Number Fields: Example Sheet 2 of 3

1. Let $\mathfrak{a}$ and $\mathfrak{b}$ be coprime ideals in $\mathcal{O}_K$. (This means there are no proper ideals dividing both $\mathfrak{a}$ and $\mathfrak{b}$.) Show that $\mathfrak{a}+\mathfrak{b}=\mathcal{O}_K$ and $\mathfrak{a}\cap\mathfrak{b}=\mathfrak{a}\mathfrak{b}$. Deduce that there is an isomorphism of rings $\mathcal{O}_K/\mathfrak{a}\mathfrak{b}\cong\mathcal{O}_K/\mathfrak{a}\times\mathcal{O}_K/\mathfrak{b}$.

2. Let $K=\mathbb{Q}(\sqrt{-5})$. Show by computing norms, or otherwise, that $\mathfrak{p}=(2,1+\sqrt{-5})$, $\mathfrak{q}_1=(7,3+\sqrt{-5})$ and $\mathfrak{q}_2=(7,3-\sqrt{-5})$ are prime ideals in $\mathcal{O}_K$. Which (if any) of the ideals $\mathfrak{p},\mathfrak{q}_1,\mathfrak{q}_2,\mathfrak{p}^2,\mathfrak{p}\mathfrak{q}_1,\mathfrak{p}\mathfrak{q}_2$ and $\mathfrak{q}_1\mathfrak{q}_2$ are principal? Factor the principal ideal $(9+11\sqrt{-5})$ as a product of prime ideals.

3. Let $K=\mathbb{Q}(\sqrt{-m})$ where $m>0$ is the product of distinct primes $p_1,\ldots,p_k$. Show that $(p_i)=\mathfrak{p}_i^2$ where $\mathfrak{p}_i=(p_i,\sqrt{-m})$. When are the ideals $\prod\mathfrak{p}_i^{r_i}$ and $\prod\mathfrak{p}_i^{s_i}$ in the same ideal class? Deduce that the class group Cl_K contains a subgroup isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{k-1}$. [*If you like, just do the case* $m\not\equiv 3 \pmod 4$.]

4. Let p be an odd prime and $K=\mathbb{Q}(\zeta_p)$ where ζ_p is a primitive pth root of unity. Determine $[K:\mathbb{Q}]$. Calculate $N_{K/\mathbb{Q}}(\pi)$ and $\mathrm{Tr}_{K/\mathbb{Q}}(\pi)$ where $\pi=1-\zeta_p$.
   (i) By considering traces $\mathrm{Tr}_{K/\mathbb{Q}}(\zeta_p^j\alpha)$ show that $\mathbb{Z}[\zeta_p]\subset\mathcal{O}_K\subset\frac{1}{p}\mathbb{Z}[\zeta_p]$.
   (ii) Show that $(1-\zeta_p^r)/(1-\zeta_p^s)$ is a unit for all $r,s\in\mathbb{Z}$ coprime to p, and that $\pi^{p-1}=up$ where u is a unit.
   (iii) Prove that the natural map $\mathbb{Z}\to\mathcal{O}_K/(\pi)$ is surjective. Deduce that for any $\alpha\in\mathcal{O}_K$ and $m\geq 1$ there exist $a_0,\ldots,a_{m-1}\in\mathbb{Z}$ such that
   $$\alpha\equiv a_0+a_1\pi+\ldots+a_{m-1}\pi^{m-1}\pmod{\pi^m\mathcal{O}_K}.$$
   (iv) Deduce that $\mathcal{O}_K=\mathbb{Z}[\zeta_p]$.

5. Let $K=\mathbb{Q}(\sqrt{35})$ and $\omega=5+\sqrt{35}$. Verify the ideal equations $(2)=(2,\omega)^2$, $(5)=(5,\omega)^2$ and $(\omega)=(2,\omega)(5,\omega)$. Show that $1+\omega$ is a fundamental unit in K. Hence show that the complete solution in integers x,y of the equation $x^2-35y^2=-10$ is given by $x+\sqrt{35}y=\pm\omega(1+\omega)^n$ for $n\in\mathbb{Z}$.

6. (i) Find the fundamental unit in $\mathbb{Q}(\sqrt{7})$. Determine all the integer solutions of the equations $x^2-7y^2=m$ for $m=2,9$ and 13.
   (ii) Find the fundamental unit in $\mathbb{Q}(\sqrt{10})$. Determine all the integer solutions of the equations $x^2-10y^2=m$ for $m=-1,6$ and 7.

7. Let K be a number field of degree n, with integral basis $1,\alpha,\ldots,\alpha^{n-1}$. Let p be a prime. Let $f(X)\in\mathbb{Z}[X]$ be the minimal polynomial of α and $\overline{f}(X)\in\mathbb{F}_p[X]$ the polynomial we get by reducing the coefficients mod p.
   (i) Show that $\mathbb{Z}[X]/(f(X))\cong\mathcal{O}_K$ and $\mathcal{O}_K/p\mathcal{O}_K\cong\mathbb{F}_p[X]/(\overline{f}(X))$.
   (ii) Deduce that $p\mathcal{O}_K$ is a prime ideal if and only if $\overline{f}(X)$ is irreducible in $\mathbb{F}_p[X]$.

   [*This is a special case of Dedekind's criterion (covered later in the course).*]

8. Prove that if $x \in K$ is integral over $\mathcal{O}_K$ (i.e. x is a root of a monic polynomial with coefficients in $\mathcal{O}_K$) then $x \in \mathcal{O}_K$.

9. Let $K = \mathbb{Q}(\alpha)$ where α is a root of $f(X) = X^3 + X^2 - 2X + 8$. [*This polynomial is irreducible over* $\mathbb{Q}$ *and has discriminant* -4.503.]

   (i) Show that $\beta = 4/\alpha \in \mathcal{O}_K$ and $\beta \notin \mathbb{Z}[\alpha]$. Deduce that $\mathcal{O}_K = \mathbb{Z}[\alpha, \beta]$.

   (ii) Show that there is an isomorphism of rings $\mathcal{O}_K/2\mathcal{O}_K \cong \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2$. Deduce that 2 splits completely in K.

10. (i) Let $\mathfrak{a} \subset \mathcal{O}_K$ be a non-zero ideal. Show that every ideal in the ring $\mathcal{O}_K/\mathfrak{a}$ is principal. [*Hint: Use Question 1 to reduce to the case* $\mathfrak{a}$ *is a prime power.*]

    (ii) Deduce that every ideal in $\mathcal{O}_K$ can be generated by 2 elements.

11. Let $K = \mathbb{Q}(\alpha)$ where α is a root of $f(X) = X^3 - 7X - 1$. [*Note that* $\mathrm{disc}(f) = 5.269$ *is square-free.*] Compute $N_{K/\mathbb{Q}}(n + \alpha)$ for $|n| \leq 3$. Hence show that $(5) = \mathfrak{p}_1^2\mathfrak{p}_2$ and $(7) = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$ where the $\mathfrak{p}_i$ and $\mathfrak{q}_j$ are distinct primes. Find units generating a subgroup of $\mathcal{O}_K^*$ of finite index. [*Hint: You can show that the units you have found are independent by considering their images in* $\mathcal{O}_K/7\mathcal{O}_K \cong \mathbb{F}_7 \times \mathbb{F}_7 \times \mathbb{F}_7$.]

The following extra questions may or may not be harder than the earlier questions.

12. Let K be a number field of degree n, and $\mathfrak{a} \subset \mathcal{O}_K$ an ideal. Show that there is a basis $x_1, \ldots, x_n$ for K over $\mathbb{Q}$ such that $x_1 \in \mathbb{Z}$ and $\mathfrak{a} = \{\sum_{i=1}^n \lambda_i x_i : \lambda_i \in \mathbb{Z}\}$. Prove that x_1 and $N\mathfrak{a}$ have the same prime factors.

13. An *order* in a degree n number field K is a subring $R \subset K$ with $R \cong \mathbb{Z}^n$ (as groups under addition). Prove that $\mathbb{Z} + m\mathcal{O}_K \subset R \subset \mathcal{O}_K$ for some integer $m \geq 1$, and that R^* has finite index in $\mathcal{O}_K^*$.

14. For $\mathfrak{a}$ an ideal in $\mathcal{O}_K$ let $\phi(\mathfrak{a}) = |(\mathcal{O}_K/\mathfrak{a})^*|$. Show that $\phi(\mathfrak{a}) = N(\mathfrak{a}) \prod_{\mathfrak{p}|\mathfrak{a}}(1 - \frac{1}{N\mathfrak{p}})$.

15. Show that there are no integer solutions to $x^2 - 82y^2 = \pm 2$.

16. Prove Stickelberger's criterion, that $D_K \equiv 0, 1 \pmod 4$. [*Hint: Suppose first that* $K/\mathbb{Q}$ *is Galois. Write* $D_K = (P - N)^2 = (P + N)^2 - 4PN$ *where* P *is a sum over even permutations and* N *is a sum over odd permutations. Then show that* $P + N, PN \in \mathbb{Z}$. *For the general case, embed* K *in a Galois closure* $L/\mathbb{Q}$.]
    Hence compute the ring of integers of $\mathbb{Q}[X]/(f(X))$ where $f(X) = X^3 - X + 2$.