Algebraic number theory **LTCC 2008**

Problem Sheet 2

(1) Let $m \neq 1$ be a square-free integer. Compute the discriminant $d_{\mathbb{Q}(\sqrt{m})}$.

(2) Let $m \not\equiv 1 \pmod 4$ be a square-free integer and let p be an odd integer that does not divide m. Let (p) denote the principal ideal of $R_{\mathbb{Q}(\sqrt{m})}$ generated by p. Show that if the congruence $X^2 \equiv m \pmod p$ is solvable then $(p) = P_1P_2$ for two distinct prime ideals P_1 and P_2 of $R_{\mathbb{Q}(\sqrt{m})}$. [Hint: Consider $P_1 = (p, \sqrt{m}+a)$ and $P_2 = (p, \sqrt{m}-a)$ where $a \in \mathbb{Z}$ is a solution of $X^2 \equiv m \pmod p$.]

(3) (a) Let K be an algebraic number field and A a non-zero ideal of R_K. Show that if $\mathbf{N}(A)$ is a prime number then A is a prime ideal.
(b) Give an example of an algebraic number field K and non-zero prime ideal A of R_K such that $\mathbf{N}(A)$ is not a prime number.

(4) Prove that $\lim_{z\to 1+}(z-1)\zeta(z) = 1$ where $z \to 1+$ means that the limit $z \to 1$ is taken over real numbers $z > 1$.

(5) Let $n > 1$ be an integer such that $n \not\equiv 2 \pmod 4$. Show that if n has at least two distinct prime factors then $1 - \zeta_n$ is a unit in $R_{\mathbb{Q}(\zeta_n)}$ [Hint: For every $m > 1$ show that $m = \prod_{i=1}^{m-1}(1 - \zeta_m^i)$. Apply this to $m = n$ and to $m = p^a$ for every prime $p \mid n$ where p^a is the highest power of p dividing n.]

(6) Let $n > 1$ be an integer such that $n \not\equiv 2 \pmod 4$. Show that

$$\mu_{\mathbb{Q}(\zeta_n)} = \begin{cases} \{\pm\zeta_n^i : 0 \leq i \leq n-1\} & \text{if } n \text{ is odd,} \\ \{\zeta_n^i : 0 \leq i \leq n-1\} & \text{if } n \text{ is divisible by 4.} \end{cases}$$

(7) (a) Show that $\mathbb{Q}(\zeta_5)^+ = \mathbb{Q}(\sqrt{5})$.
(b) Compute $R^\times_{\mathbb{Q}(\zeta_5)^+}$, i.e. the group of units of the ring of integers of $\mathbb{Q}(\zeta_5)^+$. [Hint: Use question (7) on Problem Sheet 1 to compute a fundamental unit of $\mathbb{Q}(\sqrt{5})$.]
(c) Compute C^+, i.e. the group of cyclotomic units of $\mathbb{Q}(\zeta_5)^+$.
(d) Use Theorem 11.4 to compute the class number $h_{\mathbb{Q}(\zeta_5)^+}$.

(8) Show that the equation $X^{p-1} = 1$ has $p - 1$ solutions in $\mathbb{Q}_p$.

(9) Prove the following generalisation of Hensel's lemma: Let p be a prime number and $f(X) \in \mathbb{Z}_p[X]$. Suppose that $a_0 \in \mathbb{Z}_p$ satisfies

$$\begin{aligned} f'(a_0) &\equiv 0 \pmod{p^M}, \\ f'(a_0) &\not\equiv 0 \pmod{p^{M+1}}, \\ f(a_0) &\equiv 0 \pmod{p^{2M+1}}, \end{aligned}$$

for some $M \geq 0$. Show that there exists a unique $a \in \mathbb{Z}_p$ such that $f(a) = 0$ and $a \equiv a_0 \pmod{p^{M+1}}$.

(10) Let $f(X) = (X^2-2)(X^2-17)(X^2-34)$. Show that the equation $f(X) = 0$ has solutions in $\mathbb{R}$ and in $\mathbb{Q}_p$ for every p, but has no solutions in $\mathbb{Q}$.