METU, Spring 2018, Math 523.

Exercise Set 9

1. Set $\alpha = \sqrt[3]{5^2 \cdot 7}$ and consider $L = \mathbf{Q}(\alpha)$. (Recall that $\mathcal{O}_L$ has no power basis! In other words there isn't any element $\theta \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathbf{Z}[\theta]$.)

    - Show that $[\mathcal{O}_L : \mathbb{Z}[\alpha]] = 5$ and $[\mathcal{O}_L : \mathbb{Z}[\alpha^2/5]] = 7$.
    - Find the ideal prime decomposition of $p\mathcal{O}_L$ for $p \in \{2, 3, 5, 7\}$.

2. Set $\zeta = \exp(2\pi i/23)$. Consider $L = \mathbf{Q}(\zeta)$ and $K = (\sqrt{-23})$. Recall that $K \subset L$ and $\mathcal{O}_K = \mathbf{Z}[\theta]$ with $\theta = (1 + \sqrt{-23})/2$. Take $\mathfrak{p} = \langle 2, \theta \rangle \subset \mathcal{O}_K$. Let $\mathfrak{P} \subset \mathcal{O}_L$ be a prime ideal lying over $\mathfrak{p}$.

    - Show that $f(\mathfrak{P}|\mathfrak{p}) = 11$. Conclude that $\mathfrak{P} = \langle 2, \theta \rangle \subset \mathcal{O}_L$.
    - Show that $\mathfrak{p}$ is not principal in $\mathcal{O}_K$ whereas $\mathfrak{p}^3 = (\theta - 2)$.
    - Show that $\mathfrak{P}$ is not principal.
    - Show that if 2 is irreducible in the ring $\mathbf{Z}[\zeta]$.
    - Verify that the product

    $$(1 + \zeta^2 + \zeta^4 + \zeta^5 + \zeta^6 + \zeta^{10} + \zeta^{11}) \cdot (1 + \zeta + \zeta^5 + \zeta^6 + \zeta^7 + \zeta^9 + \zeta^{11})$$

    is divisible by 2 in the ring $\mathbf{Z}[\zeta]$.
    - Show that $\mathbf{Z}[\zeta]$ is not a UFD.

3. Let $L = \mathbf{Q}(\sqrt{2}, \sqrt{3})$. You are given that $\mathcal{O}_L = \mathbf{Z}[\alpha]$ where $\alpha = (\sqrt{2} + \sqrt{6})/2$.

    - Show that $L/\mathbf{Q}$ is normal and $\mathrm{Gal}(L/\mathbf{Q}) \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.
    - Prove that the fields $K_1 = \mathbf{Q}(\sqrt{2}), K_2 = \mathbf{Q}(\sqrt{3})$ and $K_3 = \mathbf{Q}(\sqrt{6})$ are all proper subfields of L.
    - Find a prime ideal $\mathfrak{P} \subset \mathcal{O}_L$ lying over p (by giving generators) for each prime $p \in \{2, 3, 5\}$. What is the inertia index $e(\mathfrak{P}|p\mathbf{Z})$ and residual degree $f(\mathfrak{P}|p\mathbf{Z})$?
    - Determine $\mathfrak{p}_i = \mathfrak{P} \cap K_i$ for each $i \in \{1, 2, 3\}$. (There are 9 cases in total.)
    - Let β be an element in $\mathcal{O}_L$ such that $L = \mathbf{Q}(\beta)$. Suppose that $f(x) = \min(\beta, \mathbf{Q})$. Does there exist a prime p such that the reduction of $f(x)$ modulo p is irreducible in $(\mathbf{Z}/p\mathbf{Z})[x]$?