Solutions to Sheet 10

Exercise 1

Let $p \geq 2$ be a prime number and let $K = \mathbb{Q}(\zeta)$ be the p-th cyclotomic field, where $\zeta = \mathrm{e}^{2\pi\mathrm{i}/p} \in \mathbb{C}$. The minimal polynomial of ζ over $\mathbb{Q}$ is $\Phi_n(X) = X^{p-1} + \cdots + X + 1$. Let $l_1, \ldots, l_n$ be prime numbers such that $l_i \equiv 1 \bmod p$ for all i and set $L = l_1 \cdots l_n$.

1. Show that there xists $x \in \mathbb{Z}$ with $\Phi(xLp) > 1$.
2. Denote by l a prime number that divides $\Phi_p(xLp)$. Show that $l \notin \{l_1, \ldots, l_n\}$ and $l \neq p$.
3. Let $\mathfrak{l}$ be a prime ideal of $\mathcal{O}_K$ containing l. Show that $f(\mathfrak{l}|l\mathbb{Z}) = 1$ and deduce that $l \equiv 1 \bmod p$.
4. Deduce that there exists infinitely many prime numbers l such that $l \equiv 1 \bmod p$.

Solution.

1. This is simple analysis. The term X^{p-1} dominates and gets arbitrarily large.

2. One quickly finds $\Phi_p(xLp) \equiv 1 \bmod l_i$ and mod p.

3. Again, this is an application of Dedekind-Kummer. Again, we can apply Dedekind-Kummer with respect to ζ, as $\mathcal{O}_K = \mathbb{Z}[\zeta]$, i.e., $[\mathcal{O}_K : \mathbb{Z}[\zeta]] = 1$. Now $\mathfrak{l}$ corresponds to some factor of the decomposition of $\Phi_n(X) \bmod l$. As $\Phi_n(xLp) \equiv 0 \bmod l$ (i.e., thre is a root), there is at least one linear term in the decomposition of $\Phi_n(X)$. Let this term correspond to some prime ideal $\mathfrak{l}' \mid l\mathcal{O}_K$, which now has residue degree $f(\mathfrak{l}'|l) = 1$ (again, by 3.11). But $\mathbb{Q}(\zeta)/\mathbb{Q}$ is Galois, so the residue degrees of primes over l are all the same. Hence $f(\mathfrak{l}|l) = 1$. Proposition 40 now yields that $l \equiv 1 \bmod p$.

4. Given any finite list $l_1, \ldots, l_n$ of primes leaving residue 1 mod p, we can take their product L and find some integer $x > 1$ such that $\Phi_n(xLp) > 1$ by part 1. Now any prime l dividing $\Phi_n(xLp)$ is not among the l_i and $\neq p$ by part 2, and part 3 shows that $l \equiv 1 \bmod p$. So no finite list of primes 1 mod p can contain all such primes.

Exercise 2

Let $m < 0$ be a squarefree integer and set $K = \mathbb{Q}(\sqrt{m})$.

1. Show that $\mathrm{N}_{K/\mathbb{Q}}(x) > \left|\Delta_{K/\mathbb{Q}}\right|/4$ for all $x \in \mathcal{O}_K \setminus \mathbb{Z}$.

Solution.

1. Remember the formula for the discriminant of quadratic number fields:

$$\Delta_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}} = \begin{cases} 4m, & \text{if } m \equiv 2, 3 \pmod 4 \\ m, & \text{if } m \equiv 1 \pmod 4. \end{cases}$$

If $m \equiv 1 \bmod 4$, this has been basically solved by sheet 6, exercise 2.3: There we found that for all $x \in \mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ we have

$$\mathrm{N}_{K/\mathbb{Q}}(x) \geq \left|\frac{m-1}{4}\right| > \left|\frac{m}{4}\right| = \left|\frac{\Delta_{K/\mathbb{Q}}}{4}\right|.$$

The case $m \equiv 2, 3 \bmod 4$ is handled similarly. We have $\mathcal{O}_K = \mathbb{Z}[\sqrt{m}]$, and $\mathrm{N}_{K/\mathbb{Q}}(a + b\sqrt{m}) = a^2 + mb^2 \geq m = |\Delta_K|/4$.

Exercise 3

1. Show that $\mathrm{Cl}(\mathbb{Q}(\sqrt{-2023})) = \{1\}$.
2. Show that $\mathrm{Cl}(\mathbb{Q}(\sqrt{-67})) = \{1\}$.

Solution. The Idea for both calculations is to follow the proof of lemma 4.4 in the lecture notes. Let $K = \mathbb{Q}(\sqrt{m})$ with some squarefree integer $m < 0$ identified as a subfield of $\mathbb{C}$, and let $I \subset \mathcal{O}_K$ be any ideal. We can follow the proof of lemma 4.4 verbatim until just before equation (4.1) to obtain a *reduced* $\mathbb{Z}$*-basis* of (a_1, a_2) of I. That is, we find elements $a_1, a_2 \in \mathcal{O}_K$ with $I = a_1\mathbb{Z} + a_2\mathbb{Z}$, such that

$$\left|\frac{a_2}{a_1}\right| \geq 1, \quad \mathrm{Re}\left(\frac{a_2}{a_1}\right) \leq 1/2 \quad \text{and} \quad \mathrm{Im}\left(\frac{a_2}{a_1}\right) \geq 0.$$

just as in the notes we set $\tau = \frac{a_2}{a_1}$ and find that these conditions relate to $|\tau| \geq 1$, $|\mathrm{Re}\,\tau| \leq 1/2$ and $\mathrm{Im}(\tau) \geq 0$. In particular, we find $\mathrm{Im}\,\tau \geq \sqrt{3}/2$. Lemma 1.44 reads $\Delta_K(I) = \mathrm{N}(I)^2\Delta_K = \mathrm{N}(I)^2 bm$, where $b = 4$ if $m \equiv 2, 3 \bmod 4$ and $b = 1$ otherwise. Equation (4.1) also goes through, we find $\Delta_K(I) = -4|a_1|^4 \mathrm{Im}(\tau)^2$. Combining these equations, we arrive at

$$\mathrm{N}(I)\sqrt{\frac{-bm}{3}} \geq |a_1|^2 = \mathrm{N}_{K/\mathbb{Q}}(a_1).$$

As $a_1 \in I$ we find $I \mid a_1\mathcal{O}_K$, so there is some ideal J with $IJ = a_1\mathcal{O}_K$ (i.e., $[J]$ is the inverse of $[I]$ in $\mathrm{Cl}(K)$). Now

$$\mathrm{N}(I)\,\mathrm{N}(J) = \mathrm{N}(IJ) = \mathrm{N}(a_1\mathcal{O}_K) = \mathrm{N}_{K/\mathbb{Q}}(a_1) = |a_1|^2 \leq \mathrm{N}(I)\sqrt{\frac{-bm}{3}},$$

implying that

$$\mathrm{N}(J) \leq \sqrt{\frac{-bm}{3}}.$$

The hope is now that this is not too large and leaves us with a number of cases that we can handle. So let's see.

1. Note that $2023 = 17^2 \cdot 7$, so that really $K = \mathbb{Q}(\sqrt{-7})$. As -7 is 1 mod 4, we have $b = 1$, and we find $\mathrm{N}(J) \leq \sqrt{\frac{7}{3}} < 2$. There are no prime ideals with norm that low (they cannot lie over a integer prime) so the only possibility is $J = \mathcal{O}_K$. But now $[I] = [J] = \mathrm{id}_{\mathrm{Cl}(K)}$, and $\mathrm{Cl}(K) = \{1\}$.

2. Again, -67 is 1 mod 4, but it is already squarefree and relatively large, so we'll have to make use of Dedekind kummer. But first of all, note that again $b = 1$, so we find

$$\mathrm{N}(J) \leq \sqrt{\frac{67}{3}} < \sqrt{23} < 5.$$

Now let's inspect the primes above 2 and 3. The ring $\mathcal{O}_K$ is generated as $\mathbb{Z}$-module by $\frac{1+\sqrt{-67}}{2}$, which has minimal polynomial T^2+T+17 (I think). Mod 2 we have $T^2+T+17 \equiv T^2+T+1$, which is irreducible and mod 3 we have $T^2+T+17 \equiv T^2+T+2$, which is irreducible. So we find by Dedekind-Kummer that both 2 and 3 are inert in $\mathcal{O}_K$, hence the only ideal with norm ≤ 4 is $J = 2\mathcal{O}_K$, which is principal. In particular, we find that I has to be principal, hence $\mathrm{Cl}(K) = \{1\}$.

Max von Consbruch, email: mvconsbruch@uni-bonn.de. Date: December 18, 2023