Math 620 – Fall 2024 – Harry Tamvakis
PROBLEM SET 4 – Due October 24, 2024

Let K be a number field and $\mathcal{O}$ be its ring of integers. The next two problems will prove that a rational prime p ramifies in K if and only if p divides the discriminant d_K.

1) (a) Let $p\mathcal{O}$ have prime factorization $\prod_i P_i^{e_i}$. Prove that p ramifies if and only if the ring $\mathcal{O}/p\mathcal{O}$ has non-zero nilpotent elements.

(b) Let $\omega_1, \ldots, \omega_n$ be an integral basis of $\mathcal{O}$, used to represent the elements λ of $\mathcal{O}$ by integer matrices $A(\lambda)$. Reduction of the entries of $A(\lambda)$ mod p gives matrices representing elements of $\mathcal{O}/p\mathcal{O}$. Prove that a nilpotent element (or matrix) has trace zero.

(c) Suppose that $A(\lambda)$ is nilpotent mod p. Then $A(\omega_i\lambda)$ will be nilpotent mod p for all $i \in [1, n]$. By expressing λ in terms of the ω_i and computing $\mathrm{Tr}(A(\lambda\omega_i))$, show that if λ is nilpotent mod p and $\lambda \notin p\mathcal{O}$, then $d_K \equiv 0 \pmod{p}$, hence p divides d_K.

2) Assume that p does not ramify in K.

(a) Prove that $\mathcal{O}/p\mathcal{O}$ is isomorphic to a finite product $\prod_i F_i$ of finite fields F_i of characteristic p.

(b) Let $\pi_i : \mathcal{O} \to F_i$ be the composition of the canonical map $\mathcal{O} \to \mathcal{O}/p\mathcal{O}$ with the projection $\mathcal{O}/p\mathcal{O} \to F_i$. Show that the trace form

$$T_i(x, y) := \mathrm{Tr}_{F_i/\mathbb{F}_p}(\pi_i(x)\pi_i(y))$$

is non-degenerate. Deduce that $\sum_i T_i$ is also nondegenerate.

(c) We have $d_K = \mathrm{Tr}(\omega_i\omega_j)$. Reducing the entries of the matrix mod p, we obtain the matrix of the reduced bilinear form T_0 on the $\mathbb{F}_p$-vector space $\mathcal{O}/p\mathcal{O}$. Show that T_0 coincides with $\sum_i T_i$, hence T_0 is non-degenerate. Deduce that $d_K \neq 0$ mod p, so p does not divide d_K.

The next three problems give a direct proof that the discriminant Δ_n of the n-th cyclotomic polynomial $\Phi_n(x)$ satisfies

$$\Delta_n = \frac{(-1)^{\varphi(n)/2} n^{\varphi(n)}}{\prod_{p|n} p^{\varphi(n)/(p-1)}}. \qquad (1)$$

3) (a) The *Möbius function* μ is defined by

$$\mu(n) := \begin{cases} 1 & \text{if } n = 1, \\ (-1)^k & \text{if } n = p_1 \cdots p_k, \\ 0 & \text{if } n = p^2 m \end{cases}$$

where $p, p_1, \ldots, p_k$ are rational primes. Prove that if $F(n) = \sum_{d|n} f(d)$, then

$$f(n) = \sum_{d|n} \mu(d) F(n/d) = \sum_{d|n} \mu(n/d) F(d).$$

(b) Prove the formula

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}. \tag{2}$$

4) Let p be a rational prime. Prove that

$$\Phi_{mp}(x) = \begin{cases} \Phi_m(x^p) & \text{if } \gcd(m,p) = p, \\ \Phi_m(x^p)/\Phi_m(x) & \text{if } \gcd(m,p) = 1. \end{cases}$$

Deduce that

$$\Phi_n(1) = \begin{cases} p & \text{if } n = p^k, \\ 1 & \text{if } n \neq p^k. \end{cases}$$

5) (a) Let ζ be a root of $\Phi_n(x)$. By differentiating (2), show that

$$\Phi_n'(\zeta) = n\zeta^{n-1} \prod_{d|n, d\neq n} (\zeta^d - 1)^{\mu(n/d)}.$$

Deduce that the discriminant Δ_n of $\Phi_n(x)$ satisfies

$$|\Delta_n| = \prod_{\zeta} |\Phi_n'(\zeta)| = n^{\varphi(n)} \prod_{d|n, d\neq n} \prod_{\zeta} |1 - \zeta^d|^{\mu(n/d)}.$$

(b) Prove that

$$\prod_{\zeta} (1 - \zeta^d) = \left(\Phi_{n/d}(1)\right)^{\varphi(n)/\varphi(n/d)}.$$

(c) Deduce that

$$|\Delta_n| = \frac{n^{\varphi(n)}}{\prod_{p|n} p^{\varphi(n)/(p-1)}}.$$

Finally, apply Problem 1 on Homework #2 to prove equation (1).