Exercise Sheet 11
Algebraic Number Theory

December 21, 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 $\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(E_1/K) \times \mathrm{Gal}(E_2/K)$

Solution. 1. The definition of $(\mathfrak{P}, L/K)$ implies that it generates the decomposition group. However $\mathfrak{p}$ splits completely if and only if $|D_{\mathfrak{P}}| = 1 = ef$ which is equivalent to the generator of the decomposition group being 1.

2. For $\tau \in D_{L/K}(\mathfrak{P}_L)$ we have $\tau|_E(\mathfrak{P}_E) = \tau|_E(\mathfrak{P}_L \cap E) \subset \mathfrak{P}_L \cap E$, the latter inclusion follows from the fact that E/K is Galois and $\tau(\mathfrak{P}_L) \subset \mathfrak{P}_L$. Therefore $D_{L/K}(\mathfrak{P}_L)|_E \subset D_{E/K}(\mathfrak{P}_E) \subset \mathrm{Gal}(E/K)$. The Frobenius automorphism $\sigma_E = (\mathfrak{B}_E, E/K)$ is uniquely characterized by the following property:
$$\sigma_E(x) \equiv x^{N(\mathfrak{p})} \pmod{\mathfrak{P}_E} \text{ for all } x \in \mathcal{O}_{E/K}.$$
Since $\sigma_L = (\mathfrak{P}_L, L/K)$ is Frobenius we have
$$\sigma_L(x) \equiv x^{N(\mathfrak{p})} \,(\mathrm{mod}\, \mathfrak{P}_L),$$
hence for $x \in O_{E/K}$ we have
$$\sigma_L(x) - x^{N(\mathfrak{p})} \in E \cap \mathfrak{P}_L = \mathfrak{P}_E,$$
by uniqueness, $\sigma_L|_E = \sigma_E$, as we wanted.

3. Follows directly from part b).

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
$$\mathrm{Nr}(\mathfrak{a}) = |A/\mathrm{Nr}_{K/Q}(\mathfrak{a})|.$$

Solution. First consider a prime ideal $\mathfrak{P} \subset O_K$ and a non negative integer $l \geq 0$. From the multiplicativity of the norm we deduce

$$\mathrm{Nr}_{K/Q}(\mathfrak{P}^l) = (\mathrm{Nr}_{K/Q}(\mathfrak{P}))^l.$$

Let $\mathfrak{p} = \mathfrak{P} \cap A$ (recall that A is a PID, so that $\mathfrak{p} = (p)$ for some $p \in A$). Recall that $\mathrm{Nr}(\mathfrak{P}) = |O_K/\mathfrak{P}| = |A/\mathfrak{p}|^{f_{\mathfrak{P}/\mathfrak{p}}}$. We claim that

$$\mathrm{Nr}_{K/Q}(\mathfrak{P}) = \mathfrak{p}^{f_{\mathfrak{P}}}, \tag{1}$$

where as usual $f_{\mathfrak{P}}$ is the inertia degree of $\mathfrak{P}$ (over $\mathfrak{p}$, we omit it from notation for this exercise) First, note that

$$\mathfrak{p}^{[K:Q]} = \mathrm{Nr}_{K/Q}(\mathfrak{p}) \subset \mathrm{Nr}_{K/Q}(\mathfrak{P}) \subset \mathfrak{p}.$$

Hence, to conclude our claim, it suffices to show that

$$(\mathrm{Nr}_{K/Q}(\mathfrak{P}))A_{\mathfrak{p}} = \mathfrak{p}^{f_{\mathfrak{P}}} A_{\mathfrak{p}}.$$

By the properties of localization we have

$$(\mathrm{Nr}_{K/Q}(x))A_{\mathfrak{p}} = \mathrm{Nr}_{K_{\mathfrak{p}}/Q_{\mathfrak{p}}}(x)A_{\mathfrak{p}},$$

for any $x \in K$.

Let $x \in \mathfrak{P}$, then by Proposition 4.1 we have

$$|A_{\mathfrak{p}}/(\mathrm{Nr}_{O_{K,\mathfrak{p}}/A_{\mathfrak{p}}}(x))| = |O_{K,\mathfrak{p}}/xO_{K,\mathfrak{p}}|$$

and $|A/\mathfrak{p}|^{f_{\mathfrak{P}}} = |O_{K,\mathfrak{p}}/\mathfrak{P}O_{K,\mathfrak{p}}| \mid |O_{K,\mathfrak{p}}/xO_{K,\mathfrak{p}}|$, where we used that $O_{K,\mathfrak{p}}/\mathfrak{P}O_{K,\mathfrak{p}} \simeq O_K/\mathfrak{P}$. It follows that $v_{\mathfrak{p}}(\mathrm{Nr}_{O_{K,\mathfrak{p}}/A_{\mathfrak{p}}}(x)) \geq f_{\mathfrak{P}}$ and since x was arbitrary we see $\mathrm{Nr}_{K/Q}(\mathfrak{P})_{\mathfrak{p}} \subset \mathfrak{p}^{f_{\mathfrak{P}}} A_{\mathfrak{p}}$. For the latter inclusion we need slightly more work. By the Chinese remainder Theorem, we have an isomorphism

$$O_K \xrightarrow{\sim} \prod_{\substack{\mathfrak{Q} \in \mathrm{spec}_{\mathfrak{p}}\, O_K \\ \mathfrak{Q} \neq \mathfrak{P}}} O_K/\mathfrak{Q} \times O_K/\mathfrak{P}^2.$$

Let $x \in \mathfrak{P} \smallsetminus \mathfrak{P}^2$ and let $x_0 \in O_K$ be so that

$$\begin{aligned} x_0 &\equiv 1 \,(\mathrm{mod}\, \mathfrak{Q}) \qquad \mathfrak{P} \neq \mathfrak{Q} \in \mathrm{spec}_{\mathfrak{p}}\, O_K \\ x_0 &\equiv x \,(\mathrm{mod}\, \mathfrak{P}^2). \end{aligned}$$

Then we have

$$O_{K,\mathfrak{p}}/xO_{K,\mathfrak{p}} = O_{K,\mathfrak{p}}/\mathfrak{P}O_{K,\mathfrak{p}}.$$

Again, by Proposition 4.1 we have

$$|A_{\mathfrak{p}}/\,\mathrm{Nr}_{O_{K,\mathfrak{p}}/A_{\mathfrak{p}}}(x)| = |O_{K,\mathfrak{p}}/xO_{K,\mathfrak{p}}|.$$

Hence, we get

$$|A_{\mathfrak{p}}/\,\mathrm{Nr}_{O_{K,\mathfrak{p}}/A_{\mathfrak{p}}}(x)| = |A/\mathfrak{p}|^{f_{\mathfrak{P}}}$$

and we conclude that $N_{K/Q}(\mathfrak{P})A_{\mathfrak{p}} = \mathfrak{p}^{f_{\mathfrak{P}}} A_{\mathfrak{p}}$ and so the desired claim (1)

Now it is easy to conclude. For prime powers we have

$$\mathrm{Nr}(\mathfrak{P}^l) = \mathrm{Nr}(\mathfrak{P})^l = |A/\,\mathrm{Nr}_{K/Q}(\mathfrak{P})|^l = |A/\,\mathrm{Nr}_{K/Q}(\mathfrak{P})^l| = |A/\,\mathrm{Nr}_{K/Q}(\mathfrak{P}^l)|.$$

The general case follows by the Chinese remainder theorem.

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.

Solution. Multiplicativity follows from the mulitplicativity of the norm on ideals. To show that it is well defined first note that the norm map is non-degenerate and therefore $\mathrm{Nr}(\mathfrak{b}) \neq 0$. Now consider $\mathfrak{f} = \mathfrak{a}\mathfrak{b}^{-1} = \mathfrak{a}'\mathfrak{b}'^{-1}$. Then we have $\mathfrak{a}\mathfrak{b}' = \mathfrak{a}'\mathfrak{b}$ and hence $\mathrm{Nr}(\mathfrak{a}\mathfrak{b}') = \mathrm{Nr}(\mathfrak{a}'\mathfrak{b})$. Therefore we have

$$\begin{aligned}\mathrm{Nr}(\mathfrak{f}) &= \mathrm{Nr}(\mathfrak{a})\,\mathrm{Nr}(\mathfrak{b})^{-1} = \mathrm{Nr}(\mathfrak{a})\,\mathrm{Nr}(\mathfrak{b}')\,\mathrm{Nr}(\mathfrak{b}')^{-1}\,\mathrm{Nr}(\mathfrak{b})^{-1} \\ &= \mathrm{Nr}(\mathfrak{a}')\,\mathrm{Nr}(\mathfrak{b})\,\mathrm{Nr}(\mathfrak{b}')^{-1}\,\mathrm{Nr}(\mathfrak{b})^{-1} = \mathrm{Nr}(\mathfrak{a}')\,\mathrm{Nr}(\mathfrak{b}')^{-1}.\end{aligned}$$

Hence the norm is well defined.

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

   $$r_K(n_1 n_2) = r_K(n_1) r_K(n_2) \quad \text{for} \quad (n_1, n_2) = 1.$$

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

   $$\#\{\mathfrak{a} \text{ an ideal of } O_K : N(\mathfrak{a}) \leq X\} \leq C_\epsilon X^{1+\epsilon}.$$

Solution. 1. Let $n_1, n_2 \in \mathbb{N}$ be positive coprime integers. Define the set

$$\mathfrak{S}(n) := \{\text{ideals } \mathfrak{a} \subset O_K : \mathrm{Nr}(a) = n\},$$

and consider the map

$$g : \begin{array}{c}\mathfrak{S}(n_1) \times \mathfrak{S}(n_2) \to \mathfrak{S}(n_1 n_2) \\ (\mathfrak{a}, \mathfrak{b}) \mapsto \mathfrak{a}\mathfrak{b}\end{array}.$$

We want to show that this map is bijective by constructing an inverse function $h : \mathfrak{S}(n_1 n_2) \to \mathfrak{S}(n_1) \times \mathfrak{S}(n_2)$. Let $\mathfrak{c} \in \mathfrak{S}(n_1 n_2)$ with prime decomposition

$$\mathfrak{c} = {\mathfrak{p}_1}^{e_1} \cdots {\mathfrak{p}_r}^{e_r}.$$

Remember that the norm of a prime ideal is always some power of a prime number. Thus we can factor $\mathfrak{c}$ as follows,

$$\mathfrak{c} = \mathfrak{c}_1 \mathfrak{c}_2 \qquad \text{with} \qquad \mathfrak{c}_1 := \prod_{\substack{i=1 \\ \mathrm{Nr}(\mathfrak{p}_i) | n_1}}^{r} {\mathfrak{p}_i}^{e_i} \quad \text{and} \quad \mathfrak{c}_2 := \prod_{\substack{i=1 \\ \mathrm{Nr}(\mathfrak{p}_i) | n_2}}^{r} {\mathfrak{p}_i}^{e_i}.$$

By construction, we also have $\mathrm{Nr}(\mathfrak{c}_1) = n_1$ and $\mathrm{Nr}(\mathfrak{c}_2) = n_2$. We then define

$$h(\mathfrak{c}) := (\mathfrak{c}_1, \mathfrak{c}_2).$$

It can be checked easily that the function h thus defined is indeed the inverse of g.

Now, we have

$$r_K(n_1 n_2) = |\mathfrak{S}(n_1 n_2)| = |\mathfrak{S}(n_1) \times \mathfrak{S}(n_2)| = |\mathfrak{S}(n_1)||\mathfrak{S}(n_2)| = r_K(n_1) r_K(n_2),$$

which is what we wanted to prove.

2. Let p be a prime, and let
$$pO_K = {\mathfrak{p}_1}^{e_1} \cdots {\mathfrak{p}_r}^{e_r}$$
be the prime decomposition of pO_K. As in exercise 2 the norms of the prime ideals $\mathfrak{p}_i$ are all powers of p, and more precisely
$$\mathrm{Nr}(\mathfrak{p}_i) = p^{f_i} \quad \text{with} \quad f_i := [O_K/\mathfrak{p}_i : \mathbb{F}_p].$$
On the other hand, all ideals in O_K whose norm is a power of p must be a product of the prime ideals above p, that is, a product of the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. Thus, we have
$$\mathfrak{S}(p^\ell) = \{{\mathfrak{p}_1}^{\ell_1} \cdots {\mathfrak{p}_r}^{\ell_r} \in O_K : f_1\ell_1 + \ldots + f_r\ell_r = \ell\},$$
where $\mathfrak{S}(n)$ was defined in 1. Hence
$$\begin{aligned} r_k(p^\ell) &= \#\{(\ell_1, \ldots, \ell_r) \in \mathbb{N}^r : f_1\ell_1 + \ldots + f_r\ell_r = \ell\} \\ &\leq \#\{(\ell_1, \ldots, \ell_d) \in \mathbb{N}^d : \ell_1 + \ldots + \ell_d = \ell\} \\ &\leq \#\{(\ell_1, \ldots, \ell_d) \in \mathbb{N}^d : \ell_1, \ldots, \ell_d \leq \ell\} \\ &= (\ell+1)^d, \end{aligned}$$
which is exactly the upper bound we wanted to show.

3. Let $\epsilon > 0$. Let P_ϵ be the set defined as
$$P_\epsilon := \{p \text{ prime} \mid p \leq e^{\frac{d}{\epsilon}}\}.$$
By the definition of P_ϵ and by the well-known inequality $\ell + 1 \leq e^\ell$, which holds for all $\ell \in \mathbb{N}$, we have that
$$\frac{(\ell+1)^d}{p^{\epsilon\ell}} \leq 1 \qquad \text{for all} \quad p \notin P_\epsilon \quad \text{and} \quad \ell \in \mathbb{N}.$$
Next, we define the positive real number M_ϵ as follows,
$$M_\epsilon := \max_{\lambda \in [0,\infty)} \frac{(\lambda+1)^d}{2^{\epsilon\lambda}}.$$
Now, given a positive integer n with prime decomposition
$$n = {p_1}^{\ell_1} \cdots {p_r}^{\ell_r},$$
it follows from the results proven in 1 and 2 that
$$\frac{r_K(n)}{n^\epsilon} \leq \prod_{i=1}^{r} \frac{(\ell_i+1)^d}{{p_i}^{\epsilon\ell_i}} \leq \prod_{\substack{i=1 \\ p_i \in P_\epsilon}}^{r} \frac{(\ell_i+1)^d}{{p_i}^{\epsilon\ell_i}} \leq \prod_{\substack{i=1 \\ p_i \in P_\epsilon}}^{r} \frac{(\ell_i+1)^d}{2^{\epsilon\ell_i}} \leq {M_\epsilon}^{|P_\epsilon|}.$$
Thus
$$r_K(n) \leq C_\epsilon n^\epsilon,$$
where we have set $C_\epsilon := {M_\epsilon}^{|P_\epsilon|}$.

4. Let $\epsilon > 0$. Using the bound shown in 3, we immediately get
$$\#\{\mathfrak{a} \text{ an ideal of } O_K : \mathrm{Nr}(\mathfrak{a}) \leq X\} = \sum_{n \leq X} r_K(n) \leq C_\epsilon \sum_{n \leq X} n^\epsilon \leq C_\epsilon X^{1+\epsilon},$$
where C_ϵ is the same constant that appears in 3.