ASSIGNMENT 1: SOLUTIONS

Question 1.

Solution. 262537412640768743.99999999999925007259719 $\square$

Question 2.

Solution. $x^8 - 40x^6 + 222x^4 - 1440x^3 - 5368x^2 - 2880x + 2521$ $\square$

Question 3.

Solution. $q = e^{-2\pi\sqrt{5}}$:

$$x^4 - 1263616x^3 - 195559424x^2 - 17716740096x + 68719476736,$$

$q = e^{-2\pi\sqrt{23}}$:

$$\begin{aligned} x^6 &- 12207823847424x^5 - 282053056407797760x^4 - 6487747282636929761280x^3 \\ &- 1983005594297881434521 60x^2 - 402801258919114398131814 4x + 4722366482869645213696. \end{aligned}$$

$\square$

Question 4.

Solution. ($1 \Rightarrow 2$) Let n be the degree of a monic polynomial in $\mathbb{Z}[x]$ that α satisfies. Show that $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis for $\mathbb{Z}[\alpha]$ (use the euclidean algorithm to show that every element in $\mathbb{Z}[\alpha]$ can be written in terms of these generators).

($2 \Rightarrow 3$) Set $R = \mathbb{Z}[\alpha]$.

($3 \Rightarrow 1$) Suppose $\{e_1, \ldots, e_n\}$ generates for R over $\mathbb{Z}$. Then multiplication by α in R can be represented by an $n \times n$ matrix with integral entries. It follows that that characteristic polynomial of this matrix, $p(x) \in \mathbb{Z}[x]$ is monic and $p(\alpha) = 0$ by the Cayley Hamilton theorem. Therefore α is integral.

$\square$

Question 5.

Solution. Note that $\mathbb{Z}[\alpha, \beta]$ can be generated over $\mathbb{Z}$ by $\{\alpha^i\beta^j \mid i, j \in \mathbb{N}\}$. Suppose that there are monic polynomials $p(x), q(x) \in \mathbb{Z}[x]$ of degrees n, m respectively such that $p(\alpha) = q(\beta) = 0$. Use this to show that the set $\{\alpha^i\beta^j \mid 0 \leq i \leq n, 0 \leq j \leq m\}$ generates $\mathbb{Z}[\alpha, \beta]$ over $\mathbb{Z}$.

Since $R = \mathbb{Z}[\alpha, \beta] \subset K$ is a subring of finite type, and $\alpha + \beta, \alpha\beta \in R$ it follows directly from (4) that $\alpha + \beta, \alpha\beta$ are integral. Conclude that $\mathcal{O}_K$ is a subring K. $\square$

Question 6.

Solution. ($\Leftarrow$) This direction follows directly from the definition of an algebraic integer.

($\Rightarrow$) Let S be the set of all monic polynomials in $\mathbb{Z}[x]$ that α satisfies. Note that S is non-empty since α is integral. Let $p(x)$ be a minimal element of S where S is ordered by degree and let $q(x)$ be the monic minimal polynomial of α over $\mathbb{Q}$. Then $q(x) \mid p(x)$. Suppose that $\deg p(x) > \deg q(x)$. Then $p(x)$ is reducible in $\mathbb{Q}[x]$ and by Gauss' Lemma it is reducible in $\mathbb{Z}[x]$, thus we obtain another monic polynomial in $\mathbb{Z}[x]$ that α satisfies whose degree is less than that of $p(x)$. This is a contradiction to the minimality of $p(x)$ in S with respect to degree. It follows that $q(x) = p(x)$ since both polynomials were taken to be monic. Therefore, the monic minimal polynomial of α has integer coefficients.

Remark: It is important to show that the (unique) minimal polynomial is both *monic* and has integral coefficients. Note that you can always take a minimal polynomial of an algebraic number to be in $\mathbb{Z}[x]$ by clearing denominators. Also, a choice of minimal polynomial is not unique unless you specify that it is monic (or some other condition that lets you nail down your choice as unique—multiplication by any element of $\mathbb{Q}^\times$ will give you another minimal polynomial).

$\square$