p-adic numbers, LTCC 2010

Manuel Breuning
King's College London

Solutions to selected exercises

Exercise 1.13. The *product formula* states that
$$|x|_\infty \cdot \prod_p |x|_p = 1$$
for all $x \in \mathbb{Q}^\times$ (where the product runs over all prime numbers p). Prove this formula.

Solution. Let $x \in \mathbb{Q}^\times$ and consider the prime factorisation $x = \pm p_1^{e_1} \cdots p_n^{e_n}$ where $p_1, \dots, p_n$ are distinct prime numbers and $e_1, \dots, e_n \in \mathbb{Z}$. For a prime number p we then have
$$|x|_p = \begin{cases} 1 & \text{if } p \notin \{p_1, p_2, \dots, p_n\} \\ p_i^{-e_i} & \text{if } p = p_i \text{ for } i = 1, \dots, n. \end{cases}$$
Furthermore $|x|_\infty = p_1^{e_1} \cdots p_n^{e_n}$. Hence
$$|x|_\infty \cdot \prod_p |x|_p = p_1^{e_1} \cdots p_n^{e_n} \cdot \prod_{i=1}^n p_i^{-e_i} = 1$$
as required.

Exercise 1.16. Let $(K, |\ \ |)$ be a valued field with completion $(\hat{K}, \|\ \ \|)$. Show that $|\ \ |$ is non-archimedean if and only if $\|\ \ \|$ is non-archimedean.

Solution. The statement is obvious if one uses the characterisation of non-archimedean absolute values stated in Remark 1.3: since $\|\ \ \|$ extends $|\ \ |$ we have
$$\begin{aligned} |\ \ | \text{ is non-archimedean} &\iff |n| \le 1 \text{ for all } n \in \mathbb{N} \\ &\iff \|n\| \le 1 \text{ for all } n \in \mathbb{N} \\ &\iff \|\ \ \| \text{ is non-archimedean.} \end{aligned}$$
The following is a proof which is independent of this characterisation.

First assume that $\|\ \ \|$ is non-archimedean. Let $x, y \in K$. Using that $\|\ \ \|$ extends $|\ \ |$ we then obtain
$$|x + y| = \|x + y\| \le \max\{\|x\|, \|y\|\} = \max\{|x|, |y|\}$$
which shows that $|\ \ |$ is non-archimedean.

Now assume that $|\ \ |$ is non-archimedean. Let $x, y \in \hat{K}$. Let $\varepsilon > 0$. Since K is dense in $\hat{K}$ there exist $u, v \in K$ such that $\|x - u\| < \varepsilon$ and $\|y - v\| < \varepsilon$. Hence it follows that (using that $\|\ \ \|$ extends $|\ \ |$ and that $\|\ \ \|$ is an absolute value)
$$|u| = \|u\| = \|u - x + x\| \le \|u - x\| + \|x\| < \varepsilon + \|x\|.$$
Similarly $|v| < \varepsilon + \|y\|$. Therefore
$$\|u + v\| = |u + v| \le \max\{|u|, |v|\} < \max\{\varepsilon + \|x\|, \varepsilon + \|y\|\} = \varepsilon + \max\{\|x\|, \|y\|\}.$$
Using this we obtain
$$\|x+y\| = \|x-u+y-v+u+v\| \le \|x-u\|+\|y-v\|+\|u+v\| < \varepsilon+\varepsilon+\varepsilon+\max\{\|x\|, \|y\|\}.$$

Hence $\|x+y\| < 3\varepsilon + \max\{\|x\|, \|y\|\}$ for every $\varepsilon > 0$, which implies that $\|x+y\| \leq \max\{\|x\|, \|y\|\}$, i.e. $\| \ \|$ is non-archimedean.

Exercise 2.10. Let K be a non-archimedean valued field and $\hat{K}$ its completion. Let R and M be the ring of integers and maximal ideal of K, and let $\hat{R}$ and $\hat{M}$ be the ring of integers and maximal ideal of $\hat{K}$. Show that $R \subseteq \hat{R}$ and $M \subseteq \hat{M}$, and that the induced map of residue class fields $R/M \to \hat{R}/\hat{M}$ is an isomorphism.

Solution. We write $| \ |$ for the absolute value on K and on $\hat{K}$; this will not cause any confusion because by definition of the completion the absolute value on $\hat{K}$ extends the absolute value on K.

From the definitions $R = \{x \in K : |x| \leq 1\}$ and $\hat{R} = \{x \in \hat{K} : |x| \leq 1\}$ it follows immediately that $R \subseteq \hat{R}$. Also $M = \{x \in K : |x| < 1\}$ and $\hat{M} = \{x \in \hat{K} : |x| < 1\}$ immediately implies $M \subseteq \hat{M}$. Therefore we obtain an induced homomorphism of residue class fields $f : R/M \to \hat{R}/\hat{M}$, $f(u+M) = u + \hat{M}$. The homomorphism f is injective because a ring homomorphism between fields is always injective. It remains to be shown that f is surjective. Let $x \in \hat{R}$. Since K is dense in $\hat{K}$, there exists $u \in K$ such that $|u - x| < 1$. It follows that

$$|u| = |u - x + x| \leq \max\{|u - x|, |x|\} \leq 1,$$

so $u \in R$. Now $u - x \in \hat{M}$, hence

$$f(u + M) = u + \hat{M} = (x + u - x) + \hat{M} = x + \hat{M}$$

which completes the proof of the surjectivity of f.

Exercise 2.23. Find $a_0, a_1, a_2, \dots \in \{0, 1, \dots, p-1\}$ such that $-1 = a_0 + a_1 p + a_2 p^2 + \dots$ in $\mathbb{Z}_p$.

Solution. In $\mathbb{Q}_p$ we have

$$1 + p + p^2 + \cdots + p^{k-1} = \frac{1 - p^k}{1 - p}.$$

Since $p^k \to 0$ as $k \to \infty$, we obtain

$$1 + p + p^2 + \cdots = \sum_{i=0}^{\infty} p^i = \frac{1}{1-p}.$$

Thus

$$-1 = (p-1) \cdot \frac{1}{1-p} = (p-1) + (p-1)p + (p-1)p^2 + \dots,$$

so $a_0 = p-1, a_1 = p-1, a_2 = p-1, \dots$.