EXERCISE SHEET #7

Exercises marked with a ✎ are to be handed in before **Monday November 11** 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 (Dedekind–Kummer) {✎ : 8 points} – Let K be a number field of degree n, with ring of integers $\mathcal{O}_\mathrm{K}$. Fix an algebraic integer $\alpha \in \mathcal{O}_\mathrm{K}$ so that $\mathrm{K} = \mathbb{Q}(\alpha)$, and let $\mathrm{R} := \mathbb{Z}[\alpha]$ be the subring of $\mathcal{O}_\mathrm{K}$ generated by α. Denote by $f \in \mathbb{Z}[\mathrm{X}]$ the monic minimal polynomial of α.

The goal of the exercise is show that, for all but finitely many primes p, the decomposition of $p\mathcal{O}_\mathrm{K}$ as a product of prime ideals of $\mathcal{O}_\mathrm{K}$ can be determined by factoring f modulo p.

1.1. Prove that the quotient group $\mathcal{O}_\mathrm{K}/\mathrm{R}$ is finite.

Let p be a prime number. We assume that $(*)$ *p does not divide the order of the group $\mathcal{O}_\mathrm{K}/\mathrm{R}$.*

1.2. If condition $(*)$ is satisfied, prove that the inclusion $j : \mathbb{Z}[\alpha] \hookrightarrow \mathcal{O}_\mathrm{K}$ induces an isomorphism $\mathrm{R}/p\mathrm{R} \simeq \mathcal{O}_\mathrm{K}/p\mathcal{O}_\mathrm{K}$. *Hint: you may start by proving that $p\mathcal{O}_\mathrm{K} \cap \mathrm{R} = p\mathrm{R}$.*

For a polynomial $g \in \mathbb{Z}[\mathrm{X}]$, we write $\bar{g}$ for the polynomial in $\mathbb{F}_p[\mathrm{X}]$ obtained by reducing the coefficients of g modulo p. Note that the map $g \mapsto \bar{g}$ is a surjective ring morphism $\mathbb{Z}[\mathrm{X}] \to \mathbb{F}_p[\mathrm{X}]$.

Let us factor $\bar{f}$ in $\mathbb{F}_p[\mathrm{X}]$ as $\bar{f} = \bar{f_i}^{e_i} \cdot \bar{f_2}^{e_2} \cdot \dots \cdot \bar{f_r}^{e_r}$, where $f_1, \dots, f_r \in \mathbb{Z}[\mathrm{X}]$ are monic polynomials such that the $\bar{f_i}$'s are distinct irreducible polynomials in $\mathbb{F}_p[\mathrm{X}]$, and $e_1, \dots, e_r \in \mathbb{Z}_{\geqslant 1}$. For all $i = 1, \dots, r$, let $\mathfrak{p}_i := p\mathcal{O}_\mathrm{K} + f_i(\alpha)\mathcal{O}_\mathrm{K}$ be the ideal of $\mathcal{O}_\mathrm{K}$ generated by p and $f_i(\alpha)$.

1.3. For $i = 1, \dots, r$, consider the ideal $\mathfrak{m}_i := p\mathrm{R} + f_i(\alpha)\mathrm{R} \subset \mathrm{R}$. Prove that $\mathfrak{m}_i$ is a maximal ideal of R, and that the quotient $\mathrm{R}/\mathfrak{m}_i$ has order $p^{\deg f_i}$.

1.4. Deduce that $\mathfrak{p}_i$ is a prime ideal of $\mathcal{O}_\mathrm{K}$, that $\mathfrak{p}_i$ lies above p and that $f(\mathfrak{p}_i/p) = \deg f_i$.

1.5. Prove that $\mathfrak{p}_i + \mathfrak{p}_j = \mathcal{O}_\mathrm{K}$ for all $i \neq j$. *Hint: $\bar{f_i}$ and $\bar{f_j}$ are coprime in $\mathbb{F}_p[\mathrm{X}]$.*

1.6. By showing that $\prod_{i=1}^r f_i(\alpha)^{e_i} \in p\mathcal{O}_\mathrm{K}$, prove that $p\mathcal{O}_\mathrm{K} \supset \prod_{i=1}^r \mathfrak{p}_i^{e_i}$.

1.7. Comparing norms, deduce that $p\mathcal{O}_\mathrm{K} = \prod_i \mathfrak{p}_i^{e_i}$.

Therefore, for any prime p satisfying condition $(*)$, the decomposition of $p\mathcal{O}_\mathrm{K}$ can be read off from the the decomposition of $\bar{f}$ as a product of irreducible polynomials in $\mathbb{F}_p[\mathrm{X}]$.

1.8. Let α be as above. We let $\mathrm{D}_\alpha = \mathrm{D}(1, \alpha, \dots, \alpha^{n-1})$ and Δ_K be the discriminant of K. Prove that $\mathrm{D}_\alpha = (\#\mathcal{O}_\mathrm{K}/\mathbb{Z}[\alpha])^2 \cdot \Delta_\mathrm{K}$ in $\mathbb{Z}$.

1.9. Deduce that a prime p such that p^2 does not divide D_α satisfies $(*)$.

As an application, consider the following example. Let $\beta \in \mathbb{C}$ be a root of $f(\mathrm{X}) := \mathrm{X}^3 - \mathrm{X} - 1 \in \mathbb{Z}[\mathrm{X}]$, and $\mathrm{K} := \mathbb{Q}(\beta)$ be the corresponding number field.

1.10. Prove that $f(\mathrm{X})$ is irreducible.

1.11. In the ring of integers of K, describe the factorisation of primes $p \in \{2, 3, \dots, 23\}$.

Exercise 2 – Let $d \neq 0, 1$ be a square free integer, and $\mathrm{K} = \mathbb{Q}(\sqrt{d})$ be the corresponding quadratic field. We let $\mathcal{O}_\mathrm{K}$ denote the ring of integers of K.

2.1. For a prime p, what are the possible types of decomposition of $p\mathcal{O}_\mathrm{K}$ as a product of prime ideals?

2.2. Depending on the value of $d \bmod 4$, make a list of the primes that ramify in $\mathcal{O}_\mathrm{K}$. Deduce that there are only finitely many primes that ramify in K.

For any integer $a \in \mathbb{Z}$, and any prime number p, define the Legendre symbol

$$\left(\frac{a}{p}\right) := \begin{cases} 0 & \text{if } p \mid a, \\ +1 & \text{if } p \nmid a \text{ and } a \text{ is a square modulo } p, \\ -1 & \text{if } p \nmid a \text{ and } a \text{ is not a square modulo } p. \end{cases}$$

2.3. Prove that the map $a \mapsto \left(\frac{a}{p}\right)$ is multiplicative.

2.4. Let p be an odd prime. Describe the splitting behaviour of $p\mathcal{O}_\mathrm{K}$ in terms of $\left(\frac{d}{p}\right)$.

Hint: you may use the previous exercise.

2.5. Prove that 2 ramifies in K if and only if $d \equiv 2, 3 \bmod 4$.

2.6. Prove that 2 splits in K if and only if $d \equiv 1 \bmod 8$. When is 2 inert in K?

2.7. ($\star$) Let $f \in \mathbb{Z}[\mathrm{X}]$ be a non-constant polynomial with integral coefficients. Prove that there are infinitely many primes p such that the equation $f(x) \equiv 0 \bmod p$ has a solution.

2.8. Deduce from the preceding question that there are infinitely many primes that split in K.

Exercise 3 – Let A be a Dedekind ring of characteristic 0, with field of fractions K. Let L/K be a finite field extension of degree n, and B denote the integral closure of A in L. Let $\mathfrak{p}$ be a non zero prime ideal of A. Since B is a Dedekind ring, one can decompose the ideal $\mathfrak{p}\mathrm{B}$ as $\mathfrak{p}\mathrm{B} = \mathfrak{P}_1^{e_1} \cdot \dots \cdot \mathfrak{P}_r^{e_r}$ for some distinct non zero prime ideals $\mathfrak{P}_i$ of B and positive integers e_i.

As in the lecture notes, for all $i \in \{1, \dots, r\}$, we let $f(\mathfrak{P}_i/\mathfrak{p}) := [\mathrm{B}/\mathfrak{P}_i : \mathrm{A}/\mathfrak{p}]$ denote the residual degree of $\mathfrak{P}_i$ over $\mathfrak{p}$ and $e(\mathfrak{P}_i/\mathfrak{p}) := e_i$ denote the ramification index.

3.1. Prove that

$$\sum_{i=1}^{r} e(\mathfrak{P}_i/\mathfrak{p}) \cdot f(\mathfrak{P}_i/\mathfrak{p}) = \dim_{\mathrm{A}/\mathfrak{p}}(\mathrm{B}/\mathfrak{p}\mathrm{B}) = [\mathrm{L} : \mathrm{K}].$$

Exercise 4 – Let A be a ring. Let $\mathrm{B}_1, \dots, \mathrm{B}_r$ be rings containing A which, as A-modules, are free and finitely generated. Let $\mathrm{B} := \prod_{i=1}^r \mathrm{B}_i$ denote the product ring. For any ring R containing A, we denote by D(R/A) the discriminant of R over A.

4.1. Prove that we have $\mathrm{D}(\mathrm{B}/\mathrm{A}) = \prod_{i=1}^r \mathrm{D}(\mathrm{B}_i/\mathrm{A})$.
