Justify all arguments completely. Every ring R is assumed to have a unit $1 \in R$. Reference specific results whenever possible.

(1) Let G be a simple group of order 168. Show that G is isomorphic to a subgroup of A_8, the alternating group of degree 8. Show that G is not isomorphic to a subgroup of A_6.

Proof. Note that $7 \mid 168$ and $7 \nmid |A_6| = \frac{6!}{2}$. Hence, $G \not\leq A_6$.

Since G is simple, any Sylow subgroups of G is not normal. Note that $|G| = 2^3 \cdot 3 \cdot 7$. We have $n_7 = 8$ because $n_7 \mid 24$ and $n_7 \equiv 1 \pmod 7$. Let G acts on the Sylow 7-subgroups by conjugation then the group action induces a group homomorphism $\phi : G \to S_8$. Since G is simple, ϕ is injective. Thus, it remains to show that $\phi(G) \leq A_8$. Let $\epsilon : S_8 \to \mathbb{Z}/2\mathbb{Z}$ be the signature map. Then we have $\epsilon \circ \phi : G \to \mathbb{Z}/2\mathbb{Z}$. Since G is simple, we have $\ker \epsilon \circ \phi = G$ or $\ker \epsilon \circ \phi = 1$. Since $|G| > 2$, we cannot have $\ker \epsilon \circ \phi = 1$. Hence, we have $\phi(G) \leq \ker \epsilon = A_8$. □

(2) Let K be a field and A be a finite-dimensional, semisimple K-algebra. Let $Z(A)$ denote the center of A. Prove that two finitely-generated A-modules M and M' are isomorphic as A-modules if and only if they are isomorphic as $Z(A)$-modules.

Proof. First of all, A is a finite-dimensional K-algebra implies that A is Artinian. Since A is semisimple, $A \cong \prod_{i=1}^n M_{n_i}(D_i)$ for some $n_i \in \mathbb{N}$ and D_i are division algebra over K. Thus, $Z(A) \cong \prod_{i=1}^n Z(D_i)$, which is a product of fields.

$\Longrightarrow$: Assume $M \cong M'$. Since $Z(A)$ is a subalgebra of A, any A-module homomorphism is naturally a $Z(A)$-module homomorphism. Thus, we have $M \cong_{Z(A)} M'$.

$\Longleftarrow$: Assume $M \cong_{Z(A)} M'$ are finitely generated A-module. Therefore we have

$$M \cong \bigoplus_{i=1}^n S_i^{\oplus k_i}, \quad M' \cong \bigoplus_{i=1}^n S_i^{\oplus q_i}$$

where $S_i \cong D_i^{n_i}$ are simple A-modules. Because $Z(A)$ is a product of fields and each S_i is a $Z(D_i)$-vector space, we have $S_i^{k_i} \cong_{Z(A)} S_i^{q_i}$ if and only if $k_i = q_i$. Thus, $M \cong_A M'$. □

(3) Let f and g be polynomials in $\mathbb{C}[x_1, ..., x_{24}]$. Suppose that for each value $z \in \mathbb{C}^{24}$ at which $f(z) = 0$, we also have $g(z) = 0$. Prove that f divides some power of g.

Proof. By Hilbert's Nullstellensatz, the defining ideal of $V(g)$ is $\sqrt{(g)}$. Since f vanishes on $V(g)$, we have $f \in \sqrt{(g)}$. Thus, $f \mid g^n$ for some $n \in \mathbb{Z}_{>0}$. □

(4) Define the Jacobson radical of a ring to be the intersection of all maximal left ideals of this ring. Let $\phi : R \to S$ be a surjective morphism of rings. Prove that the image by ϕ of the Jacobson radical of R is contained in the Jacobson radical of S.

Proof. Suppose $\mathfrak{m}$ is a maximal ideal in R. Since ϕ is surjective, $\phi(\mathfrak{m})$ is an ideal in S. If $\phi(\mathfrak{m}) \neq S$ and it is not maximal, then there exists a maximal ideal $\mathfrak{a}$ such that $\phi(\mathfrak{m}) \subsetneq \mathfrak{a} \subsetneq S$. Then $\mathfrak{m} \subsetneq \phi^{-1}(\mathfrak{a}) \subsetneq R = \phi^{-1}(S)$ is a contradiction since $\mathfrak{m}$ is maximal. Hence, $\phi(\mathfrak{m})$ is a maximal ideal in S. Therefore, we have $\phi(\mathfrak{m})$ is either a maximal ideal or S. Thus, $\phi(J(R)) = \phi(\cap_{\mathfrak{m} \subset R} \mathfrak{m}) \subseteq \cap_{\mathfrak{m} \subset R} \phi(\mathfrak{m}) = J(S)$. □

(5) Construct an example (or merely prove the existence) of a 10×10 matrix over $\mathbb{R}$ with minimal polynomial $(x+1)^2(x^4+1)$ which is not similar to a matrix over $\mathbb{Q}$.

Proof. The main reason is that irreducible polynomials over R has degree at most 2 since $\mathbb{C}$ is algebraically closed and $[\mathbb{C} : \mathbb{R}] = 2$.

Note that $x^4+1=(x^2+1)^2-(2x^2)=(x^2+1-\sqrt{2}x)(x^2+1+\sqrt{2}x)$. Thus, we have

$$\begin{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & \sqrt{2} \end{pmatrix} & & \\ & \begin{pmatrix} 0 & -1 \\ 1 & \sqrt{2} \end{pmatrix} & \\ & & \begin{pmatrix} & & & & & -1 \\ 1 & & & & & -2 \\ & 1 & & & & -1 \\ & & 1 & & & 0 \\ & & & 1 & & -1 \\ & & & & 1 & -2 \end{pmatrix} \end{pmatrix} \in \mathrm{Mat}_{10\times 10}(\mathbb{R})$$

is a matrix with minimal polynomial $(x+1)^2(x^4+1)$ which is not similar to a matrix over $\mathbb{Q}$. □

(6) Let F be a field of characteristic not 2. Show that if $f(x)=x^8+ax^4+bx^2+c$ is an irreducible polynomial over F for some $a,b,c\in F$ then the Galois group of the splitting field of f is solvable.

Proof. Since $\operatorname{char} F \neq 2$, $f'(x)\neq 0$. Because f is irreducible and $f'(x)\neq 0$, we must have $\gcd(f,f')=1$; hence, f is separable. Let K be the splitting field of f over F. Then K/F is a Galois extension. Note that $f(x)=g(x^2)$ where $g(x)=x^4+ax^2+bx+c$, which is also separable. The splitting field of g is a subfield $F\subseteq E\subseteq K$, and E/F is Galois as well. Because $\mathrm{Gal}(E/F)\leq S_4$ is solvable and $\mathrm{Gal}(K/E)\cong(\mathbb{Z}/2)^4$ is solvable, we have $\mathrm{Gal}(K/F)$ is solvable (any extension of solvable groups is solvable). □