Algebraic Number Theory 2019-20
Example Sheet 3

Hand in the answers to questions 2, 4 and 8 (marked with †).
Deadline 12 noon Monday, Week 8 (18 November)
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 $K = \mathbb{Q}(\sqrt{-5})$. 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) Compute the norms of the ideals $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{b}'$.

†2. Let K be a number field and let $\theta \in \mathcal{O}_K$ satisfy $\mathrm{Nm}_{K/\mathbb{Q}}(\theta) = ab$, where a and b are coprime rational integers. Prove that
$$\langle a, \theta\rangle\langle b, \theta\rangle = \langle\theta\rangle.$$
(You may want to prove the inclusion in each direction separately.)
Correction: This originally said $\theta \in K$, but it should say $\theta \in \mathcal{O}_K$.

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

†4. Let $K = \mathbb{Q}(\sqrt{3})$. Use the Dedekind–Kummer theorem to factorise the ideal $\langle 11\rangle$ into prime ideals of $\mathcal{O}_K$. For each prime ideal $\mathfrak{p}$ which appears as in the factorisation, show that it is principal by writing down an element $\pi \in \mathcal{O}_K$ such that $\mathfrak{p} = \langle\pi\rangle$.

5. Let $K = \mathbb{Q}(\sqrt{-5})$. You may want to make use of Q1 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.

6. 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 $p \equiv 3 \bmod 4$.

7. 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.)

†8. Let α be a root of the polynomial $f(X) = X^3 - X^2 - 2X - 8$ and let $K = \mathbb{Q}(\alpha)$. You may use the following facts without proof:
- f is irreducible over $\mathbb{Q}$.
- $\Delta(1, \alpha, \alpha^2) = -2012$.
- $\beta = (\alpha^2 + \alpha)/2$ is an algebraic integer.

(i) Explain briefly how to show that $\{1, \alpha, \beta\}$ is an integral basis for K.
(ii) Why can we use the Dedekind–Kummer theorem (with the element α) to factorise $\langle 3\rangle$ and $\langle 5\rangle$ in $\mathcal{O}_K$, but not $\langle 2\rangle$?
(iii) Factorise the ideals $\langle 3\rangle$ and $\langle 5\rangle$ in $\mathcal{O}_K$, and determine the norm of each prime ideal in their factorisations.
(iv) Verify that $\alpha\beta = 4 + 2\beta$.
(v) Let $\mathfrak{a} = \mathbb{Z}.2 + \mathbb{Z}.\alpha + \mathbb{Z}.2\beta$. You may use without proof the facts that $\mathfrak{a}$ is an ideal in $\mathcal{O}_K$, and that $\beta^2 = 6 + 2\alpha + 3\beta$.
By considering $(1+\alpha+\beta)\beta$, or otherwise, show that $\mathfrak{a}$ is not a prime ideal.

9. This question is a continuation of Q8.
(i) Verify that $\mathfrak{p} = \mathbb{Z}.2 + \mathbb{Z}.\alpha + \mathbb{Z}.\beta$, $\mathfrak{q} = \mathbb{Z}.2 + \mathbb{Z}.\alpha + \mathbb{Z}.(\beta + 1)$ and $\mathfrak{r} = \mathbb{Z}.2 + \mathbb{Z}.(1 + \alpha) + \mathbb{Z}.\beta$ are ideals in $\mathcal{O}_K$.
(ii) Use change-of-basis matrices to show that $\mathrm{Nm}(\mathfrak{p}) = \mathrm{Nm}(\mathfrak{q}) = \mathrm{Nm}(\mathfrak{r}) = 2$.
(iii) Deduce that $\mathfrak{p}, \mathfrak{q}, \mathfrak{r}$ are prime ideals and $\langle 2\rangle = \mathfrak{p}\mathfrak{q}\mathfrak{r}$.
(iv) By comparing this factorisation with the Dedekind–Kummer theorem, prove that $\mathcal{O}_K \neq \mathbb{Z}[\gamma]$ for any γ. (How many monic irreducible polynomials of degree 1 are there modulo 2?)

10. 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 $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$.
Note: in this question, $\mathfrak{p}^{-1}$ means $\{x \in K : x\mathfrak{p} \subseteq R\}$ (i.e. replace $\mathcal{O}_K$ in the definition from lectures by R). Similarly $\langle 2\rangle$ means $2R$ not $2\mathcal{O}_K$.

11. 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: $\langle\alpha, \beta\rangle^{-1} = \langle\alpha^{-1}, \beta^{-1}\rangle$.