Problem 1. 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 $B$ 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 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 $\mathbb{Z}$.

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 $x^i y^j$... 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 $(I_n)_{n \geq 1}$ such that $I_n \subseteq I_{n+1}$.

Let $\alpha_n := 3^{2^{-n}}$. Check that it lies in $A$ (...). For any $n \geq 1$, we have $\alpha_n^2 = \alpha_n$. Let $I_n = \alpha_n A :$ we have $I_n \subseteq I_{n+1}$ for any $n \geq 1$. If we had $I_n \subseteq I_{n+1}$ 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 $1/3 = (1/\alpha_{n+1})^{3^{2^{-n}}} \in A$ (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 $I_n \subseteq I_{n+1}$.

(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 $\mathcal{A}_K := \mathcal{A} \cap K$. Notice that it is a ring.

(a) What is $\mathcal{A}_Q$? 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 $\mathbb{Q}[X] \rightarrow \mathbb{Q}[\sqrt{d}]$ 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 $\sigma_1, \sigma_2 : K \rightarrow \mathbb{C}$ 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 $\sigma : K \rightarrow K$...
Problem 3. We consider $M$, $Q$, $K$ three abelian groups and an exact sequence of abelian groups
$$0 \rightarrow K \rightarrow M \rightarrow Q \rightarrow 0.$$ This means that $\alpha$ and $\beta$ are homomorphism of groups such that

---

5. $M$ as in Module, $Q$ as in Quotient, $K$ as in Kernel
We say that this sequence splits if there exists a section \( s \) namely an homomorphism of groups \( s : Q \to M \) such that

\[
\pi \circ s = \text{id}_Q
\]

(1) Under the assumption that the sequence splits, show that we have an isomorphism of groups

\[
M \cong K \times Q.
\]

(Or alternatively, \( M \cong K \oplus Q \) as \( \mathbb{Z} \)-modules!). Consider the morphism of groups

\[
\Phi : \iota(K) \oplus s(Q) \to M, \ (k, q) \mapsto k + q.
\]

It is surjective: for \( m \in M \), we have \( m - s(\pi(m)) \in \iota(K) = \ker(\pi) \) (this is because \( \pi(m - s(\pi(m)) = \pi(m) - \text{id} \circ \pi(m) = 0 \) so \( m = \Phi(m - s(\pi(m)), s(\pi(m))) \). It is injective because if for \( q \in Q \) we have \( s(q) \in \iota(K) = \ker(\pi) \), then \( \pi(s(q)) = 0 \) so \( q = 0 \). So

\[
M \cong \iota(K) \oplus s(Q) \cong K \oplus Q.
\]

(2) Give homomorphisms of groups which yield the following exact sequence

\[
0 \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/8\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \to 0.
\]

Does it split? Justify your answer.

Consider the morphism of groups \( \alpha : \mathbb{Z} \to \mathbb{Z}/8\mathbb{Z} \) given by \( x \mapsto 4x \mod 8 \). Its kernel is \( 2\mathbb{Z} \) so it yields an injective morphism of groups \( \tilde{\alpha} : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/8\mathbb{Z} \).

Consider the morphism of groups \( \beta : \mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \) given by \( x \mapsto x \mod 4 \). It is surjective and its kernel contains \( 8\mathbb{Z} \). So it yields a surjective morphism of groups \( \tilde{\beta} : \mathbb{Z}/8\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \).

We have \( \ker(\tilde{\beta}) = 4\mathbb{Z}/8\mathbb{Z} = \text{Im}(\tilde{\alpha}) \) so these morphisms do yield the required exact sequence.

It does not split. Otherwise, we would have an isomorphism of groups \( \mathbb{Z}/8\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \) and any element of \( \mathbb{Z}/8\mathbb{Z} \) would have order at most 4. (ie, they would be annihilated by \( 4 \in \mathbb{Z} \) when you see these abelian groups as \( \mathbb{Z} \)-modules).

(3) Give homomorphisms of groups which yield the following exact sequence

\[
0 \to \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0
\]

and show that it splits namely find a section \( s \).

Consider the morphism of groups \( \alpha : \mathbb{Z} \to \mathbb{Z}/6\mathbb{Z} \) given by \( x \mapsto 2x \mod 6 \). Its kernel is \( 3\mathbb{Z} \) so it yields an injective morphism of groups \( \tilde{\alpha} : \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z} \).

Consider the morphism of groups \( \beta : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \) given by \( x \mapsto x \mod 2 \). It is surjective and its kernel contains \( 6\mathbb{Z} \). So it yields a surjective morphism of groups \( \tilde{\beta} : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \).

We have \( \ker(\tilde{\beta}) = 2\mathbb{Z}/6\mathbb{Z} = \text{Im}(\tilde{\alpha}) \) so these morphisms do yield the required exact sequence.

Consider the morphism of groups \( s : \mathbb{Z} \to \mathbb{Z}/6\mathbb{Z} \) given by \( x \mapsto 3x \mod 6 \). Its kernel is \( 2\mathbb{Z} \). So it yields an injective morphism of groups \( \tilde{s} : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z} \). We have \( \tilde{\beta}(\tilde{s}(x \mod 2)) = \tilde{\beta}(s(x)) = \beta(3x \mod 6) = \beta(3x) = 3x \mod 2 = x \mod 2 \). So \( \tilde{s} \) is a section.

(4) Let \( A \) be a ring. We define likewise an exact sequence of \( A \)-modules by replacing "abelian groups" "homomorphisms of groups" above by "\( A \)-modules" and "homomorphisms of \( A \)-modules".

Suppose that \( A \) is a field which we denote by \( k \). Suppose that \( M, Q, K \) are finite dimensional vector spaces over \( k \).

(a) Suppose that we have an exact sequence of \( k \)-vector-spaces

\[
0 \to K \overset{i}{\to} M \overset{\pi}{\to} Q \to 0
\]

Show that it splits. Let \( \{q_1, \ldots, q_m\} \) a basis for \( Q \). We pick \( m_i \in M \) such that \( \pi(m_i) = q_i \). Define the \( k \)-linear map

\[
Q \to M, q_i \mapsto m_i.
\]

One easily checks that it is a section.
(b) Show that if $M$ is a finite dimensional $k$-vector-space, then any subspace of $M$ has a complement.

Let $K$ be a subspace of $M$. We have an exact sequence of vector spaces

$$0 \to K \to M \to K/M \to 0$$

(the first map is the inclusion, thesecond map the projection) which splits as explained in the previous question. Let $s$ be a section. We have

$$M = K \oplus s(Q).$$

**Problem 4.** Recall that $\mathbb{R}^2$ is naturally a $M_2(\mathbb{R})$-module. Let $t$ denote the matrix $t = \begin{pmatrix} 3 & -2 \\ 2 & -1 \end{pmatrix}$. Define the structure of $\mathbb{R}[X]$-module on $\mathbb{R}^2$ arising from the homomorphism of rings

$$\mathbb{R}[X] \to M_2(\mathbb{R}), \quad P \mapsto P(t).$$

Show that $\mathbb{R}^2$ sits in an exact sequence of $\mathbb{R}[X]$-modules of the form

$$0 \to K \hookrightarrow \mathbb{R}^2 \overset{\pi}{\rightarrow} Q \to 0$$

where $K$ and $Q$ are one-dimensional $\mathbb{R}$-vector-spaces. Identify them as $\mathbb{R}[X]$-modules. Does this sequence split?

See the course notes. You compute that $t$ has 1 as unique eigenvalue and that the corresponding eigenspace has basis $v := e_1 + e_2$. Since it is a subspace of $\mathbb{R}^2$ that is stable $t$, the subspace $R_v$ is a actually a sub-$\mathbb{R}[X]$-module of $\mathbb{R}^2$ (again, see courses notes for that statement, or book page 341). The morphism of $\mathbb{R}[X]$-modules

$$\mathbb{R}[X] \to \mathbb{R}v, \quad P \mapsto P.v$$

is surjective and its kernel is a submodule (hence an ideal) of $\mathbb{R}[X]$ containing $(X - 1)$. Since the map is not zero and since $(X - 1)$ is a maximal ideal, the kernel is exactly $(X - 1)$. So, as $\mathbb{R}[X]$-modules, we have

$$kv \cong \mathbb{R}[X]/(X - 1).$$

We have an exact sequence of $\mathbb{R}[X]$-modules

$$0 \to R_v \hookrightarrow \mathbb{R}^2 \overset{\pi}{\rightarrow} \mathbb{R}^2/R_v \to 0$$

where $\iota$ is just the inclusion and $\pi$ the projection $\mathbb{R}^2 \to \mathbb{R}^2/R_v$ (since $R_v$ is a sub-$\mathbb{R}[X]$-module of $\mathbb{R}^2$, this is indeed a morphism of $\mathbb{R}[X]$-modules).

As a $\mathbb{R}$-vector space, $\mathbb{R}^2/R_v$ is a one dimensional with basis $e_1$ (image of $e_1$ in the quotient). It is also a $\mathbb{R}[X]$-module and we study the map

$$\mathbb{R}[X] \to \mathbb{R}^2/R_v, \quad P \mapsto P.e_1.$$ 

It is surjective. Its kernel is an ideal $\mathcal{I}$ of $\mathbb{R}[X]$ and by the isomorphism theorem we have $\mathbb{R}[X]/\mathcal{I} \cong \mathbb{R}^2/R_v$ as $\mathbb{R}[X]$-modules, and therefore also as $\mathbb{R}$-vector spaces. So we already know without computation that $\mathbb{R}[X]/\mathcal{I}$ is one dimensional over $\mathbb{R}$ so $\mathcal{I}$ is of the form $(X - a)$. We have

$$(X - 1).e_1 = (X - 1).e_1 = e_2 = \bar{e}_1 = e_1 = 3e_1 + 2e_2 - e_1 = 2e_1 + 2e_2 = 0$$

so the kernel of that map contains $(X - 1)$ and therefore is equal to it. So

$$\mathbb{R}[X]/(X - 1) \cong \mathbb{R}^2/R_v$$

as $\mathbb{R}[X]$-modules.

If the sequences split, we would have

$$\mathbb{R}^2 \cong \mathbb{R}[X]/(X - 1) \oplus \mathbb{R}[X]/(X - 1)$$

as $\mathbb{R}[X]$-modules. This would mean that $(X - 1)$ acts by zero on $\mathbb{R}^2$ and therefore $t - 1$ acts by zero on $\mathbb{R}^2$ namely that $t$ is the identity matrix. Contradiction.