Math 204A, Fall 2017

Algebraic Number Theory, HW 5

Due Wednesday November 15th 2017 at noon/after class

From [RME]:

- Section 5.6: *15, 16, 18* (page 67)

Problem A. Let $p > 2$ be a prime and $n \geq 1$. Choose a primitive p^n–th root of unity ζ. (In other words $\zeta^{p^n} = 1$ but $\zeta^{p^{n-1}} \neq 1$.)

(a) Explain why $\Phi_p(X^{p^{n-1}})$ is the minimal polynomial of ζ over $\mathbb{Q}$.

(b) Prove the formula

$$\Delta(\zeta) = \Delta(1, \zeta, \ldots, \zeta^{\phi(p^n)-1}) = (-1)^{\frac{1}{2}\phi(p^n)} \cdot p^{p^{n-1}(pn-n-1)}.$$

(c) Conclude that $\mathcal{O}_{\mathbb{Q}(\zeta)} = \mathbb{Z}[\zeta]$ and $d_{\mathbb{Q}(\zeta)} = \Delta(\zeta)$.

Problem B. Let K be a number field of degree n over $\mathbb{Q}$. Every ideal class in Cl_K contains a nonzero ideal $I \subset \mathcal{O}_K$ with $N(I) \leq M'_K$ where

$$M'_K = \prod_{i=1}^{n} \sum_{j=1}^{n} |\sigma_i(\alpha_j)|.$$

(Here the σ_i denote the embeddings $K \hookrightarrow \mathbb{C}$ and $\{\alpha_1, \ldots, \alpha_n\}$ is an integral basis.) Do not show this. Later we will prove the same statement with M'_K replaced by the *Minkowski* constant

$$M_K = \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}.$$

(Here s has the usual meaning; the number of conjugate pairs of non-real embeddings $K \hookrightarrow \mathbb{C}$.)

(a) Let $K = \mathbb{Q}(\sqrt{d})$ for a square-free integer d. Calculate M_K and M'_K (for the natural choice of basis for $\mathcal{O}_K$).

(b) Compute the constants M_K and M'_K for the field $K = \mathbb{Q}(\sqrt[3]{2})$ (take the $\mathbb{Z}$-basis for $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}]$ to be $\{1, \alpha, \alpha^2\}$ where $\alpha = \sqrt[3]{2}$).

(c) Find the class number of $\mathbb{Q}(\sqrt[3]{2})$. (You may use the Minkowski bound.)

Problem C.

(a) Let $d \in \mathbb{Z}$ be squarefree and $K = \mathbb{Q}(\sqrt{d})$. Write $(2) = 2\mathcal{O}_K$ as a product of prime ideals. (Discuss each case $d \equiv 1, 2, 3, 5, 6, 7 \pmod 8$ separately.)

(b) Which primes p split in $\mathbb{Q}(\sqrt{-11})$? State your answer as certain congruence conditions on p modulo 11. Which primes p are inert? Ramified?