Algebraic Number Theory (88-798)
5777 Semester B
Question Sheet 5
Due 26/6/2017, ב' בתמוז תשע"ז

(1) Let K be a field complete with respect to an Archimedean absolute value $|\cdot|$. The aim of this exercise is to prove Ostrowski's theorem that there exists either an isomorphism $\sigma : K \to \mathbb{R}$ or an isomorphism $\sigma : K \to \mathbb{C}$ such that there exists $s \in (0, 1]$ such that for all $a \in K$ we have $|a| = |\sigma(a)|_\infty$. Here $|\cdot|_\infty$ is the usual absolute value on $\mathbb{R}$ or $\mathbb{C}$.
  (a) Prove that $\operatorname{char} K = 0$ and hence that $\mathbb{Q}$ embeds in K.
  (b) Replacing the absolute value by an equivalent one if necessary, show that $\mathbb{R}$ embeds in K and that $|\cdot|_{|\mathbb{R}} = |\cdot|_\infty$.
  (c) Let $a \in K$ be arbitrary and consider the function $f_a : \mathbb{C} \to \mathbb{R}$ given by $f(z) = |a^2 - (z + \bar{z})a + z\bar{z}|$. Show that $m = \min\{f_a(z) : z \in \mathbb{C}\}$ exists and that to obtain Ostrowski's theorem it is enough to prove that $m = 0$.
  (d) Prove that there exists $z_0 \in S = \{z \in \mathbb{C} : f_a(z) = m\}$ such that $|z_0|_\infty$ is maximal.
  (e) Assume by way of contradiction that $m > 0$ and let $0 < \varepsilon < m$. Let $z_1 \in \mathbb{C}$ be a root of the polynomial $g(x) = x^2 - (z_0 + \overline{z_0})x + z_0\overline{z_0} + \varepsilon$. Prove that $f_a(z_1) > m$.
  (f) For any $n \in \mathbb{N}$ consider the polynomial $G_n(x) = (g(x) - \varepsilon)^n + (-1)^{n+1}\varepsilon^n$. Show that $G_n(z_1) = 0$ and that $|G_n(a)|^2 \geq f_a(z_1)m^{2n-1}$.
  (g) Show that $|G_n(a)| \leq m^n + \varepsilon^n$. Conclude that $f_a(z_1) \leq m$. Now finish the proof.

(2) Let K be a field with a non-Archimedean absolute value $|\cdot|$. Let $a_n \in K$ for all $n \in \mathbb{N}$. Prove that the series $\sum_{n=1}^{\infty} a_n$ converges (i.e. its sequence of partial sums is a Cauchy sequence) if and only if $|a_n| \to 0$. Note that one direction of this statement fails in the Archimedean setting and is one of the most common mistakes made by students in Infi 1.

(3) Let K be a field with absolute value $|\cdot|$. Prove that this absolute value can be extended to the completion $\hat{K}$ by defining $|x| = \lim_{n\to\infty} |a_n|$, where $(a_n) \in R_K$ is a sequence representing $x \in \hat{K}$.

(4) Show that K is dense in the completion $\hat{K}$ and that $\hat{K}$ is indeed complete, i.e. for every Cauchy sequence (a_n) of elements of $\hat{K}$ there exists $\ell \in \hat{K}$ which is the limit of the sequence in the usual sense: for every $\varepsilon > 0$ there exists N such that $|a_n - \ell| < \varepsilon$ for all $n > N$.

(5) Let p be a prime number and let $\mathbb{Z}_p'$ be the ring of formal series $\sum_{n=0}^{\infty} a_n p^n$, where $a_n \in \{0, 1, \ldots, p-1\}$; this is an example you saw in the ring theory course. Given $\sum_{n=0}^{\infty} a_n p^n \in \mathbb{Z}_p'$, prove that the sequence $b_k = a_0 + a_1 p + \cdots + a_k p^k$ is a Cauchy sequence of rational numbers with respect to the absolute value $|\cdot|_p$. Hence the equivalence class of $\{b_k\}$ is an element of $\mathbb{Q}_p$. Prove that it actually lies in $\mathbb{Z}_p$ and that this construction gives an isomorphism of rings $\mathbb{Z}_p' \simeq \mathbb{Z}_p$.

(6) Let $n > 2$. Prove that the cyclotomic field $\mathbb{Q}(\zeta_n)$ contains at least one quadratic subfield, i.e. that there exists a field $K \subset \mathbb{Q}(\zeta_n)$ such that $[K : \mathbb{Q}] = 2$.

(7) Let G be a finite abelian group. Show that there exists a Galois extension $L/\mathbb{Q}$ such that $\mathrm{Gal}(L/\mathbb{Q}) \simeq G$.