Algebraic Number Theory: Problem Sheet 3. 2019.

Topics covered: factorisation of ideals.

1. Prove that the equivalence relation defined in the lectures on the set of non-zero ideals is indeed an equivalence relation.

2. Let P be a prime ideal of $\mathcal{O}_K$, the ring of integers of a number field K. Show that if $\alpha \in P$, $\alpha \neq 0$, is chosen so that $|\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)|$ is minimal, then α is an irreducible element. Deduce that if $\mathcal{O}_K$ is a UFD then every prime ideal is principal, and so $\mathcal{O}_K$ is a PID.

3. The rings $\mathbb{Z}[\sqrt{6}]$ and $\mathbb{Z}[\sqrt{7}]$ are PIDs. Exhibit generators for their ideals $(3, \sqrt{6})$, $(5, 4 + \sqrt{6})$, $(2, 1 + \sqrt{7})$.

   [Hint: Compute the norm of each of the given ideals of the form (p, α) and find an element $\beta \in \mathcal{O}_K$ of suitable norm.]

4. Find the prime factorisations of the ideals $(3), (5)$ and (7) in $\mathbb{Z}[\sqrt{-5}]$. Show that the prime ideal factors of (7) are not principal.

5. Let $K \subseteq L$ be fields and let I be an ideal of $\mathcal{O}_K$. Define $I \cdot \mathcal{O}_L$ to be the ideal of $\mathcal{O}_L$ generated by the products $i\ell$, such that $i \in I, \ell \in \mathcal{O}_L$. Show that, for any ideals I, J of $\mathcal{O}_K$, any $n \in \mathbb{N}$ and any principal ideal $(a) = a\mathcal{O}_K$ of $\mathcal{O}_K$, $(IJ) \cdot \mathcal{O}_L = (I \cdot \mathcal{O}_L)(J \cdot \mathcal{O}_L)$, $I^n \cdot \mathcal{O}_L = (I \cdot \mathcal{O}_L)^n$ and $(a) \cdot \mathcal{O}_L = a\mathcal{O}_L$ (the principal ideal of $\mathcal{O}_L$ generated by the same element). Let $K = \mathbb{Q}(\sqrt{-13})$ and let $I = (2, \sqrt{-13} + 1)$. Show that $I^2 = (2)$ and that I is not principal. Let $L = \mathbb{Q}(\sqrt{-13}, \sqrt{2})$. Show that $I \cdot \mathcal{O}_L$ is the principal ideal of $\mathcal{O}_L$ generated by $\sqrt{2}$ (we say that I has been *made principal* in the extension).

6. Let P, Q be distinct nonzero prime ideals in $\mathcal{O}_K$. Show that $P + Q = \mathcal{O}_K$ and $P \cap Q = PQ$.

7. Let $d \not\equiv 1 \bmod 4$ be a square-free integer and define $K := \mathbb{Q}(\sqrt{d})$; so $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. Let p be a rational prime. Suppose that $d \equiv a^2 \bmod p$. Define $P := (p, a + \sqrt{d}), P' := (p, a - \sqrt{d}) \subseteq \mathcal{O}_K$. Show that P and P' are both prime ideals with $N(P) = N(P') = p$, and that $(p) = PP'$. Show that $P = P'$ if and only if $p | 2d$.

8. Let $d \equiv 1 \bmod 4$ be a square-free integer, with $d \neq 1$. Show that the ring $\mathbb{Z}[\sqrt{d}]$ is never a UFD. [Hint: Consider factoring $d - 1$.]

Further Practice: Exercises in Chapter 5 of Stewart and Tall.