MATHEMATICAL TRIPOS PART III (2017–18)

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

1. Let $d \neq 0, 1$ be a square-free integer and consider $K = \mathbb{Q}(\sqrt{d})$. Determine the set of primes p in $\mathbb{Q}$ which ramify in $K/\mathbb{Q}$.

2. Let ζ_n be a primitive n-th root of unity. Recall the Legendre symbol from lectures. Let p be an odd prime.

   (i) By considering the splitting of primes in $\mathrm{Gal}(\mathbb{Q}(\zeta_4)/\mathbb{Q})$, prove the supplementary law
   $$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}.$$
   Deduce, using the form of quadratic reciprocity proved in lectures, the law of quadratic reciprocity in the form (q odd prime)
   $$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}.$$

   (ii) Show that $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\zeta_8)$, and prove the supplementary law
   $$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

3. Let $L'_n = \mathbb{Q}_p(\zeta_n + \zeta_n^{-1}) \subseteq L_n = \mathbb{Q}_p(\zeta_n)$ for $n = mp^e$, $e \geq 1$ and $p \nmid m$. Compute the ramification groups of L'_n in the upper numbering. It might be useful to think of $\mathrm{Gal}(L'_n/\mathbb{Q}_p)$ as a decomposition group inside $\mathrm{Gal}(\mathbb{Q}(\zeta_n + \zeta_n^{-1})/\mathbb{Q})$, and similarly for L_n.

4. Let $K/\mathbb{Q}_p$ be a finite extension and let $|-|$ be the extension to K of the p-adic absolute value $|-|_p$ on $\mathbb{Q}_p$. Consider the exponential series $\exp(T) = \sum_{n=0}^{\infty} \frac{T^n}{n!}$ and the logarithm $\log(1+T) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{T^n}{n}$. Let $x \in K$. Show that $\exp(x)$ converges when $|x| < p^{-1/(p-1)}$ and that $\log(1+x)$ converges when $|x| < 1$.

5. Let $K/\mathbb{Q}_p$ be a finite extension and let $q = \# k_K$. Show, using the previous exercise, that $U_K^{(n)} \cong (\mathcal{O}_K, +)$ as (topological) groups for large enough n, and find an explicit lower bound for n. Deduce that
   $$K^\times \cong \mathbb{Z} \times \mathbb{Z}/(q-1) \times \mathbb{Z}/p^a \times \mathbb{Z}_p^{[K:\mathbb{Q}_p]}$$
   as (topological) groups for some $a \geq 0$, and that any finite index subgroup is open.

6. Show that the Hilbert class field of $K = \mathbb{Q}(\sqrt{-14})$ equals $L = K(\sqrt{2\sqrt{2} - 1})$.

7. Let $p \neq 23$ be a prime. Show that the equation $p = x^2 + xy + 6y^2$ has a solution $(x, y) \in \mathbb{Z}^2$ if and only if $T^2 + 23$ and $T^3 - T + 1$ both have roots in $\mathbb{F}_p$.

8. Let $L = \mathbb{Q}(\zeta_n)$ and $K = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$. Show, using class field theory, that $h_K \mid h_L$, where $h_M = \#Cl_M$ denotes the class number of a number field M.

9. For this exercise, you should use the abstract characterization of the local Artin map $Art_{\mathbb{Q}_p}$ as stated in lectures, and the 'additional properties', but not the explicit form given. Let $p > 2$ (for simplicity, similar results hold for $p = 2$ as well).

   (i) Let $K/\mathbb{Q}_p$ be the unramified extension of degree f. Show that $N(K/\mathbb{Q}_p) = \langle p^f \rangle \times \mathbb{Z}_p^\times$.

   (ii) Let $n \geq 1$ and consider $L = \mathbb{Q}_p(\zeta_{p^n})$. Show that $N_{L/\mathbb{Q}_p}(1 - \zeta_{p^n}) = p$. Show further that $1 + p^n\mathbb{Z}_p \subseteq N(L/\mathbb{Q}_p)$ (*Hint: It might be useful to first do the case $n \geq 1$, then the exponential map to extend the result to general n*). Deduce that $N(L/\mathbb{Q}_p) = \langle p \rangle \times (1 + p^n\mathbb{Z}_p)$.

   (iii) Prove the local Kronecker–Weber theorem, i.e. show that if $K/\mathbb{Q}_p$ is finite abelian, then there exists an m such that $K \subseteq \mathbb{Q}_p(\zeta_{p^m})$.

10. Let $p > 2$ and let $\zeta \in \mathbb{Q}_p$ be a $(p-1)$-th root of unity (not necessarily primitive).

    (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) Let $K/\mathbb{Q}_p$ be a totally ramified extension of degree $p - 1$. Show that $K = \mathbb{Q}_p(\sqrt[p-1]{a})$ for some $a \in \mathbb{Q}_p$, and then that $K = K_\zeta$ for some $(p-1)$-th root of unity ζ.

    (iii) Find the ζ such that $K_\zeta = \mathbb{Q}_p(\zeta_p)$.

11. This exercise aims to deduce the global Kronecker–Weber theorem from the local Kronecker–Weber theorem. Let $K/\mathbb{Q}$ be an abelian extension and let S be the set of primes of $\mathbb{Q}$ which ramify K. Let $p \in S$ and let $\mathfrak{p}$ be a prime of K above p. By the local Kronecker–Weber theorem, we have $K_\mathfrak{p} \subseteq \mathbb{Q}_p(\zeta_{n_p})$ for some $n_p \geq 1$. Let $e_p = v_p(n_p)$ and set $n = \prod_{p \in S} p^{e_p}$. Show that $K(\zeta_n) = \mathbb{Q}(\zeta_n)$, and deduce that $K \subseteq \mathbb{Q}(\zeta_n)$.