

Solutions to Sheet 13

Exercise 1

Let K be a number field of degree d .

1. Show that there exists a constant C , depending only on K , with the following property. If I is a principal ideal of \mathcal{O}_K , then $I = \alpha \mathcal{O}_K$ for some $\alpha \in \mathcal{O}_K$ such that $|\sigma(\alpha)| \leq C N(I)^{1/d}$ for every real or complex embedding of K .
2. Let $K \subset \mathbb{R}$ be a quadratic number field. Let $\eta \in \mathcal{O}_K^\times$ be such that $\mathcal{O}_K^\times = \{\pm \eta^n; n \in \mathbb{Z}\}$. Show that, in this case, one can take $C = \max\{|\eta|, |\eta|^{-1}\}^{1/2}$.
3. Do there exists $x, y \in \mathbb{Z}$ with $x^2 - 82y^2 = 2$?

Solution.

1. Assume that $I = (\alpha) \neq (0)$. Then $I = (u\alpha)$ for every unit $u \in \mathcal{O}_K^\times$. The map \mathcal{L} from the proof of Dirichlet's unit theorem extends to a map

$$\mathcal{L} : \mathcal{O}_K \setminus \{0\} \rightarrow \mathbb{R}^{r+s}, \xi \mapsto (\log |\sigma_1(\xi)|, \dots, \log |\sigma_r(\xi)|, 2 \log |\sigma_{r+1}(\xi)|, \dots, 2 \log |\sigma_{r+s}(\xi)|),$$

which is a morphism of monoids.

We have seen in the lecture that the image of \mathcal{O}_K^\times under this map is a lattice in a linear subspace V . Here V is given by those vectors of \mathbb{R}^{r+s} whose coordinates sum up to 0. We are interested in the image of the set $\alpha \mathcal{O}_K^\times$ under \mathcal{L} . This is contained in the affine-linear subspace $\mathcal{L}(\alpha) + V$.

The exercise now translates to: There is some constant $C > 0$ depending only on K such that there is a point $\xi = (\xi_1, \dots, \xi_r, 2\xi_{r+1}, \dots, 2\xi_{r+s}) \in \mathcal{L}(\alpha) + \mathcal{L}(\mathcal{O}_K^\times) \subset \mathcal{L}(\alpha) + V$ with

$$\max \xi_i \leq \frac{1}{d} \log N(I) + \log(C)$$

We define a norm $\|-\|$ on \mathbb{R}^{r+s} via

$$\|(x_1, \dots, x_{r+s})^t\| = \max(|x_1|, \dots, |x_s|, \frac{1}{2}|x_{s+1}|, \dots, \frac{1}{2}|x_{r+s}|)$$

and a linear function $S : \mathbb{R}^{r+s} \rightarrow \mathbb{R}$ by

$$S((x_1, \dots, x_{r+s})^t) = \sum_{i=1}^{r+s} x_i.$$

Let W be the vector space spanned by

$$w_0 = (1, \dots, 1, 2, \dots, 2)$$

with r ones and s twos and write $\mathcal{L}(\alpha) = w + v$ where $v \in V$ and $w \in W$. We have

$$S(\mathcal{L}(\alpha)) = \log N(I),$$

hence we obtain (as $w \in \mathbb{R}w_0$, $S(v) = 0$ and $N(I) \geq 1$)

$$\|w\| = \frac{1}{d} |S(w)| = \frac{1}{d} |S(w+v)| = \frac{1}{d} |S(\mathcal{L}(\alpha))| = \frac{1}{d} \log N(I).$$

All we need to do is to find a point of $\mathcal{L}(\alpha\mathcal{O}_K^\times)$ close to w . For $\nu \in V$ define $d(\nu) = \inf_{\gamma \in \mathcal{L}(\mathcal{O}_K^\times)} (\|\nu - \gamma\|)$, and set $C = \sup_{\nu \in V} d(\nu)$. This is well-defined because $\mathcal{L}(\mathcal{O}_K^\times)$ is a lattice in V . Now C only depends on K , and we find a point

$$\mathcal{L}(\alpha) + \mathcal{L}(\mathcal{O}_K^\times) \ni w + \nu_0 = \xi = (\xi_1, \dots, \xi_r, 2\xi_{r+1}, \dots, 2\xi_{r+s})$$

with $\nu_0 \in V$ and $\|\nu_0\| \leq C$. In particular,

$$\max \xi_i \leq \|\xi\| \leq \|w\| + \|\nu_0\| \leq \frac{1}{d} \log N(I) + C.$$

This solves the exercise.

2. Let η be as in the question and assume $|\eta| < 1$. Let $\sigma_1, \sigma_2 : K \hookrightarrow \mathbb{R}$ be the two real embeddings of K (i.e., σ_1 is the identity on $K \subset \mathbb{R}$ and σ_2 is "conjugation"). Suppose $I = (\alpha)$. Then we can pick n such that

$$\sigma_1(\eta^n \alpha) = |\eta|^n |\sigma_1(\alpha)| \in (|\eta|^{1/2} N(I)^{1/2}, |\eta|^{-1/2} N(I)^{1/2}).$$

Now

$$|\sigma_2(\eta^n \alpha)| = |\eta|^{-n} |\sigma_2(\alpha)| = (|\eta|^{-n} \sigma_1(\alpha)^{-1}) N(I) \leq \frac{1}{|\eta|^{1/2}} N(I)^{1/2}.$$

3. Let $K = \mathbb{Q}(\sqrt{82})$. A unit as in 2 is given by $\eta = 9 + \sqrt{82}$. This can be checked similarly to sheet 11, exercise 4. Also, note that (by Dedekind-Kummer) $2\mathcal{O}_K = \mathfrak{p}^2$ for some prime ideal \mathfrak{p} . Now $N(\mathfrak{p}) = 2$, and a solution to $x^2 - 82y^2 = 2$ would result in \mathfrak{p} being principal. By part one and two, it suffices to show that there is no solution with

$$\max |x \pm \sqrt{82}y| \leq N(2\mathcal{O}_K)^{1/2} \sqrt{9 + \sqrt{82}} < 7.$$

But there are no such solutions as $\sqrt{82} > 7$.

Exercise 2

Show that

$$\zeta_{\mathbb{Q}(\sqrt{6})} \zeta_{\mathbb{Q}(\sqrt{7})} \zeta_{\mathbb{Q}(\sqrt{42})} = \zeta_{\mathbb{Q}(\sqrt{6}, \sqrt{7})} \zeta_{\mathbb{Q}}^2.$$

Solution. Here we will only sketch a solution. The details are tedious. Recall that from the lecture (Example 3.12, say) we have for quadratic fields $K = \mathbb{Q}(\sqrt{m})$ with discriminand Δ_K

$$p\mathcal{O}_K = \begin{cases} \text{prime ideal,} & \text{if } \left(\frac{\Delta_K}{p}\right) = -1 \\ \mathfrak{p}_1 \mathfrak{p}_2, & \text{(totally split) if } \left(\frac{\Delta_K}{p}\right) = 1 \\ \mathfrak{p}^2, & \text{(totally ramified) if } \left(\frac{\Delta_K}{p}\right) = 0. \end{cases}$$

Also, note that for K as above we have

$$\begin{aligned} \zeta_K(s) &= \prod_{\mathfrak{p}} \left(1 - \frac{1}{N(\mathfrak{p}^s)}\right)^{-1} = \prod_{p \in \mathbb{Z}} \prod_{\text{prime } \mathfrak{p} | p\mathcal{O}_K} \left(1 - \frac{1}{N(\mathfrak{p}^s)}\right)^{-1} \\ &= \prod_{\left(\frac{\Delta_K}{p}\right) = -1} \left(1 - \frac{1}{N(\mathfrak{p})^{2s}}\right)^{-1} \prod_{\left(\frac{\Delta_K}{p}\right) = 1} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-2} \prod_{\left(\frac{\Delta_K}{p}\right) = 0} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} \end{aligned}$$

This yields some expansion of $\zeta_{\mathbb{Q}(\sqrt{6})}\zeta_{\mathbb{Q}(\sqrt{7})}\zeta_{\mathbb{Q}(\sqrt{42})}$ in terms of factors indexed by prime numbers.

Write $L = \mathbb{Q}(\sqrt{6}, \sqrt{7})$. We want to do something similar as above for the function $\zeta_{\mathbb{Q}(\sqrt{6}, \sqrt{7})}$. Recall that if $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$ we have $e_1 = \cdots = e_g = e$, $f(\mathfrak{p}_1) = \cdots = f(\mathfrak{p}_g) = f$ and $efg = 4$. Also, as $\text{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$ is not cyclic, we cannot have inert primes, i.e., we never have $f = 4$. Indeed, if there was an inert prime $\mathfrak{p} \mid p$, we'd find $\text{Gal}(L/\mathbb{Q}) = D(\mathfrak{p}|p) \cong \text{Gal}(\kappa(\mathfrak{p})/\mathbb{F}_p)$, and the latter (being the Galois group of an extension of finite fields) is cyclic. Hence, the only possible splitting behaviours of a prime $p \in \mathbb{Z}$ are:

$$\begin{aligned} g = 4 &\implies \prod_{\mathfrak{p}|p} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} = (1 - p^{-s})^{-4} \\ f = 2, g = 2 &\implies \prod_{\mathfrak{p}|p} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} = (1 - p^{-2s})^{-2} \\ e = 2, f = 2, g = 1 &\implies \prod_{\mathfrak{p}|p} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} = (1 - p^{-2s})^{-1} \\ e = 2, f = 1, g = 2 &\implies \prod_{\mathfrak{p}|p} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} = (1 - p^{-s})^{-2} \\ e = 4, f = 1, g = 1 &\implies \prod_{\mathfrak{p}|p} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} = (1 - p^{-s})^{-1}. \end{aligned}$$

But one easily checks that Δ_L has only prime divisors 2, 3, 7, so that all other primes are unramified on \mathcal{O}_L . Using this and that

$$\left(\frac{42}{p}\right) = \left(\frac{6}{p}\right) \left(\frac{7}{p}\right),$$

we can show that the Euler factors at each prime p coincide for both functions.

Exercise 3

Let K be a number field and let

$$\log : \mathbb{C} \setminus (-\infty, 0] \rightarrow \mathbb{C}$$

denote the principal branch of the complex logarithm. The variable \mathfrak{p} always runs over the non-zero primes of \mathcal{O}_K in the following.

1. Show that

$$\lim_{s \rightarrow 1^+} \frac{1}{\log(s-1)} \sum_{\mathfrak{p}} \log(1 - N(\mathfrak{p})^{-s}) = 1.$$

2. Show that

$$\sum_{\mathfrak{p}; f(\mathfrak{p}) > 1} \frac{1}{N(\mathfrak{p})} + \sum_{\mathfrak{p}} \sum_{n=2}^{\infty} \frac{1}{n N(\mathfrak{p})^n} < \infty.$$

3. Using 1 and 2, deduce that there exists infinitely many prime ideals \mathfrak{p} of \mathcal{O}_K with $f(\mathfrak{p}) = 1$.

Solution. The following is a bit unprecise as I sometimes forgot to insert absolute-value brackets. But it works out if we simply assume $s \in \mathbb{R}$ everywhere.

1. We know that the Dedekind-zeta function $\zeta_K(s)$ is holomorphic in $\operatorname{Re} s > 1$, has a pole of order 1 at $s = 1$ with residue $\kappa > 0$ and has an Euler product

$$\zeta_K(s) = \prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-s})^{-1}.$$

Hence we find

$$\lim_{s \rightarrow 1^+} \left((s-1) \prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-s})^{-1} \right) = \kappa,$$

and the claim follows after taking logarithms.

2. Note that there are at most $[K : \mathbb{Q}]$ prime ideals of \mathcal{O}_K above each prime number $p \in \mathbb{Z}$. If \mathfrak{p} lies above p and $f(\mathfrak{p}) > 1$, we have (by definition) $N(\mathfrak{p}) \geq p^2$. Hence we obtain that

$$\sum_{\mathfrak{p}, f(\mathfrak{p}) > 1} N(\mathfrak{p})^{-s} \leq [K : \mathbb{Q}] \sum_p p^{-2s},$$

which is (absolutely) convergent for $\operatorname{Re} s > \frac{1}{2}$. Similarly, we find that

$$\frac{1}{[K : \mathbb{Q}]} \sum_{\mathfrak{p}} \sum_{n=2}^{\infty} \frac{1}{n N(\mathfrak{p})^{sn}} \leq \sum_p \sum_{n=2}^{\infty} \frac{1}{n p^{sn}} < \sum_p p^{-2s} \sum_{n=0}^{\infty} p^{-sn} < \left(\sum_{n=0}^{\infty} 2^{-sn} \right) \sum_p p^{-2s}.$$

This is absolutely convergent for $\operatorname{Re} s > 0$.

3. Recall that $\log(1+t) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} t^n$ for $|t| < 1$. We plug this into the logarithm of the euler product to obtain for $\operatorname{Re} s > 1$

$$\log \zeta_K(s) = - \sum_{\mathfrak{p}} \log(1 - N(\mathfrak{p})^{-s}) = \sum_{\mathfrak{p}} \sum_{n=1}^{\infty} \frac{1}{n} N(\mathfrak{p})^{-ns}.$$

Splitting off the $n = 1$ terms, this yields

$$\log \zeta_K(s) = \sum_{\mathfrak{p}, f(\mathfrak{p})=1} N(\mathfrak{p})^{-s} + \sum_{\mathfrak{p}, f(\mathfrak{p})>1} N(\mathfrak{p})^{-s} + \sum_{\mathfrak{p}} \sum_{n=2}^{\infty} \frac{1}{n N(\mathfrak{p})^{sn}}.$$

The left hand side of this equation diverges for $s \rightarrow 1^+$, but the last two terms of the RHS remain finite by part 2. The claim follows.