Problem 1. Let $\omega \in \mathbb{C}$. We say that $\omega$ is an algebraic number if there exists a nonzero polynomial $P \in \mathbb{Q}[X]$ such that $P(\omega) = 0$. \footnote{1. Compare with Problem 1 of HW3.} Let $\Omega$ denote the set of all algebraic numbers.

1. Show that the following assertions are equivalent for $\omega \in \mathbb{C}$.
   i. $\omega \in \Omega$
   ii. The subring $\mathbb{Q}[\omega]$ of $\mathbb{C}$ generated by $\omega$ and $\mathbb{Q}$ is finite dimensional over $\mathbb{Q}$.
   iii. The subring $\mathbb{Q}[\omega]$ of $\mathbb{C}$ generated by $\omega$ and $\mathbb{Q}$ is a field.
   iv. There is a subring $R$ of $\mathbb{C}$ containing $\omega$ and $\mathbb{Q}$ and which is finite dimensional as a vector space over $\mathbb{Q}$.
   \[ i \Rightarrow ii : \] see Problem 1 of HW1. If $\omega$ is algebraic, you proved that the ideal $\{ P \in \mathbb{Q}[X], P(\omega) = 0 \}$ is generated by an irreducible polynomial $\Pi_\omega$ and that $\mathbb{Q}[x] \cong \mathbb{Q}[X]/\Pi_\omega$ is finite dimensional over $\mathbb{Q}$ with dimension $\deg(\Pi_\omega)$.
   \[ ii \Rightarrow iii : \] clear.
   \[ iii \Rightarrow i : \] Let $R$ a subring of $\mathbb{C}$ containing $\omega$ and such that $\mathbb{Q} \subset R \subset \mathbb{C}$. Suppose that $R$ has finite dimension $N$ over $\mathbb{Q}$. Then
   \[ \{ 1, \omega, \ldots, \omega^N \} \]
   is a family of vectors in $R$ which cannot be linearly independent over $\mathbb{Q}$. So there is $P \in \mathbb{Q}[X] \setminus \{0\}$ such that $P(\omega) = 0$.

2. Given $x, y \in \mathbb{C}$ we denote by $\mathbb{Q}[x, y]$ the subring of $\mathbb{C}$ generated by $x$, $y$ and $\mathbb{Q}$. We admit (compare with Problem 1 of HW3) that $\mathbb{Q}[x, y]$ is the image of the morphism of rings
   \[ \mathbb{Q}[X, Y] \longrightarrow \mathbb{C} \]
   \[ P \longmapsto P(x, y) \].
   a) Suppose that $x$ and $y$ are algebraic numbers. Show that $\mathbb{Q}[x, y]$ is a finite dimensional $\mathbb{Q}$-vector space. Deduce that it is a field.
   Let $P \neq 0$ with degree $p$ such that $P(x) = 0$ and $Q \neq 0$ with degree $q$ such that $Q(y) = 0$ (you can think of the minimal polynomials $\Pi_x$ and $\Pi_y$ but not necessarily). The vector space $\mathbb{Q}[x, y]$ is made of the $\mathbb{Q}$-linear combinations of $(x^iy^j)_{0\leq i, j < q}$. It is generated over $\mathbb{Q}$ by $(x^iy^j)_{0\leq i < p, 0 \leq j < q}$. So it is finite dimensional. In HW3 Problem 1 you proved that a finite dimensional algebra is always a field...
   b) Show that $x + y$ is an algebraic number. It lies in the ring $\mathbb{Q}[x, y]$ which is finite dimensional over $\mathbb{Q}$.

3. Show that the set of algebraic numbers $\Omega$ is a subfield of $\mathbb{C}$. $x + y$, $x - y$ and $xy$ lie in $\mathbb{Q}[x, y]$...

4. Prove that $\Omega$ is not a finite dimensional vector space over $\mathbb{Q}$. \footnote{2. You may for example use elements like the $\epsilon$ we worked with in Problem 5 of HW2... and make the prime number $p$ vary.}
   If $\Omega$ had finite dimension $N$ then for any $\omega \in \Omega$ the dimension of $\mathbb{Q}[\omega]$ would be $\leq N$. But in HW2 we had the example of a $p^{th}$ root of 1 (where $p$ is a prime number) such that the ideal $\{ P \in \mathbb{Q}[X], P(\omega) = 0 \}$ is generated by $\Phi_p$ so $\mathbb{Q}[\epsilon]$ has dimension $\deg(\Phi_p) = p - 1$. Since $p$ can be made as large as we want ($\geq N + 2$ in particular) it means $\Omega$ is not finite dimensional.
Let $A$ be a subring of $\mathbb{C}$ containing $\mathbb{Z}$. We say that $A$ is a finitely generated abelian group if there exists $N \geq 1$, elements $u_1, \ldots, u_N \in A$ and a surjective morphism of groups

$$\mathbb{Z}^N \to A, \quad (x_1, \ldots, x_N) \mapsto \sum_{i=1}^N x_i u_i.$$ 

We then say that $\{u_1, \ldots, u_N\}$ generates $A$ as an abelian group.

**Problem 2.** Let $A$ denote the set of roots in $\mathbb{C}$ of all monic polynomials of $\mathbb{Z}[X]$.

1. Show that $1/3$ is not in $A$. Let $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X] \setminus \{0\}$. If $P(1/3) = 0$ then

$$3^n P(1/3) = 1 + 3a_{n-1} + \cdots + a_0 3^n$$

so $3$ divides $1$. Contradiction.

2. Show that the following assertions are equivalent for $z \in \mathbb{C}$.
   
   i. $z \in A$
   
   ii. The subring $\mathbb{Z}[z]$ of $\mathbb{C}$ generated by $z$ is finitely generated as an abelian group.
   
   iii. There is a subring $\mathcal{B}$ of $\mathbb{C}$ containing $z$ which is finitely generated as an abelian group.

   i $\Rightarrow$ ii: Let $A \subseteq \mathbb{Z}[z]$ monic with degree $n \geq 1$ such that $A(z) = 0$. An element in $\mathbb{Z}[z]$ is of the form $P(z)$ for $P \in \mathbb{Z}[X]$. The Euclidean division of $P$ by the monic polynomial $A \in \mathbb{Z}[X]$ is $P = AQ + R$ where $R \in \mathbb{Z}[X]$ has degree $< \deg(A)$. So $P(z) = R(z) \in \sum_{i=0}^{\deg(A)-1} \mathbb{Z}z^i$ and $\mathbb{Z}[z]$ is finitely generated by $\{1, \ldots, z^{\deg(A)-1}\}$ as an abelian group.

   ii $\Rightarrow$ iii clear.

   iii $\Rightarrow$ i Using the hint: The matrix $B := [b_{i,j}]_{1 \leq i,j \leq N}$ in $M_N(\mathbb{Z})$ satisfies $B \vec{u} = z\vec{u}$ where $\vec{u}$ is the complex vector with coordinates $(u_1, \ldots, u_N)$. Therefore $z$ is a root for the monic polynomial $\det(XI_N - B)$ which has degree $N$ and coefficients in $\mathbb{Z}$ because $B$ has coefficients in $\mathbb{Z}$.

3. Show that $A$ is a subring of $\mathbb{C}$. Remark that $\mathbb{Z}[x,y]$ is generated by finitely many $x^iy^j\ldots$ so every element in $\mathbb{Z}[x,y]$ is in $A$.

4. Show that $A$ is not noetherian that is to say there is a sequence of ideals $(J_n)_{n \geq 1}$ such that $J_n \subseteq J_{n+1}$. Let $\alpha_n := 3^{2^{-n}}$. Check that it lies in $A$. For any $n \geq 1$, we have $\alpha_{n+1}^2 = \alpha_n$. Let $J_n = \alpha_n A$; we have $J_n \subseteq J_{n+1}$ for any $n \geq 1$. If we had $J_n = J_{n+1}$ for some $n \geq 1$, it would mean that there is $n \geq 1$ such that $\alpha_{n+1} \in \alpha_n A$. So $\alpha_{n+1}/\alpha_n = 1/\alpha_{n+1} \in A$. But then $1/3 = (1/\alpha_{n+1})^{2^{n+1}} \in A$ (since $A$ is a ring). Contradiction.

5. Given $K$ a field. Is $K$ noetherian? Is $K[X]$ noetherian? yes for both, you should be able to justify it by studying the sequences of ideals such that $J_n \subseteq J_{n+1}$.

6. Let $K$ be a number field that is to say a field $K$ such that

$$\mathbb{Q} \subseteq K \subseteq \mathbb{C}$$

and which is a finite dimensional vector space over $\mathbb{Q}$. Let $\mathcal{A}_K := A \cap K$. Notice that it is a ring.

---

3. You may use the Euclidean division of by a monic polynomial in $\mathbb{Z}[X]$. See HW2.
4. For iii $\Rightarrow$ i: let $\{u_1, \ldots, u_N\}$ be a generating set for the abelian group $\mathcal{B}$. Check that there are elements $(b_{i,j})_{i,j}$ in $\mathbb{Z}$ such that $zu_i = \sum_{j=1}^{n} b_{i,j} u_j$. Then consider the matrix $[b_{i,j}]$. Show that it has $z$ as an eigenvalue and finds a monic polynomial in $\mathbb{Z}[X]$ which has $z$ as a root.
5. You can find inspiration in Problem 1 and study $\mathbb{Z}[x,y]$ where $x$ and $y$ are algebraic integers.
6. You may consider the ideal generated by $\alpha_n = 3^{2^{-n}}$. 

(a) What is $A_Q$? It is $\mathbb{Z}$. Take $a/b$ with $a, b \in \mathbb{Z}$, $b \geq 1$ such that $a \wedge b = 1$ and suppose that there is a monic polynomial in $\mathbb{Z}[X]$ that has $a/b$ as a root. Conclude that $b = 1$...

(b) Let $d \in \mathbb{Z} - \{0, 1\}$ with no square factor (that is to say there is no prime $p$ such that $p^2$ divides $d$).

(i) Check that $\mathbb{Q}[\sqrt{d}]$ is a number field. What is its dimension over $\mathbb{Q}$? It is called a quadratic field. Let’s call it $K$.

The kernel of $\mathbb{Q}[X] \to \mathbb{Q}[\sqrt{d}]$ is generated by $X^2 - d$ so $K$ has dimension 2 over $\mathbb{Q}$ with basis $1, \sqrt{d}$ (see HW3).

(ii) What are the 2 morphisms of fields $\sigma_1, \sigma_2 : K \to \mathbb{C}$ which fix $\mathbb{Q}$? What are their respective images? Recall that a morphism of fields is just a morphism of rings but between two fields (sending the identity element to the identity element). A morphism of rings $\sigma : K \to K$ fixing $\mathbb{Q}$ is a $\mathbb{Q}$-linear map so it is completely determined by the image of the basis $\{1, \sqrt{d}\}$. But 1 is sent onto 1 so $\sigma$ is determined by the image of $\sqrt{d}$ which satisfies

\[ (\sigma(\sqrt{d}))^2 = (\sigma(\sqrt{d})) = \sigma(d) = d \]

so $\sigma(\sqrt{d}) = \pm \sqrt{d}$. If $\sigma(\sqrt{d}) = \sqrt{d}$ then $\sigma$ is the identity of $K$ (call it $\sigma_1$), otherwise $\sigma(\sqrt{d}) = -\sqrt{d}$ and we call this morphism $\sigma_2$. It satisfies

\[ \sigma_2(a + b\sqrt{d}) = a - b\sqrt{d}. \]

Check that $\sigma_i(A_K) = A_K$ for $i \in \{1, 2\}$: first notice that $\sigma_i(K) = K$. Then it is easy to check that for a morphism of rings $K \to K$ we have $\sigma(A_K) \subset A_K$ and then use that $\sigma$ is bijective (in fact here $\sigma_i$ is its own inverse).

(iii) Let $z \in K$ and $m_z : K \to K, x \mapsto zx$. Recall that it is a $\mathbb{Q}$-linear map and since $K$ is finite dimensional over $\mathbb{Q}$, the trace and determinant of $m_z$ are well-defined. Define

\[
\begin{align*}
K & \to \mathbb{Q} \\
T : & z \mapsto \text{trace}(m_z) \\
N : & z \mapsto \text{det}(m_z).
\end{align*}
\]

Express $T(z)$ and $N(z)$ using $\sigma_1(z)$ and $\sigma_2(z)$. Write the matrix of $m_z$ in the basis $\{1, \sqrt{d}\}$ and check that $T(z) = \sigma_1(z) + \sigma_2(z)$ and $N(z) = \sigma_1(z)\sigma_2(z)$.

(iv) Find a condition involving $N(z)$ and $T(z)$ for $z \in K$ to be an element of $A_K$. If $z \in A_K$ then $\sigma_i(z) \in A_K$ and therefore (by the previous question) $T(z), N(z) \in A_K \cap \mathbb{Q} \subset A_Q = \mathbb{Z}$. Conversely, notice that $z$ is a root for the characteristic polynomial of $m_z$ which is $X^2 - T(z)X + N(z)$ and which lies in $\mathbb{Z}[X]$ if $T(z), N(z) \in \mathbb{Z}$. So the condition is $T(z)$ and $N(z) \in \mathbb{Z}$.

(v) Show that

\[
A_K = \begin{cases} 
\mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2 \text{ or } 3 \mod 4, \\
\mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 1 \mod 4.
\end{cases}
\]

Clearly we always have $\mathbb{Z}[\sqrt{d}] \subseteq A_K$. Notice that if $d \equiv 1 \mod 4$ we have $T\left(\frac{1+\sqrt{d}}{2}\right) \in \mathbb{Z}$ and $N\left(\frac{1+\sqrt{d}}{2}\right) \in \mathbb{Z}$ so $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] \subseteq A_K$.

Let $z = a + b\sqrt{d} \in K$ and suppose it lies in $A_K$. We have $2a \in \mathbb{Z}$ and $a^2 - db^2 \in \mathbb{Z}$. Let On note $b = \frac{r}{s}$ with $r, s \in \mathbb{Z}$, $s \geq 1$, $r \wedge s = 1$. 


- If \( a \in \mathbb{Z} \), then \( s^2 \) divides \( d \) so \( s = 1 \) and \( b \in \mathbb{Z} \) since \( d \) is square free.
  So \( z \in \mathbb{Z}[\sqrt{d}] \).

- Otherwise \( a = \frac{(1 + 2k)}{2} \) where \( k \in \mathbb{Z} \) and \( s^2(1 + 2k)^2 - 4r^2d \in 4s^2\mathbb{Z} \).
  So 4 divides \( s^2 \). So \( s = 2u \) where \( u \geq 1 \). We have \( 4u^2(1 + 2k)^2 - 4r^2d \in 16u^2\mathbb{Z} \) so \( u^2(1 + 2k)^2 - r^2d \in 4u^2\mathbb{Z} \) and \( d \equiv 1 \mod 4 \). Furthermore, \( u^2 \) divides \( r^2d \) and is prime to \( r^2 \) while \( d \) is square free: so \( u = 1 \).
  We have \( a = \frac{(1 + 2k)}{2} \) and \( b = \frac{r}{2} \) where \( r \) is odd and \( s = 2 \). So
  \[ z = r\left(\frac{1 + \sqrt{\Delta}}{2}\right) + (a - b) \in \mathbb{Z}\left[\frac{1 + \sqrt{\Delta}}{2}\right]. \]