Lecture 2, October 10, 2019

Normed fields. Ostrowski's theorem. Review

Normed field. *A normed field* is a field $F = (F, 0_F, 1_F, +, \cdot, \|\cdot\|)$ with a function

$$\|\cdot\|\colon F \to [0, +\infty) \ ,$$

called a *norm*, that has the following three properties.

1. For every $x \in F$ one has $\|x\| \geq 0$, and $\|x\| = 0$ iff $x = 0_F$.
2. For every $x, y \in F$ one has $\|xy\| = \|x\| \cdot \|y\|$ (multiplicativity).
3. For every $x, y \in F$ one has $\|x + y\| \leq \|x\| + \|y\|$ (triangle inequality).

In Exercise 1 you can prove that $d(x, y) = \|x - y\|$ is a metric on F. We give three examples of normed fields, more precisely three families of norms on fields.

Trivial norm. For every field F, the function $\|\cdot\|$ with $\|0_F\| = 0$ and $\|x\| = 1$ if $x \neq 0_F$ is a norm (Exercise 2), called a *trivial norm*.

Usual absolute value. For the field of fractions $F = \mathbb{Q}$, the function $\|\cdot\|$ with $\|x\| = |x| = x$ for $x \geq 0$ and $\|x\| = |x| = -x$ for $x < 0$ is a norm. More generally, $\|x\| = |x|^c$ for any real constant $c \in (0, 1]$ is a norm (Exercise 3).

p-adic norms. For every real constant $c \in (0, 1)$, every prime $p = 2, 3, 5, 7, 11, \dots$, and the field of fractions $F = \mathbb{Q}$, the function $\|\cdot\|$, given for nonzero $x \in \mathbb{Q}$ by

$$\|x\| = c^{\mathrm{ord}_p(x)} \text{ and for zero by } \|0\| = 0 \ ,$$

is a norm. Here for nonzero $\frac{a}{b} \in \mathbb{Q}$, $\mathrm{ord}_p(\frac{a}{b}) = m \in \mathbb{Z}$ equals to the unique integer such that $\frac{a}{b} = p^m \cdot \frac{c}{d}$ with $\frac{c}{d} \in \mathbb{Q}$ and p not dividing cd (i.e. p divides neither c nor d). For zero we set $\mathrm{ord}_p(0) = \infty$.

We prove that every p-adic norm $\|\cdot\|$ is a norm. It clearly has property 1. Multiplicativity of p-adic norm follows from additivity of p-adic order: for every two fractions α and β (and every prime p) we have the equality

$$\mathrm{ord}_p(\alpha\beta) = \mathrm{ord}_p(\alpha) + \mathrm{ord}_p(\beta) \quad \text{(Exercise 5)} \ .$$

Here $\infty + m = m + \infty = \infty + \infty = \infty$ for any $m \in \mathbb{Z}$. From the previous lecture we know that for p-adic norms the triangle inequality holds in the stronger form with + replaced by maximum. We show that for every two fractions α and β (and every prime p) one has

$$\|\alpha + \beta\| \leq \max(\|\alpha\|, \|\beta\|) .$$

Due to the multiplicativity of norm we have for every $n \in \mathbb{N} = \{1, 2, \dots\}$ that $\|n\alpha + n\beta\| = \|n\| \cdot \|\alpha + \beta\|$, $\|n\alpha\| = \|n\| \cdot \|\alpha\|$ and $\|n\beta\| = \|n\| \cdot \|\beta\|$. Taking n to be a common multiple of the denominators of both fractions we may assume that $\alpha, \beta \in \mathbb{Z}$. Moreover we may assume that $\alpha\beta \neq 0$ (Exercise 6). Thus

$$\alpha = p^m a,\ \beta = p^n b,\ m, n \in \mathbb{N}_0 = \{0, 1, \dots\},\ m \leq n,\ a, b \in \mathbb{Z} ,$$

and p does not divide ab. So $m = \mathrm{ord}_p(\alpha)$, $n = \mathrm{ord}_p(\beta)$, $\alpha + \beta = p^m(a + p^{n-m}b)$, and $\mathrm{ord}_p(\alpha + \beta) \geq m$. Therefore, since the positive c is less than 1,

$$\|\alpha + \beta\| = c^{\mathrm{ord}_p(\alpha+\beta)} \leq c^m = \max(c^m, c^n) = \max(\|\alpha\|, \|\beta\|) .$$

We may have $\alpha + \beta = 0$, but this is no problem since we set $c^\infty = 0$.

Product formula. The "true" p-adic norm $\|\cdot\|_p$ has $c = \frac{1}{p}$:

$$\|x\|_p = p^{-\mathrm{ord}_p(x)} \text{ for } x \neq 0 \text{ and } \|0\|_p = 0 .$$

The reason for this choice of c is that then all p-adic norms and the absolute value $|\cdot|$, which is sometimes denoted as $|\cdot| = |\cdot|_\infty$, are bound together by the nice identity

$$\prod_{p=2,3,5,\dots \text{ or } p=\infty} \|x\|_p = 1 \text{ for every } x \in \mathbb{Q} \setminus \{0\} ,$$

called the *product formula.* You can prove it in Exercise 7.

Theorem (A. Ostrowski, 1916). *Let $\|\cdot\|$ be a norm on the field of fractions $\mathbb{Q}$. Then exactly one of the three following cases occurs.*

1. *It is a trivial norm.*

2. *There is a real $c \in (0, 1]$ such that $\|x\| = |x|^c$.*

3. *There is a real* $c \in (0,1)$ *and a prime number* p *such that* $\|x\| = c^{\mathrm{ord}_p(x)}$ *(here* $c^\infty = 0$*).*

Proof. Suppose that $\|\cdot\|$ is not of the form 1 and is not trivial. Due to multiplicativity of norm and Exercise 4 there exists an $n \in \mathbb{N}$ such that $\|n\| \neq 1$. Two cases remain to be handled.

The case when there is an $n \in \mathbb{N}$ **with** $\|n\| > 1$**.** Let n_0 be the smallest such n. It is clear by Exercise 4 that $n_0 \geq 2$. There is a unique real number $c > 0$ such that $\|n_0\| = n_0^c$. We can expand every $n \in \mathbb{N}$ in the base n_0 as

$$n = a_0 + a_1 n_0 + a_2 n_0^2 + \cdots + a_s n_0^s,\ a_i, s \in \mathbb{N}_0,\ 0 \leq a_i < n_0,\ \text{and } a_s \neq 0 \ .$$

For $n_0 = 10$ it is the usual decadic notation. So

$$\begin{aligned}
\|n\| &= \|a_0 + a_1 n_0 + a_2 n_0^2 + \cdots + a_s n_0^s\| \\
&\leq \|a_0\| + \|a_1\| \cdot \|n_0\| + \|a_2\| \cdot \|n_0\|^2 + \cdots + \|a_s\| \cdot \|n_0\|^s \\
&\leq 1 + n_0^c + n_0^{2c} + \cdots + n_0^{sc} \leq n_0^{sc} \sum_{i=0}^{\infty} \left(\frac{1}{n_0^c}\right)^i \\
&\leq n^c C \ .
\end{aligned}$$

On the second line we used multiplicativity of norm and the triangle inequality. On the third line we used the inequality $\|m\| \leq 1$ for $0 \leq m < n_0$ and the definition of the number c. On the fourth line we defined the constant $C > 0$ by the sum of the stated infinite series, which is a convergent geometric series, and we used the inequality $n_0^s \leq n$. For every $n \in \mathbb{N}_0$ we therefore have the inequality $\|n\| \leq C n^c$.

This inequality in fact holds even with $C = 1$. For every $m, n \in \mathbb{N}$ the inequality and multiplicativity of norm give

$$\|n\|^m = \|n^m\| \leq C\,(n^m)^c = C\,(n^c)^m \ .$$

Taking the m-th root of the expression we get $\|n\| \leq C^{1/m} n^c$. For $m \to \infty$, $C^{1/m} \to 1$. Indeed $\|n\| \leq n^c$ for every $n \in \mathbb{N}_0$.

In a similar way we deduce the opposite inequality $\|n\| \geq n^c$, $n \in \mathbb{N}_0$. For every $n \in \mathbb{N}$ the above base n_0 expansion shows that $n_0^{s+1} > n \geq n_0^s$. From

$\|n_0^{s+1}\| \leq \|n\| + \|n_0^{s+1} - n\|$ (the triangle inequality) we get

$$\begin{aligned}\|n\| &\geq \|n_0^{s+1}\| - \|n_0^{s+1} - n\| \geq n_0^{(s+1)c} - (n_0^{s+1} - n)^c \\ &\geq n_0^{(s+1)c} - (n_0^{s+1} - n_0^s)^c = n_0^{(s+1)c}\left(1 - \left(1 - \frac{1}{n_0}\right)^c\right) \\ &\geq n^c C' \ .\end{aligned}$$

On the first line we used the definition of the number c and the already proven upper bound $\|m\| \leq m^c$, $m \in \mathbb{N}_0$. On the second line we used the inequality $n \geq n_0^s$. On the third line we defined the constant $C' > 0$ by the stated expression in brackets (which is independent of n) and used the inequality $n_0^{s+1} > n$. As before the m-th root trick shows that for every $n \in \mathbb{N}_0$, $\|n\| \geq n^c$.

Thus for every $n \in \mathbb{N}_0$ one has $\|n\| = n^c$. By multiplicativity of norm and Exercise 4 we see that $\|x\| = |x|^c$ for every $x \in \mathbb{Q}$. Exercise 3 shows that $c \in (0, 1]$. We have deduced that the norm $\|\cdot\|$ has form 2.

The remaining case when $\|n\| \leq 1$ for every $n \in \mathbb{N}$ and there is an $n \in \mathbb{N}$ with $\|n\| < 1$. Again we denote by n_0 the least such n, and again $n_0 \geq 2$. We claim that $n_0 = p$ is a prime. If n_0 had a decomposition $n_0 = n_1 n_2$ with $n_i \in \mathbb{Z}$ and $1 < n_1, n_2 < n_0$, we would get the contradiction

$$1 > \|n_0\| = \|n_1 n_2\| = \|n_1\| \cdot \|n_2\| = 1 \cdot 1 = 1$$

(we used multiplicativity of norm and that $\|m\| = 1$ for every $m \in \mathbb{N}$ with $1 \leq m < n_0$). We show that every other prime $q \neq p$ has norm $\|q\| = 1$. For contrary let $q \neq p$ be another prime with norm $\|q\| < 1$. We take large enough $m \in \mathbb{N}$ such that $\|p\|^m, \|q\|^m < \frac{1}{2}$. By a well known result in elementary number theory in Exercise 8 there are integers a and b with $aq^m + bp^m = 1$. Taking norm of this equality we get the contradiction

$$1 = \|1\| = \|aq^m + bp^m\| \leq \|a\| \cdot \|q\|^m + \|b\| \cdot \|p\|^m < 1 \cdot \frac{1}{2} + 1 \cdot \frac{1}{2} = 1 \ .$$

Here we used the triangle inequality, multiplicativity of norm, and the fact that now $\|a\| \leq 1$ for every $a \in \mathbb{Z}$.

Hence $\|q\| = 1$ for every prime q different from p. From this we get with the help of multiplicativity of norm, Exercise 4, and the prime factorization of a nonzero fraction x the expression

$$\|x\| = \left\| \prod_{q=2,\,3,\,5,\,\ldots} q^{\mathrm{ord}_q(x)} \right\| = \prod_{q=2,\,3,\,5,\,\ldots} \|q\|^{\mathrm{ord}_q(x)} = \|p\|^{\mathrm{ord}_p(x)} = c^{\mathrm{ord}_p(x)} \ ,$$

where $c = \|p\| \in (0,1)$; $\|0\| = c^{\mathrm{ord}_p(0)} = c^\infty = 0$ too. We have deduced that the norm $\|\cdot\|$ has form 3. $\Box$

I took the previous proof from the book

N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Springer-Verlag, New York, 1984,

which contains interesting material on the p-adic norm $\|\cdot\|_p$ and on the related p-adic analysis. Unfortunately we have to part with this topic, look at least at Exercise 9.

Review. I review some results on metric spaces you learned in "Matematická analýza II". For a metric space (M,d), a point $a \in M$, and a real number $r > 0$, the set of points

$$B(a,\, r) = \{x \in M \mid d(a,\, x) < r\}$$

is called an *(open) ball (with center a and radius r).* A set $X \subset M$ is *open* if

$$\forall\, a \in X\; \exists\, r > 0: \;B(a,r) \subset X\;.$$

A set $X \subset M$ is *closed* if the set $M \setminus X$ is open. For a sequence $(a_n) \subset M$ and a point $a \in M$ we write

$$\lim a_n = a \text{ if } \lim d(a_n,\, a) = 0$$

and we call sequences, for which such a exists, *convergent.* Note that the last limit is just the limit of a real sequence (with respect to the usual metric $|x - y|$ on the real axis). Closed sets are characterized by closedness to limits (Exercise 11). The sets $\emptyset$ and M are both open and closed, the family of open sets is closed to finite intersections and arbitrary unions, and for closed sets this holds with the operations of intersection and union interchanged. Finally, we call $X \subset M$ a *compact* set if

$$\forall\,(a_n) \subset X\; \exists\,(a_{k_n}) \subset (a_n): \;\lim a_{k_n} = a \in X\;.$$

Thus in a compact set X every sequence of points has a convergent subsequence with limit in X. For example, $[0,1) \subset \mathbb{R}$ is *not* a compact subset of the Euclidean space $(\mathbb{R}, d_2)$ because the sequence $(1 - \frac{1}{n}) \subset [0,1)$ has no convergent subsequence with limit in $[0,1)$ (Exercise 12).

Exercises

1. Prove that for a field norm $\| \cdot \|$ the function $d(x, y) = \|x - y\|$ is a metric.

2. Prove that the trivial norm is a norm.

3. Prove that $\|x\| = |x|^c$, $x \in \mathbb{Q}$ and $c > 0$, is a norm if and only if $c \leq 1$.

4. In every normed field, $\|0_F\| = 0$, $\|1_F\| = \| - 1_F\| = 1$, $\|x\| = \| - x\|$, and $\|1_F/x\| = 1/\|x\|$ (for $x \neq 0_F$).

5. Prove that the function $\mathrm{ord}_p(\cdot)$ is additive.

6. Prove that if one of the elements is zero then the strong triangle inequality holds. In our proof of the strong triangle inequality for p-adic norms, was it really necessary to reduce it first to $\alpha, \beta \in \mathbb{Z}$ and then to nonzero $\alpha\beta$?

7. Prove the product formula. Is it really an infinite product?

8. Recall the proof of the fact that for every two coprime integers m, n there exist numbers $a, b \in \mathbb{Z}$ such that $am + bn = 1$.

9. Consider the metric space $(\mathbb{Q}, \|x - y\|_p)$ with a p-adic metric. Prove that in it the infinite series

   $$\sum_{n=1}^{\infty} a_n, \;\; a_n \in \mathbb{Q} \;,$$

   converges if and only if in it $\lim a_n = 0$.

10. Prove that every ball is an open set.

11. Let (M, d) be a metric space and $X \subset M$. Prove that the set X is closed iff every sequence $(a_n) \subset X$ satisfies: if (a_n) has the limit $a \in M$ then $a \in X$.

12. Why $(1 - \frac{1}{n}) \subset [0, 1)$ has no convergent subsequence with limit in $[0, 1)$?