Exercise sheet #2

Exercises marked with a ✎ are to be handed in before **Monday October 7** 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 – Let M be a free $\mathbb{Z}$-module of rank n, and consider a $\mathbb{Z}$-linear map $f : \mathrm{M} \to \mathrm{M}$.

1.1. In a given $\mathbb{Z}$-basis $\mathrm{B} = (e_1, \ldots, e_n)$ of M, the map f has a matrix $\mathrm{A} \in \mathrm{M}_n(\mathbb{Z})$. How do the matrices of f in two $\mathbb{Z}$-bases of M compare?

1.2. Deduce from the previous question that the quantity $|\det f| \in \mathbb{Z}$ is defined unambiguously.

1.3. Prove that there is an isomorphism of $\mathbb{Z}$-modules $\mathrm{M}/\operatorname{Ker}(f) \cong \operatorname{Im}(f)$.

1.4. Prove that the image $\operatorname{Im}(f)$ is a free $\mathbb{Z}$-module of rank $n' \leqslant n$.

1.5. We assume here that the kernel of f is finite. Prove that $|\det f| = \#(\mathrm{M}/\operatorname{Im}(f))$.

Now let K be a number field of degree n, and R be a subring of K which, as a $\mathbb{Z}$-module, is free of rank n. For any $\beta \in \mathrm{R} \smallsetminus \{0\}$, the norm of β is the determinant, denoted by $\mathrm{N}(\beta)$, of the $\mathbb{Z}$-linear map $m_\beta : \mathrm{R} \to \mathrm{R}$ defined by $m_\beta : x \mapsto \beta x$.

1.6. Show that $\mathrm{N}(\beta) \in \mathbb{Z}$.

1.7. Give a relation between $|\mathrm{N}(\beta)|$ and the cardinality of the quotient ring $\mathrm{R}/(\mathrm{R}\beta)$.

Exercise 2 (Quadratic number fields) – Recall that a nonzero integer d is called squarefree if and only if, for any prime p, $p \mid d \Rightarrow p^2 \nmid d$. For any squarefree integer d, $\sqrt{d}$ denotes the complex number $\sqrt{d}$ (resp. $i\sqrt{-d}$) if d is positive (resp. negative).

Let K be a quadratic field extension of $\mathbb{Q}$ (i.e., the extension $\mathrm{K}/\mathbb{Q}$ has degree 2).

2.1. Show that there exists a squarefree integer $d \neq 0$ such that $\mathrm{K} = \mathbb{Q}(\sqrt{d})$.

2.2. Prove that d is uniquely determined by K. In other words, for distinct nonzero squarefree integers d_1, d_2, show that the fields $\mathbb{Q}(\sqrt{d_1})$ and $\mathbb{Q}(\sqrt{d_2})$ are not isomorphic.

2.3. Make a list of the embeddings $\mathrm{K} \hookrightarrow \mathbb{C}$.

2.4. Let $x = a + b\sqrt{d} \in \mathrm{K}$. Compute the trace $\mathrm{Tr}_{\mathrm{K}/\mathbb{Q}}(x)$ and the norm $\mathrm{N}_{\mathrm{K}/\mathbb{Q}}(x)$, and deduce an expression of the minimal polynomial of x over $\mathbb{Q}$.

Exercise 3 (Integers in quadratic fields) {✎ : 5 points} – Let $d \neq 0$ be a squarefree integer and $\mathrm{K} = \mathbb{Q}(\sqrt{d})$ be the corresponding quadratic field. Let $\mathcal{O}_d$ denote the set of algebraic integers in K. Recall that $\mathcal{O}_d$ is a subring of K. We let $\mathcal{O}_d^\times$ denote the group of units of $\mathcal{O}_d$.

3.1. Show that $x \in \mathrm{K}$ belongs to $\mathcal{O}_d$ if and only if $\mathrm{Tr}_{\mathrm{K}/\mathbb{Q}}(x)$ and $\mathrm{N}_{\mathrm{K}/\mathbb{Q}}(x)$ are integers.

3.2. Let $\mathrm{R} = \mathbb{Z}[\sqrt{d}]$. Prove that R is a subring of $\mathcal{O}_d$.

If $d \equiv 2, 3 \bmod 4$, we let $\alpha_d = \sqrt{d}$. If $d \equiv 1 \bmod 4$, we set $\alpha_d := (1+\sqrt{d})/2$.

3.3. Prove first that α_d is integral over $\mathbb{Z}$. Then show that $\mathcal{O}_d = \mathbb{Z}[\alpha_d]$.

3.4. Show that $x \in \mathrm{K}$ is a unit of $\mathcal{O}_d$ if and only if $\mathrm{N}_{\mathrm{K}/\mathbb{Q}}(x) = \pm 1$. *Hint:* $\mathrm{N}_{\mathrm{K}/\mathbb{Q}}$ *is multiplicative.*

3.5. If $d < 0$, determine $\mathcal{O}_d^\times$.

We now specialise to the case where $\mathrm{K} = \mathbb{Q}(\sqrt{2})$ (i.e., $d = 2$), and we consider $\epsilon := 1 + \sqrt{2} \in \mathbb{Q}(\sqrt{2})$.

3.6. Show that ϵ is a unit in $\mathcal{O}_2$, and that ϵ is not a root of unity. Deduce that $\mathcal{O}_2^\times$ is infinite.

3.7. By using powers of ϵ, provide infinitely many solutions $(x, y) \in \mathbb{Z}^2$ to the equation $x^2 - 2y^2 = \pm 1$.

Exercise 4 – Let K be a field of characteristic 0 or a finite field. Fix an algebraic closure C of K. Assume that K'/K is a finite extension of degree n. Consider the set $\mathrm{S} := \{\sigma : \mathrm{K}' \to \mathrm{C} : \sigma|_{\mathrm{K}} = \mathrm{id}\}$ of field morphisms $\mathrm{K}' \to \mathrm{C}$ whose restriction to K is trivial.

4.1. Show that S is finite and that $\#\mathrm{S} = n$.

Exercise 5 (Trace and norm in extensions) {✎ : 5 points} – Let K be a field of characteristic 0 or a finite field, and L/K be a finite extension of degree n. Given $x \in \mathrm{L}$, we let $m_x : \mathrm{L} \to \mathrm{L}$ denote the K-linear map "multiplication by x". We let $\mathrm{Tr}_{\mathrm{L}/\mathrm{K}}$ and $\mathrm{N}_{\mathrm{L}/\mathrm{K}}$ denote the trace and the norm (relative to the extension L/K), respectively.

5.1. Prove that the trace $\mathrm{Tr}_{\mathrm{L}/\mathrm{K}} : \mathrm{L} \to \mathrm{L}$ is K-linear, and that $\mathrm{Tr}_{\mathrm{L}/\mathrm{K}}(y) \in \mathrm{K}$ for all $y \in \mathrm{L}$.

5.2. Show that the norm $\mathrm{N}_{\mathrm{L}/\mathrm{K}} : \mathrm{L} \to \mathrm{L}$ is multiplicative (that is to say, $\mathrm{N}_{\mathrm{L}/\mathrm{K}}(yz) = \mathrm{N}_{\mathrm{L}/\mathrm{K}}(y)\,\mathrm{N}_{\mathrm{L}/\mathrm{K}}(z)$ for all $y, z \in \mathrm{L}$), and that $\mathrm{N}_{\mathrm{L}/\mathrm{K}}(y) \in \mathrm{K}$ for all $y \in \mathrm{L}$.

5.3. Describe the restrictions to K of $\mathrm{Tr}_{\mathrm{L}/\mathrm{K}} : \mathrm{L} \to \mathrm{L}$ and $\mathrm{N}_{\mathrm{L}/\mathrm{K}} : \mathrm{L} \to \mathrm{L}$.

5.4. Let M/L be an arbitrary extension, and $x \in \mathrm{M}$ be algebraic over L. Show that x is algebraic over K, and relate the degree of x over L to its degree over K.

5.5. Let M/L be a finite extension. Show that, for all $x \in \mathrm{M}$, we have

$$\mathrm{Tr}_{\mathrm{L}/\mathrm{K}}(\mathrm{Tr}_{\mathrm{M}/\mathrm{L}}(x)) = \mathrm{Tr}_{\mathrm{M}/\mathrm{K}}(x), \text{ and } \mathrm{N}_{\mathrm{L}/\mathrm{K}}(\mathrm{N}_{\mathrm{M}/\mathrm{L}}(x)) = \mathrm{N}_{\mathrm{M}/\mathrm{K}}(x).$$

Let $\alpha \in \mathrm{L}$. Assume that the minimal polynomial f_α of α over K has degree d. We denote the roots of f_α in $\bar{\mathrm{K}}$ by $\alpha_1, \ldots, \alpha_d$.

5.6. Prove that d divides $[\mathrm{L} : \mathrm{K}] = n$. *Hint: consider the extension* $\mathrm{K}(x)$ *of* K.

5.7. Prove that the characteristic polynomial of $m_\alpha : \mathrm{L} \to \mathrm{L}$ equals $f_\alpha^{[\mathrm{L}:\mathrm{K}]/d}$.

5.8. Deduce that $\mathrm{Tr}_{\mathrm{L}/\mathrm{K}}(\alpha) = \dfrac{[\mathrm{L} : \mathrm{K}]}{d} \displaystyle\sum_{i=1}^{d} \alpha_i$ and that $\mathrm{N}_{\mathrm{L}/\mathrm{K}}(\alpha) = \left(\displaystyle\prod_{i=1}^{d} \alpha_i\right)^{[\mathrm{L}:\mathrm{K}]/d}$.

Exercise 6 – Let K be a field of characteristic 0. Let A be a subring of K such that K is the field of fractions of A. Let L/K be a finite field extension of degree n. Fix an element $\alpha \in \mathrm{L}$ which is integral over A.

6.1. Prove that the coefficients of the characteristic polynomial of m_α are integral over A.

6.2. Deduce that $\mathrm{Tr}_{\mathrm{L}/\mathrm{K}}(\alpha)$ and $\mathrm{N}_{\mathrm{L}/\mathrm{K}}(\alpha)$ are integral over A.
