Universität Tübingen
Fachbereich Mathematik
D. Agostini, K. Heesterbeek, C. Nollau

Algebraic Number Theory
SS 2026

Sheet 11

If you want your solutions to be corrected, upload them on URM by the end of July 13.
Write your name and matriculation number on each sheet. If you upload the exercises as a group, only one person can do it instead of the whole group.
The exercises marked with $*$ might be more complicated or involved than the others.

Exercise 11.1 In this longer exercise we want to show that $\mathbf{Z}[\zeta_{23}]$ is not an UFD. Consider first the number field $K = \mathbf{Q}(\sqrt{-23})$.

(i) Show that $2\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ for two distinct prime ideals $\mathfrak{p}_1, \mathfrak{p}_2 \subseteq \mathcal{O}_K$.

(ii) Show that $\mathrm{Cl}(K) \cong \mathbf{Z}/3\mathbf{Z}$ with a generator given by $[\mathfrak{p}_1]$.

The next points could be a bit more involved than the usual exercises, but try to do them nevertheless, it is good training. Consider now the cyclotomic field $L = \mathbf{Q}(\zeta_{23})$. We know from the lectures that $K \subseteq L$, and we have also seen that

$$\mathrm{Aut}(L/K) = \{\sigma \in \mathrm{Aut}(L/\mathbf{Q}) \,|\, \sigma(\zeta_p) = \zeta_p^{2m}, m \in \mathbf{F}_{23}^{\times}\}$$

(iii) Show that 2 is unramified in L and if $\mathfrak{q} \subseteq \mathcal{O}_L$ is any prime ideal lying over 2, show that the decomposition group $D_{\mathfrak{q}}$ is equal to $\mathrm{Aut}(L/K)$. Conclude that $2\mathcal{O}_L = \mathfrak{q}_1\mathfrak{q}_2$ for two distinct prime ideals $\mathfrak{q}_1, \mathfrak{q}_2 \subseteq \mathcal{O}_K$.

(iv) Up to renumbering, show that $\mathfrak{q}_i \cap \mathcal{O}_K = \mathfrak{p}_i$ and $\mathfrak{p}_i\mathcal{O}_K = \mathfrak{q}_i$ for $i = 1, 2$. (*Hint:* use that $p\mathcal{O}_L \cap \mathcal{O}_K = p\mathcal{O}_K$ and that $(p\mathcal{O}_K)\mathcal{O}_L = p\mathcal{O}_L$).

(v) Show that

$$(\mathfrak{q}_1)^{11} \cap \mathcal{O}_K = \left(\prod_{\sigma \in \mathrm{Aut}(L/K)} \sigma(\mathfrak{q}_1)\right) \cap \mathcal{O}_K = \mathfrak{p}_1^{11}.$$

(vi) Show that $\mathfrak{p}_1^{11}$ is not principal in $\mathcal{O}_K$ and that $\mathfrak{q}_1$ is not principal in $\mathcal{O}_L$. Conclude that $\mathbf{Z}[\zeta_{23}]$ is not an UFD

It actually holds that $\mathrm{Cl}(L) \cong \mathbf{Z}/3\mathbf{Z}$ with a generator given by $[\mathfrak{q}_1]$.

Exercise 11.2 For the following pairs of integers numbers (d, p) with p prime, check whether d is a square modulo p or not (you do not have to check that the numbers p are prime):

$$(10, 1009), (261, 2017), (32001, 32003)$$