MATHEMATICAL TRIPOS PART III (2025-26)

Local Fields - Example Sheet 2 of 3 **T.A. Fisher**

1. Prove the Chinese Remainder Theorem in the following form:

   Let R be a ring (commutative with a 1) and let $I_1, \ldots, I_n \subset R$ be ideals with $I_i + I_j = R$ for all $i \neq j$. Then
   (i) $\cap_{i=1}^n I_i = \prod_{i=1}^n I_i$ ($= I$ say),
   (ii) $R/I \cong R/I_1 \times \ldots \times R/I_n$.

2. Let R be a Dedekind domain. Use the theorem on unique factorization into prime ideals, and the previous exercise, to show that

   (i) If R has only finitely many prime ideals then it is a PID.

   (ii) If $I \subset R$ is an ideal then $I = (a, b)$ for some $a, b \in R$.

For the next two exercises, the absolute value on a p-adic field K is normalised so that $|\pi_K| = 1/q$ where π_K is a uniformiser and q is the order of the residue field. We use the usual absolute value on $\mathbb{R}$, and the square of the usual absolute value on $\mathbb{C}$.

3. Let L/K be a finite extension of p-adic fields. Let $|\cdot|_K$ and $|\cdot|_L$ be the normalised absolute values, and let $n = [L : K]$.

   (i) Show that $|x|_L = |x|_K^n$ for all $x \in K$.

   (ii) Deduce that $|N_{L/K}(x)|_K = |x|_L$ for all $x \in L$.

4. Let L/K be an extension of number fields.

   (i) Let v be a place of K. Show that $|N_{L/K}(x)|_v = \prod_{w|v} |x|_w$ for all $x \in L$.

   (ii) Deduce the product formula:

   If $x \in K^*$ then $\prod_v |x|_v = 1$ where v runs over all places of K.

For the next three exercises (which follow on one from the other) let K be a field complete with respect to a discrete valuation, with valuation ring $\mathcal{O}$ and residue field k.

5. Let $f(X)$ be a polynomial in $\mathcal{O}[X]$ and suppose $\overline{f}(X) = \phi_1(X)\phi_2(X)$ where $\phi_1, \phi_2 \in k[X]$ are coprime. Show that there exist polynomials $f_1, f_2 \in \mathcal{O}[X]$ with $f(X) = f_1(X)f_2(X)$, $\deg f_1 = \deg \phi_1$, and $\overline{f}_i = \phi_i$ for $i = 1, 2$.

6. Let $f(X)$ be a monic irreducible polynomial in $K[X]$. Show that if $f(0) \in \mathcal{O}$ then $f \in \mathcal{O}[X]$.

7. Let L/K be a finite extension and write $|\cdot|_K$ for the absolute value on K.

   (i) Let $x \in L$. Show that if $N_{L/K}(x) \in \mathcal{O}$ then $N_{L/K}(1 + x) \in \mathcal{O}$.

   (ii) Prove directly that $|x|_L = |N_{L/K}(x)|_K$ is an absolute value on L.

8. Show that $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^3 \cong (\mathbb{Z}/3\mathbb{Z})^m$ where $m = 2$ if $p \equiv 1 \pmod 3$ and $m = 1$ if $p \equiv 2 \pmod 3$. What happens when $p = 3$? Show that if $K = \mathbb{Q}(\sqrt[3]{d})$ for d a cube-free integer, then 3 splits in $K/\mathbb{Q}$ (i.e. there is more than one prime of K above 3) if and only if $d \equiv \pm 1 \pmod 9$.

9. Prove that $\mathbb{R}$, $\mathbb{Q}_2$, $\mathbb{Q}_3$, $\mathbb{Q}_5$, ... are pairwise non-isomorphic as fields (no topology).

10. Let $U_r = 1 + p^r\mathbb{Z}_p$. Show that for r sufficiently large $U_r/U_{r+m} \cong \mathbb{Z}/p^m\mathbb{Z}$. *Use this* to prove that if p is odd then $(\mathbb{Z}/p^n\mathbb{Z})^*$ is cyclic. (You may assume the case $n = 1$.) What happens when $p = 2$?

11. Let K be a finite extension of $\mathbb{Q}_p$ with residue field of order q. Show that if $e(K/\mathbb{Q}_p) < p - 1$ then K contains exactly $q - 1$ roots of unity. Does the same conclusion hold if we weaken the hypothesis to $e(K/\mathbb{Q}_p) \leqslant p - 1$?

12. Give a direct proof that $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ is sequentially compact.

13. Show that $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \cong \widehat{\mathbb{Z}}$ and $\mathrm{Gal}(\mathbb{Q}(\cup_{n\geqslant 1}\mu_n)/\mathbb{Q}) \cong \widehat{\mathbb{Z}}^\times$.

14. For an integer $M > 1$ define $\mathbb{Z}_M = \varprojlim \mathbb{Z}/M^n\mathbb{Z}$ with respect to the natural surjections $\mathbb{Z}/M^{n+1}\mathbb{Z} \to \mathbb{Z}/M^n\mathbb{Z}$. Prove that $\mathbb{Z}_M \cong \prod_{p|M} \mathbb{Z}_p$. In particular, $\mathbb{Z}_M$ is an integral domain if and only if M is a prime power, and $\mathbb{Z}_{p^k} \cong \mathbb{Z}_p$ for $k \geqslant 1$.

15. For each $n \geqslant 1$ let $K_n = \mathbb{Q}_p(a_n)$ where $a_n \in \overline{\mathbb{Q}}_p$ is a root of unity of order coprime to p. Suppose that $K_1 \subset K_2 \subset \ldots$. Let $s_n = \sum_{i=1}^n a_i p^i$ and $s = \lim_{n\to\infty} s_n \in \mathbb{C}_p$.

    (i) Show that if $\sigma, \tau \in \mathrm{Gal}(K_n/K_{n-1})$ are distinct then $|\sigma(s_n) - \tau(s_n)| = p^{-n}$.

    (ii) Deduce that $[K_n : K_{n-1}] \leqslant [\mathbb{Q}_p(s) : \mathbb{Q}_p]$.

    (iii) By making a suitable choice of $a_1, a_2, \ldots$ prove that $\overline{\mathbb{Q}}_p$ is not complete.