Exercise sheet #5

Exercises marked with a ✎ are to be handed in before **Monday October 28** at noon, in the mailbox at Spiegelgasse 1. Each of these is worth a number of points, as indicated.
Questions marked with a ⋆ are more difficult.

Exercise 1 – Let K be a number field of degree n, whose ring of integers is denoted by $\mathcal{O}_K$. Write r_1 for the number of reals embeddings of K, and r_2 for the number of pairs of complex embeddings. We denote by $\sigma : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ the canonical embedding of K. We identify $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ with $\mathbb{R}^n$.

1.1. Let M be a free $\mathbb{Z}$-submodule of K of rank n. Prove that $\sigma(M)$ is a lattice in $\mathbb{R}^n$.

1.2. In the same setting, prove that the volume of $\sigma(M) \subset \mathbb{R}^n$ is $2^{-r_2} \cdot \left|\det[\sigma_i(x_j)]_{1\leqslant i,j\leqslant n}\right|$, for any choice of $\mathbb{Z}$-basis $x_1, \dots, x_n$ of M.

1.3. Let I be an integral ideal in $\mathcal{O}_K$. Prove that $\sigma(I)$ is a lattice in $\mathbb{R}^n$.

1.4. For any integral ideal I in $\mathcal{O}_K$, show that the volume of $\sigma(I)$ equals $2^{-r_2} \cdot |\Delta_K|^{1/2} \cdot N(I)$.

Exercise 2 (Hermite's theorem) – The goal of this exercise is to prove the following important result of Hermite: *In $\mathbb{C}$, there are only finitely many number fields with bounded discriminant.*

2.1. Let $d \geqslant 1$ be an integer and $C \in \mathbb{R}_{>0}$. Prove that there are only finitely many monic polynomials $f \in \mathbb{Z}[X]$ of degree d, whose coefficients are bounded (in absolute value) by C.

2.2. Let $\overline{\mathbb{Z}}$ denote the subring of $\mathbb{C}$ consisting of all complex numbers which are algebraic integers over $\mathbb{Z}$. Let $d \geqslant 1$ be a given integer. For any $C > 0$, consider the set

$$S := \{x \in \overline{\mathbb{Z}} : [\mathbb{Q}(x) : \mathbb{Q}] = d, \text{ and all the conjugates of } x \text{ have complex absolute value } \leqslant C\}.$$

Prove that S is finite.

Let K be a number field of discriminant Δ_K, and degree n over $\mathbb{Q}$. Write $\{\sigma_1, \dots, \sigma_n\}$ for the n distinct $\mathbb{Q}$-embeddings $K \to \mathbb{C}$. We order these so that the first r_1 embeddings are real, and the last $2r_2$ are complex.

2.3. Let $x \in K$ be such that $\sigma_i(x) \neq \sigma_1(x)$ for all $i \in \{2, \dots, n\}$. Prove that $K = \mathbb{Q}(x)$.

2.4. Let $\delta \in \mathbb{R} \smallsetminus \{0\}$. If $r_1 > 0$, we let

$$B := \left\{ (y_1, \dots, y_{r_1}, z_1, \dots, z_{r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \ : \begin{cases} |y_1| \leqslant 2^n(\pi/2)^{-r_2}|\delta|^{1/2}, \\ |y_i| \leqslant 1/2 \text{ for } 2 \leqslant i \leqslant r_1, \\ |z_j| \leqslant 1/2 \text{ for } 1 \leqslant j \leqslant r_2 \end{cases} \right\}.$$

If $r_1 = 0$, we let

$$B := \left\{ (z_1, \dots, z_{r_2}) \in \mathbb{C}^{r_2} \ : \begin{cases} |z_1 - \bar{z_1}| \leqslant 2^n(\pi/2)^{1-r_2}|\delta|^{1/2}, \ |z_1 + \bar{z_1}| \leqslant 1/2, \\ \text{and } |z_j| \leqslant 1/2 \text{ for } 2 \leqslant j \leqslant r_2 \end{cases} \right\}.$$

Prove that B is a compact and convex subset of $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \simeq \mathbb{R}^{r_1+2r_2}$ which is symmetric about the origin. Prove that $\mu(B) = 2^{n-r_2}|\delta|^{1/2}$. *Hint:* B *is a product of discs, intervals, and rectangles.*

2.5. Let $\delta \in \mathbb{R}_{>0}$. Assuming that $|\Delta_K| \leqslant \delta$, prove that the degree n of K is bounded from above.

2.6. Prove that there exists $x \in \mathcal{O}_K \smallsetminus \{0\}$ such that $\sigma(x) \in B$. Deduce that $K = \mathbb{Q}(x)$. *Hint: use* **2.3**.

2.7. Conclude that, in $\mathbb{C}$, there are only finitely many number fields with discriminant bounded by δ.

Exercise 3 (A non monogenic ring of integers) – Let us consider the integral polynomial $F(X) = X^3 - X^2 - 2X - 8 \in \mathbb{Z}[X]$. We choose a root $\alpha \in \mathbb{C}$ of $F(X)$, and let $K := \mathbb{Q}(\alpha)$.

3.1. Prove that $F(X)$ is irreducible in $\mathbb{Q}[X]$. Deduce that K has degree 3. *Hint: show that* $F(X)$ *has no roots in* $\mathbb{Z}$.

3.2. It is clear that $\alpha \in \mathcal{O}_K$. Prove that $D(1, \alpha, \alpha^2) = -4 \cdot 503$.

3.3. Let $\beta := (\alpha^2 + \alpha)/2 \in K$. Check that β is a root of $G(X) = X^3 - 3X^2 - 10X - 8 \in \mathbb{Z}[X]$. Deduce that β is integral. Prove that $K = \mathbb{Q}(\beta)$.

3.4. Let $A := \mathbb{Z} + \ \mathbb{Z}\alpha + \mathbb{Z}\beta$. Prove that A is a subring of K, and that $\mathbb{Z}[\alpha] \subsetneq A \subseteq \mathcal{O}_K$.

3.5. By a direct computation, show that $D(1, \alpha, \beta) = -503$. Conclude that $A = \mathcal{O}_K$.

3.6. For any $\gamma \in \mathcal{O}_K$, prove that $D(1, \gamma, \gamma^2)$ is even. Deduce that $\mathbb{Z}[\gamma]$ is a strict subring of $\mathcal{O}_K$.

Hence the ring of integers of $\mathcal{O}_K$ is $\mathbb{Z}[\alpha, \beta]$, and $\mathcal{O}_K$ cannot be written as $\mathcal{O}_K = \mathbb{Z}[\gamma]$ for any $\gamma \in \mathcal{O}_K$. One says that $\mathcal{O}_K$ is not monogenic.

Exercise 4 (Class groups of some quadratic fields) {✎ : 10 points} – Let K be a number field with ring of integers $\mathcal{O}_K$. Let $h_K := \#\mathrm{Cl}(O_K)$ denote the order of the class group of $\mathcal{O}_K$. We let $M_K := \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \cdot |\Delta_K|^{1/2}$ denote the Minkowski constant of K.

4.1. Prove that $\mathcal{O}_K$ is a principal ideal domain if and only if $h_K = 1$.

4.2. Prove that $\mathrm{Cl}(\mathcal{O}_K)$ is generated by prime ideals of $\mathcal{O}_K$ of norm $\leqslant M_K$.

4.3. Let $n \geqslant 1$ be an integer which is coprime to h_K. Let $u, v \in \mathcal{O}_K$ be two coprime elements whose product is an n-th power in $\mathcal{O}_K$. Show that, up to multiplication by units, both u and v are n-th powers in $\mathcal{O}_K$.

In the remainder of this exercise, K will be a quadratic field: we write $K = \mathbb{Q}(\sqrt{d})$ for a suitable squarefree integer $d \neq 0, 1$.

4.3. Compute the discriminant of $\mathcal{O}_K$, and express r_1, r_2 in terms of d. Give an expression of the Minkowski constant of K in terms of d.

4.4. If $d \in \{-7, -3, -2, -1, 2, 3, 5, 13\}$, prove that $\mathcal{O}_K$ is principal.

4.5. For $d \in \{-19, -15, -11, -5, 6, 7, 17, 21, 29, 33\}$, prove that any ideal of K is in the class of an integral ideal of norm 1 or 2.

4.6. For $d \in \{-19, -11, 21, 29\}$, show that $2\mathcal{O}_K$ is a prime ideal. Deduce that $\mathcal{O}_K$ is principal in these cases. *Hint: you may show that there are no elements of norm* 2 *in* $\mathcal{O}_K$.

4.7. If $d \equiv 2, 3 \bmod 4$, show that K contains a principal ideal of norm 2 if and only if $\exists a, b \in \mathbb{Z}$ such that $a^2 - db^2 = \pm 2$. Deduce that $\mathcal{O}_K$ is principal for $d = 6, 7$.

4.8. If $d = -5$, prove that $\mathcal{O}_K$ has two ideal classes. *Hint: Show that the ideal* $(2, \sqrt{d}+1)$ *has norm* 2.

4.9. Find all integers $(x, y) \in \mathbb{Z}^2$ such that $y^3 = x^2 + 5$.
