Algebraic Number Theory 2019-20
Example Sheet 4

Hand in the answers to questions 4 and 6 (marked with †).
Deadline 12 noon Monday, Week 10 (2 December)
For questions about the example sheet, it is best to ask them on Moodle. Questions must be asked before 5 pm on Friday to get an answer before the deadline.

1. Let $K = \mathbb{Q}(\sqrt{-2})$. Show that $\mathcal{O}_K$ is a principal ideal domain. Deduce that every prime $p \equiv 1, 3 \pmod 8$ can be written as $p = x^2 + 2y^2$ with $x, y \in \mathbb{Z}$. (You will need to use quadratic reciprocity from Introduction to Number Theory.)

2. Compute the class groups of the following quadratic fields.
$$\mathbb{Q}(\sqrt{5}), \quad \mathbb{Q}(\sqrt{-6}), \quad \mathbb{Q}(\sqrt{7}).$$

3. Prove that the class group of $\mathbb{Q}(\sqrt{-30})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

†4. Let $K = \mathbb{Q}(\sqrt{26})$. You may use without proof the following factorisations of ideals in $\mathcal{O}_K = \mathbb{Z}[\sqrt{26}]$:
   - $\langle 2 \rangle = \mathfrak{p}_2^2$ where $\mathfrak{p}_2 = \langle 2, \sqrt{26} \rangle$ is a prime ideal of norm 2.
   - $\langle 3 \rangle$ is a prime ideal in $\mathcal{O}_K$.
   - $\langle 5 \rangle = \mathfrak{p}_5 \mathfrak{q}_5$ where $\mathfrak{p}_5 = \langle 5, 1+\sqrt{26} \rangle$ and $\mathfrak{q}_5 = \langle 5, -1+\sqrt{26} \rangle$ are prime ideals of norm 5.

   (i) Write a list of the quadratic residues (i.e. squares) mod 13. Use this to show that $\mathfrak{p}_2$ is not principal.
   (ii) Find the prime factorisation of $\langle 6 + \sqrt{26} \rangle$ in $\mathcal{O}_K$.
   (iii) Use the Minkowski bound to prove that $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$.

5. Show that the cyclotomic field $\mathbb{Q}(\zeta_5)$ has class number 1.

†6. Let d be a square-free composite positive integer such that $-d \equiv 2$ or $3 \bmod 4$. Let p be a prime factor of d and let $K = \mathbb{Q}(\sqrt{-d})$.
   (i) Prove that $\mathcal{O}_K$ contains no element of norm $\pm p$.
   (ii) By considering the prime factorisation of the ideal $\langle p \rangle$, prove that the class number of K is even.

7. Let $\mathfrak{a}, \mathfrak{b}$ be ideals of $\mathcal{O}_K$ such that there is no prime ideal which divides both $\mathfrak{a}$ and $\mathfrak{b}$. Suppose that
$$\mathfrak{a}\mathfrak{b} = \mathfrak{c}^n$$
for some ideal $\mathfrak{c} \subseteq \mathcal{O}_K$ and some positive integer n. Prove that there are ideals $\mathfrak{a}', \mathfrak{b}' \subseteq \mathcal{O}_K$ such that
$$\mathfrak{a} = (\mathfrak{a}')^n, \quad \mathfrak{b} = (\mathfrak{b}')^n.$$

8. (i) Prove that the ring of integers of $\mathbb{Q}(\sqrt{-11})$ is a PID.
   (ii) Prove that if $x, y \in \mathbb{Z}$ satisfy $x^3 = y^2 + 11$, then there exist $u, v \in \mathbb{Z}$ such that
$$\left(\frac{u + v\sqrt{-11}}{2}\right)^3 = y + \sqrt{-11}.$$
   (iii) Show that the equation $x^3 = y^2 + 11$ has exactly four solutions in rational integers. Verify that two of these solutions are $(15, \pm 58)$; find the other two.

9. Prove that the only integer solutions to the equation $x^3 = y^2 + 2$ are $(3, \pm 5)$.

10. (i) Using Minkowski's theorem on ideal classes, prove that if K is a number field of degree greater than 1, then $|\Delta_K| > 1$.
    (ii) Show that there are constants $A > 1$ and $c > 0$ such that, for every number field K, $|\Delta_K| > cA^n$.

11. (i) Let C be a positive real number and $s \in \mathbb{N}$. Verify that the symmetric convex set
$$S(s, C) = \{(y_1, z_1, \ldots, y_s, z_s) \in \mathbb{R}^{2s} : |y_1| < 1,\ |z_1| < C,\ y_i^2 + z_i^2 < 1 \text{ for } i = 2, \ldots, s\}$$
has volume $4\pi^{s-1}C$.
    (ii) Let Δ be a positive integer. Let K be a number field such that $i = \sqrt{-1} \in K$ and $|\Delta_K| \leq \Delta$.
      (a) Prove that K has signature $(0, s)$ for some s.
      (b) Let $\iota_K \colon K \to \mathbb{R}^{2s}$ be the canonical embedding of K. Use Minkowski's theorem on lattices to prove that, for a suitable constant C depending only on s and Δ (but not on K), there is a non-zero element $\alpha \in \mathcal{O}_K$ such that $\iota_K(\alpha) \in S(s, C)$.
      (c) Label the embeddings of K as $\sigma_1, \overline{\sigma_1}, \ldots, \sigma_s, \overline{\sigma_s}$. Observe that $|\sigma_1(\alpha)| < \sqrt{1 + C^2}$ and $|\sigma_i(\alpha)| < 1$ for $i = 2, \ldots, s$. Obtain a bound for the coefficients of the minimal polynomial of α over $\mathbb{Q}$.
      (d) By considering $\mathrm{Nm}_{K/\mathbb{Q}}(\alpha)$, prove that $|\sigma_1(\alpha)| > 1$ and hence $\sigma_1(\alpha) \neq \sigma_i(\alpha)$ or $\overline{\sigma_i}(\alpha)$ for $i = 2, \ldots, s$.
      (e) Deduce that $[K : \mathbb{Q}(\alpha)] \leq 2$.
      (f) Show that $K = \mathbb{Q}(i, \alpha)$ (observe that if $[K : \mathbb{Q}(\alpha)] = 2$, then $\sigma_{1|\mathbb{Q}(\alpha)}$ is a real embedding and use this to show that $\mathbb{Q}(i, \alpha) \neq \mathbb{Q}(\alpha)$).
    (iii) Combining (c) and (f) above, show that there are only finitely many number fields K of degree $2s$ satisfying $i \in K$ and $|\Delta_K| \leq \Delta$.
    (iv) You may assume that for every number field L of degree n, $|\Delta_{L(i)}| \leq 4^n |\Delta_L|^2$ (if you are feeling adventurous, you could prove this). Use (iii) to show that there are only finitely many number fields L of degree n satisfying $|\Delta_L| \leq \Delta$.
    (v) Using Q10, show that for any Δ, there are only finitely many number fields whose discriminant has absolute value at most Δ.