alpha + p^k\mathbb{Z}_p) = \{a\}$, we conclude that $\sigma(a) = a$, as desired.

*3. Show that there is a canonical isomorphism $\mathbb{Z}[[X]]/(X-p) \xrightarrow{\sim} \mathbb{Z}_p$.

Solution: See Proposition 2.6 in Section 2 of Chapter 2 of Neukirch.

4. Show that for any absolute value $|\ |$ on a field K, the maps $+, \cdot \colon K \times K \to K$ and $(\ )^{-1} \colon K \smallsetminus \{0\} \to K \smallsetminus \{0\}$ are continuous for the induced topology.

Solution: Since K is a metric space and $K \times K$ is endowed with the product metric, it suffices to check the sequential criterion for continuity in all cases. Let $(x_n, y_n)_{n\geqslant 0}$ be a sequence in $K \times K$ converging to (x, y). Then

$$|(x_n + y_n) - (x+y)| \leqslant |x_n - x| + |y_n - y| \xrightarrow{n\to\infty} 0,$$

because $x_n \to x$ and $y_n \to y$ as $n \to \infty$ and hence addition is continuous. Furthermore

$$\begin{aligned}
|x_n y_n - xy| &= |(x_n - x + x)(y_n - y + y) - xy| \\
&= |(x_n - x)(y_n - y) + (x_n - x)y + x(y_n - y)| \\
&\leqslant |(x_n - x)(y_n - y)| + |(x_n - x)y| + |x(y_n - y)| \\
&= |x_n - x||y_n - y| + |y||x_n - x| + |x||y_n - y| \xrightarrow{n\to\infty} 0
\end{aligned}$$

and it follows that multiplication is continuous. To show that the inverse is continuous, suppose that $x \neq 0$. Then $|x_n| \to |x| > 0$ as $|\ | \colon K \to \mathbb{R}$ is continuous, so $x_n \neq 0$ for all $n \gg 0$ and $|x_n|^{-1}$ remains bounded for $n \to \infty$. Thus

$$|x_n^{-1} - x^{-1}| = |x_n^{-1}x^{-1}||x - x_n| = |x_n|^{-1}|x|^{-1}|x - x_n| \xrightarrow{n\to\infty} 0,$$

as desired.

5. Let K be a complete non-archimedean field. Show that a series $\sum_{n=0}^{\infty} a_n$ with summands in K converges if and only if $\lim\limits_{n\to\infty} a_n = 0$ in K.

Solution: Suppose that a_n does not converge to 0. Then $\left|\sum_{n=0}^{m+1} a_n - \sum_{n=0}^{m} a_n\right| = |a_{m+1}| \not\to 0$ and it follows that the partial sums do not form a Cauchy sequence and hence $\sum_{n=0}^{\infty} a_n$ does not converge.

Conversely, suppose that $\lim\limits_{n\to\infty} a_n = 0$. Let m, k be positive integers. Recall that, by §10 Proposition 5, the metric induced by the norm on the non-archimedean field K is an ultrametric satisfying the strong triangle inequality. We calculate

$$\left|\sum_{n=0}^{m+k} a_n - \sum_{n=0}^{m} a_n\right| = \left|\sum_{n=m+1}^{m+k} a_n\right| \leqslant \max\{|a_{m+1}|, \dots, |a_{m+k}|\} \xrightarrow{m\to\infty} 0$$

and conclude that the partial sums form a Cauchy sequence and hence the infinite series converges as K is complete.

6. Let K be a field that is complete with respect to a p-adic absolute value. Consider $x \in K$ with $|x| < 1$ and $\alpha, \beta \in \mathbb{Z}_p$ 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) $F_\alpha(x) := \sum_{n\geqslant 0} \binom{\alpha}{n} x^n \in K$ is well-defined and satisfies $|F_\alpha(x) - 1| < 1$.
   (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 $((1+x)^\alpha)^\beta = (1+x)^{\alpha\beta}$?

   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 $\lim\limits_{k\to\infty} a_k = \alpha$. It follows that $\lim\limits_{k\to\infty} \binom{a_k}{n} = \binom{\alpha}{n}$, because $\binom{X}{n} \in \mathbb{Z}_p[X]$ is a polynomial and it follows from exercise 4 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 $|\binom{\alpha}{n}| \leqslant 1$. Since $|x| < 1$ and the norm is multiplicative, it follows that $\left|\binom{\alpha}{n}x^n\right| \leqslant |x|^n \to 0$ as $n \to \infty$. By exercise 5 the series $F_\alpha(x)$ converges. Choosing $m \gg 0$ such that $\left|\sum_{n>m} \binom{\alpha}{n} x^n\right| < 1$, we calculate

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

(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:

http://www.math.uconn.edu/~kconrad/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. $\square$

(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 $|x|$, $|y| < 1$.

*7. *(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

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

which is an open neighborhood of α in $\mathbb{Z}_p$. Let $a_1 \in U$ 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:

`http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/hensel.pdf` .