HW #11

ALGEBRAIC NUMBER THEORY, GU4043; INSTRUCTOR: GYUJIN OH

Due Tuesday, April 9 by 11:59pm on Gradescope.

Question 1. Let $L = \mathbb{Q}(\sqrt{3})$.

(1) Show that $h_L = 1$, so that the Hilbert class field of L is $H_L = L$.
(2) Let $K = L(\sqrt{-1})$. Show that every prime ideal $\mathfrak{p} \subset \mathcal{O}_L$ is unramified in K.
(3) Why are (1) and (2) consistent with the global class field theory?

Hint. Compute the conductor $\mathfrak{f}_{K/L}$.

Question 2. In this question, we determine the ray class fields of $\mathbb{Q}$. Let ∞ denote the unique archimedean prime of $\mathbb{Q}$.

(1) Let $m > 1$ is such that $v_2(m) \neq 1$. Show that the kernel of the Artin map
$$\mathrm{Art}^m_{\mathbb{Q}(\zeta_m)/\mathbb{Q}} : J^m_{\mathbb{Q}} \to \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}),$$
is equal to $P^{m\infty}_{\mathbb{Q}}$. Deduce that $\mathbb{Q}(\zeta_m)$ is the ray class field of $\mathbb{Q}$ for modulus $m\infty$. Deduce that $\mathfrak{f}_{\mathbb{Q}(\zeta_m)/\mathbb{Q}} = n\infty$ with $n|m$.
(2) Retaining the same notation as (1), show that $\mathbb{Q}(\zeta_m) \subset \mathbb{Q}(\zeta_n)$. Deduce that $n = m$.
(3) For $m \geq 1$ odd, show that $\mathbb{Q}(\zeta_{2m}) = \mathbb{Q}(\zeta_m)$. Deduce that, for $n \geq 1$,
$$\mathfrak{f}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}} = \begin{cases} 1 & \text{if } n = 1 \\ \frac{n}{2}\infty & \text{if } n \text{ is even, } \frac{n}{2} \text{ is odd} \\ n\infty & \text{otherwise.} \end{cases}$$
(4) For a finite extension $K/\mathbb{Q}_2$, show that the local conductor $\mathfrak{f}_{K/\mathbb{Q}_2}$ cannot be equal to 1.
(5) Using (3) and (4), deduce that the ray class field of $\mathbb{Q}$ for modulus $\mathfrak{m}$ is
$$\mathbb{Q}(\mathfrak{m}) = \begin{cases} \mathbb{Q}(\zeta_n) & \text{if } \mathfrak{m} = n\infty \\ \mathbb{Q}(\zeta_n)^+ := \mathbb{Q}(\zeta_n + \zeta_n^{-1}) & \text{if } \mathfrak{m} = n. \end{cases}$$

Question 3. In this question, we revisit HW7, Question 1, on the primes $p \neq 2, 7$ of the form $p = x^2 + 14y^2$ for some integers $x, y \in \mathbb{Z}$. We have already seen that $\mathrm{Cl}(\mathbb{Q}(\sqrt{-14})) \cong \mathbb{Z}/4\mathbb{Z}$.

(1) Let $K = \mathbb{Q}(\sqrt{-14})$ and $K' = K(\sqrt{2})$. Show that K'/K is an unramified extension (including the archimedean primes).

Hint. Use that $K' = \mathbb{Q}(\sqrt{2}, \sqrt{-7})$ and that 2 splits completely in $\mathbb{Q}(\sqrt{-7})$.

(2) Let $K'' = K'(\sqrt{2\sqrt{2} - 1})$. Using that $(2\sqrt{2} - 1)(-2\sqrt{2} - 1) = -7$, show that $K'' = K'(\sqrt{-2\sqrt{2} - 1})$. Using the discriminant, show that K''/K' is unramified at every prime coprime to 2 (including the archimedean primes).

(3) Note that $2\sqrt{2}-1=(1+\sqrt{2})^2-4$, so that $K''=K'(\alpha)$, where
$$\alpha=\frac{1+\sqrt{2}+\sqrt{2\sqrt{2}-1}}{2},\quad \alpha^2-(1+\sqrt{2})\alpha+1=0.$$
Using the discriminant, show that K''/K' is unramified at every prime.

(4) Show that K''/K is an abelian extension. Deduce that $K''=H_K$.

(5) Show that, for $p\neq 2,7$ a rational prime,
$$p=x^2+14y^2 \text{ for some } x,y\in\mathbb{Z}\Leftrightarrow \left(\frac{-14}{p}\right)=1 \text{ and } X^4+2X^2-7\equiv 0 \pmod{p} \text{ has an integer solution.}$$

Question 4. Let $n>1$ be an odd integer, and let K be a local field of characteristic 0 that contains μ_n. For $a,b\in K^\times$ with $a\neq -b$, show that
$$(a,b)=(a,a+b)(a+b,b).$$

Hint. Let $a+b=c$. Then, we have
$$1=(1-ac^{-1},ac^{-1})=(bc^{-1},ac^{-1}).$$
Use that -1 is an n-th power.

Question 5. Let p be an odd rational prime, and let $K=\mathbb{Q}(\zeta_p)$. Let $\pi=1-\zeta_p$, which generates the unique prime ideal $\mathfrak{p}=(\pi)$ lying over p (more precisely, $p=\mathfrak{p}^{p-1}$), and define $e_i=1-\pi^i$ for $i\geq 1$.

(1) Using HW9, show that, in $K_\mathfrak{p}$, $(1+\pi^2\mathcal{O}_{K_\mathfrak{p}},\times)\cong(\pi^2\mathcal{O}_{K_\mathfrak{p}},+)$. Deduce that $(\mathcal{O}_{K_\mathfrak{p}}^\times)^p\supset 1+\pi^{p+1}\mathcal{O}_{K_\mathfrak{p}}$.

(2) For $i,j\geq 1$ with $i+j\geq p+1$, use $e_i+\pi^ie_j=e_{i+j}$ and Question 4 to show that $(e_i,e_j)_\mathfrak{p}=1$.

Hint. Using (1), show that e_{i+j} is a p-th power in $K_\mathfrak{p}$. Apply Question 4 to (e_i,π^ie_j).

(3) Show that, if $x\in 1+\pi^i\mathcal{O}_{K_\mathfrak{p}}$, x can be expressed as an infinite product
$$x=e_i^{m_i}e_{i+1}^{m_{i+1}}\cdots,\qquad \text{for some } m_i,m_{i+1},\cdots\in\mathbb{Z}.$$
Here, the above expression means that the sequence $x_i,x_{i+1},\cdots\in\mathcal{O}_{K_\mathfrak{p}}$ defined by
$$x_j:=e_i^{m_i}e_{i+1}^{m_{i+1}}\cdots e_j^{m_j},\quad j\geq i,$$
converges to x.

Hint. Note that $\mathcal{O}_{K_\mathfrak{p}}/\pi\mathcal{O}_{K_\mathfrak{p}}\cong\mathbb{F}_p$ with representatives $\{0,1,\cdots,p-1\}$. Deduce that, if $x\equiv 1+r\pi^i \pmod{\pi^{i+1}}$, $0\leq n\leq p-1$, then $\frac{x}{e_i^{-r}}\equiv 1 \pmod{\pi^{i+1}}$.

(4) Show that for $a,b\in K^\times$ coprime to each other and to p, such that $a,b\equiv 1 \pmod{\pi^{\frac{p+1}{2}}}$, the p-th power residue symbols satisfy
$$\left(\frac{a}{b}\right)=\left(\frac{b}{a}\right).$$