Exercise Sheet 11
Algebraic Number Theory

December 2, 2025

Exercise 1. Let A a dedekind Ring that satisfies Hypothesis 3.2 in the notes and $K = \mathrm{Frac}(A)$. Let $L/E/K$ be finite galois extensions and $\mathfrak{p} \subset A$ be unramified in L. Let $O_{L/K}$ be the intragal closure of A in L. Let $\mathfrak{P} = \mathfrak{P}_L \subset O_{L/K}$ be a prime ideal above $\mathfrak{p}$ and $\mathfrak{P}_E = \mathfrak{P} \cap E$. Show that the following holds for the Frobenius automorphism:

1. A prime $\mathfrak{p}$ is said to split completely in L if for each prime $\mathfrak{P}$ of L dividing $\mathfrak{p}$ we have $e_{\mathfrak{P}/\mathfrak{p}} = f_{\mathfrak{P}/\mathfrak{p}} = 1$. Show that $\mathfrak{p}$ splits completely in L if and only if
$$(\mathfrak{P}, L/K) = 1.$$
2. The Frobenius behaves well with respect to restriction, i.e.
$$(\mathfrak{P}_E, E/K) = (\mathfrak{P}_L, L/K)|_E.$$
3. Suppose E_1, E_2 are Galois over K, $K = E_1 \cap E_2$ and that $L = E_1E_2$. What is the image of $(\mathfrak{P}_L, E_1E_2/K)$ under the isomorphism $\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(E_1/K) \times \mathrm{Gal}(E_2/K)$

Exercise 2. We use the notation as in Chapter 4 of the lecture notes. Given $\mathfrak{a} \subset O_K$ an ideal, its ideal norm $\mathrm{Nr}_{K/Q}(\mathfrak{a}) \subset A$ is the ideal generated by the norms of the elements of $\mathfrak{a}$. Prove that
$$\mathrm{Nr}(\mathfrak{a}) = |A/\,\mathrm{Nr}_{K/Q}(\mathfrak{a})|.$$

Exercise 3. Let $\mathfrak{f} = \mathfrak{a}.\mathfrak{b}^{-1}$ be a fractional ideal. We define its norm as a rational number $\mathrm{Nr}(\mathfrak{f}) = \mathrm{Nr}(\mathfrak{a})\,\mathrm{Nr}(\mathfrak{b})^{-1}$. Show that this is well defined and multiplicative.

Exercise 4. Let $K/\mathbb{Q}$ be a number field of degree d with ring of integers O_K. In this exercise, we want to find an upper bound for the quantity
$$\#\{\mathfrak{a} \text{ an ideal of } O_K : N(\mathfrak{a}) \leq X\}.$$

1. Let $r_K : \mathbb{N} \to \mathbb{C}$ be the arithmetic function given by
$$r_K(n) := \#\{\mathfrak{a} \text{ an ideal of } O_K : N(\mathfrak{a}) = n\}.$$
Prove that r_K is multiplicative, i.e. that
$$r_K(n_1n_2) = r_K(n_1)r_K(n_2) \quad \text{for} \quad (n_1, n_2) = 1.$$
2. Show that, for any prime p and any positive integer ℓ, we have the bound
$$r_K(p^\ell) \leq (\ell + 1)^d.$$
3. (difficult) Let $\epsilon > 0$. Show that there exists a constant $C_\epsilon > 0$ such that
$$r_K(n) \leq C_\epsilon n^\epsilon \quad \text{for all} \quad n \in \mathbb{N}.$$
4. Conclude that for any $\epsilon > 0$ there exists a constant $C_\epsilon > 0$ such that
$$\#\{\mathfrak{a} \text{ an ideal of } O_K : N(\mathfrak{a}) \leq X\} \leq C_\epsilon X^{1+\epsilon}.$$