MATHEMATICAL TRIPOS PART III (2016–17)

Local Fields - Example Sheet 4 of 4 **C. Johansson**

A local field K has valuation ring $\mathcal{O}_K$, normalised discrete valuation v_K, uniformiser π_K, and residue field k_K, and $q = \#k_K$ is a power of p. We fix an algebraic closure $\overline{K}$ of K and consider all algebraic extensions of K as subfields of $\overline{K}$.

1. Let $(I, \leq)$ be a directed system. Let $J \subseteq I$ be a subset such that for all $i \in I$, there exists $j \in J$ with $i \leq j$. Show that $(J, \leq)$ is a directed system. If $(G_i, f_{ik})_{i,k \in I, i \leq k}$ is an inverse system of topological groups indexed by I, then $(G_i, f_{ik})_{i,k \in J, i \leq k}$ is an inverse system indexed by J. Show that there is a natural isomorphism
$$\varprojlim_{i \in I} G_i \xrightarrow{\sim} \varprojlim_{j \in J} G_j.$$

2. Let M/K be a Galois extension of fields (not necessarily finite).
   (i) Let I be the directed system of finite Galois subextensions L/K of M/K. Prove that the map
$$\phi : \mathrm{Gal}(M/K) \to \prod_{L \in I} \mathrm{Gal}(L/K);$$
$$\phi(\sigma) = (\sigma|_L)_{L \in I},$$
   is injective with image $\varprojlim_{L \in I} \mathrm{Gal}(L/K)$.
   (ii) Show that $\varprojlim_{L \in I} \mathrm{Gal}(L/K)$ is a compact Hausdorff space, when each $\mathrm{Gal}(L/K)$ is given the discrete topology (which is also its Krull topology). You may use the fact that an arbitrary product of compact topological spaces is compact (Tychonoff's Theorem).
   (iii) Show that ϕ is a homeomorphism onto its image, and deduce that $\mathrm{Gal}(M/K)$ is compact and Hausdorff.

3. Let M/K be a Galois extension of fields. Prove that the map $L \mapsto \mathrm{Gal}(M/L)$ defines a bijection between the subextensions L/K of M/K and the closed subgroups of $\mathrm{Gal}(M/K)$, with inverse $H \mapsto M^H = \{x \in M \mid h(x) = x \ \forall h \in H\}$.

4. Consider the directed set $(\mathbb{Z}_{\geq 1}, |)$, i.e. a is "less than or equal to" b if $a \mid b$.
   (i) Show that $(\mathbb{Z}/n\mathbb{Z}, f_{m,n})_{n.m \in \mathbb{Z}_{\geq 1}, m|n}$ is an inverse system of topological groups, where $\mathbb{Z}/n\mathbb{Z}$ is given the discrete topology and $f_{m,n} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is the natural map (for $m \mid n$).
   (ii) Put $\widehat{\mathbb{Z}} = \varprojlim_{n \in \mathbb{Z}_{\geq 1}} \mathbb{Z}/n\mathbb{Z}$. Let q be a prime power and let $\overline{\mathbb{F}}_q$ be an algebraic closure of $\mathbb{F}_q$. Show that there is an isomorphism $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \cong \widehat{\mathbb{Z}}$ sending $1 \in \widehat{\mathbb{Z}}$ to the q-th power Frobenius map on $\overline{\mathbb{F}}_q$.

(iii) Show that $\mathbb{Z} \subseteq \widehat{\mathbb{Z}}$ is a non-closed subgroup, and compute its fixed field in $\overline{\mathbb{F}}_q$ under the isomorphism $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \cong \widehat{\mathbb{Z}}$.

5. Let $K/\mathbb{Q}$ be a finite extension with ring of algebraic integers $\mathcal{O}_K$, and let $\mathfrak{p} \subseteq \mathcal{O}_K$ be a maximal ideal containing p. Recall the valuation $v_\mathfrak{p}$ on K and the completion $K_\mathfrak{p}$ from Question 1, Example Sheet 2. Assume that $K/\mathbb{Q}$ is Galois. Show that $K_\mathfrak{p}/\mathbb{Q}_p$ is Galois, and that the homomorphism

$$\mathrm{Gal}(K_\mathfrak{p}/\mathbb{Q}_p) \to \mathrm{Gal}(K/\mathbb{Q});$$

$$\sigma \mapsto \sigma|_K,$$

is injective. Show that the image of this map consists of all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\sigma(\mathfrak{p}) = \mathfrak{p}$ (this subgroup is called the *decomposition group* of $K/\mathbb{Q}$ at $\mathfrak{p}$).

6. Let R be a ring and let $F(X,Y) \in R[[X,Y]]$ be a formal group over R.

   (i) Let $g(X) \in R[[X]]$ and assume that $g(X) \equiv aX$ modulo X^2, where $a \in R^\times$. Prove that there exists a power series $h(X) \in R[[X]]$ such that $g(h(X)) = X$.

   (ii) Prove that $F(X,0) = X$ (*Hint: Put* $f(X) = F(X,0)$*, and consider* $f(f(X))$).

   (iii) Show that there exists a power series $i(X) \in R[[X]]$ with $i(X) \equiv -X$ modulo X^2 such that $F(X, i(X)) = 0$. Compute $i(X)$ for $F = \widehat{\mathbb{G}}_m$.

7. Let K be a local field and let L/K and M/L be finite abelian extensions. Show that $N(LM/K) = N(L/K) \cap N(M/K)$ and $N((L \cap M)/K) = N(L/K)N(M/K)$.

8. Prove the Existence Theorem: If K is a local field and $H \subseteq K^\times$ is an open subgroup of finite index, show that there is a finite abelian extension L/K such that $N(L/K) = H$. You may use the theorem about the norm groups of Lubin–Tate extensions stated in lectures. Show also that if K has characteristic 0, then any finite index subgroup of $K^\times$ is automatically open.

9. Redo Questions 9 and 13 from Example Sheet 3 using local class field theory, except for the computation of the *lower* ramification groups in Question 9.

10. Let $p > 2$ and let $\zeta \in \mathbb{Q}_p$ be a $(p-1)$-th root of unity.

    (i) Show that the extension $K_\zeta/\mathbb{Q}_p$ obtained by adjoining a root of the polynomial $X^{p-1} - \zeta p$ is Galois, and totally ramified of degree $p-1$

    (ii) Show that any totally ramified extension $K/\mathbb{Q}_p$ of degree $p-1$ is equal to K_ζ for some $(p-1)$-th root of unity ζ.

    (iii) Find the ζ such that $K_\zeta = \mathbb{Q}_p(\zeta_p)$, where ζ_p is a primitive p-th root of unity.

11. Let K be a local field and let L/K be a finite abelian extension. Let $n \in \mathbb{Z}_{\geq 0}$. Let π be a uniformizer of K and let $L_{n,\pi}$ be the field of π^n-division points for a Lubin–Tate $\mathcal{O}_K$-module for π. Show that $U_K^{(n)} \subseteq N(L/K)$ if and only if there exists a finite unramified extension M/K such that $L \subseteq L_{n,\pi}M$.

12. Let K be a local field, and let π_1, π_2 be uniformizers in K. Let $n \in \mathbb{Z}_{\geq 0}$ and let L_{n,π_i} be the field of π^n-division points of a Lubin-Tate $\mathcal{O}_K$-module for π_i, $i = 1, 2$. Set $L_{\pi_i} = \bigcup_{n=1}^{\infty} L_{n,\pi_i}$ for $i = 1, 2$. Find a condition on π_1 and π_2 that is equivalent to $L_{n,\pi_1} = L_{n,\pi_2}$. Deduce that $L_{\pi_1} = L_{\pi_2}$ if and only if $\pi_1 = \pi_2$. Show also that we may find a finite unramified extension M/K, depending on n, such that $L_{n,\pi_1}M = L_{n,\pi_2}M$.

13. The Hilbert norm residue symbol $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \times \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \to \{\pm 1\}$ is defined by

$$(a, b)_p = \begin{cases} 1 & \text{if } ax^2 + by^2 = 1 \text{ for some } x, y \in \mathbb{Q}_p \\ -1 & \text{otherwise.} \end{cases}$$

(i) Show that if $K = \mathbb{Q}_p(\sqrt{a})$ then $(a, b)_p = 1$ if and only if $b = N_{K/\mathbb{Q}_p}(\beta)$ for some $\beta \in K$. Deduce that $(a, b)_p = (a, -ab)_p$, and that $(\cdot, \cdot)_p$ is bilinear.

(ii) Find a basis for $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ as an $\mathbb{F}_2$-vector space and compute the matrix of $(\cdot, \cdot)_p$ relative to this basis. Deduce that the Hilbert norm residue symbol is bilinear and non-degenerate.

14. Let K be a field and let $f(X) \in K[X]$ be a separable polynomial of degree n, with splitting field L/K. There is a surjective ring homomorphism $\phi : K[X_1, ..., X_n] \to L$ given by $X_i \mapsto \alpha_i$, where $\alpha_1, \ldots, \alpha_n$ are the roots of f. Let I denote the kernel of ϕ. If $\sigma \in S_n$, the symmetric group on $\{1, \ldots, n\}$, then σ defines an automorphism of $K[X_1, ..., X_n]$ given by

$$(\sigma F)(X_1, ..., X_n) = F(X_{\sigma(1)}, ..., X_{\sigma(n)}).$$

Show that the Galois group $\mathrm{Gal}(f/K) := \mathrm{Gal}(L/K)$ of f can be identified with those $\sigma \in S_n$ such that $\sigma(I) = I$. We will think of Galois group of polynomials as permutation groups on the roots.

Now consider an irreducible polynomial $f(X) \in \mathbb{Q}[X]$, with roots $\alpha_1, ..., \alpha_n$ inside some algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$. Show that $\mathrm{Gal}(f/\mathbb{Q}_p) \subseteq \mathrm{Gal}(f/\mathbb{Q})$ as permutation groups. Now assume that f is monic, and in $\mathbb{Z}[X]$. Let $\overline{f} \in \mathbb{F}_p[X]$ denote the reduction of f modulo p. If $\overline{f}$ is separable (i.e. p does not divide the discriminant of f), show that there is natural bijection between the roots of f in $\overline{\mathbb{Q}}_p$ and the roots of $\overline{f}$ in the residue field of $\overline{\mathbb{Q}}_p$ (which is an algebraic closure of $\mathbb{F}_p$). Then show that $\mathrm{Gal}(f/\mathbb{Q}_p) = \mathrm{Gal}(\overline{f}/\mathbb{F}_p)$ as permutation groups with respect to this bijection, and conclude that we have $\mathrm{Gal}(\overline{f}/\mathbb{F}_p) \subseteq \mathrm{Gal}(f/\mathbb{Q})$ as permutation groups in a natural way.

How does this relate to Question 5?