Exercise sheet #6

Exercises marked with a ✎ are to be handed in before **Monday November 4** 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 (An upper bound on the class number) {✎ : 6 points} – Let K be a number field of degree n.

1.1. Let $\mathrm{X} \geqslant 2$. Prove that there are only finitely many ideals $\mathfrak{b}$ of $\mathcal{O}_\mathrm{K}$ with $\mathrm{N}\mathfrak{b} \leqslant \mathrm{X}$. Moreover, prove that the number of such ideals can be bounded only in terms of n and X. *Hint: you may prove that, for $m \geqslant 1$, $\#\{\mathfrak{b} \subset \mathcal{O}_\mathrm{K} : \mathrm{N}\,\mathfrak{b} = m\} \leqslant \#\{(x_1, \ldots, x_n) \in \mathbb{Z}^n_{\geqslant 1} : \prod_{i=1}^n x_i = m\}$.*

For any non-zero integral ideal of $\mathfrak{a} \subset \mathcal{O}_\mathrm{K}$, define $\tau(\mathfrak{a})$ to be the number of non-zero ideals $\mathfrak{b} \subset \mathcal{O}_\mathrm{K}$ which divide $\mathfrak{a}$.

1.2. Prove that $\tau(\mathfrak{a})$ is well-defined, and that $\tau(\mathfrak{a}) = \prod_{\mathfrak{p}} (v_\mathfrak{p}(\mathfrak{a}) + 1)$, where the product is over all non-zero prime ideals $\mathfrak{p} \subset \mathcal{O}_\mathrm{K}$, and $v_\mathfrak{p}$ denotes the $\mathfrak{p}$-adic valuation.

Let us first prove the so-called "divisor bound" for ideals of K: *For all $\delta > 0$, there is a constant $c > 0$, depending at most on n and δ, such that $\tau(\mathfrak{a}) \leqslant c \cdot (\mathrm{N}\mathfrak{a})^\delta$ for all non-zero ideals $\mathfrak{a} \subset \mathcal{O}_\mathrm{K}$.*

Let $\delta > 0$ and $\mathfrak{p} \subset \mathcal{O}_\mathrm{K}$ be a non-zero prime ideal.

1.3. If $\mathrm{N}\mathfrak{p} \geqslant \exp(1/\delta)$, prove that $(\mathrm{N}\mathfrak{p}^v)^\delta \geqslant v + 1$ for all integers $v \geqslant 0$. *Hint:* $\forall u \in \mathbb{R}$, $\exp(u) \geqslant u + 1$.

1.4. If $\mathrm{N}\mathfrak{p} \leqslant \exp(1/\delta)$, prove that $\dfrac{v+1}{(\mathrm{N}\mathfrak{p}^v)^\delta} \leqslant \dfrac{(\mathrm{N}\mathfrak{p})^\delta}{\log\{(\mathrm{N}\mathfrak{p})^\delta\}}$ for all integers $v \geqslant 0$.

Now, let $\mathfrak{a}$ be a non-zero integral ideal of $\mathcal{O}_\mathrm{K}$.

1.5. Writing $\tau(\mathfrak{a})/(\mathrm{N}\mathfrak{a})^\delta$ as a finite product over prime ideals, show that

$$\frac{\tau(\mathfrak{a})}{(\mathrm{N}\mathfrak{a})^\delta} \leqslant \prod_{\mathrm{N}\mathfrak{p} \leqslant \exp(1/\delta)} \frac{(\mathrm{N}\mathfrak{p})^\delta}{\log\{(\mathrm{N}\mathfrak{p})^\delta\}},$$

where the product runs over non-zero prime ideals $\mathfrak{p} \subset \mathcal{O}_\mathrm{K}$ such that $\mathrm{N}\mathfrak{p} \leqslant \exp(1/\delta)$.

1.6. Conclude the proof of the divisor bound.

Let Δ_K be the discriminant of K, h_K be the class number of $\mathcal{O}_\mathrm{K}$, and $\mathrm{M}_\mathrm{K} = (4/\pi)^{r_2} \cdot n! \cdot n^{-n} \cdot |\Delta_\mathrm{K}|^{1/2}$ denote the Minkowski constant of K.

1.7. Prove that $h_\mathrm{K} \leqslant \displaystyle\sum_{1 \leqslant n \leqslant \mathrm{M}_\mathrm{K}} \#\{\text{ideals } \mathfrak{b} \subset \mathcal{O}_\mathrm{K} : \mathrm{N}\mathfrak{b} = n\} \leqslant \sum_{1 \leqslant n \leqslant \mathrm{M}_\mathrm{K}} \tau(n\mathcal{O}_\mathrm{K})$.

1.8. Deduce from the above the following upper bound on h_K: *For all $\delta > 0$, there exists a constant $c' > 0$, depending at most on n and δ, such that $h_\mathrm{K} \leqslant c' \cdot |\Delta_\mathrm{K}|^{1/2+\delta}$.*

Exercise 2 (Fundamental units in real quadratic fields) {✎ : 3 points} – Let $d > 1$ be a squarefree integer.

If $d \equiv 2, 3 \bmod 4$, we let $b_d \geqslant 0$ denote the smallest integer such that one of $db_d^2 + 1$ or $db_d^2 - 1$ is the square of an integer $a_d \geqslant 0$. We let $\varepsilon_d := a_d + b_d\sqrt{d} \in \mathbb{Q}(\sqrt{d})$.

2.1. Check that ε_d is well-defined.

2.2. Prove that ε_d is the fundamental unit in the ring of integers of $\mathbb{Q}(\sqrt{d})$.

If $d \equiv 1 \bmod 4$, we let $b_d \geqslant 0$ denote the smallest integer such that one of db_d^2+4 or db_d^2-4 is the square of an integer $a_d \geqslant 0$. We let $\varepsilon_d := \frac{a_d+b_d\sqrt{d}}{4} \in \mathbb{Q}(\sqrt{d})$.

2.3. Prove that ε_d is the fundamental unit in the ring of integers of $\mathbb{Q}(\sqrt{d})$.

2.4. Write a table of the fundamental units in $\mathbb{Q}(\sqrt{d})$ for $d \in \{2,3,6,7,10,11\}$. Same question for $d \in \{5,13,17,21\}$.

2.5. The fundamental unit in $\mathbb{Q}(\sqrt{67})$ is $48842+5967\sqrt{67}$. What is the drawback of this method to compute the fundamental unit of $\mathbb{Q}(\sqrt{d})$?

Exercise 3 (Counting units in real quadratic fields) – For any squarefree integer $d \geqslant 2$, we let $\varepsilon_d > 1$ denote the fundamental unit of $\mathbb{Q}(\sqrt{d})$. Consider the following two subsets of $\mathbb{R}$:

$$\mathrm{U}_{fun} := \{\varepsilon_d,\ d \geqslant 2 \text{ squarefree}\}, \qquad \text{and} \qquad \mathrm{U}_{all} := \{\varepsilon_d^k,\ d \geqslant 2 \text{ squarefree}, k \geqslant 1\}.$$

Thus, U_{fun} contains all fundamental units of real quadratic fields.

3.1. For any $\mathrm{X} \geqslant 2$, prove that $\mathrm{U}_{fun} \cap (1,\mathrm{X}]$ is a finite set. We write $f(\mathrm{X})$ for its cardinality.

3.2. Let $d > 1$ be a squarefree integer and u be a unit in $\mathbb{Q}(\sqrt{d}) \subset \mathbb{R}$. We write $u = a + b\sqrt{d}$ for some half-integers $a, b \in \frac{1}{2}\mathbb{Z}$. Prove that $1 < u < \mathrm{X}$ if and only if $1 < a < (\mathrm{X}^2 \pm 1)/(2\mathrm{X})$.

3.3. Given $a \in \frac{1}{2}\mathbb{Z}$ satisfying the above inequalities and a sign $\sigma \in \{\pm 1\}$, prove that there is a unique choice of $b \in \frac{1}{2}\mathbb{Z}$ and squarefree $d > 1$ such that $a + b\sqrt{d}$ is a unit of norm σ. *Hint:* $a^2 + \sigma = b^2 d$.

3.4. Counting the number of possibilities for a and σ, deduce that $\#\mathrm{U}_{all} \cap (1,\mathrm{X}] = 2\mathrm{X} + \mathrm{O}(1)$ as $\mathrm{X} \to \infty$. We write $a(\mathrm{X})$ for $\#\mathrm{U}_{all} \cap (1,\mathrm{X}]$.

3.5. Prove that $a(\mathrm{X}) = \sum_{k=1}^{\infty} f(\mathrm{X}^{1/k})$ for X large enough, where the sum is actually finite.

The Möbius function $\mu : \mathbb{Z}_{\geqslant 1} \to \{-1,0,1\}$ satisfies $\displaystyle\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1. \end{cases}$

3.6. Deduce from the previous question that $f(\mathrm{X}) = \sum_{j=1}^{\infty} \mu(j) \cdot a(\mathrm{X}^{1/j})$ for X large enough.

3.7. Conclude that $f(\mathrm{X}) = 2\mathrm{X} + o(\mathrm{X})$ as $\mathrm{X} \to \infty$. In particular, we have $\lim_{\mathrm{X}\to\infty} \frac{1}{\mathrm{X}} \#\mathrm{U}_{fun} \cap (1,\mathrm{X}] = \frac{1}{2}$.

Exercise 4 (Localisation of ideals) – Let A be an integral domain, and $\mathrm{S} \subset \mathrm{A} \smallsetminus \{0\}$ be a multiplicatively stable subset which contains 1. We denote the localisation of A at S by $\mathrm{A}' := \mathrm{S}^{-1}\mathrm{A}$.

4.1. Let I' be an ideal of A'. Prove that $(\mathrm{I}' \cap \mathrm{A}) \cdot \mathrm{A}' = \mathrm{I}'$.

4.2. Deduce that the map $r : \mathrm{I}' \mapsto \mathrm{I}' \cap \mathrm{A}$ is a non-decreasing injective map from the set of ideals of A' to the set of ideals of A.

4.3. Let P' be a prime ideal of A'. Prove that $r(\mathrm{P}') = \mathrm{P}' \cap \mathrm{A}$ is a prime ideal of A, and that $r(\mathrm{P}') \cap \mathrm{S} = \varnothing$.

4.4. Deduce that the map $s : \mathrm{P}' \mapsto \mathrm{P}' \cap \mathrm{A}$ provides a bijection from the set of prime ideals of A' to the set of prime ideals of A which are disjoint from S. You may show that the map $\mathrm{P} \mapsto \mathrm{P} \cdot \mathrm{A}'$ is the inverse of s.
