Exercise Sheet 10
Algebraic Number Theory

November 26, 2025

Exercise 1. The notation and assumptions are as in Chapter III in the lecture notes. Let A be a Dedekind domain with field of fraction Q and let K be a galois extension of Q of degree d and B the integral closure of A in K. We assume Hypothesis 3.2. We furthermore define the inertia field as follows: Let $\mathfrak{P} \in \operatorname{spec}(B)$ non-zero. The inertia field $T_{\mathfrak{P}}$ of $\mathfrak{P}$ is the fixed field of the inertia group of $\mathfrak{P}$, i.e.,

$$T_{\mathfrak{P}} = \{x \in K : \forall \sigma \in I_{\mathfrak{P}} \ \sigma(x) = x\}.$$

Let $e = e_{\mathfrak{p}}, f = f_{\mathfrak{p}}$ and $g = |\operatorname{spec}_{\mathfrak{p}}(B)|$. Complete the diagram below by adding the missing degrees of field extensions, indices of groups and ramification indices and inertia degrees of the ideals.

fields	*groups*	*ideals*	*ramification indices*	*interia degrees*	*residue field*
K	$\{id\}$	$\mathfrak{P}$			$k_{\mathfrak{P}} = B/\mathfrak{P}$
					1
$T_{\mathfrak{P}}$	$I_{\mathfrak{P}}$	$\mathfrak{P}_T = \mathfrak{P} \cap T_{\mathfrak{P}}$			$k_{\mathfrak{P}_T} = (B \cap T_{\mathfrak{P}})/\mathfrak{P}_T$
			1		
$Z_{\mathfrak{P}}$	$D_{\mathfrak{P}}$	$\mathfrak{P}_Z = \mathfrak{P} \cap Z_{\mathfrak{P}}$			$k_{\mathfrak{P}_Z} = (B \cap Z_{\mathfrak{P}})/\mathfrak{P}_Z$
Q	$G = \operatorname{Gal}(K/Q)$	$\mathfrak{p} = \mathfrak{P} \cap A$			$k_{\mathfrak{p}} = A/\mathfrak{p}$

Exercise 2. Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field (d square free integer). Let D be the discriminant of K, we recall (Exercise Sheet 5) that that $D = 4d$ if $d \equiv 2, 3 \pmod 4$ and $D = d$ if $d \equiv 1 \pmod 4$.

The goal of this exercise is to prove that K is a subfield of the cyclotomic field $\mathbb{Q}(\zeta_{|D|})$. For an odd prime p we defined in Exercise Sheet 4

$$\tau_p = \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{a}{p}\right) e^{\frac{2\pi a i}{p}}.$$

and we proved that $\tau_p^2 = (-1)^{\frac{p-1}{2}} p$

1. Suppose that d is odd. Let $\tau = \prod_{p|d} \tau_p$, Show that $\tau^2 = \pm d$.
2. Now let d be any square free integer. Show that $\mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}(\zeta_{|D|})$.

Exercise 3 (Quadratic reciprocity)**.** With this exercise we give a proof of Quadratic reciprocity using the cyclotomic extension. Let $p, q \in \mathbb{Z}_{\geq 1}$ be two distinct odd primes.

1. Show that q is unramified in $\mathbb{Q}(\zeta_p)$.

   Hint: see Exercise 4, Exercise Sheet 8.

2. Let $K/\mathbb{Q}$ be the unique quadratic extension contained in $\mathbb{Q}(\zeta_p)$. Show that $K = \mathbb{Q}\left(\sqrt{\left(\frac{-1}{p}\right)p}\right)$.

3. Consider the surjective homomorphism

$$\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q});\ \sigma \mapsto \sigma|_K.$$

   Show that it maps the Frobenius $(q, \mathbb{Q}(\zeta_p)/\mathbb{Q})$ to the Frobenius at $(q, K/\mathbb{Q})$ and that, under the isomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$, its kernel is $\{z^2 \mid z \in \mathbb{F}_p^\times\}$.

4. Deduce the following equivalences

   - q splits in K if and only if $(q, K/\mathbb{Q})$ is trivial.
   - $(q, K/\mathbb{Q})$ is trivial if and only if $\left(\frac{q}{p}\right) = 1$.

5. Show that q splits in K if and only if $\left(\frac{(-1)^{\frac{p-1}{2}}p}{q}\right) = 1$ and conclude the proof of quadratic reciprocity.

Exercise 4 (Minkowski Theorem 2)**.** [1] In this exercise, we prove the Minkowski Theorem 2 with an harmonic analysis approach. We will use the Poisson summation formula for lattices in $\mathbb{R}^n$, which states the following. For every nice enough [2] integrable function $f \in L^1(\mathbb{R})$ and every lattice $\Lambda \subset \mathbb{R}^n$ we have

$$\sum_{\lambda \in \Lambda} f(\lambda) = \mathrm{covol}(\Lambda)^{-1} \sum_{\lambda \in \widehat{\Lambda}} \widehat{f}(\lambda),$$

where $\mathrm{covol}(\Lambda)$ is denoted in the notes as $\mathrm{vol}(\Lambda)$. Here $\widehat{f}$ is the Fourier transform of f and is defined as

$$\widehat{f}(y) = \int_{\mathbb{R}^n} f(x) e^{-2\pi i \langle x, y \rangle}\, \mathrm{d}x, \qquad y \in \mathbb{R}^n,$$

with $\langle\ ,\ \rangle$ being the Euclidean inner product. The set $\widehat{\Lambda} \subset \mathbb{R}^n$ is a lattice and is called dual lattice of Λ, its precise definition will not be relevant for this exercise. One key tool will be the convolution, For $f_1, f_2 \in L^1(\mathbb{R}^n)$ we define the convolution $f_1 * f_2(y) = \int_{\mathbb{R}^n} f(x)g(y-x)\, \mathrm{d}x$. You can check that $f_1 * f_2 \in L^1(\mathbb{R}^n)$.

1. Show that $\widehat{f_1 * f_2} = \widehat{f_1}\ \widehat{f_2}$.

2. Suppose $f_1, f_2 \in C_c(\mathbb{R}^n)$ have compact supports[3] V_1 and V_2 respectively. Show that $\mathrm{supp}(f_1 * f_2) \subset V_1 + V_2$.

3. Suppose that $f \in L^1(\mathbb{R}^n)$ is even, that is $f(x) = f(-x)$ for almost every $x \in \mathbb{R}^n$. Show that $\widehat{f}$ is real valued.

4. Suppose $f \in L^1(\mathbb{R}^n)$ and $h \in C_c^\infty(\mathbb{R}^n)$ (that is, h is smooth and has compact support), show that $f * h \in C^\infty(\mathbb{R}^n)$.

   Hint: Show that $\frac{\mathrm{d}}{\mathrm{d}x}(f * h) = f * \frac{\mathrm{d}}{\mathrm{d}x} h$.

We recall that the Minkowksi second theorem states the following: Let $V \subset \mathbb{R}^n$ be a compact symmetric with respect to 0 convex set and $\Lambda \subset \mathbb{R}^n$ be a lattice. Suppose that $\mathrm{vol}(V) \geq 2^n \mathrm{covol}(\Lambda)$, then $V \cap \Lambda \smallsetminus \{0\} \neq \varnothing$. The idea is to create a function $f \in C_c^\infty(\mathbb{R}^n)$ that approximates the indicator function of V, $\widehat{f} \geq 0$ and then apply the Poisson summation formula to it.

[1] This is taken from a source that I will cite in the solutions

[2] By nice enough we mean that both sides converge absolutely; we will assume that every function that we construct here is nice enough and it is actually not hard to prove if one wants to.

[3] $\mathrm{supp}(f) = \overline{\{x \in \mathbb{R}^n \mid f(x) \neq 0\}}$

5. Let $\omega \in C_c^\infty(\mathbb{R})$ be a smooth, non-negative, even function such that $\mathrm{supp}(\omega) \subset \frac{1}{2}V$.[4] Also normalize ω so that $\int_{\mathbb{R}^n} w(x)\, \mathrm{d}x = 1$. Let $\epsilon > 0$ and $\omega_\epsilon(x) = \frac{1}{\epsilon^n}\omega(\epsilon^{-1}x)$. Show that $g_\epsilon = 1_{\frac{V}{2}} * \omega_\epsilon$ satisfies the following properties:

   - g_ϵ is a smooth, real valued, even function
   - $g_\epsilon \leq 1_{(1+\epsilon)\frac{V}{2}}$.
   - $\int_{\mathbb{R}^n} g_\epsilon(z)\, \mathrm{d}z = \mathrm{vol}(\frac{V}{2}) = \frac{1}{2^n}\,\mathrm{vol}(V)$

6. Let $f_\epsilon = g_\epsilon * g_\epsilon$. Show that $f_\epsilon \leq \frac{\mathrm{vol}(V)}{2^n} 1_{(1+\epsilon)V}$ and $\widehat{f_\epsilon} \geq 0$.

7. By choosing $\epsilon > 0$ appropriately, show the Minkowski second theorem in case $\mathrm{vol}(V) > 2^n\,\mathrm{covol}(\Lambda)$ and conclude as done in class.

[4] You can assume that such a function exists, but why does it exist?