Exercise Sheet 10
Algebraic Number Theory

December 19, 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

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

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 $\mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}(\zeta_{|D|})$.

Solution. 1. Consider τ as defined in the exercise. Then we have

$$\tau^2 = \prod_{p|d} (-1)^{\frac{p-1}{2}} \tau.$$

If $d \equiv 1 \pmod 4$, then the number of $p|d$ so that $p \equiv 3 \mod 4$ is even, and so $\prod_{p|d}(-1)^{\frac{p-1}{2}} = 1$.
If $d \equiv 3 \pmod 4$, then the number of $p|d$ so that $p \equiv 3 \pmod 4$ is odd and so $\prod_{p|d}(-1)^{\frac{p-1}{2}} = -1$.

2. First assume that $d \equiv 1 \pmod 4$, so that $d = D$. Then $\tau^2 = d$. Also notice that $\tau \in \mathbb{Q}(\{\zeta_p \mid p|d\}) \subset \mathbb{Q}(\zeta_{|D|})$. Hence d is a square in $\mathbb{Q}(\zeta_{|D|})$, that is $\mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}(\zeta_{|D|})$.

   Now suppose $d \equiv 3 \pmod 4$. Then $\tau^2 = -d$. In this case however $D = 4d$ and, since $4|D$, we see that $i \in \mathbb{Q}(\zeta_{|D|})$. Hence $(i\tau)^2 = d$ and again we deduce that $\mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}(\zeta_{|D|})$.

   Suppose now that $d \equiv 2 \pmod 4$. Then $\frac{d}{2}$ is either $\equiv 1 \pmod 4$ or $\equiv 3 \pmod 4$. In the first case, we set $D^* = \frac{d}{2}$ and in the latter case, we set $D^* = 2d$. Then by the same argument as before, we have that
   $$\mathbb{Q}(\sqrt{d/2}) \subset \mathbb{Q}(\zeta_{|D^*|}) \subset \mathbb{Q}(\zeta_{|D|}),$$
   since $D^*|D$. We also have
   $$\sqrt{2} = e^{\pi i/4} + e^{-\pi i/4} \in \mathbb{Q}(\zeta_8).$$
   Notice that $8|D = 4d$ and so $\mathbb{Q}(\zeta_8) \subset \mathbb{Q}(\zeta_{|D|})$ and we deduce again $\mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}(\zeta_{|D|})$.

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.

Solution. 1. From Exercise Sheet 8, Exercise 4 we know that the discriminant of $\mathbb{Q}(\zeta_p)$ is divisible only by p. Hence if $q \neq p$, then q is unramified in $\mathbb{Q}(\zeta_p)$.

2. Recall τ_p from the previous exercise. Then $\tau_p^2 = \left(\frac{-1}{p}\right)p$ and $\tau_p \in \mathbb{Q}(\zeta_p)$. In particular, we deduce that
   $$\mathbb{Q}\left(\sqrt{(\frac{-1}{p})p}\right) \subset \mathbb{Q}(\zeta_p).$$
   The Galois group of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is cyclic, and so it has a unique subgroup of index 2. Hence $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ has a unique subextension of degree 2.

3. Let $\mathfrak{Q} \subset O_{\mathbb{Q}(\zeta_p)}$ and $\mathfrak{q} \subset O_K$ be two prime ideals above q. Then $\mathfrak{Q}$ is a prime ideal over $\mathfrak{q}$, that is $\mathfrak{Q} \cap O_K = \mathfrak{q}$. If $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ lies in $D_{\mathfrak{Q}}$ (that is, $\sigma(\mathfrak{Q}) = \mathfrak{Q}$), then it is clear that $\sigma|_K$ is in $D_{\mathfrak{q}}$. Hence, the restriction map induces a morphism
   $$D_{\mathfrak{Q}} \to D_{\mathfrak{q}};\ \sigma \mapsto \sigma|_K.$$

Let $k_{\mathfrak{Q}} = O_{\mathbb{Q}(\zeta_q)}/\mathfrak{Q}$ and $k_{\mathfrak{q}} = O_K/\mathfrak{q}$. We have the field inclusion $k_{\mathfrak{q}} \hookrightarrow k_{\mathfrak{Q}}$ and again a restriction map

$$\mathrm{Gal}(k_{\mathfrak{Q}}/\mathbb{F}_q) \to \mathrm{Gal}(k_{\mathfrak{q}}/\mathbb{F}_q);\ \sigma \mapsto \sigma|_{k_{\mathfrak{q}}}.$$

The following diagram is easily seen to be commutative:

$$\begin{array}{ccc} D_{\mathfrak{Q}} & \longrightarrow & D_{\mathfrak{q}} \\ \downarrow \wr & & \downarrow \wr \\ \mathrm{Gal}(k_{\mathfrak{Q}}/\mathbb{F}_q) & \longrightarrow & \mathrm{Gal}(k_{\mathfrak{q}}/\mathbb{F}_q) \end{array},$$

where the horizontal arrows are restriction maps. It is clear that the bottom horizontal arrow maps the Frobenius element in $\mathrm{Gal}(k_{\mathfrak{Q}}/\mathbb{F}_q)$ onto the Frobenius element in $\mathrm{Gal}(k_{\mathfrak{q}}/\mathbb{F}_q)$. Hence the top horizontal arrow must map the Frobenius onto the Frobenius, as well. Since $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q})$ is surjective, its kernel has cardinality $\frac{p-1}{2}$. The unique subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$ of cardinality $\frac{p-1}{2}$ is the subgroup of square elements.

4. If q splits in K, we have $q = \mathfrak{q}\overline{\mathfrak{q}}$, where $\mathfrak{q} \neq \overline{\mathfrak{q}}$. It follows that $D_{\mathfrak{q}}$ is trivial and so the Frobenius $(q, K/\mathbb{Q})$ is trivial. On the other hand, if $(q, K/\mathbb{Q})$ is trivial, then $\mathrm{Gal}(k_{\mathfrak{q}}/\mathbb{F}_q)$ is trivial (since the Frobenius in $\mathrm{Gal}(k_{\mathfrak{q}}/\mathbb{F}_q)$ is a generator). Hence $D_{\mathfrak{q}}$ is trivial. It follows that the unique non-trivial element σ of $\mathrm{Gal}(K/\mathbb{Q})$ maps $\sigma(\mathfrak{q}) \neq \mathfrak{q}$ and so $q = \mathfrak{q}\sigma(\mathfrak{q})$ is split.

   Now consider the second bullet point. By the previous point, we have that $(q, K/\mathbb{Q})$ is trivial, if and only if $(q, \mathbb{Q}(\zeta_p)/\mathbb{Q})$ is a square. Recall that isomorphism

$$\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \to (\mathbb{Z}/p\mathbb{Z})^\times$$

   maps σ to the unique element $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ so that $\sigma(\zeta_p) = \zeta_p^a$. We claim that under this isomorphism

$$(q, \mathbb{Q}(\zeta_p)/\mathbb{Q}) = q \,(\mathrm{mod}\, p). \tag{1}$$

   Recall that $\sigma_q = (q, \mathbb{Q}(\zeta_p)/\mathbb{Q})$ is the unique element in $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ so that $\sigma_q(x) \equiv x^q \,(\mathrm{mod}\, \mathfrak{Q})$ for all $x \in O_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}$. Let σ_q' be the unique element of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ so that $\sigma_q'(\zeta_p) = \zeta_p^q$. Then (1) is equivalent to $\sigma_q = \sigma_q'$. Let $\sum_i a_i\zeta_p^i \in \mathbb{Z}[\zeta_p] = O_{\mathbb{Q}(\zeta_p)}$ (this was proved in the previous exercise sheet). Then

$$\sigma_q'(\sum_i a_i\zeta_p^i) = \sum_i a_i\zeta_p^{qi} \equiv (\sum_i a_i\zeta_p^i)^q \,(\mathrm{mod}\, \mathfrak{Q}).$$

   Hence, by uniqueness, $\sigma_q' = \sigma_q$. We deduce so that q is a square in $\mathbb{F}_p^\times$ if and only if $(q, K/\mathbb{Q})$ is trivial.

5. We have that $(-1)^{\frac{p-1}{2}}p \equiv 1 \,(\mathrm{mod}\, 4)$. Hence from Exercise 3.4, Exercise Sheet 3, we see that q splits in $\mathbb{Q}(\sqrt{(-1)^{\frac{p-1}{2}}p})$ if and only if $(-1)^{\frac{p-1}{2}}p$ is a square $(\mathrm{mod}\, q)$. Which is what is requested to prove.

   Hence,

$$\left(\frac{(-1)^{\frac{p-1}{2}}p}{q}\right) \cdot \left(\frac{q}{p}\right) = 1,$$

   We have $\left(\frac{(-1)^{\frac{p-1}{2}}p}{q}\right) = \left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)$. This concludes the proof.

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

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

[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.

where covol(Λ) is denoted in the notes as vol(Λ). 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 $f_1 * f_2(y) = \int_{\mathbb{R}^n} f_1(x) f_2(y-x) \, \mathrm{d}x$. 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 real-valued and 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 $\dfrac{\mathrm{d}}{\mathrm{d}x}(f * h) = f * \dfrac{\mathrm{d}}{\mathrm{d}x} h$.

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.

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.

Solution. 1. We have

$$\begin{aligned}
\widehat{f_1 * f_2}(y) &= \int_{\mathbb{R}^n} (f_1 * f_2)(x) e^{-2\pi i \langle x, y \rangle} \, \mathrm{d}x \\
&= \int_{\mathbb{R}^n} \int_{\mathbb{R}^n} f_1(z) f_2(x - z) \, \mathrm{d}z e^{-2\pi i \langle x, y \rangle} \, \mathrm{d}x \\
&= \int_{\mathbb{R}^n} f_1(z) e^{-2\pi i \langle z, y \rangle} \, \mathrm{d}z \int_{\mathbb{R}^n} f_2(x') e^{-2\pi i \langle x', y \rangle} \, \mathrm{d}x' = \widehat{f_1} \cdot \widehat{f_2}(y)
\end{aligned}$$

2. Let y be so that $f_1 * f_2(y) \neq 0$, then there exists $x \in \mathrm{supp}(f_1)$ so that $y - x \in \mathrm{supp}(f_2)$. That is, $y = x + (y - x) \in \mathrm{supp}(f_1) + \mathrm{supp}(f_2)$.
3. We have

$$\begin{aligned}
\overline{\widehat{f_1}(y)} &= \int_{\mathbb{R}^n} \overline{f_1}(x) e^{2\pi i \langle x, y \rangle} \, \mathrm{d}x \\
&= \int_{\mathbb{R}^n} f_1(x) e^{-2\pi i \langle x, y \rangle} \, \mathrm{d}x = \widehat{f_1}(y).
\end{aligned}$$

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

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

4. We want to show that the limit

$$\lim_{t\to 0}\frac{f*h(x+t)-f*h(x)}{t}$$

exists for every $x\in\mathbb{R}^n$. We compute

$$\frac{1}{t}(f*h(x+t)-f*h(x))=\int_{\mathbb{R}^n} f(y)(\frac{h(x+t-y)-h(x-y))}{t}\ \mathrm{d}y.$$

The inner limit converges to $h'(x-y)$ (which is absolutely bounded as h is smooth compactly supported, and so by dominated convergence theorem $\frac{\mathrm{d}}{\mathrm{d}x}(f*h)=f*\frac{\mathrm{d}}{\mathrm{d}x}h$. By induction, we deduce that $f*h$ is smooth.

5. g_ϵ is smooth for what we just proved. The support of g_ϵ is contained in $\frac{V}{2}+\frac{\epsilon V}{2}=\frac{(1+\epsilon)}{2}V$. Let $y\in\frac{(1+\epsilon)}{2}V$, then

$$g_\epsilon(y)=\int_{V/2}\frac{1}{\epsilon^n}\omega(\epsilon^{-1}(y-x))\ \mathrm{d}x=\int_{y-\frac{V}{2}}\frac{1}{\epsilon^n}\omega(\epsilon^{-1}x)\ \mathrm{d}x\le\frac{1}{\epsilon^n}\int_{\mathbb{R}^n}\omega(\epsilon^{-1}x)\ \mathrm{d}x=1.$$

For the last assertion we have

$$\int_{\mathbb{R}^n} g_\epsilon(z)\ \mathrm{d}z=\widehat{g_\epsilon}(0)=\widehat{1_{V/2}}(0)\widehat{\omega_\epsilon}(0)=\mathrm{vol}(V/2).$$

6. It is clear that f_ϵ has support in $\frac{1+\epsilon}{2}V+\frac{1+\epsilon}{2}V\subset(1+\epsilon)V$. Let $y\in(1+\epsilon)V$. Since $1\ge g_\epsilon\ge 0$, we have

$$f_\epsilon(y)\le\int_{\mathbb{R}^n} g_\epsilon(x)\ \mathrm{d}x=\frac{1}{2^n}\,\mathrm{vol(V)}\,.$$

Also $\widehat{f_\epsilon}=\widehat{g_\epsilon}\cdot\widehat{g_\epsilon}=|\widehat{g_\epsilon}|^2$, since g_ϵ is real-valued.

7. Suppose $\mathrm{vol}(V)>2^n\,\mathrm{covol}(\Lambda)$. Let $V'=\frac{1}{1+\epsilon}V$, where $\epsilon>0$ is small enough so that $\mathrm{vol}(V')>2^n\,\mathrm{covol}(\Lambda)$, let f_ϵ constructed as before with respect to V'

$$\begin{aligned}
|V\cap\Lambda|&=\sum_{\lambda\in\Lambda}1_{(1+\epsilon)V'}(\lambda)\\
&\ge\frac{2^n}{\mathrm{vol}(V')}\sum_{\lambda\in\Lambda}f_\epsilon(\lambda)\\
&=\frac{2^n\,\mathrm{covol}(\Lambda)^{-1}}{\mathrm{vol(V')}}\sum_{\lambda\in\widehat{\Lambda}}\widehat{f}_\epsilon(\lambda)\\
&\ge\frac{2^n\,\mathrm{covol}(\Lambda)^{-1}}{\mathrm{vol}(V')}\widehat{f}_V(0)=\frac{\mathrm{vol}(V')}{2^n\,\mathrm{covol}(\Lambda)}>1.
\end{aligned}$$

The case $\mathrm{vol}(V)=2^n\,\mathrm{covol}(\Lambda)$ is deduced as in class.