Algebraic Number Theory (88-798)
5777 Semester B
Question Sheet 6
Due 12/7/2017, י״ח בתמוז תשע״ז

(1) Let K be a field and let $|\cdot|_1,\dots,|\cdot|_n$ be pairwise non-equivalent absolute values on K. Let $a_1,\dots,a_n \in K$ and let $\varepsilon > 0$. The aim of this exercise is to prove the Strong Approximation Theorem, which asserts that there exists $x \in K$ such that $|x - a_i|_i < \varepsilon$ for all $1 \le i \le n$.

(a) Prove that there exists $z \in K$ such that $|z|_1 > 1$ while $|z|_i < 1$ for all $2 \le i \le n$.
Hint: Induction on n, starting from $n = 2$. Suppose, by induction, that we have $z \in K$ that satisfies the required conditions for all the absolute values except $|\cdot|_n$. If $|z|_n = 1$, consider the element $z^m y$ for a sufficiently large power m and a suitable element $y \in K$. If $|z|_n > 1$, consider the element $z^m y/(1+z^m)$ for a sufficiently large power m and a suitable $y \in K$.

(b) Define $M = \max\{|a_i|_j, 1 \le i,j \le n\}$. For each i show that there is an element z_i satisfying $|z_i - 1|_i < \varepsilon/Mn$ and $|z_i|_j < \varepsilon/Mn$ for all $j \neq i$.

(c) Show that $x = a_1 z_1 + \cdots + a_n z_n$ works.

(2) Let K be a field with absolute value $|\cdot|$. Let V be an n-dimensional K-vector space. A norm on V is a function $|\cdot| : V \to \mathbb{R}_{\ge 0}$ such that for all $v, w \in V$ and $a \in K$ we have

(a) $|v| = 0$ if and only if $v = 0$.

(b) $|v + w| \le |v| + |w|$.

(c) $|av| = |a||v|$.

Let $\{v_1,\dots,v_n\}$ be a basis of V, and define

$$||a_1 v_1 + \cdots + a_n v_n|| = \max\{|a_1|,\dots,|a_n|\}.$$

Prove that $||\cdot||$ is a norm on V.

(3) Now suppose that K is complete with respect to its absolute value. Let $|\cdot|$ be an arbitrary norm on V. Choose a basis $\{v_1,\dots,v_n\}$ of V and define a norm $||\cdot||$ as above. The aim of this exercise and the next is to show that $|\cdot|$ and $||\cdot||$ are equivalent. Show that it suffices to find constants $\rho, \rho' > 0$ such that $\rho||x|| \le |x| \le \rho'||x||$ for all $x \in V$.

Show also that $\rho' = |v_1| + \cdots + |v_n|$ works.

(4) To prove the existence of ρ, use induction on n. First prove the claim for $n = 1$. Now, for each $i = 1, 2, \dots, n$, let $V_i \subset V$ be the span of $\{v_1,\dots,v_{i-1},v_{i+1},\dots,v_n\}$. By induction, prove that each V_i is complete with respect to the norm $|\cdot|$. Deduce that $\bigcup_{i=1}^n (V_i + v_i)$ is closed in the $|\cdot|$-topology. Prove that there exists $\rho > 0$ such that $\rho \le |v_i + w_i|$ for all i and all $w_i \in V_i$.

Now, let $x = a_1 v_1 + \cdots + a_n v_n \in V - \{0\}$ and suppose $||x|| = |a_k|$. Prove that $\rho \le |a_k^{-1} x|$ and conclude the desired claim.

(5) Let K be a field, complete with respect to the non-Archimedean absolute value $|\cdot|$. Let L/K be an algebraic extension. We proved in class that $|\cdot|$ extends uniquely to an absolute value of L. Prove that L is complete with respect to this absolute value if and only if $[L : K] < \infty$.

(6) Let K be a number field, let p be a prime number, and suppose that $p\mathcal{O}_K = P_1^{e_1} \cdots P_r^{e_r}$. Let $\mathcal{O}_{P_i}$ be the valuation ring of K_{P_i}, the completion of K with respect to the P_i-valuation. Let M_i be the maximal ideal of $\mathcal{O}_{P_i}$. Show that $p\mathcal{O}_{P_i} = M_i^{e_i}$.

(7) Let p be an odd prime and let $u \in \mathbb{Z}_p^*$ be an element that is not the square of any element of $\mathbb{Z}_p$. Let $K/\mathbb{Q}_p$ be a quadratic extension. Show that K is equal to one of $\mathbb{Q}_p(\sqrt{u})$, $\mathbb{Q}_p(\sqrt{p})$, or $\mathbb{Q}_p(\sqrt{up})$.

Note: This is another example of the behavior of $\mathbb{Q}_p$ being very different from that of $\mathbb{Q}$. Recall that the fields $\mathbb{Q}(\sqrt{d})$ are all non-isomorphic for distinct square-free integers d, so $\mathbb{Q}$ has infinitely many non-isomorphic quadratic extensions.

(8) Let p be an odd prime. For every $\lambda \in \mathbb{F}_p$, let $[\lambda] \in \mathbb{Z}_p$ be the $(p-1)$-th root of unity whose image in $\mathbb{F}_p$ is λ. Recall that we proved in class that $[\lambda]$ exists and is unique.

(a) Recall the isomorphism between $\mathbb{Z}_p$ and the ring of formal power series $\sum a_n p^n$. Which power series corresponds to $[\lambda]$?

(b) Prove that $[\lambda_0] + p[\lambda_1] + 1 \equiv [\lambda_0 + 1] + p[\lambda_1 + \frac{\lambda_0^p + 1 - (\lambda_0+1)^p}{p}] \mod p^2$, for all $\lambda_0, \lambda_1 \in \mathbb{F}_p$.

(9) If K is a valued field, let k_K be the residue field $\mathcal{O}/M$, where $\mathcal{O}$ is the valuation ring of K and M is its maximal ideal. In particular, $k_{\mathbb{Q}_p} = \mathbb{F}_p$. A finite extension $F/\mathbb{Q}_p$ is called unramified if $[k_F : \mathbb{F}_p] = [F : \mathbb{Q}_p]$. Prove that any unramified extension $F/\mathbb{Q}_p$ of degree n is isomorphic to $\mathbb{Q}_p(\zeta)$, where ζ is a primitive $(p^n - 1)$-th root of unity.