Algebraic Number Theory
Example Sheet 2

1. Let $p \geq 3$ be a prime. Let $\zeta_p = \exp(2\pi i/p)$.
   (i) Show that the roots of $X^{p-1} + X^{p-2} + \cdots + 1$ are ζ, ζ^2, ..., ζ^{p-1}.
   (ii) Suppose that $a \in \mathbb{Z}\backslash\{0\}$. Let $\sqrt[p]{a}$ be the real p-th root of a. Show that the roots of $X^p - a$ are $\sqrt[p]{a}\zeta^i$ for $i = 0, 1, \ldots, p-1$.

2. In this exercise we will complete the proof that $\mathcal{O}$ is a subring of $\mathbb{C}$. Suppose α, $\beta \in \mathcal{O}$. We showed that $\alpha + \beta \in \mathcal{O}$ (before continuing you should revise this proof). We would like to show that $\alpha\beta \in \mathcal{O}$.
   (i) If $\alpha = 0$ or $\beta = 0$ then $\alpha\beta = 0 \in \mathcal{O}$. Suppose $\alpha \neq 0$, $\beta \neq 0$. Let $\beta_1, \ldots, \beta_m$ be the conjugates of β. Show that all these are non-zero.
   (ii) Let
   $$f_\alpha(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \qquad (a_i \in \mathbb{Z})$$
   be the minimal polynomial of α. Let
   $$g(X) = \prod_{i=1}^{m} \beta_i^n f(X/\beta_i).$$
   Show that $g(X)$ is monic and has coefficients in $\mathbb{Z}$, and $g(\alpha\beta) = 0$. Hence $\alpha\beta \in \mathcal{O}$.
   (iii) Complete the proof that $\mathcal{O}$ is a subring of $\mathbb{C}$ by showing that $-\alpha \in \mathcal{O}$ (this has a one line proof).

3. Let α be a root of $f(X) = X^3 - 2X - 2$ and $\beta = \sqrt{-1}$. Construct the minimal polynomials of $\alpha + \beta$ and $\alpha\beta$. What are their norms and traces.

4. Suppose $\alpha \in \mathcal{O}$. Suppose $f(x) \in \mathbb{Z}[x]$ is monic and let $\beta \in \mathbb{C}$ be a root of the equation $f(x) = \alpha$. Show that $\beta \in \mathcal{O}$.

5. Suppose α is an algebraic number. Show that there is some non-zero $m \in \mathbb{Z}$ such that $m\alpha \in \mathcal{O}$. Deduce that if K is a number field then $K = \mathbb{Q}(\alpha)$ for some algebraic integer α.

6. Let $f(X) = X^3 + X^2 + 1$.
   (i) Show that f is irreducible.
   (ii) Let θ be a root of f and $K = \mathbb{Q}(\theta)$. Write the following elements as $\mathbb{Q}$-linear combinations of 1, θ, θ^2:
   $$(\theta+1)^4, \qquad \frac{1}{\theta^2 - 1}, \qquad \frac{\theta+1}{\theta^2+1}.$$

7. We say that a number field K is quadratic if it has degree 2. Show that every quadratic number field is of the form $\mathbb{Q}(\sqrt{d})$ for some square-free integer $d \neq 0, 1$.

8. Let K be a number field of degree n and $\theta \in K$. Define $F_\theta : K \to K$ by $F_\theta(u) = \theta u$.
   (i) Show that F_θ is a linear transformation on the $\mathbb{Q}$-vector space K.
   (ii) Show that F_θ is singular (non-invertible) if and only if $\theta = 0$.
   (iii) Suppose that $\theta \in \mathbb{Q}$ and $K = \mathbb{Q}(\alpha)$. Write down the matrix of F_θ with respect to the $\mathbb{Q}$-basis $1, \alpha, \ldots, \alpha^{n-1}$ and compute its determinant.
   (iv) Suppose that $K = \mathbb{Q}(\sqrt{-3})$ and $\theta = (1 + \sqrt{-3})/2$. Write down the matrix of F_θ with respect to the $\mathbb{Q}$-basis 1, $\sqrt{-3}$ and compute its determinant. Let $f(x)$ be the characteristic polynomial of this matrix. Calculate f and show that $f(\theta) = 0$. How does this tie in with the Cayley-Hamilton Theorem?