Algebraic Number Theory
Example Sheet 3

Hand in the answers to questions 5, 8, 13. Deadline 2pm Thursday, Week 8.

(1) Let R be a ring and $\mathfrak{a}$ be an ideal of R. Show that $\mathfrak{a} = R$ if and only if $\mathfrak{a}$ contains a unit.

(2) Let K be a number field, $\sigma : K \hookrightarrow \mathbb{C}$ be an embedding of K and let $L = \sigma(K)$.
  (i) Show that $\sigma(\mathcal{O}_K) = \mathcal{O}_L$. Thus σ induces an isomorphism $\sigma : \mathcal{O}_K \to \mathcal{O}_L$.
  (ii) Let $\mathfrak{a}$ be an ideal of $\mathcal{O}_K$. Show that $\sigma(\mathfrak{a})$ is an ideal of $\mathcal{O}_L$.
  (iii) Give a counter example to show that the following statement is false: if $\sigma : R \to S$ is a homomorphism of rings, and $\mathfrak{a}$ is an ideal of R then $\sigma(\mathfrak{a})$ is an ideal of S.

(3) Let K be a number field. We define the norm of a non-zero ideal $\mathfrak{a}$ of $\mathcal{O}_K$ by $\mathrm{Norm}(\mathfrak{a}) = \#\mathcal{O}_K/\mathfrak{a}$ (this is shown to be finite in the lectures). If $\mathfrak{a}$ and $\mathfrak{b}$ are non-zero ideals satisfying $\mathfrak{a} + \mathfrak{b} = \mathcal{O}_K$ (we say $\mathfrak{a}$ and $\mathfrak{b}$ are coprime), use the Chinese Remainder Theorem to show that

$$\mathrm{Norm}(\mathfrak{a}\mathfrak{b}) = \mathrm{Norm}(\mathfrak{a})\,\mathrm{Norm}(\mathfrak{b}).$$

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

(5) 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.
  (iii) Write $\mathfrak{a}^n$ in simplest form for $n \geq 1$.

(6) Compute the norms of the ideals $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{b}'$ in Question 5.

(7) Let $K = \mathbb{Q}(\sqrt{15})$. Let $\mathfrak{a}$ be the following ideal of $\mathcal{O}_K$:

$$\mathfrak{a} = \langle 7, 1+\sqrt{15} \rangle.$$

Compute $\mathcal{O}_K/\mathfrak{a}$ and $\mathrm{Norm}(\mathfrak{a})$.

(8) Let $f = X^3 + X^2 - 2X + 8$ and let θ be a root of f. Let $K = \mathbb{Q}(\theta)$. An integral basis for $\mathcal{O}_K$ is 1, θ, $(\theta^2+\theta)/2$ (see the last example in Chapter 3 of the online lecture notes). Let

$$\mathfrak{a} = \langle 2, 1+\theta \rangle.$$

Compute $\mathcal{O}_K/\mathfrak{a}$ and $\mathrm{Norm}(\mathfrak{a})$.

(9) Let $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ be non-zero ideals of $\mathcal{O}_K$ with $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$.
  (i) If $\mathfrak{a}$, $\mathfrak{b}$ are principal, show that $\mathfrak{c}$ is principal.
  (ii) If $\mathfrak{b}$, $\mathfrak{c}$ are principal, show that $\mathfrak{a}$ is principal.

(10) 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: $\langle \alpha, \beta \rangle^{-1} = \langle \alpha^{-1}, \beta^{-1} \rangle$.

(11) Let $\mathfrak{a}$ be a non-zero ideal of $\mathcal{O}_K$.
  (i) Show that $\mathfrak{a} \cap \mathbb{Z}$ is an ideal of $\mathbb{Z}$.
  (ii) Show that $\mathfrak{a} \cap \mathbb{Z} = a\mathbb{Z}$ for some non-zero integer a.
  (iii) Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_K$. Show that $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ for some rational prime p.

(12) 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 $\mathcal{O}_{\mathbb{Q}(\sqrt{21})}$.

(13) For this exercise you'll need the **Kummer-Dedekind Theorem**: Let p be a rational prime. Let $K = \mathbb{Q}(\theta)$ be a number field where θ is an algebraic integer. Suppose $p \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]]$. Let

$$\mu_\theta(X) \equiv f_1(X)^{e_1} f_2(X)^{e_2} \cdots f_r(X)^{e_r} \pmod{p}$$

where the polynomials $f_i \in \mathbb{Z}[X]$ are irreducible and pairwise coprime modulo p. Let $\mathfrak{p}_i = \langle p, f_i(\theta) \rangle$. Then the $\mathfrak{p}_i$ are pairwise distinct prime ideals of $\mathcal{O}_K$ and

$$\langle p \rangle = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_r^{e_r}.$$

Moreover, $\text{Norm}(\mathfrak{p}_i) = p^{\deg(f_i)}$. Use the Kummer–Dedekind Theorem to factor into prime ideals $\langle p \rangle$ in $\mathcal{O}_{\mathbb{Q}(\sqrt[3]{6})}$ 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).

(14) Let $K = \mathbb{Q}(\sqrt[3]{2})$. Determine $\mathcal{O}_K$. Show that

$$\mathcal{O}_K^* = \{\pm(1 - \sqrt[3]{2})^n : n \in \mathbb{Z}\}.$$