MATHEMATICAL TRIPOS PART III (2016–17)

Local Fields - Example Sheet 1 of 4 **C. Johansson**

Note: Absolute values are non-trivial, but not necessarily non-archimedean. v_p denotes the p-adic valuation on $\mathbb{Q}_p$, and $|-|_p$ denotes the p-adic absolute value on $\mathbb{Q}_p$.

1. In lectures, we defined absolute values on fields. More generally, if R is a ring, an *absolute value* on R is function $|-| : R \to \mathbb{R}_{\geq 0}$ satisfying the axioms for an absolute value. Show that R is an integral domain, and that $|-|$ extends uniquely to an absolute value on the fraction field of R.

2. Let R be a ring with an absolute value $|-|$. Let C denote the set of all Cauchy sequences in R.

   (i) Show that the rules $(x_n)_n + (y_n)_n = (x_n + y_n)_n$ and $(x_n)_n \cdot (y_n)_n = (x_n y_n)_n$ define a ring structure on C.

   (ii) Show that set I of the of sequences tending to 0 form a prime ideal in C. Denote the quotient C/I by $\widehat{R}$, and show that the map $j : R \to \widehat{R}$ sending $x \in R$ to the equivalence class of the constant sequence $(x)_n$ is an injective ring homomorphism.

   (iii) If $(x_n)_n \in C$, show that $\lim_{n\to\infty} |x_n|$ exists and that the function $|(x_n)_n|' = \lim_{n\to\infty} |x_n|$ is constant on cosets of I, hence defines a function $|-|' : \widehat{R} \to \mathbb{R}_{\geq 0}$.

   (iv) Show that $|-|'$ is an absolute value on $\widehat{R}$. Show moreover that $|x| = |j(x)|'$ for all $x \in R$, that $j(R)$ is dense in $\widehat{R}$, and that $\widehat{R}$ is complete with respect to $|-|'$. We call $\widehat{R}$ the *completion* of R.

   (v) Show that if R is a field, then $\widehat{R}$ is a field. Find an example of an R which is not a field, but such that $\widehat{R}$ *is* a field.

3. If $c \in \mathbb{Z}_p$ satisfies $|c|_p < 1$ show that $(1+c)^{-1} = 1 - c + c^2 - c^3 + \ldots$ Hence or otherwise find $a \in \mathbb{Z}$ such that $|4a - 1|_5 \leq 5^{-10}$.

4. Let $x = \sum_{n \geq N} a_n p^n \in \mathbb{Q}_p$, with $a_n \in \{0, 1, \ldots, p-1\}$, $N \in \mathbb{Z}$ and $a_N \neq 0$.

   (i) Show that $x \in \mathbb{Q}$ if and only if the sequence $(a_n)_n$ is eventually periodic.

   (ii) Assume that $x \in \mathbb{Z}$ and let $s_p(x) = \sum_n a_n$. Prove the formula $v_p(x!) = (x - s_p(x))/(p-1)$.

5. (Hensel's Lemma) Let K be a complete valued field with valuation ring $\mathcal{O}$ and maximal ideal $\mathfrak{m}$. Let $f(x) \in \mathcal{O}[x]$ be a monic polynomial, and assume that $a_0 \in \mathcal{O}$ is such that $f(a_0) \in \mathfrak{m}$ but $f'(a_0) \notin \mathfrak{m}$. For each $n \geq 1$, define

$$a_n = a_{n-1} - \frac{f(a_{n-1})}{f'(a_{n-1})}.$$

   Prove that $a = \lim_{n\to\infty} a_n$ exists and is a simple root of f. Show also that there are no other roots of f which are congruent to a modulo $\mathfrak{m}$.

6. Show that the equation $x^3 - 3x + 4 = 0$ has a unique solution in $\mathbb{Z}_7$, but has no solutions in $\mathbb{Z}_5$ or in $\mathbb{Z}_3$. How many are there in $\mathbb{Z}_2$?

7. Consider the series
$$\text{“ } \sqrt{1+15} \text{ ”} = 1 + \sum_{n=1}^{\infty} \binom{1/2}{n} 15^n$$
where $\binom{x}{n} = \frac{x(x-1)\cdots(x-n+1)}{n!}$. Show that the series converges to 4 with respect to the 3-adic absolute value, to -4 with respect to the 5-adic absolute value, and diverges with respect to all other absolute values on $\mathbb{Q}$.

8. Show that a subgroup of $\mathbb{Z}_p$ is open if and only if it has finite index.

9. Let $\widehat{R}$ be the completion of a ring R with respect to a non-archimedean absolute value $|-|$. Prove that $|\widehat{R}| = |R|$.

10. Let $|-|$ and $|-|'$ be two absolute values on a field K. Prove that the following are equivalent:

    (i) $|-|$ and $|-|'$ define the same topology on K.

    (ii) $|x| < 1 \implies |x|' < 1$ for all $x \in K$.

    (iii) There exists a real number $s > 0$ such that $|x|^s = |x|'$ for all $x \in K$.

    Deduce that the completion of K only depends to the equivalence class of the absolute value.

11. Let K be a field with an absolute value $|-|$. Prove that the following are equivalent:

    (i) $|-|$ is non-archimedean (i.e. satisfies the strong triangle inequality).

    (ii) The image of the natural map $\mathbb{Z} \to K$ is a bounded subset of K.

    (iii) $|x| \leq 1 \implies |x+1| \leq 1$ for all $x \in K$.

    Note that it is not necessary to use that $|-|$ satisfies the triangle inequality for the equivalence (i) $\iff$ (iii). Deduce that any absolute value on a field of positive characteristic is non-archimedean.

12. Let $X_1, X_2, ...$ be a sequence of Hausdorff topological rings with continuous homomorphisms $f_n : X_{n+1} \to X_n$ for $n \geq 1$. Let $X = \varprojlim_n X_n$. Show that X is closed inside the product topological ring $\prod_n X_n$.

13. Let R be a ring and let $x \in R$. Let S be the x-adic completion of R. Assume that R is x-torsionfree. Show that S is x-adically complete, and x-torsionfree.

14. Show that a non-archimedean absolute value on $\mathbb{Q}$ is equivalent to $|-|_p$ for a *unique* p. Show that any archimedean absolute value on $\mathbb{Q}$ is equivalent to the usual absolute value $|x| = \sqrt{x^2}$.

15. (Strassman's theorem) Let $f(T) = c_0 + c_1 T + c_2 T^2 + \ldots \in \mathbb{Z}_p[[T]]$ be a formal power series with $c_n \to 0$ as $n \to \infty$. Suppose that for some $N \geq 0$ we have $v_p(c_N) = 0$ and $v_p(c_n) > 0$ for all $n > N$. Show that $\#\{x \in \mathbb{Z}_p : f(x) = 0\} \leq N$.

MATHEMATICAL TRIPOS PART III (2016–17)

Local Fields - Example Sheet 2 of 4 **C. Johansson**

$|-|_p$ denotes the p-adic absolute value on $\mathbb{Q}_p$ and v_p denotes the p-adic valuation.

1. Let $K/\mathbb{Q}$ be a finite extension and let $\mathcal{O}_K \subseteq K$ be the subring of algebraic integers. It is a basic fact of algebraic number theory that every nonzero ideal $I \subseteq \mathcal{O}_K$ has a unique factorization
$$I = \prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}(I)}$$
where $\mathfrak{p}$ ranges through the maximal ideals of $\mathcal{O}_K$ and the $e_{\mathfrak{p}}(I) \in \mathbb{Z}_{\geq 0}$ are zero for all but finitely many $\mathfrak{p}$. Fix a maximal ideal $\mathfrak{p}$. Prove that the function $v_{\mathfrak{p}} : \mathcal{O}_K \to \mathbb{Z} \cup \{\infty\}$ defined by
$$v_{\mathfrak{p}}(x) = e_{\mathfrak{p}}(x\mathcal{O}_K)$$
if $x \neq 0$ and $v_{\mathfrak{p}}(0) = \infty$ defines a discrete valuation on $\mathcal{O}_K$. If $p \in \mathfrak{p}$, prove that $v_{\mathfrak{p}}|_{\mathbb{Z}}$ is equivalent to v_p. We denote the completion of K with respect to $v_{\mathfrak{p}}$ by $K_{\mathfrak{p}}$.

2. Using the previous exercise, or otherwise, find a valued field K and a finite extension L/K such that the absolute value on K has more than one extension to L.

3. Let K be a valued field with valuation ring $\mathcal{O}_K$ and let I be a finitely generated ideal. Show that I is principal. Deduce that $\mathcal{O}_K$ is a Noetherian ring if and only if K is a discretely valued field.

4. Let K be a complete valued field with valuation v and let $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n \in K[x]$. Let $\alpha_1, \ldots, \alpha_n$ be the roots of f in a splitting field L of f over K, and let w be the valuation on L extending v. Prove that
$$f_r(x) = \prod_{i\,:\,w(\alpha_i)=r} (x - \alpha_i) \in K[x]$$
for any $r \in \mathbb{R}$ (if you find the general case tricky, try the case when L/K is separable first). Deduce that f has at least as many factors in $K[x]$ as there are line segments on its Newton polygon.

5. In this exercise you should use the conclusions of Exercise 4, even if you have not completed it. Work over $\mathbb{Q}_2$.

   (i) Consider $f(x) = 1 - x/2 - x^2/2 + x^3 \in \mathbb{Q}_2[x]$. Draw the Newton polygon of f and show that f has three roots in $\mathbb{Q}_2$. Can you prove this using Hensel's Lemma?

   (ii) Consider $g(x) = x^5 + 2x^2 + 4 \in \mathbb{Q}_2[x]$. Draw the Newton polygon of g and show that g has a factor of degree 2 and another factor of degree 3. Can you prove that both these factors are irreducible?

(iii) Give an example of a polynomial in $\mathbb{Q}_2[x]$ which is reducible and whose Newton polygon has a single line segment.

6. Let $p > 2$, $n \geq 1$ and let $\Phi_{p^n}(x) = x^{p^{n-1}(p-1)} + x^{p^{n-1}(p-2)} + \cdots + x^{p^{n-1}} + 1$ be the p^n-th cyclotomic polynomial. It is irreducible over $\mathbb{Q}_p$ (you may assume this). Let $K = \mathbb{Q}_p(\zeta_{p^n})$, where ζ_{p^n} is a primitive p^n-th root of unity, and let w denote the unique extension of v_p to K. Define $f_n(x) = \Phi_{p^n}(x+1)$. By computing the first and last coefficient of $f_n(x)$, prove that

$$w(\zeta_{p^n}^i - 1) = \frac{1}{p^{n-1}(p-1)}$$

for all n and all i coprime to p.

7. Compute the Mahler expansions of the polynomials x^3+4x+7 and $x^4+8x^3+6x^2+5$.

8. Let $K/\mathbb{Q}_p$ be a finite extension and let $a \in \mathfrak{m}_K$. We can define a function $\mathbb{Z}_p \to K$, denoted by $(1+a)^x$, by the Mahler expansion

$$(1+a)^x := \sum_{n=0}^{\infty} \binom{x}{n} a^n.$$

(i) When $x \in \mathbb{Z}_{\geq 0}$, prove that the right hand side above is equal to $(1+a)^n$ in the usual sense. Then show that $(1+a)^{x+y} = (1+a)^x(1+a)^y$ and $(1+a)^{xy} = ((1+a)^x)^y$ (make sense of the right hand side!) for all $x, y \in \mathbb{Z}_p$.

(ii) Consider $K = \mathbb{Q}_p(\zeta_{p^n})$ where ζ_{p^n} is a primitive p^n-th root of unity. Let $\lambda_i = \zeta_{p^n}^i - 1$ for any $i = 0, 1, ..., p^n - 1$; by Exercise 6 we may define $(1+\lambda_i)^x$ for any i. Fix $m \in \{0, 1, ..., p^n - 1\}$. Prove that

$$x \mapsto \frac{1}{p^n} \sum_{i=0}^{p^n-1} \zeta_{p^n}^{-im} (1+\lambda_i)^x$$

is equal to 1 if $x \in m + p^n\mathbb{Z}_p$, and 0 otherwise.

(iii) Use this to give a different proof that the Mahler expansion of any continuous function $f : \mathbb{Z}_p \to \mathbb{Q}_p$ tends to zero.

9. (Continuity of roots) Let K be a complete valued field and let $\overline{K}$ be an algebraic closure of K with the extended absolute value. Let $f(x) = a_0 + a_1 x + \cdots + x^n$ and $g(x) = b_0 + b_1 x + \cdots + x^n$ be monic polynomials in $K[x]$, and let $\beta_1, ..., \beta_n \in \overline{K}$ be the roots of g. If $\alpha \in \overline{K}$ is a root of f, prove that there exists an i such that

$$|\alpha - \beta_i| \leq \max_{i=0,\ldots,n-1} \left(|a_i - b_i|^{1/n} |\alpha|^{i/n} \right).$$

(*Hint: Consider* $g(\alpha) - f(\alpha) = g(\alpha) = \prod_i (\alpha - \beta_i)$.) Reformulating it somewhat imprecisely, if the coefficients of g are close enough to those of f, then there is a root of g close to α.

10. (Krasner's Lemma) Let K be a complete valued field and let $\overline{K}$ be an algebraic closure of K with the extended absolute value. Let $\alpha \in \overline{K}$ be separable and let $\alpha_2, \ldots, \alpha_n \in \overline{K}$ be the K-conjugates of α. If $\beta \in \overline{K}$ is such that

$$|\alpha - \beta| < |\alpha - \alpha_i|$$

for $i = 2, ..., n$, show that $K(\alpha) \subseteq K(\beta)$. (*Hint: Let L be the Galois closure of $K(\alpha, \beta)$ over $K(\beta)$, and show that $|\alpha - \sigma(\alpha)| < |\alpha - \alpha_i|$ for all $i = 2, ..., n$ and $\sigma \in \mathrm{Gal}(L/K(\beta))$.*)

11. Let $L/\mathbb{Q}_p$ be a finite extension. Show, using the two previous exercises or otherwise, that we can find a finite extension $K/\mathbb{Q}$ and a maximal ideal $\mathfrak{p}$ containing p such that $L = K_{\mathfrak{p}}$ (in the notation of Exercise 1).

12. If you have never seen it before, prove (or look up) the Baire Category Theorem: If X is a complete metric space and U_i, $i = 1, 2, ...$ is a sequence of open dense subsets in X, then $\bigcap_{i=1}^{\infty} U_i \neq \emptyset$ (in fact it is dense in X). Use it to prove that an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ is not complete with respect to the extended absolute value.

13. Consider an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ with the extended absolute value. Let $\mathbb{C}_p$ denote its completion. Prove that $\mathbb{C}_p$ is algebraically closed.

14. This exercise is for enthusiasts. Let V be a Banach space over $\mathbb{Q}_p$, i.e. a complete normed vector space over $\mathbb{Q}_p$. Let $||-||$ be the norm on V. A collection e_i, $i \in I$, of elements in V is called an *orthonormal basis* for V if any $v \in V$ can be written uniquely as an expansion

$$v = \sum_{i \in I} a_i e_i$$

for $a_i \in \mathbb{Q}_p$ tending to zero, and moreover

$$||v|| = \max_{i \in I} |a_i|_p.$$

By "a_i tending to zero" we mean that for every $\epsilon > 0$, the set $\{i \in I \mid |a_i|_p > \epsilon\}$ is finite.

(i) Prove that if V has an orthonormal basis, then $||V|| = \{p^n \mid n \in \mathbb{Z}\} \cup \{0\}$, or in short $||V|| = |\mathbb{Q}_p|_p$.

(ii) Prove that, for any V, we can find a norm $||-||'$ equivalent to $||-||$ such that $||V||' = |\mathbb{Q}_p|_p$.

(iii) Prove the converse to the first part: If $||V|| = |\mathbb{Q}_p|_p$, then V has an orthonormal basis.

Thus, while there is no notion of a Hilbert space over $\mathbb{Q}_p$, Banach spaces over $\mathbb{Q}_p$ carry features analogous to those of Hilbert spaces over $\mathbb{R}$ or $\mathbb{C}$.

MATHEMATICAL TRIPOS PART III (2016–17)

Local Fields - Example Sheet 3 of 4 **C. Johansson**

Except where stated otherwise: p is the residue characteristic of any local field considered. A local field K has valuation ring $\mathcal{O}_K$, normalised discrete valuation v_K, uniformiser π_K, and residue field k_K. We write ζ_n for a primitive nth root of unity.

1. Let L/K be a finite extension of local fields.

   (i) Let w be the extension of v_K to L. Let π_L be a uniformizer of L, and let $\mathfrak{m}_L = \pi_L \mathcal{O}_L$. Prove that
   $$e_{L/K}^{-1} = w(\pi_L) = \min_{x \in \mathfrak{m}_L} w(x).$$

   (ii) Let v' be any valuation on K (in the given equivalence class) and let w' be its extension to L. Show that $e_{L/K} = (w'(L^\times) : v'(K^\times))$. Use this to give a direct proof that if $M/L/K$ are finite extensions, then $e_{M/K} = e_{M/L} e_{L/K}$.

2. Let L/K be a finite extension 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.

3. Let L/K be a finite extension of local fields. We say that L/K is *tamely ramified* if $e_{L/K}$ is coprime to p. Let $a \in K$ and let $m \in \mathbb{Z}_{\geq 1}$ be coprime to p. Show that $K(\sqrt[m]{a})/K$ is tamely ramified.

4. Let L/K be a finite extension and let T/K be the maximal unramified subextension of L/K. Show that L/K is tamely ramified if and only if there are elements $a_1, \ldots, a_r \in T$ and positive integers $m_1, \ldots, m_r$ coprime to p such that $L = T(\sqrt[m_1]{a_1}, \ldots, \sqrt[m_r]{a_r})$.

5. If $K/\mathbb{Q}_p$ is a finite extension, show that $U_K^{(n)} \cong (\mathcal{O}_K, +)$ as (topological) groups for sufficiently large n, and find an explicit lower bound for n.

6. Let K be a local field and let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathcal{O}_K[x]$ be a polynomial.

   (i) (Eisenstein's criterion) Assume that $\pi_K \mid a_i$, $i = 0, \ldots, n-1$ and $\pi_K^2 \nmid a_0$. Reformulate this condition in terms of the Newton polygon of f and show that f is irreducible.

   (ii) Let $\Phi_{p^n}(x) = x^{p^{n-1}(p-1)} + x^{p^{n-1}(p-2)} + \cdots + x^{p^{n-1}} + 1 \in \mathbb{Z}[x]$ be the p^n-th cyclotomic polynomial. Prove that $\Phi_{p^n}(x)$ is irreducible over $\mathbb{Q}_p$ for all $n \geq 1$.

   (iii) Find an optimal criterion for the shape of the Newton polygon of f alone to imply that f is irreducible. When this criterion is satisfied, what can you say about the extension of K given by adjoining a root of f?

7. Let L/K be a finite Galois extension of local fields, with Galois group $G = \mathrm{Gal}(L/K)$.

   (i) Show that the ramification groups $G_s := G_s(L/K)$ are normal subgroups of G for all s.

   (ii) Assume that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ and let $f(x) \in \mathcal{O}_K[x]$ be the minimal polynomial of α. Let v_L be the normalized valuation on L. Show that

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

   Deduce that the ideal $\mathfrak{D}_{L/K}$ of $\mathcal{O}_L$ generated by $f'(\alpha)$ is independent of the choice of α, 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).

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

9. Prove that $\mathbb{Q}_p$ has a unique Galois extension with Galois group $(\mathbb{Z}/2\mathbb{Z})^2$ if $p > 2$, and that $\mathbb{Q}_2$ has a unique Galois extension with Galois group $(\mathbb{Z}/2\mathbb{Z})^3$. Compute the ramification groups in all cases (both with respect to the lower and upper numbering).

10. 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. Construct a Galois extension $L/\mathbb{Q}_2$ with $\mathrm{Gal}(L/\mathbb{Q}_2) \cong S_4$.

11. Let $m \in \mathbb{Z}_{\geq 1}$. Compute the Galois group and all the ramification groups of $\mathbb{Q}_p(\zeta_m)$ in the lower and upper numbering (you may use the results in lectures in the case $m = p^n$, if you want to).

12. Let K be a local field. Prove that the abelian group structure on $U_K^{(1)} = 1 + \pi_K \mathcal{O}_K$ naturally extends to $\mathbb{Z}_p$-module structure. Let $q = \#k_K$. When K has characteristic 0, show that

$$K^\times \cong \mathbb{Z} \times \mathbb{Z}/(q-1)\mathbb{Z} \times \mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}_p^{[K:\mathbb{Q}_p]}$$

   as groups, for some $a \in \mathbb{Z}_{\geq 0}$. When K has characteristic p, show that

$$K^\times \cong \mathbb{Z} \times \mathbb{Z}/(q-1)\mathbb{Z} \times \mathbb{Z}_p^{\mathbb{Z}_{\geq 0}}.$$

13. 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?

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 $L \mapsto \mathrm{Gal}(L/K)$ 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 $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ 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?