(1) Show that the Galois group of the polynomial $f(x) = x^5 - 21x^2 + 6$ over $\mathbb{Q}$ is isomorphic to S_5. (Hint: show that the Galois group contains a 5-cycle and a transposition.)

Proof. Since $f(-1) = -16$, $f(0) = 6$ and $f(1) = -14$, we see that f has at least 3 real roots by intermediate value theorem. Together with the fact that $f'(x) = 5x^4 - 42x = x(5x^3 - 42)$ has two real roots, f has exactly 3 real roots. Therefore, f has a pair of complex roots which are complex conjugate to each other. Hence, f is separable and the splitting field of f, which we denote by K, is a Galois extension over $\mathbb{Q}$.

Now we prove that $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to S_5. Applying Eisentein's criterion with 3, we see that f is irreducible over $\mathbb{Q}$. Thus, $\mathrm{Gal}(K/\mathbb{Q})$ is a subgroup of S_5. Suppose $f(\alpha) = 0$, then f is the minimal polynomial of α; hence, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f) = 5$. Since 5 is a prime and 5 divides the order of $\mathrm{Gal}(K/\mathbb{Q})$, we conclude that $\mathrm{Gal}(K/\mathbb{Q})$ contains an element of order 5, which can only be a 5-cycle in S_5. Note that complex conjugation is a Galois action on $K/\mathbb{Q}$ that exchange two complex roots, which is a transposition. Since S_5 is generated by a 5-cycle and a transposition, we conclude that $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to S_5. □

(2) Assume R is a Noetherian commutative unital ring and M is a finitely generated R-module. Prove that there exist an integer n, an increasing sequence of submodules $\{0\} = M_0 \subset M_1 \subset \cdots \subset M_n = M$ and prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ together with R-module isomorphisms $M_i/M_{i-1} \cong R/\mathfrak{p}_i$, $i \geq 1$.

Proof. Also see stack project.

If M is finitely generated with n generators, then there exists a filtration

$$0 \subset M_1 \subset M_2 \subset \cdots \subset M_n = M$$

where $M_i = (x_1, \cdots, x_i)$ and $M_i/M_{i-1} \cong (x_i) \cong R/\operatorname{Ann}(x_i)$. It suffices to prove that R/I admits such filtration for all ideal I in R. Assume this is not true and S is the collection of ideals that admits no such filtration. Because R is Noetherian, S has a maximal element J and J cannot be prime. Since J is not prime, there exists $a, b \in R$ such that $ab \in J$ but $a \notin J$ and $b \notin J$. Now consider $aR/(J \cap aR)$ and $(R/J)/\big(aR/(J \cap aR)\big)$. There is a surjective ring homomorphism

$$\phi : R \twoheadrightarrow aR/(J \cap aR)$$
$$r \mapsto ar$$

whose kernel contains $J + bR$ since $ab \in J$. Thus, $aR/(J \cap aR) \cong R/I_1$ where $J \subsetneq I_1$ and $b \in I_1$. On the other hand, we have

$$(R/J)/\big(aR/(J \cap aR)\big) \cong R/I_2$$

for some $I_2 \supsetneq J$. By maximality of J, we have $I_1, I_2 \notin S$. However, we have a short exact sequence

$$0 \to R/I_1 \to R/J \to R/I_2 \to 0.$$

It contradicts to the assumption that R/J has no desried filtration. □

(3) Consider the subgroup of $GL_2(\mathbb{R})$ (i.e., the group of invertible 2×2 matrices with real number entries) consisting of matrices of the form $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ Show that this group is solvable. Is this group nilpotent? Prove or disprove.

Proof. For any $a, b, c, d \in \mathbb{R}$, we have

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{a} & \frac{-b}{ca} \\ 0 & \frac{1}{c} \end{pmatrix} = \begin{pmatrix} a & ad+b \\ 0 & c \end{pmatrix} \begin{pmatrix} \frac{1}{a} & \frac{-b}{ca} \\ 0 & \frac{1}{c} \end{pmatrix} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \in U_2(\mathbb{R}).$$

Thus, $U_2(\mathbb{R})$ is a normal subgroup of $B_2(\mathbb{R})$. Since $U_2(\mathbb{R}) \cong (\mathbb{R}, +)$ and $B_2(\mathbb{R})/U_2(R) \cong (\mathbb{R}^\times)^2$ are abelian, $B_2(\mathbb{R})$ is solvable. □

(4) Let R be an Artinian ring and $J \subseteq R$ be the Jacobson radical in R. Suppose that $J^2 = J$. Prove that R is isomorphic to a finite product of matrix rings $A \cong \prod_{i=1}^m M_{n_i}(D_i)$. where each D_i is a division ring.

Proof. Since R is Artinian, J is nilpotent. Because $0 = J^n = (J^{n-2})J^2 = J^{n-1} = \cdots = J$, we have R is semisimple. The result follows from the Wedderburn-Artin theorem. □

(5) Suppose R is a commutative ring. Recall that if $S \subset R$ a multiplicatively closed subset, then the localization $R[S^{-1}]$ is the collection of all formal fractions $\frac{r}{s}$ modulo the equivalence relation $\frac{r}{s} = \frac{r'}{s'}$ if $\exists s'' \in S$ such that $s''(rs' - sr') = 0$. The function $r \mapsto \frac{r}{1}$ yields a well-defined function $\pi : R \to R[S^{-1}]$.

(a) Show that π is an isomorphism if and only if $S \subset R^\times$ (the multiplicative group of units in R).

(b) Suppose R is a finite ring. Show that π need not be an isomorphism, but it is always surjective.

Proof. (a) Note that π is injective if and only if S contains no zero divisors. In this case, $\frac{1}{s} = \frac{r}{1}$ in $R[S^{-1}]$ if and only if $s \in R^\times$.

(b) If R is finite, then R is Artinian. For any $s \in S$, we have $s^n = rs^{n+1}$ for some large n and some $r \in R$. Then we have $s^n(1 - rs) = 0$. Since S is multiplicative closed, we have $\frac{1}{s} = \frac{r}{1}$ in $R[S^{-1}]$. Therefore, $\pi(r) = \frac{1}{s}$; hence, π is surjective.

□

(6) (a) For an ideal $I \subseteq \mathbb{C}[x_1, x_2]$ write $V(I) \subset \mathbb{A}^2_{\mathbb{C}}$ for the variety of the ideal I. i.e., the collection of $x \in \mathbb{C}^2$ such that $f(x) = 0$ for all $f \in I$. Likewise, write $I(V)$ for the vanishing ideal of a subset $V \subset \mathbb{C}^2$. i.e., the collection of all $f \in \mathbb{C}[x_1, x_2]$ such that $f(x) = 0$ for all $x \in V$. Provide an explicit example of an ideal I for which $V(I)$ is the union of two distinct lines in $\mathbb{C}^2$ and for which $I \neq I(V(I))$ (by a line, we mean the vanishing locus of a linear function $a_1x_1 + a_2x_2 + a_3$, where at least one of a_1, a_2 is non-zero.)

(b) Provide an example of a 4-dimensional commutative $\mathbb{Q}$-algebra A which admits no ring homomorphism $A \to \mathbb{Q}$.

Proof. (a) Let $I = (x^2y)$. Then $V(I)$ is the union of the x-axis and the y-axis, but $\sqrt{I} = (xy)$.

(b) Note that any field extension of degree 4 will work. For example, $A = \mathbb{Q}(\zeta)$ where ζ is a primitive 5-th root of unity. Then A is a 4-dimensional $\mathbb{Q}$-algebra with a ring homomorphism $f : A \to \mathbb{Q}$. Note that f is $\mathbb{Q}$-linear and any ring homomorphism from a field is injective, we obtain a contradiction that $4 = \dim_{\mathbb{Q}}(A) \leq \dim_{\mathbb{Q}}(\mathbb{Q}) = 1$.

□