**MATHEMATICAL TRIPOS PART III (2017–18)**

**Algebraic Number Theory - Example Sheet 3 of 4** **C. Johansson**

1. Let $L/K$ be a finite extension of local fields and let $q = \#k_K$. If $L/K$ is unramified of degree $n$, show that $L = K(\zeta_{q^n-1})$. Conversely, if $m$ is coprime to $q$ and $L = K(\zeta_m)$, show that $L/K$ is unramified and compute its degree. Here $\zeta_r$ denotes a primitive $r$-th root of unity, for any $r$.

2. Let $L/K$ be a finite Galois extension of local fields, with Galois group $G = \mathrm{Gal}(L/K)$. Assume that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ and let $f(T) \in \mathcal{O}_K[T]$ be the minimal polynomial of $\alpha$. Let $v_L$ be the normalized valuation on $L$. Show that

$$v_L(f'(\alpha)) = \sum_{1\neq\sigma\in G} i_G(\sigma) = \sum_{s\in\mathbb{Z}_{\geq 0}} (\#G_s - 1).$$

Deduce that the ideal $\mathfrak{D}_{L/K}$ of $\mathcal{O}_L$ generated by $f'(\alpha)$ is independent of the choice of $\alpha$, and that it is equal to $\mathcal{O}_L$ if and only if $L/K$ is unramified ($\mathfrak{D}_{L/K}$ is called the *different* of $L/K$).

3. Compute the lower and upper ramification groups of $\mathbb{Q}_3(\zeta_3, \sqrt[3]{2})/\mathbb{Q}_3$.

4. Prove that $\mathbb{Q}_2$ has a unique Galois extension with Galois group $(\mathbb{Z}/2\mathbb{Z})^3$ (you may use the results of Question 12, Example Sheet 1). Compute the lower and upper ramification groups.

5. Let $K = \mathbb{F}_p((t))$. Let $L$ be the extension of $K$ obtained by adjoining a root of $f(X) = X^p - X - t^{1-p}$. Show that $L/K$ is Galois and compute the lower ramification groups of $L/K$ *(Hint: If $\alpha$ and $\beta$ are roots of $f$, consider $(\alpha-\beta)^p$)*.

6. Prove that if $L/K$ is a Galois extension of local fields with Galois group $S_4$, then the residue characteristic of $K$ is 2. Can you find a Galois extension $L/\mathbb{Q}_2$ with $\mathrm{Gal}(L/\mathbb{Q}_2) \cong S_4$?

7. 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

$$\varprojlim_{i\in I} G_i \xrightarrow{\sim} \varprojlim_{j\in J} G_j.$$

8. 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. You may use the fact that an arbitrary product of compact topological spaces is compact (Tychonoff's Theorem) *(Hint: Show that the inverse limit is closed inside the product).*

(iii) Show that $\phi$ is a homeomorphism onto its image when $\mathrm{Gal}(M/K)$ is given the Krull topology, and deduce that $\mathrm{Gal}(M/K)$ is compact and Hausdorff.

9. 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 $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \cong \widehat{\mathbb{Z}}$.

10. Let $K$ be a local field, let $K^{sep}$ be a separable closure of $K$ and let $n \in \mathbb{Z}_{\geq 1}$. If $K$ has characteristic 0, show that there are only finitely many extensions $K \subseteq L \subseteq K^{sep}$ of degree $n$. What happens if $K$ has characteristic $p$?

11. (R. Coleman) This question extends Question 7, Sheet 2. For any $n \geq 1$, let

$$f_n(T) = \sum_{k=1}^{n} \frac{T^k}{k!} \in \mathbb{Q}[T]$$

and set $E_n(T) = n! f_n(T) \in \mathbb{Z}[T]$. Let $p \geq 8$ be a prime. By Bertrand's postulate, there is a prime $q$ such that $p/2 < q < p - 2$. Let $\mathrm{Gal}(E_p/\mathbb{Q}) \subseteq S_p$ be the Galois group of $E_p$ over $\mathbb{Q}$.

(i) Show that $E_p$ is irreducible (in fact $E_n$ is irreducible for all $n$).

(ii) By considering the Newton polygon of $E_p$ for the prime $q$, show that the Galois group of $E_p$ contains a $q$-cycle. By a theorem of Jordan, this implies that $A_p \subseteq \mathrm{Gal}(E_p/\mathbb{Q})$.

(iii) Let $\alpha_1, \ldots, \alpha_n$ be the roots of $E_n$. Set $D_n = \prod_{i \neq j}(\alpha_i - \alpha_j)$; $D_n$ is the discriminant of $E_n$ up to sign. Prove that $|D_n| = (n!)^n$ *(Hint: Use the formulas $f_n'(T) = f_{n-1}(T)$ and $f_n(T) = f_{n-1}(T) + T^n/n!$).* Deduce that $\mathrm{Gal}(E_p/\mathbb{Q}) = S_p$.

(iv) Deduce that for any finite group $G$, there exists a Galois extension $L/K$ of number fields with $\mathrm{Gal}(L/K) \cong G$.