M2P4 Rings and Fields
Answers Sheet 2.

1. Let p be a prime number. Then $\left\{\frac{a}{p^k} : a, k \in \mathbb{Z}\right\}$ is a subring of $\mathbb{Q}$ which is an integral domain. (Recall that an integral domain contains 1, so $m\mathbb{Z}$, for example, is not an integral domain if $m > 1$.)

2. We have $f(x) = (x - \alpha)q(x) + r$ where $r \in \mathbb{C}$. Put $x = \alpha$ to obtain $r = f(\alpha)$.

(1) We need $a_0 - 3 - 2 - 1 = 0$, so $a_0 = 6$.

(2) Note that $x^2 + 1$ divides $x^n - 1$ if and only if i and $-i$ are roots of $x^n - 1$. Hence the relevant values of n are the multiples of 4.

3. It is straightforward to prove that $\mathbb{H}$ is a subring of the ring of 2×2 matrices over $\mathbb{C}$, containing the identity matrix.

If $\begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ then $|z|^2 + |w|^2 \neq 0$ and

$$\frac{1}{|z|^2 + |w|^2} \begin{pmatrix} \bar{z} & -w \\ \bar{w} & z \end{pmatrix} \in \mathbb{H}$$

is the required inverse.

If $\alpha \in \mathbb{C}$ and $|\alpha| = 1$ and $r = \begin{pmatrix} 0 & \alpha \\ -\bar{\alpha} & 0 \end{pmatrix}$, then $r \in \mathbb{H}$ and $r^2 + 1 = 0$. We have no contradiction, since $\mathbb{H}$ is not commutative, so $\mathbb{H}$ is not a field.

4. If $3 = (a + ib)(c + id)$ then $9 = (a^2 + b^2)(c^2 + d^2)$. But 3 is not a sum of two squares; hence $a^2 + b^2 = 1$ or $c^2 + d^2 = 1$ and one of $a + ib$ and $c + id$ is a unit.

On the other hand, 13 is not irreducible, since $13 = (3 + 2i)(3 - 2i)$.

5. If α is algebraic over $\mathbb{Q}$ then $f(\alpha) = 0$ for some $f(x) \in \mathbb{Q}[x]$. Multiply by the product of the denominators of the coefficients in $f(x)$ to obtain $g(x) \in \mathbb{Z}[x]$ such that $g(\alpha) = 0$. The converse is easy.

6. It is reasonably straightforward to prove that θ is a bijection. Since $\mathbb{Q}$ is countable, so is $\mathbb{Z}[x]$. But each $f(x) \in \mathbb{Z}[x]$ has finitely many roots. Also, the union of countably many finite sets is countable. Thus, the set of $\alpha \in \mathbb{C}$ such that $f(\alpha) = 0$ for some $f(x) \in \mathbb{Z}[x]$ is countable. As we have seen, this is the set of algebraic numbers over $\mathbb{Q}$.

Since $\mathbb{C}$ is uncountable, some (indeed, uncountably many) complex numbers are not algebraic over $\mathbb{Q}$.