MA 472

Course Title: Local Fields

Model Solution No: 1

a) A **valuation** on k is a real valued function

$$k \to \mathbb{R}, \qquad b \mapsto |b|,$$

satisfying the following three conditions

- $|b| \geq 0$, and $|b| = 0$ iff $b = 0$;
- $|bc| = |b||c|$;
- there is some $C \geq 0$ such that $|1 + b| \leq C$ for all $b \in k$ satisfying $|b| \leq 1$.

The **trivial** valuation on k is given by $|b| = 1$ for all $b \neq 0$.

A valuation is said to be **non-archimedean** if we can take $C = 1$ in the above definition, otherwise it is said to be **archimedean**.

b) Suppose $|1 + b| \leq 2$ for all $b \in k$ satisfying $|b| \leq 1$. Homogenizing we get

$$|a_1 + a_2| \leq 2 \max\{|a_1|, |a_2|\}.$$

By induction
$$|a_1 + a_2 + \cdots + a_{2^n}| \leq 2^n \max|a_j|.$$

Given $a_1, \ldots, a_N$, choose n so that $2^{n-1} < N \leq 2^n$. Let $a_{N+1} = \cdots = a_{2^n} = 0$. Then
$$|a_1 + a_2 + \cdots + a_N| \leq 2^n \max|a_j| \leq 2N \max|a_j|.$$

In particular, applying this with all $a_j = 1$ we get $|N| \leq 2N$.

Now let $b, c \in k$ and n a positive integer. Then

$$|b + c|^n = \Big| \sum_{r=0}^{n} \binom{n}{r} b^r c^{n-r} \Big|.$$
$$\leq 2(n+1) \max_r \Big| \binom{n}{r} \Big| |b|^r |c|^{n-r}$$
$$\leq 4(n+1) \max_r \binom{n}{r} |b|^r |c|^{n-r}$$
$$\leq 4(n+1)(|b| + |c|)^n.$$

Taking n-th roots and letting $n \to \infty$ we get the triangle inequality.

c) Consider
$$a_n = b_1 \frac{c^{-n}}{1+c^{-n}} + b_2 \frac{c^n}{1+c^n}.$$

Note that as $n \to \infty$, $\dfrac{c^{-n}}{1+c^{-n}}$ converges to 1 with respect to $|\ |_1$ and converges to 0 with respect to $|\ |_2$. The reverse is true for $\dfrac{c^n}{1+c^n}$. Hence $a_n \to b_i$ with respect to $|\ |_i$. We can take $a = a_n$ for n large enough.

MA 472

Course Title: Local Fields

Model Solution No: 2

a) We are given that k is a complete non-archimedean field. Complete means that every Cauchy sequence converges. Non-archimedean means

$$|a + b| \leq \max\{|a|, |b|\}.$$

Given $\sum_{n=0}^{\infty} a_n$, let $s_m = \sum_{n=0}^{m} a_n$ be the sequence of partial sums. The series converges if and only if the sequence of partial sums converges, and the latter happens if and only if the sequence of partial sums is Cauchy.

Suppose that the sequence of partial sums is Cauchy. Then

$$a_n = s_n - s_{n-1} \to 0 \qquad \text{as } n \to \infty.$$

Conversly suppose that $a_n \to 0$ as $n \to \infty$. We want to show that s_n is Cauchy. Let $\epsilon > 0$ be given. Then there is N such that for all $n \geq N$, $|a_n| < \epsilon$. Hence, if $m \geq n \geq N$ then

$$|s_m - s_n| \leq |a_{n+1} + a_{n+2} + \cdots + a_m|$$
$$\leq \max\{|a_{n+1}|, \ldots, |a_m|\} < \epsilon.$$

This shows that s_n is Cauchy.

b) Let $a_n = (15/14)^n$. Then $\sum a_n$ converges in $\mathbb{Q}_p$ if and only if $|a_n|_p \to 0$ as $n \to \infty$. This happens if and only if $|15/14|_p < 1$. i.e. if and only if $p = 3$ or $p = 5$.

In $\mathbb{Q}_3$ and $\mathbb{Q}_5$,

$$\sum_{n=0}^{\infty} \left(\frac{15}{14}\right)^n = \frac{1}{1 - \frac{15}{14}} = -14.$$

c) For positive integer n write $v_p(n)$ for the exponent of p in the prime-power factorization of n. Thus

$$|n|_p = p^{-v_p(n)}.$$

We want to estimate $v_p(n!)$. There are precisely $\lfloor \frac{n}{p} \rfloor$ integers $1 \leq m \leq n$ divisible by p. Of these $\lfloor \frac{n}{p^2} \rfloor$ are divisible by p^2 and so on. Thus

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots$$
$$\leq \frac{n}{p} + \frac{n}{p^2} + \frac{n}{p^3} + \cdots$$
$$= \frac{n}{p - 1}.$$

Hence
$$\left|\frac{p^n}{n!}\right|_p \leq p^{-n+n/(p-1)}.$$

This goes to 0 as $n \to \infty$ provided $p > 2$. Hence $\sum p^n/n!$ converges in $\mathbb{Q}_p$ if p is odd.

Course Title: Local Fields

Model Solution No: 3

a) Suppose $f(a) = f(b) = 0$ and

$$|a - a_0| < 1, \qquad |b - a_0| < 1.$$

By the ultrametric inequality,

$$|b - a| \leq \max\{|b - a_0|, |a - a_0|\} < 1.$$

Now by Taylor,

$$f(b) = f(a) + f'(a)(b - a) + \frac{f''(a)}{2}(b - a)^2 + \cdots.$$

Note that $f^{(n)}(X)/n!$ is in $\mathcal{O}[X]$. Moreover $f(b) = f(a) = 0$. Thus, by the ultrametric inequality again

$$|f'(a)||b - a| \leq |b - a|^2.$$

Now

$$f'(a) = f'(a_0) + f''(a_0)(a - a_0) + \cdots,$$

showing that

$$|f'(a)| = |f'(a_0)| = 1.$$

This proves

$$|b - a| \leq |b - a|^2,$$

which implies $b = a$ as required.

b) Take $a_0 = 1$ and $f(X) = X^n - 7$. Then

$$|f(1)|_3 < 1, \qquad |f'(1)|_3 = |n|_3 = 1$$

since $3 \nmid n$. By Hensel, the polynomial f has a root in $\mathbb{Z}_3$.

c) Let $f(X) = X^4 - X^2 + X + 1$. Then

$$f(0) \equiv 1, \quad f(1) \equiv 2, \quad f(2) \equiv 0,$$
$$f(3) \equiv 1, \quad f(4) \equiv 0 \pmod{5}.$$

Any root x of $f(X)$ in $\mathbb{Z}_5$ is equivalent to 2 or 4 modulo 5. We will show by Hensel that there is precisely one root congruent to each of 2, 4 modulo 5. For this all we need to note is

$$f'(2) \equiv 4, \qquad f'(4) \equiv 4 \pmod{5}.$$

(Student can save time by noting that -1 is a root!)

MA 472

Course Title: Local Fields

Model Solution No: 4

a) Let π be a prime element for k. Suppose β is the root of the Eisenstein polynomial

$$f_0 + f_1\beta + \cdots + f_n\beta^n$$

where $|f_n| = 1$, $|f_0| = |\pi|$ and

$$|f_j| \leq |\pi|, \qquad \text{for } j = 2, \ldots, n - 1.$$

By Eisenstein's criterion the polynomial is irreducible, so $k(\beta)/k$ has degree n. Now

$$|\beta|^n = |f_n\beta^n| \leq |f_0 + f_1\beta + \cdots + f_{n-1}\beta^{n-1}| \leq |\pi|.$$

Hence $|\beta| < 1$. Thus $|f_j\beta^j| < |\pi|$ for $j = 2, \ldots, n - 1$. Hence $|\beta|^n = |\pi|$ showing that $k(\beta)/k$ is totally ramfied, and the β is a prime element.

b) ζ is a root of $(X^p - 1)/(X - 1)$. Thus $\lambda = \zeta - 1$ is a root of

$$\frac{(X + 1)^p - 1}{X} = X^{p-1} + f_{p-2}X^{p-2} + \cdots + f_0,$$

where $f_0 = p$, and

$$f_1 = \binom{p}{2}, \ldots, f_{p-2} = \binom{p}{p-1}$$

are all divisible by p. Thus λ is the root of an Eisenstein polynomial. Hence $\mathbb{Q}_p(\theta)$ is completely ramified and λ is a prime element.

c) Let $f(X) = X^3 - X - 1$. Note that $f(0) = f(1) = f(-1) = -1$, so f does not have any roots in $\mathbb{F}_3$ or $\mathbb{Z}_3$. Hence the extension $\mathbb{Q}_3(\theta)/\mathbb{Q}_3$ has degree 3. Moreover, if k_v is the residue field, then $k_v/\mathbb{F}_3$ also has degree 3. But

$$[\mathbb{Q}_3(\theta) : \mathbb{Q}_3] = e \cdot [k_v : \mathbb{F}_3].$$

where e is the ramification index. Thus $e = 1$ and so the extension is unramified.

MA 472

Course Title: Local Fields

Model Solution No: 5

a) **Strassman's Theorem:** Let k be a complete non-archimedean field and let

$$f(X) = \sum_0^\infty f_n X^n.$$

Suppose that $f_n \to 0$ as $n \to \infty$, but not all f_n are zero. Then there is a finite number of $b \in \mathcal{O}$ such that $f(b) = 0$.

More precisely, there are at most N such b, where N is given by

$$|f_N| = \max_n |f_n|, \qquad |f_n| < |f_N| \qquad \text{for all } n > N.$$

b) Note α, β are the roots of $X^2 - AX - B$, thus $\alpha + \beta = A$, and

$$\alpha^2 = A\alpha + B, \qquad \beta^2 = A\beta + B.$$

Hence
$$\alpha^{m+2} = A\alpha^{m+1} + B\beta^m, \qquad \beta^{m+2} = A\beta^{m+1} + B\beta^m.$$

Note $u_0 = 2 = \alpha^0 + \beta^0$, $u_1 = A = \alpha^1 + \beta^1$. Suppose that

$$u_m = \alpha^m + \beta^m, \qquad u_{m+1} = \alpha^{m+1} + \beta^{m+1}.$$

Then

$$\begin{aligned} u_{m+2} &= Au_{m+1} + Bu_m \\ &= A(\alpha^{m+1} + \beta^{m+1}) + B(\alpha^m + \beta^m) \\ &= \alpha^{m+2} + \beta^{m+2}. \end{aligned}$$

Induction gives $u_m = \alpha^m + \beta^m$ for all $m \geq 0$.

We're given
$$\alpha \equiv 8 \pmod{7^2}, \qquad \beta \equiv 1 \pmod{7^2}.$$

So
$$\alpha = 1 + \alpha_1, \qquad \alpha_1 \equiv 7 \pmod{7^2}$$

and
$$\beta = 1 + \beta_1, \qquad \beta_1 \equiv 0 \pmod{7^2}.$$

By the Binomial Theorem

$$
\begin{aligned}
u_m - 2 &= (1 + \alpha_1)^m + (1 + \beta_1)^m - 2 \\
&= (\alpha_1 + \beta_1)m + (\alpha_1^2 + \beta_1^2)\frac{m(m-1)}{2} + \cdots \\
&= \sum_{n=0}^{\infty} f_n m^n
\end{aligned}
$$

where $f_0 = 0$, $f_1 \equiv 7 \pmod{7^2}$ and $f_n \equiv 0 \pmod{7^2}$ for $n \geq 2$. Moreover, clearly $f_n \to 0$ in $\mathbb{Z}_7$ as $n \to \infty$. By Strassman's Theorem, $u_m - 2$ has at most $N = 1$ zeros in $\mathbb{Z}_7$. By $u_0 = 2$. Hence $u_m = 2$ iff $m = 0$.