Algebraic Number Theory 2019
Example Sheet 3

Hand in the answers to questions 3, 7, 11 (marked with †).
Deadline 2pm Friday, Week 8.

1. Let $\alpha_1, \ldots, \alpha_m$ be elements of $\mathcal{O}_K$ and suppose that $\langle \alpha_1, \ldots, \alpha_m \rangle = \langle \alpha \rangle$. Show that $\mathrm{Norm}(\alpha)$ divides each of $\mathrm{Norm}(\alpha_1), \ldots, \mathrm{Norm}(\alpha_n)$.

2. Let K be a number field. Let α, β be non-zero elements of $\mathcal{O}_K$.
   (i) Show that $\langle \alpha \rangle^{-1} = \langle \alpha^{-1} \rangle$.
   (ii) Give an counterexample to the following claim: $\langle \alpha, \beta \rangle^{-1} = \langle \alpha^{-1}, \beta^{-1} \rangle$.

†3. Let $K = \mathbb{Q}(\sqrt{-5})$. In $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ let

$$\mathfrak{a} = \langle 2, 1+\sqrt{-5} \rangle, \qquad \mathfrak{b} = \langle 3, 1+\sqrt{-5} \rangle, \qquad \mathfrak{b}' = \langle 3, 1-\sqrt{-5} \rangle.$$

   (i) Show that

$$\mathfrak{a}^2 = \langle 2 \rangle, \qquad \mathfrak{b}\mathfrak{b}' = \langle 3 \rangle, \qquad \mathfrak{a}\mathfrak{b} = \langle 1+\sqrt{-5} \rangle, \qquad \mathfrak{a}\mathfrak{b}' = \langle 1-\sqrt{-5} \rangle.$$

   This shows that the Algebra II example of non-unique factorisation $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ comes from grouping the ideal factorization of 6 in two different ways: $(\mathfrak{a}^2) \cdot (\mathfrak{b}\mathfrak{b}')$ and $(\mathfrak{a}\mathfrak{b}) \cdot (\mathfrak{a}\mathfrak{b}')$.
   (ii) Show that $\mathfrak{a}$, $\mathfrak{b}$ and $\mathfrak{b}'$ are non-principal.

4. Compute the norms of the ideals $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{b}'$ in Q3.

5. Let R be the ring $\mathbb{Z}[\sqrt{-3}]$ (recall that this is not equal to $\mathcal{O}_K$, where $K = \mathbb{Q}(\sqrt{-3})$). Let $\mathfrak{p}$ be the ideal $\langle 2, 1+\sqrt{-3} \rangle$ of R.
   (a) Show that $\mathfrak{p}^2 = \langle 2 \rangle \mathfrak{p}$.
   (b) Compute the fractional ideal $\mathfrak{p}^{-1}$ of R, and show that it is equal to $\mathcal{O}_K$.
   (c) Show that $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$.

6. You're given that $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is a principal ideal domain for $d = 6$, 7, 21. Exhibit a generator for the following ideals.
   (i) $\langle 3, \sqrt{6} \rangle$, $\langle 5, 4+\sqrt{6} \rangle$ in $\mathcal{O}_{\mathbb{Q}(\sqrt{6})}$.
   (ii) $\langle 2, 1+\sqrt{7} \rangle$ in $\mathcal{O}_{\mathbb{Q}(\sqrt{7})}$.
   (iii) $\langle 3, \sqrt{21} \rangle$ in $\mathcal{O}_{\mathbb{Q}(\sqrt{21})}$.

†7. Let $K = \mathbb{Q}(\sqrt{3})$. Use the Dedekind–Kummer theorem to factorise the following ideals of $\mathcal{O}_K$ into prime ideals:

$$\langle 2 \rangle, \quad \langle 3 \rangle, \quad \langle 5 \rangle.$$

   Correction. You should also factorise $\langle 11 \rangle$ into prime ideals of $\mathcal{O}_K$.
   Deduce the factorisation of the following ideals of $\mathcal{O}_K$ into prime ideals:

$$\langle 10 \rangle, \quad \langle 30 \rangle.$$

   For each prime ideal $\mathfrak{p}$ which appears as a factor of any of $\langle 2 \rangle$, $\langle 3 \rangle$, $\langle 5 \rangle$ or $\langle 11 \rangle$, show that it is principal by writing down an element $\pi \in \mathcal{O}_K$ such that $\mathfrak{p} = \langle \pi \rangle$.

8. Let $K = \mathbb{Q}(\sqrt{-5})$. You may want to make use of Q3 while answering this question.
   (a) Find all ideals in $\mathcal{O}_K$ of the following norms:
$$4, \quad 6, \quad 9.$$
   (b) Find an integer N such that there are exactly 10 ideals of $\mathcal{O}_K$ of norm N.

9. Let $K = \mathbb{Q}(i)$. Recall from Introduction to Number Theory that for any rational prime p, -1 is a quadratic residue mod p if and only if $p \equiv 1 \bmod 4$. Use the Dedekind–Kummer theorem to prove the following factorisations of ideals of $\mathcal{O}_K$:
   (i) $\langle 2 \rangle = \langle 1+i \rangle^2$;
   (ii) $\langle p \rangle$ is a product of two distinct prime ideals if $p \equiv 1 \bmod 4$;
   (iii) $\langle p \rangle$ is a prime ideal if $p \equiv 3 \bmod 4$.

   Use Minkowski's theorem on ideal classes to prove that $\mathbb{Z}[i]$ is a PID. This reproves a fact from Introduction to Number Theory, where it was proved by showing that $\mathbb{Z}[i]$ is a Euclidean domain. (Note that it is not obvious from Dedekind–Kummer alone that the prime ideals in case (ii) are principal.)

   Deduce that a rational prime p is a sum of two squares if and only if it is $\equiv 1 \bmod 4$.

10. Let p be a rational prime and let K be a number field. We say that p is **ramified** in K if, in the factorisation into prime ideals of $\mathcal{O}_K$:
$$\langle p \rangle = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_r^{e_r},$$
there is some i such that $e_i \geq 2$.

   Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field. Use the Dedekind–Kummer theorem to prove that p is ramified in K if and only if p divides the discriminant of K. (You will need to consider the cases $d \equiv 1, 2, 3 \bmod 4$ separately.)

†11. Let $K = \mathbb{Q}(\sqrt{11})$. Factorise the ideals $\langle 2 \rangle$ and $\langle 3 \rangle$ of $\mathcal{O}_K$ into prime ideals. Show that $\mathcal{O}_K$ has a unique proper ideal of norm ≤ 3, and that this ideal is principal. Use Minkowski's theorem on ideal classes to deduce that $\mathbb{Z}[\sqrt{11}]$ is a principal ideal domain.

12. Let $K = \mathbb{Q}(\sqrt[3]{6})$. Factorise $\langle p \rangle$ into prime ideals in $\mathcal{O}_K$ for $p = 2,\ 5,\ 13$, checking that the factors are principal (you may suppose that $1,\ \sqrt[3]{6},\ \sqrt[3]{6}^2$ is an integral basis).