Algebraic Number Theory (88-798)
5779 Semester A
Question Sheet 5

(1) Let K be a field complete with respect to an Archimedean valuation $|\cdot|$. 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 valuation on $\mathbb{R}$ or $\mathbb{C}$.
   (a) Prove that $\operatorname{char} K = 0$ and hence that $\mathbb{Q}$ embeds in K.
   (b) Replacing the valuation 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) Show that K is dense in the completion $\hat{K}$ (with its metric topology) 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 $n > N$.

(3) 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 $a_n \in \{0, 1, \ldots, p-1\}$. 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 valuation $|\cdot|_p$. 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 $\mathbb{Z}'_p \simeq \mathbb{Z}_p$.

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

(5) 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-adic valuation. Let $\mathfrak{m}_i$ be the maximal ideal of $\mathcal{O}_{P_i}$. Show that $p\mathcal{O}_{P_i} = \mathfrak{m}_i^{e_i}$.

(6) 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 $\mathbb{Z}_p$. Fix an algebraic closure of $\mathbb{Q}_p$, and let $K/\mathbb{Q}_p$ be a quadratic extension contained in this algebraic closure. 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.

(7) 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, from an earlier exercise, 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 $\lambda_0, \lambda_1 \in \mathbb{F}_p$.

(8) If K is a valued field, let k_K be the residue field $\mathcal{O}/\mathfrak{m}$, where $\mathcal{O}$ is the valuation ring of K and $\mathfrak{m}$ 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.

(9) Prove the following statement, which is called Krasner's Lemma and turns out to be very useful. Let K be a non-Archimedean Henselian valued field, and let $\overline{K}$ be an algebraic closure. Let $\alpha = \alpha_1 \in \overline{K}$ be separable over K, and let $\alpha_1, \dots, \alpha_r$ be all its conjugates over K. Suppose that $\beta \in \overline{K}$ satisfies $|\alpha - \beta| < |\alpha - \alpha_i|$ for all $2 \le i \le r$. Then $K(\alpha) \subseteq K(\beta)$.

Hint: Suppose the claim is false. Show that there exists an embedding $\sigma : K(\alpha, \beta) \to \overline{K}$ that fixes β but not α.

(10) Let p be a prime number, and let ζ_p be a primitive p-th root of unity. Show that $\mathbb{Q}_p(\zeta_p)$ contains a primitive $(p-1)$-st root of $-p$.

(11) 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 $[K : \mathbb{Q}] = 2$.

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

(13) The last question is a whirlwind introduction to Witt vectors. It may be useful to consult the seventh question on this question sheet for inspiration.

(a) Let p be a fixed prime and let $X_0, X_1, X_2, \dots$ be variables. For every $n \ge 0$, set $W_n = X_0^{p^n} + pX_1^{p^{n-1}} + \cdots + p^n X_n$. Show that there exist polynomials $S_0, S_1, \dots, P_0, P_1, \dots \in \mathbb{Z}[X_0, X_1, \dots, Y_0, Y_1, \dots]$ such that

$$\begin{aligned} W_n(S_0, S_1, S_2, \dots) &= W_n(X_0, X_1, \dots) + W_n(Y_0, Y_1, \dots) \\ W_n(P_0, P_1, P_2, \dots) &= W_n(X_0, X_1, \dots) \cdot W_n(Y_0, Y_1, \dots). \end{aligned}$$

(b) Let A be any commutative ring. Let $W(A)$ be the set $A^{\mathbb{N}} = \{a = (a_0, a_1, a_2, \dots) | a_i \in A\}$ with the operations

$$\begin{aligned} a + b &= (S_0(a,b), S_1(a,b), \dots) \\ ab &= (P_0(a,b), P_1(a,b), \dots). \end{aligned}$$

Prove that this is a commutative ring. It is called the ring of Witt vectors of A.

(c) Assume that the commutative ring A is p-torsion, so that $p\alpha = 0$ for every $\alpha \in A$. For every $a = (a_0, a_1, \dots) \in W(A)$ consider

$$a^{(n)} = W_n(a) = a_0^{p^n} + pa_1^{p^{n-1}} + \cdots + p^n a_n.$$

Consider also the maps $V, F : W(A) \to W(A)$ given by

$$\begin{aligned} V(a) &= (0, a_0, a_1, \dots) \\ F(a) &= (a_0^p, a_1^p, \dots). \end{aligned}$$

These maps are called the transfer map (transfer is Verschiebung in German, hence the standard notation V) and the Frobenius map, respectively. Prove the following identities:

$$\begin{aligned} (V(a))^{(n)} &= pa^{(n-1)} \\ a^{(n)} &= (F(a))^{(n)} + p^n a_n. \end{aligned}$$

(d) Restricting even further, let k be a field of characteristic p. Then V is an endomorphism of the underlying abelian group of $W(k)$, whereas F is a ring endomorphism. Moreover, $F(V(a)) = V(F(a)) = pa$ for any $a \in W(k)$.

(e) Let k be a perfect field of characteristic p; recall this means that the map $x \mapsto x^p$ is an automorphism. Then $W(k)$ is a complete discrete valuation ring with residue field k.

(f) Finally, show that $W(\mathbb{F}_p) \simeq \mathbb{Z}_p$.