Math 80220 Algebraic Number Theory
Problem Set 9

Andrei Jorza

due Friday, April 13

Caution: In many places, most notably Sage, the higher ramification groups are shifted left by 1: the -1 group being D, the 0 group being I, the 1 group being P, etc. It is a constant source of annoyance.

1. Suppose $K = \mathbb{Q}(\alpha)$ is a number field with α algebraic with minimal polynomial $f(X)$. Show that if the discriminant of $1, \alpha, \ldots, \alpha^{n-1}$ is square-free then $\mathcal{O}_K = \mathbb{Z}[\alpha]$. [Hint: Write $1, \alpha, \ldots, \alpha^{n-1}$ in terms of an integral basis.]

2. Let α be a root of $f(X) = X^3 - X - 1$.
   (a) Show that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.
   (b) Compute $\mathcal{D}_{K/\mathbb{Q}}$ and determine explicitly all ramified primes $\mathfrak{q}/\mathfrak{p}$ of $K/\mathbb{Q}$.

3. (a) Let K be a number field. Show that $||\mathcal{D}_{K/\mathbb{Q}}|| = |\operatorname{disc}(K)|$. [Hint: Use volumes.]
   (b) Suppose $M/L/K$ are number fields. Show that $\mathcal{D}_{M/K} = \mathcal{D}_{M/L}\mathcal{D}_{L/K}$.

4. Let $K = \mathbb{Q}(\zeta_{p^n})$ with ring of integers $\mathcal{O}_K = \mathbb{Z}[\zeta_{p^n}]$. Recall from class that p is totally ramified in K and $p\mathcal{O}_K = \mathfrak{q}^{\varphi(p^n)}$ where $\mathfrak{q} = (\zeta_{p^n} - 1)$.
   (a) Suppose $p \nmid b$ and $1 \leq r \leq n$. Show that $v_\mathfrak{q}(\zeta_{p^n}^{p^r b} - 1) = \varphi(p^n)/\varphi(p^{n-r}) = p^r$. [Hint: Look at how p factors in the intermediary extension $\mathbb{Q}(\zeta_{p^{n-r}})$ and in K itself. It should work out in a couple of lines.]
   (b) Show that $D_{\mathfrak{q}/p,0} = D_{\mathfrak{q}/p,1} \cong (\mathbb{Z}/p^n\mathbb{Z})^\times$ and for $s \geq 0$
   $$D_{\mathfrak{q}/p,p^s+1} = \ldots = D_{\mathfrak{q}/p,p^{s+1}} \cong 1 + p^{s+1}(\mathbb{Z}/p^n\mathbb{Z}).$$
   (c) Show directly that $\mathcal{D}_{K/\mathbb{Q}} = (\Phi'_{p^n}(\zeta_{p^n})) = \mathfrak{q}^{p^{n-1}(np-n-1)}$ and verify directly that
   $$v_\mathfrak{q}(\mathcal{D}_{K/\mathbb{Q}} = \sum_{\ell \geq 1}(|D_{\mathfrak{q}/p,\ell}| - 1).$$

5. Let $p \neq q$ be two odd primes. From algebra you know that if we write $p^* = (-1)^{(p-1)/2}p$ then $\mathbb{Q}(\sqrt{p^*}) \subset \mathbb{Q}(\zeta_p)$. (E.g., $\mathbb{Q}(\sqrt{\operatorname{disc}(K)}) = \mathbb{Q}(\sqrt{p^*}) \subset K$.)
   (a) Show that q splits in $\mathbb{Q}(\sqrt{p^*})$ if and only if q is a product of evenly many prime ideals of $\mathbb{Q}(\zeta_p)$.
   (b) Deduce the following equality of Legendre symbols: $\left(\dfrac{p^*}{q}\right) = \left(\dfrac{q}{p}\right)$. [Hint: Use your knowledge of how a prime splits in an extension using factorizations of polynomials modulo primes.]
   (c) Show quadratic reciprocity:
   $$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$
   [Hint: Use that $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ and the multiplicativity of Legendre symbols.]