Exercise sheet #4

Exercises marked with a ✎ are to be handed in before **Monday October 21** at noon, in the mailbox at Spiegelgasse 1. Each of these is worth a number of points, as indicated. Questions marked with a $\star$ are more difficult.

Exercise 1 (Eisenstein's criterion) – Let A be a principal ideal domain, with field of fractions K. Let $\mathrm{F} = \sum_{i=0}^{d} a_i \mathrm{X}^i \in \mathrm{A}[\mathrm{X}]$ be a monic polynomial of degree $d \geqslant 1$. We assume that there exists a prime element p in A such that $a_i \in p\mathrm{A}$ for all $0 \leqslant i \leqslant d-1$, and such that $a_0 \notin p^2\mathrm{A}$. The goal of the exercise is to prove that F is irreducible in A[X] (and in K[X]).

We let R denote the quotient ring $\mathrm{A}/p\mathrm{A}$, and $r : \mathrm{A}[\mathrm{X}] \to \mathrm{R}[\mathrm{X}]$ denote the induced reduction map.

1.1. Prove that r is a ring morphism. What does $r(\mathrm{F})$ look like?

Assume that $\mathrm{F} = \mathrm{G} \cdot \mathrm{H}$ with $\mathrm{G}, \mathrm{H} \in \mathrm{K}[\mathrm{X}]$. Since F is monic, we may assume that G, H are monic.

1.2. Show that the roots of G, H in $\bar{\mathrm{K}}$ are integral over A. Deduce that $\mathrm{G}, \mathrm{H} \in \mathrm{A}[\mathrm{X}]$.

1.3. Prove that there exists $d' \in \mathbb{Z}_{\geqslant 0}$ and $\mathrm{G}_1, \mathrm{H}_1 \in \mathrm{A}[\mathrm{X}]$ with $\mathrm{G} = \mathrm{X}^{d'} + p \cdot \mathrm{G}_1$ and $\mathrm{H} = \mathrm{X}^{d-d'} + p \cdot \mathrm{H}_1$, with $\deg \mathrm{G}_1 < \deg \mathrm{G}$ and $\deg \mathrm{H}_1 < \deg \mathrm{H}$.

1.4. Prove that one of G or H is constant. Conclude that F is irreducible in A[X].

Exercise 2 (Cyclotomic polynomials) – Let $m \geqslant 2$ be an integer and let $\mathrm{U}_m^* \subset \mathbb{C}^\times$ denotes the set of primitive m-th roots of unity. Consider the m-th cyclotomic polynomial:

$$\Phi_m(\mathrm{X}) := \prod_{\zeta \in \mathrm{U}_m^*} (\mathrm{X} - \zeta) \in \mathbb{C}[\mathrm{X}].$$

2.1. Show that $\prod_{d|m} \Phi_d(\mathrm{X}) = \mathrm{X}^m - 1$, where the product is over positive divisors d of m.

2.2. Prove that $\Phi_m(\mathrm{X})$ is a monic polynomial of degree $\varphi(m)$ (where φ is Euler's totient function).

2.3. Prove that $\Phi_m(\mathrm{X})$ has integral coefficients. *Hint: You may argue by induction on m. For the induction step, write down the Euclidean division of $\mathrm{X}^m - 1$ by $\prod_{\substack{d|m \\ d<m}} \Phi_d(\mathrm{X})$ in $\mathbb{Z}[\mathrm{X}]$ (why is there such an Euclidean division?) and use uniqueness of the Euclidean division in $\mathbb{C}[\mathrm{X}]$.*

For the rest of the exercise, we assume that $m = p^k$, for a prime number p and a certain $k \geqslant 0$.

2.4. Prove that $\Phi_m(1) = p$.

2.5. For $k \geqslant 1$, show that $\Phi_m(\mathrm{X}) \equiv \Phi_p(\mathrm{X})^{p^{k-1}} \bmod p$.

2.6. Prove that $\Phi_m(\mathrm{X})$ is irreducible. *Hint: use Eisenstein's criterion on $\Phi_m(\mathrm{X}+1)$, and the previous question. Start by treating the case $k = 1$.*

Exercise 3 – Let K be a number field of degree n over $\mathbb{Q}$. We denote the ring of algebraic integers in K by $\mathcal{O}_K$. We let $\sigma_1, \ldots, \sigma_n$ denote the $\mathbb{Q}$-embeddings of K in $\mathbb{C}$.

3.1. Prove the existence of a basis $\alpha_1, \ldots, \alpha_n$ for K over $\mathbb{Q}$ with $\alpha_i \in \mathcal{O}_K$ for all $i \in \{1, \ldots, n\}$.

Given such a basis $\alpha_1, \ldots, \alpha_n$, we let $\delta := \det\left(\sigma_i(\alpha_j)\right)_{1 \leqslant i,j \leqslant n}$. Note that $\delta^2 = \mathrm{D}(\alpha_1, \ldots, \alpha_n) := \Delta$.

3.2. Explain why δ is an algebraic integer, and why Δ is a non-zero (rational) integer.

Let $\beta \in \mathcal{O}_K$. There exists a unique n-tuple $(x_1, \ldots, x_n) \in \mathbb{Q}^n$ such that $\beta = \sum_{j=1}^n x_j \alpha_j$.

3.3. For $1 \leqslant k \leqslant n$, let γ_k denote the determinant of the matrix $\left[b_{i,j}\right]_{1 \leqslant i,j \leqslant n}$ where $b_{i,j} = \sigma_i(\alpha_j)$ for $1 \leqslant i \leqslant n$ and $j \neq k$, and $b_{i,k} = \sigma_i(\beta)$. Prove that $x_j = \gamma_j/\delta$ for all $1 \leqslant j \leqslant n$.

3.4. Prove that Δx_j is an integer.

3.5. Deduce that, for any $\beta \in \mathcal{O}_K$, there exists a unique n-uple of integers $m_1, \ldots, m_n \in \mathbb{Z}$ such that $\beta = \dfrac{1}{\Delta} \displaystyle\sum_{i=1}^n m_i \cdot \alpha_i$, and Δ divides m_j^2 in $\mathbb{Z}$ for all j.

3.6. Assume that $\alpha_1, \ldots, \alpha_n$ are algebraic integers such that $\mathrm{D}(\alpha_1, \ldots, \alpha_n)$ is a square-free integer. Prove that $\alpha_1, \ldots, \alpha_n$ is a $\mathbb{Z}$-basis of $\mathcal{O}_K$.

Exercise 4 (Cyclotomic fields) {✎ : 6 points} – Let p be a prime number and $k \geqslant 1$. We let $m := p^k$ and we fix a primitive m-th root of unity ζ_m (in $\mathbb{C}$ for example). We let $K = \mathbb{Q}(\zeta_m)$, and $\mathcal{O}_K$ denote the ring of integers of K. The goal of the exercise is to prove that $\mathcal{O}_K = \mathbb{Z}[\zeta_m]$.

4.1. What is the degree of K over $\mathbb{Q}$? For brevity, we let $n = [K : \mathbb{Q}]$.

Write $\lambda_m := 1 - \zeta_m \in \mathbb{Z}[\zeta_m]$, and $\Delta_m := \mathrm{D}(1, \zeta_m, \ldots, \zeta_m^{n-1})$. It is clear that $K = \mathbb{Q}(\lambda_m)$ and that we have $\mathbb{Z}[\lambda_m] \subset \mathcal{O}_K$.

4.2. Prove that Δ_m is an integer dividing m^n in $\mathbb{Z}$. *Hint: The minimal polynomial of ζ_m is $\Phi_m(X)$, we have $X^m - 1 = \Phi_m(X) \cdot f(X)$ for a certain $f \in \mathbb{Z}[X]$ and we know that $\Delta_m = \mathrm{N}_{K/\mathbb{Q}}(\Phi'_m(\zeta_m))$.*

4.3. Prove that $\mathbb{Z}[\zeta_m] = \mathbb{Z}[\lambda_m]$ and that $\mathrm{D}(1, \lambda_m, \lambda_m^2, \ldots, \lambda_m^{n-1}) = \Delta_m$. *Hint: Δ_m can be expressed as a Vandermonde determinant.*

4.4. Show that $\mathrm{N}_{K/\mathbb{Q}}(\lambda_m) = p$. For $j \in \{1, \ldots n-1\}$, prove that λ_m divides $1 - \zeta_m^j$ in $\mathbb{Z}[\zeta_m]$. Deduce that p/λ_m^j lies in $\mathbb{Z}[\lambda_m]$ for all $0 \leqslant j \leqslant n-1$.

4.5. For any $\beta \in \mathcal{O}_K$, for any $j \in \{0, \ldots, n-1\}$, prove that $\beta p/\lambda_m^j$ lies in $\mathcal{O}_K$.

The n-tuple $(1, \lambda_m, \ldots, \lambda_m^{n-1})$ is a $\mathbb{Q}$-basis of K composed of algebraic integers. By **3.5** above, any $\beta \in \mathcal{O}_K$ can be written in a unique way as $\beta = \Delta_m^{-1} \cdot (m_0 + m_1\lambda + \cdots + m_{n-1}\lambda_m^{n-1})$, where $m_0, \ldots, m_{n-1}$ are integers such that Δ_m divides m_j^2.

Assume for a contradiction that $\mathbb{Z}[\lambda_m]$ is a strict submodule of $\mathcal{O}_K$.

4.7. Prove that there exists $\beta_0 \in \mathcal{O}_K$ of the form $\beta_0 = p^{-1} \cdot (a_j\lambda_m^j + \cdots + a_{n-1}\lambda_m^{n-1})$ for some $j \in \{1, \ldots, n-1\}$, where $a_j, \ldots, a_{n-1}$ are integers, and p does not divide m_j.

4.8. Prove that a_j is divisible by λ_m in $\mathcal{O}_K$. *Hint: multiply β_0 by p/λ_m^{j-1}.*

4.9. Comparing $\mathrm{N}_{K/\mathbb{Q}}(a_j)$ and $\mathrm{N}_{K/\mathbb{Q}}(\lambda_m)$, obtain a contradiction. Conclude that $\mathcal{O}_K = \mathbb{Z}[\zeta_m]$.

Exercise 5 (A Diophantine equation) {✎ : 4 points} – In 1659, Fermat claimed that he could solve the following problem: *Determine all solutions $(x, y) \in \mathbb{Z}^2$ of the equation $y^2 = x^3 - 2$.*

Solve the problem. *Hint: You may want to use $R = \mathbb{Z}[\sqrt{-2}]$. First prove that R is Euclidean for the norm map.*
