- The duration of the exam is 120 minutes.
- It is probably quite difficult to solve every exercise within the given time. Therefore the maximal grade can be achieved even if not all questions are answered.
- Basic results/definitions of algebra can be used directly, but please attempt to make it clear which result you are using.
- Every result stated in the lecture notes can be used without proof. Please mention it when you do so (write "by the lectures" or similar).
- The results obtained in the exercises cannot be used without reproving them. It is of course allowed to reproduce arguments used during the exercise sessions.
- The results proved in other (advanced) courses should not be used, unless you supply a proof using the results of the lecture notes (and basic results of algebra).
- When the aim of a question is to show a particular result, that result can be used to answer the *following* questions of the same exercise, even if you did not manage to prove that result. In any case, please make it explicit when you use a result from a previous question (write e.g. "by (c)" if you use the result of Question (c)).
- A few facts from the lectures are recalled on the next page.

We recall the following facts from the lectures, which can thus be used without proof. When K is a number field, we denote by $\mathcal{O}_K$ its ring of integers.

Fact 1. Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field, with $d \in \mathbb{Z}$ square-free. Then the absolute discriminant of K is

$$d_K = \begin{cases} d & \text{if } d = 1 \mod 4 \\ 4d & \text{if } d = 2, 3 \mod 4. \end{cases}$$

Fact 2. Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field, with $d \in \mathbb{Z}$ square-free. Consider the polynomial in $\mathbb{Z}[X]$

$$Q = \begin{cases} X^2 - d & \text{if } d = 2, 3 \mod 4 \\ X^2 - X - \frac{d-1}{4} & \text{if } d = 1 \mod 4. \end{cases}$$

Then we have a ring isomorphism

$$\varphi \colon \mathbb{Z}[X]/Q \xrightarrow{\sim} \mathcal{O}_K, \quad X \mapsto \begin{cases} \sqrt{d} & \text{if } d = 2, 3 \mod 4 \\ \frac{1+\sqrt{d}}{2} & \text{if } d = 1 \mod 4. \end{cases}$$

Fact 3. Let K be a number field. Then every class in the ideal class group $\mathcal{C}(\mathcal{O}_K)$ contains a nonzero ideal $I \subset \mathcal{O}_K$ such that

$$\mathrm{N}(I) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|d_K|},$$

with the usual notation.

Fact 4. Let K be a number field. Then there exists a group isomorphism

$$(\mathcal{O}_K)^\times \simeq \mathbb{Z}^{r_1+r_2-1} \times G,$$

where $G \subset K^\times$ is the subgroup of roots of unity, with the usual notation.

Fact 5. Let p be an odd prime number, and $\xi \in \mathbb{C}$ a primitive p-th root of unity. We consider the number field $K = \mathbb{Q}(\xi) \subset \mathbb{C}$. Then:

(i) The system $(1, \xi, \dots, \xi^{p-2})$ is a $\mathbb{Z}$-basis of $\mathcal{O}_K$.

(ii) The field extension $K/\mathbb{Q}$ is Galois, and there exists a group isomorphism

$$j \colon \mathrm{Gal}(K/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})^\times$$

such that $\sigma(\xi) = \xi^{j(\sigma)}$ for any $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$.

(iii) The absolute discriminant of K is $d_K = (-1)^{\frac{p-1}{2}} p^{p-2}$,

(iv) The ideal $(1-\xi)\mathcal{O}_K$ is prime in $\mathcal{O}_K$, and we have

$$p\mathcal{O}_K = ((1-\xi)\mathcal{O}_K)^{p-1}.$$