Lent Term 2023

Number Fields: Example Sheet 1 of 3

1. Find the minimal polynomials over $\mathbb{Q}$ of
$$(1+i)\sqrt{3}, \qquad i+\sqrt{3}, \qquad 2\cos(2\pi/7).$$

2. Which of the following are algebraic integers?
$$\sqrt{5}/\sqrt{2},\ (1+\sqrt{3})/2,\ (\sqrt{3}+\sqrt{7})/2,\ \frac{3+2\sqrt{6}}{1-\sqrt{6}},\ (1+\sqrt[3]{10}+\sqrt[3]{100})/3,\ 2\cos(2\pi/19).$$

3. Let $d>1$ be an integer. Show that the only units in the ring
$$\mathbb{Z}[\sqrt{-d}] = \{a+b\sqrt{-d} : a,b\in\mathbb{Z}\}$$
are ± 1.

4. (i) Explain why the equations
$$2\cdot 11 = (5+\sqrt{3})(5-\sqrt{3})$$
and
$$(2+\sqrt{7})(3-2\sqrt{7}) = (5-2\sqrt{7})(18+7\sqrt{7})$$
are not inconsistent with the fact $\mathbb{Z}[\sqrt{3}]$ and $\mathbb{Z}[\sqrt{7}]$ have unique factorisation.
   (ii) Find equations to show that $\mathbb{Z}[\sqrt{d}]$ is not a UFD for $d=-10,-13,-14$.

5. Let K be a field with $\mathrm{char}(K)\neq 2$. Show that every extension L/K of degree 2 is of the form $L=K(\sqrt{a})$ with $a\in K^*$, $a\notin (K^*)^2$. Show further that $K(\sqrt{a})=K(\sqrt{b})$ if and only if $a/b\in (K^*)^2$.

6. Let $A\subseteq B\subseteq C$ be rings.
   (i) Show that if B is finite over A, and C is finite over B, then C is finite over A.
   (ii) Show that if B is integral over A, and C is integral over B, then C is integral over A.

   Now let $\mathbb{Q}\subseteq K\subseteq L$ be finite extensions of fields.
   (i) Show that if $\alpha\in L$ is integral over $\mathcal{O}_K$ it is an algebraic integer.
   (ii) Show that if $f\in K[x]$ is monic, and $f^n\in\mathcal{O}_K[x]$ for some n, then $f\in\mathcal{O}_K[x]$.

7. Let $K=\mathbb{Q}(\theta)$ where θ is a root of X^3-2X+6. Show that $[K:\mathbb{Q}]=3$ and compute $N_{K/\mathbb{Q}}(\alpha)$ and $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$ for $\alpha=n-\theta$, $n\in\mathbb{Z}$ and $\alpha=1-\theta^2, 1-\theta^3$.

8. Let $K=\mathbb{Q}(\delta)$ where $\delta=\sqrt[3]{d}$ and $d\neq 0,\pm1$ is a square-free integer. Show that $\Delta(1,\delta,\delta^2)=-27d^2$. By calculating the traces of θ, $\delta\theta$, $\delta^2\theta$, and the norm of θ, where $\theta=u+v\delta+w\delta^2$ with $u,v,w\in\mathbb{Q}$, show that the ring of integers $\mathcal{O}_K$ of K satisfies
$$\mathbb{Z}[\delta]\subset\mathcal{O}_K\subset\tfrac{1}{3}\mathbb{Z}[\delta].$$

9. Let $K = \mathbb{Q}(\alpha)$ be a number field. Suppose $\alpha \in \mathcal{O}_K$ and let $f \in \mathbb{Z}[X]$ be its minimal polynomial.

   (i) Show that if the discriminant of f is a square-free integer then $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

   (ii) Compute an integral basis for K in the cases $f(X) = X^3 + X + 1$ and $f(X) = X^3 - X - 4$.

   [*The discriminant of* $X^3 + aX + b$ *is* $-4a^3 - 27b^2$.]

10. Let $K = \mathbb{Q}(i, \sqrt{2})$. By computing the relative traces $\mathrm{Tr}_{K/k}(\theta)$ where k runs through the three quadratic subfields of K, show that the algebraic integers θ in K have the form $\frac{1}{2}(\alpha + \beta\sqrt{2})$, where $\alpha = a + ib$ and $\beta = c + id$ are Gaussian integers. By considering $N_{K/k}(\theta)$ where $k = \mathbb{Q}(i)$ show that

$$\begin{aligned} a^2 - b^2 - 2c^2 + 2d^2 &\equiv 0 \pmod{4}, \\ ab - 2cd &\equiv 0 \pmod{2}. \end{aligned}$$

   Hence prove that an integral basis for K is $1, i, \sqrt{2}, \frac{1}{2}(1+i)\sqrt{2}$, and calculate the discriminant D_K.

11. Suppose that K is a number field of degree $n = r + 2s$ in the usual notation (r is the number of real embeddings of K and s the number of pairs of complex conjugate embeddings). Show that the sign of the discriminant D_K is $(-1)^s$.

12. Let $f(X) \in \mathbb{Q}[X]$ be an irreducible polynomial of degree n, and $\theta \in \mathbb{C}$ a root of f.

   (i) Show that $\mathrm{disc}(f) = (-1)^{\binom{n}{2}} N_{K/\mathbb{Q}}(f'(\theta))$ where $K = \mathbb{Q}(\theta)$.

   (ii) Let $f(X) = X^n + aX + b$. Write down the matrix representing multiplication by $f'(\theta)$ with respect to the basis $1, \theta, \ldots, \theta^{n-1}$ for K. Hence show that

$$\mathrm{disc}(f) = (-1)^{\binom{n}{2}}((1-n)^{n-1}a^n + n^n b^{n-1}).$$

The following extra questions are just for fun. They can be answered using material from the Part IB course *Groups Rings and Modules.*

12. Let $\omega \neq 1$ be a cube root of unity, and let $p \neq 3$ be a prime.

   (i) By considering units in $\mathbb{Z}[\omega]$ show that $x^2 + 3y^2$ represents p if and only if $x^2 + xy + y^2$ represents p.

   (ii) Use that $\mathbb{F}_p^*$ is cyclic to find a condition on p for the congruence $x^2 + x + 1 \equiv 0 \pmod{p}$ to be soluble.

   (iii) Use unique factorisation in $\mathbb{Z}[\omega]$ to determine the set of primes in (i).

13. Show that the rings $\mathbb{Z}[i]$ and $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ are Euclidean. Hence find all integer solutions to the equations $y^2 = x^3 - 4$ and $y^2 + y = x^3 - 2$.

14. Let $n \geq 3$ be an integer. Suppose $f, g, h \in \mathbb{C}[X]$ are coprime polynomials satisfying $f^n + g^n = h^n$. Use unique factorisation in $\mathbb{C}[X]$ to construct a new solution to this equation involving polynomials of smaller degree. Deduce that f, g, h must be constant.