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 $|\sigma(\alpha)| \leq C\,\mathrm{N}(I)^{1/d}$ 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 $I = (\alpha)$. Then $I = (u\alpha)$ for every unit $u \in \mathcal{O}_K^\times$. Look at the morphism

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

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 of course 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 $x = (x_1, \ldots, x_r, 2x_{r+1}, \ldots, 2x_{r+s}) \in \mathcal{L}(\alpha) + \mathcal{L}(\mathcal{O}_K^\times) \subset \mathcal{L}(\alpha) + V$ with

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

We write W for the vector space spanned by

$$w_0 = \frac{1}{d}(1, \ldots, 1).$$

This is orthogonal to the subspace V. Write $\mathcal{L}(\alpha) = w + v$ where $v \in V$ and $w \in W$. We have

$$\|\mathcal{L}(\alpha)\|_1 = \log \mathrm{N}(I),$$

hence we obtain

$$\|w\|_\infty \leq \|\mathcal{L}(\alpha)\|_\infty \leq \frac{1}{d}\log \mathrm{N}(I).$$

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 $d(\nu) = \inf_{\gamma\in\mathcal{L}(\mathcal{O}_K^\times)}(\|\nu - \gamma\|_\infty)$, 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

$$(x_1, \ldots, x_r, 2x_{r+1}, \ldots, 2x_{r+s}) = x = w + \nu_0$$

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

$$\max x_i \leq \|x\|_\infty \leq \|w\|_\infty + \|\nu_0\|_\infty \leq \frac{1}{d}\log \mathrm{N}(I) + C.$$

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

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

Now

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

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 $\mathrm{N}(\mathfrak{p}) = 2$, and a solution to $x^2 - 82y^2 = 2$ would result in $\mathfrak{p}$ being principal. By part 1 and two, it suffices to show that there is no solution with

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

But there are no such solutios 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. [Will add later]

Exercise 3

Let K be a number field and let

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

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
$$\lim_{s \to 1^+} \frac{1}{\log(s-1)} \sum_{\mathfrak{p}} \log(1 - \mathrm{N}(\mathfrak{p})^{-s}) = 1.$$
2. Show that
$$\sum_{\mathfrak{p};\ f(\mathfrak{p})>1} \frac{1}{\mathrm{N}(\mathfrak{p})} + \sum_{\mathfrak{p}} \sum_{n=2}^{\infty} \frac{1}{n\,\mathrm{N}(\mathfrak{p})^n} < \infty.$$
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

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

Hence we find

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

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) $\mathrm{N}(\mathfrak{p}) \geq p^2$. Hence we obtain that

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

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

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

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 $\operatorname{Re} s > 1$

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

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

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

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

Max von Consbruch, email: mvconsbruch@uni-bonn.de. Date: January 23, 2024