MATHEMATICAL TRIPOS PART III (2011–12)

Local Fields - Example Sheet 4 of 4 **T.A. Fisher**

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

2. Prove that $\mathbb{Q}_2$ has a unique Galois extension with Galois group $(\mathbb{Z}/2\mathbb{Z})^3$. Compute its ramification groups.

3. Prove that there is at most one prime p for which $\mathbb{Q}_p$ has a Galois extension with Galois group S_4. If you like, you can try to construct such an extension.

4. Prove that $\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p$ is a totally ramified Galois extension, determine its degree, its Galois group and all the ramification groups G_i. [Hint: $1-\zeta$ is a uniformiser.]

For the next three exercises K is a finite extension of $\mathbb{Q}_p$.

5. Suppose L/K is a Galois, totally and tamely ramified extension of degree n. Prove that $\mu_n \subset K$ and $L = K(\sqrt[n]{\pi_K})$. How many totally and tamely ramified Galois extensions does $\mathbb{Q}_5$ have? [Hint: You may use Kummer's theorem: suppose k is any field of characteristic prime to n, containing μ_n. Then every cyclic Galois extension of degree n of k is of the form $k(\sqrt[n]{\alpha})$ for some $\alpha \in k$.]

6. Let L/K be a finite Galois extension that is totally ramified. Let $G = \mathrm{Gal}(L/K)$ and for $\sigma \in G$ put $i_{L/K}(\sigma) = v_L(\sigma(\pi_L) - \pi_L)$. Let $\delta(L/K) = v_L(\mathcal{D}_{L/K})$. Show that
$$\delta(L/K) = \sum_{1 \neq \sigma \in G} i_{L/K}(\sigma) = \sum_{i=0}^{\infty} (|G_i| - 1)$$
where $G_i \subset G$ is the ith higher ramification group.

7. (i) Show that if L/K is finite then $N_{L/K}(L^*) \subset K^*$ is an open subgroup.
   (ii) Show that if $K = \mathbb{Q}_p$ and $L = \mathbb{Q}_p(\zeta_m)$ then
   $$N_{L/K}(L^*) = \begin{cases} \langle p, 1 + p^n\mathbb{Z}_p \rangle & \text{if } m = p^n, \\ \langle p^f, \mathbb{Z}_p^* \rangle & \text{if } m = p^f - 1. \end{cases}$$
   [Hint: For $p \neq 2$ we know that $\mathbb{Z}_p^* \cong (\mathbb{Z}/p\mathbb{Z})^* \times \mathbb{Z}_p$ and so $1 + p^n\mathbb{Z}_p$ is the only subgroup of $\mathbb{Z}_p^*$ of index $p^{n-1}(p-1)$.]
   (iii) (Local version of the Kronecker-Weber theorem.) Deduce by local class field theory that if $K/\mathbb{Q}_p$ is abelian then $K \subset \mathbb{Q}_p(\zeta_d)$ for some d.

8. Let L/K be a Galois extension of fields with $G = \mathrm{Gal}(L/K)$ cyclic of order n, generated by σ. Let $A \in \mathrm{GL}_m(L)$ with $A\sigma(A)\ldots\sigma^{n-1}(A) = I_m$. Show there exists $B \in \mathrm{GL}_m(L)$ with $A = B^{-1}\sigma(B)$.

9. The Hilbert norm residue symbol $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 \times \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 \to \mu_2$ 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 is a field (with $\mathrm{char}(K) \neq 2$) and $a,b \in K^*$, then $ax^2+by^2=1$ is soluble for $x,y \in K$ if and only if b is a norm for $K(\sqrt{a})/K$.

(ii) Deduce that the Hilbert norm residue symbol is bilinear.

(iii) Show that the Hilbert norm residue symbol is non-degenerate by computing it on a basis for $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$. (You should split into the cases $p=2$ and $p>2$.)

10. Show that $J_{\mathbb{Q}} \cong \mathbb{Q}^* \times \prod_p \mathbb{Z}_p^* \times \mathbb{R}_{>0}$.

11. Let L/K be a Galois extension of number fields and $G = \mathrm{Gal}(L/K)$. Define an action of G on J_L, extending the action on L^*, and check that the subgroup of J_L fixed by G is J_K. Deduce that $L^* \cap J_K = K^*$ and hence the natural map $C_K \to C_L$ is injective. Is this last result still true if L/K is not Galois?

12. Let L/K be a Galois extension of number fields with $G = \mathrm{Gal}(L/K)$ cyclic. Show that $\widehat{H}^0(G, J_L) \cong \oplus_{v \in M_K} K_v^*/N_{L_w/K_v}(L_w^*)$. [Recall that a direct sum consists of tuples where all but finitely many elements are the identity.]

13. (i) Let K be a p-adic field. Use the theory of the Herbrand quotient (for G a cyclic group of order n acting trivially on K^*) to show that

$$|K^*/(K^*)^n| = \frac{n|\mu_n(K)|}{|n|_K}$$

where $\mu_n(K)$ is the group of nth roots of unity in K.

(ii) Let K be a number field containing the nth roots of unity. Show that there is a finite set of places S_0 of K such that for all finite sets of places $S \supset S_0$ we have

$$\prod_{v \in S} |K_v^*/(K_v^*)^n| = n^{2|S|} \,.$$

14. Let K be a field with $\mathrm{char}(K) \neq 2$.

(i) Suppose L/K is a Galois extension with $\mathrm{Gal}(L/K) \cong C_2 \times C_2$ and let K_1, K_2, K_3 be the intermediate quadratic extensions. Show that

$$N_{K_1/K}(K_1^*) N_{K_2/K}(K_2^*) = K^* \cap N_{L/K_3}(L^*).$$

[Hint: If $z \in L^*$ with $N_{L/K_3}(z) \in K^*$ use Hilbert's Theorem 90 to construct $x \in K_1^*$ with $z/x \in K_2^*$.]

(ii) Let $a,b,c \in K^*$. Show that $f = X^2 - bY^2 - cZ^2 + acT^2$ is soluble over K if and only if $g = X^2 - bY^2 - cZ^2$ is soluble over $K(\sqrt{ab})$.

15. Let $Q(x,y,z) = ax^2+by^2+cz^2$ where a,b,c are non-zero integers with abc square-free. Show that if Q is soluble over the rationals then $-bc$ is a square mod p for all primes p dividing a, and likewise under all permutations of a,b,c. Under what additional assumptions on a,b,c is the converse true?