MA 472

Note: This is a reading course. The students were required to study on their own Chapters 1,2,4,6–11 of “Local Fields” by Cassels.

MA 472

MATHEMATICS DEPARTMENT
FOURTH YEAR UNDERGRADUATE EXAMS

Course Title: Local Fields

Model Solution No: 1

Note: Part (a) is bookwork. Parts (b) and (c) are unseen.

a) Suppose K/k is totally ramified of degree n. Let π be a prime element for K. Then for every $\alpha \in k$, $v_\pi(\alpha) \equiv 0 \pmod{n}$. Suppose that

$$f_0 + f_1\pi + \cdots f_{n-1}\pi^{n-1} = 0,$$

where $f_i \in k$. Then each term has a distinct π-adic valuation modulo n. By the ultrametric inequality, the 'largest' term must be zero. Hence every term is zero. This shows that $K = k(\pi)$.

Now π is the root of a polynomial

$$f_0 + f_1\pi + \cdots + f_n\pi^n = 0$$

with coefficients $f_i \in \mathcal{O}_k$ and $f_n = 1$. Then $\pi \mid f_0$ so $\pi^n \mid f_0$, so $\pi^2 \mid \pi f_1$ so $\pi \mid f_1$, so $\pi^n \mid f_1$ and so on. Finally $f_0 = -\pi^n + O(\pi^{n+1})$, so $\pi^n \mid\mid f_0$. This shows that π is the root of an Eisenstein polynomial.

b) Since f is monic and its reduction modulo p is irreducible, f is irreducible in $\mathbb{Z}_p[X]$. Write k_v for the residue field of $\mathbb{Q}_p(\theta)$. Then $[k_v : \mathbb{F}_p] = p$ and $[\mathbb{Q}_p(\theta) : \mathbb{Q}] = p$. However,

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

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

c) By (b) all we have to do is show that $f(X) = X^4 + 2$ is irreducible over $\mathbb{F}_5$. First note that

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

Hence f does not have roots in $\mathbb{F}_5$. Next we would like to show that it does not factor as a product of two quadratics. Suppose

$$X^4 + 2 \equiv (X^2 + aX + b)(X^2 + cX + d) \pmod{5}.$$

Comparing coefficients of X^2 we obtain $c \equiv -a \pmod{5}$. From the other coefficients we obtain

$$b + d \equiv a^2, \qquad bd \equiv 2, \qquad a(d - b) \equiv 0.$$

If $a \not\equiv 0$ then $b \equiv d$ and so $b^2 \equiv 2$, which is impossible. Hence $a \equiv 0$, and so $b \equiv -d$, and so $b^2 \equiv 3$ which again is impossible.

MA 472

MATHEMATICS DEPARTMENT
FOURTH YEAR UNDERGRADUATE EXAMS

Course Title: Local Fields

Model Solution No: 2

Note: Part (a) is bookwork. They haven't seen parts (b) and (c) before, but the inequality in part (c) is bookwork.

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

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

Conversely 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

$$\begin{aligned}|s_m - s_n| &\leq |a_{n+1} + a_{n+2} + \cdots + a_m| \\ &\leq \max\{|a_{n+1}|, \dots, |a_m|\} < \epsilon.\end{aligned}$$

This shows that s_n is Cauchy.

b) By (a) we would like to show that $|p^n/n|_p \to 0$ as $n \to \infty$. Let $m_n = v_p(n)$ be the exponent of p is the prime-power factorization of n. Then $m_n \leq \log(n)/\log(p)$. Moreover,

$$\left|\frac{p^n}{n}\right|_p = \left(\frac{1}{p}\right)^{n-m_n}.$$

Clearly $n - m_n \to \infty$, and so $|p^n/n|_p \to 0$.

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

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

Hence

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

This goes to ∞ as $n \to \infty$ provided $p > 2$. Hence $\sum n!/p^n$ does not converge in $\mathbb{Q}_p$ if p is odd.

MA 472

MATHEMATICS DEPARTMENT
FOURTH YEAR UNDERGRADUATE EXAMS

Course Title: Local Fields

Model Solution No: 3

Note: Part (a) is bookwork. Parts (b), (c) are similar to some exercises in the book.

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

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

Hence

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

Clearly $u_m = (\alpha^m - \beta^m)/(\alpha - \beta)$ holds for $m = 0$, 1. Suppose that

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

Then

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

Induction gives $u_m = \frac{\alpha^m - \beta^m}{\alpha - \beta}$ for all $m \geq 0$.

c) We're given

$$\alpha \equiv \beta \equiv 1 \pmod{5}.$$

So

$$\alpha = 1 + \alpha_1, \qquad \alpha_1 \equiv 0 \pmod{5}$$

and

$$\beta = 1 + \beta_1, \qquad \beta_1 \equiv 0 \pmod 5.$$

By the Binomial Theorem

$$\begin{aligned} u_m &= \frac{(1+\alpha_1)^m - (1+\beta_1)^m}{\alpha_1 - \beta_1} \\ &= m + (\alpha_1 + \beta_1)\frac{m(m-1)}{2} + (\alpha_1^2 + \alpha_1\beta_1 + \beta_1^2)\frac{m(m-1)(m-2)}{3!} \cdots \\ &= \sum_{n=0}^{\infty} f_n m^n \end{aligned}$$

where $f_0 = 0$, $f_1 = 1$ and $f_n \equiv 0 \pmod 5$ for $n \geq 2$. Moreover, clearly $f_n \to 0$ in $\mathbb{Z}_5$ as $n \to \infty$. By Strassman's Theorem, u_m has at most $N = 1$ zeros in $\mathbb{Z}_5$. But $u_0 = 0$. Hence $u_m = 0$ iff $m = 0$.

MA 472

MATHEMATICS DEPARTMENT
FOURTH YEAR UNDERGRADUATE EXAMS

Course Title: Local Fields

Model Solution No: 4

Note: Parts (a), (b) are a special case of Hensel's Lemma, proven in the book. Part (c) is unseen.

a) Let $a_0 \in \mathcal{O}$ satisfy
$$|f(a_0)| < 1, \qquad |f'(a_0)| = 1.$$
Let $a_1 = a_0 - f(a_0)/f'(a_0)$. By Taylor's Theorem,
$$f(a_1) = f(a_0) + f'(a_0) \cdot \frac{-f(a_0)}{f'(a_0)} + O(f(a_0)^2) = O(f(a_0)^2).$$
In otherwords,
$$|f(a_1)| \leq |f(a_0)|^2.$$
Moreover, since $|a_1 - a_0| = |f(a_0)| < 1$, $|f'(a_1) - f'(a_0)| < 1$, and so $|f'(a_1)| = 1$. Now repeat the argument to get that
$$|f(a_n)| \leq |f(a_0)|^{2^n},$$
showing that $f(a_n) \to 0$ as $n \to \infty$. However, $|a_{n+1} - a_n| = |f(a_n)|$, so the sequence a_n converges to some a. Finally,
$$a - a_0 = (a_1 - a_0) + (a_2 - a_1) + \cdots ,$$
which shows that $|a - a_0| < 1$, as required.

b) 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 $b = a$ establishing uniqueness.

c) Let $f(X) = X^{p-1} - 1 \in \mathbb{Z}_p[X]$. Now f has at most $p-1$ roots as it has degree $p-1$. Let $a_0 \in \{1, 2, \ldots, p-1\}$. Then $f(a_0) \equiv 0 \pmod{p}$ and $f'(a_0) \not\equiv 0 \pmod{p}$. By part (a), for each a_0 there is a unique $a \equiv a_0 \pmod{p}$ such that $f(a) = 0$. Thus there are at least $p - 1$ roots in $\mathbb{Z}_p$ and hence exactly $p - 1$ roots.

MA 472

MATHEMATICS DEPARTMENT
FOURTH YEAR UNDERGRADUATE EXAMS

Course Title: Local Fields

Model Solution No: 5

Note: Part (a) is bookwork. A special case (with $C = 1$) of part (b) is in the book. Part (c) is a special case of a result in the book.

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 $| \ |$ on k satisfies the triangle inequality and $|e| \leq C$ for all e in the ring generated by $1 \in k$. Let a, $b \in k$. The Binomial Theorem states

$$(a+b)^n = \sum_{r=0}^{n} \binom{n}{r} a^r b^{n-r}.$$

From the triangle inequality,

$$|a+b|^n \leq \sum_{r=0}^{n} \left| \binom{n}{r} \right| |a|^r |b|^{n-r}.$$

But $\binom{n}{r}$ belongs to the ring generated by 1, and so

$$|a+b|^n \leq C \sum_{r=0}^{n} |a|^r |b|^{n-r} \leq C(n+1) \max\{|a|, |b|\}^n.$$

Taking n-th roots and letting $n \to \infty$ we obtain $|a+b| \leq \max\{|a|, |b|\}$.

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.