1. Let $R$ be a commutative ring with $1 \neq 0$.

(a) Prove that the nilradical of $R$ is equal to the intersection of the prime ideals of $R$. Hint: it’s easy to show using the definition of prime that the nilradical is contained in every prime ideal. Conversely, suppose that $f$ is not nilpotent and consider the set $S$ of ideals $I$ of $R$ with the property that \( n > 0 \implies f^n \notin I \). Show that $S$ has maximal elements and that any such maximal element must be a prime ideal.

**Solution:** Suppose that $f \in R$ is not nilpotent and let $S$ be the set $S$ of ideals $I$ of $R$ with the property that \( n > 0 \implies f^n \notin I \). Ordering $S$ by inclusion, note that every chain is bounded above: if $I_1 \subseteq I_2 \subseteq \cdots$ is a chain, then $I = \bigcup I_i$ is an upper bound which clearly lies in $S$. By Zorn’s lemma, $S$ has a maximal element, say $M$, which we claim is prime. Indeed, suppose that $uv \in M$ but that $u \notin M$ and $v \notin M$. Then the ideals $M + (u)$ and $M + (v)$ strictly contain $M$ so do not belong to $S$ by maximality of $M$. Thus, there exist $m$ and $n$ such that $f^n \in M + (u)$ and $f^m \in M + (v)$. It follows that $f^{m+n} \in M + (uv) = M$ and hence that $M$ is not in $S$, a contradiction. Thus, either $u$ or $v$ lies in $M$ and $M$ is prime. We deduce that $f$ is not contained in the prime ideal $M$, and hence that $f$ is not contained in the intersection of all prime ideals. Conversely, if $p$ is any prime ideal and $f$ is nilpotent then $0 = f^n \in p$ for some $n$, and an easy induction argument using that $p$ is prime shows that $f$ must be in $p$.

(b) Suppose that $R$ is reduced, i.e. that the nilradical of $R$ is the zero ideal. If $p$ is a minimal prime ideal of $R$, show that the localization $R_p$ has a unique prime ideal and conclude that $R_p$ is a field.

**Solution:** By a previous exercise, the prime ideals of the localization $R_p$ are those prime ideals of $R$ not meeting $R \setminus p$, or in other words, the prime ideals of $R$ contained in $p$. As $p$ is minimal, there is a unique such prime ideal: namely $p$ itself. We claim that the image of $p$ in $R_p$ is the zero ideal. Indeed, by part (a), any $f \in p$ is nilpotent in $R_p$ so there exists $s \in R \setminus p$ such that $s f^n = 0$ for some $n > 0$. We deduce by commutativity that $sf \in R$ is nilpotent, whence it must be zero since $R$ is reduced, and we conclude that $f$ is zero in $R_p$ as desired. Thus, $R_p$ is a ring whose only prime ideal is 0 and therefore must be a field. (If $T$ is any such ring and $x \in T$ is nonzero, then $(x)$ can not be contained in any maximal ideal, since maximal ideals are prime and hence $(x)$ is the unit ideal so $x$ is a unit.)

(c) Again supposing $R$ to be reduced, prove that $R$ is isomorphic to a subring of a direct product of fields.

**Solution:** We have a canonical ring homomorphism

$$R \to \prod_{p \text{ minimal}} R_p$$

whose kernel is the intersection of all minimal primes. By part (a), this kernel is the nilradical of $R$, so since $R$ is reduced the above map is injective. By part (b), the right
hand side is a product of fields, so we conclude that $R$ is isomorphic to a subring of a direct product of fields.

2. Let $R$ be a commutative ring with $1 \neq 0$ and let $\varphi : R \to R$ be a ring homomorphism. If $R$ is noetherian and $\varphi$ is surjective, show that $\varphi$ must be injective too, and hence an isomorphism. (Hint: Consider the iterates of $\varphi$ and their kernels.) Can you give a counter-example to this when $R$ is not noetherian?

**Solution:** Let $\varphi^n$ be the composition of $\varphi$ with itself $n$-times and denote by $I_n$ the kernel of $\varphi^n$. Then we have a chain of ideals

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

in the noetherian ring $R$, so we conclude that this chain stabilizes, hence $I_n = I_{n+1}$ for some $n \geq 1$. Suppose $x \in \ker \varphi$. Since $\varphi^n$ is surjective, we can write $x = \varphi^n(y)$ whence $0 = \varphi(x) = \varphi^{n+1}(y)$ and we deduce that $y \in I_{n+1} = I_n$ and hence that $x = \varphi^n(y) = 0$. Thus, $\varphi$ is injective.

As a counterexample in the case of non-noetherian $R$, consider the ring $R$ of infinitely differentiable real-valued functions on the interval $[0,1]$ and the map $\varphi : R \to R$ given by differentiation. This map is surjective, since for any $f$, the function $F(x) := \int_0^x f(u)du$ is well-defined and infinitely differentiable. However, $\varphi$ is not injective as it kills the constant functions.

3. As usual, for a prime $p$ we write $F_p = \mathbb{Z}/p\mathbb{Z}$ for the field with $p$ elements.

(a) Find all monic irreducible polynomials in $F_p[X]$ of degree $\leq 3$ for $p = 2, 3, 5$.

**Solution:** For $p = 2$ the monic irreducibles are

$$x^3 + x^2 + 1, \ x^3 + x + 1, \ x^2 + x + 1, \ x + 1, \ x$$

for $p = 3$ they are

$$x^3 + x^2 + x + 2, \ x^3 + x^2 + 2x + 1, \ x^3 + x^2 + 2, \ x^3 + 2x^2 + x + 1$$

$$x^3 + 2x^2 + 2x + 2, \ x^3 + 2x^2 + 1, \ x^3 + 2x + 1, \ x^3 + 2x + 2$$

$$x^2 + x + 2, \ x^2 + 2x + 2, \ x^2 + 1, \ x + 1, \ x + 2, \ x$$
for $p = 5$ they are

\[
x^3 + x^2 + x + 3, \ x^3 + x^2 + x + 4, \ x^3 + x^2 + 3x + 1, \ x^3 + x^2 + 3x + 4
\]

\[
x^3 + x^2 + 4x + 1, \ x^3 + x^2 + 4x + 3, \ x^3 + x^2 + 1, \ x^3 + x^2 + 2, \ x^3 + 2x^2 + x + 3
\]

\[
x^3 + 2x^2 + x + 4, \ x^3 + 2x^2 + 2x + 2, \ x^3 + 2x^2 + 2x + 3, \ x^3 + 2x^2 + 4x + 2
\]

\[
x^3 + 2x^2 + 4x + 4, \ x^3 + 2x^2 + 1, \ x^3 + 2x^2 + 3, \ x^3 + 3x^2 + x + 1, \ x^3 + 3x^2 + x + 2
\]

\[
x^3 + 3x^2 + 2x + 2, \ x^3 + 3x^2 + 2x + 3, \ x^3 + 3x^2 + 4x + 1, \ x^3 + 3x^2 + 4x + 3
\]

\[
x^3 + 3x^2 + 2, \ x^3 + 3x^2 + 4, \ x^3 + 4x^2 + x + 1, \ x^3 + 4x^2 + x + 2, \ x^3 + 4x^2 + 3x + 1
\]

\[
x^3 + 4x^2 + 3x + 4, \ x^3 + 4x^2 + 4x + 2, \ x^3 + 4x^2 + 4x + 4, \ x^3 + 4x^2 + 3, \ x^3 + 4x^2 + 4
\]

\[
x^3 + x + 1, \ x^3 + x + 4, \ x^3 + 2x + 1, \ x^3 + 2x + 4, \ x^3 + 3x + 2, \ x^3 + 3x + 3, \ x^3 + 4x + 2
\]

\[
x^3 + 4x + 3, \ x^2 + x + 1, \ x^2 + x + 2, \ x^2 + 2x + 3, \ x^2 + 2x + 4, \ x^2 + 3x + 3, \ x^2 + 3x + 4
\]

\[
x^2 + 4x + 1, \ x^2 + 4x + 2, \ x^2 + 2, \ x^2 + 3, \ x + 1, \ x + 2, \ x + 3, \ x + 4, \ x
\]

(b) Prove that for $f \in \mathbb{F}_p[X]$ monic and irreducible, the ideal $(f(X))$ is maximal and hence that $\mathbb{F}_p[X]/(f(X))$ is a field. Show that $\mathbb{F}_p[X]/(f(X))$ has finite cardinality $p^{\deg f}$ and use part (??) to explicitly construct finite fields of orders 8, 9, 25, 125.

**Solution:** We showed that $\mathbb{F}_p[X]$ is Euclidean and hence a PID and hence a UFD. In particular, irreducible implies prime (using UFD) and prime implies maximal (using PID). We conclude that for a monic irreducible $f$, the ring $\mathbb{F}_p[X]/(f(X))$ is a field. As an $\mathbb{F}_p$-vector space, $\mathbb{F}_p[X]/(f(X))$ has basis $1, X, X^2, \ldots, X^{\deg f-1}$ and hence this field has cardinality $p^{\deg f}$. Choosing specific examples of monic irreducibles as found in part (a) yields specific examples of finite fields of size $2^3$, $3^2$, $5^2$, and $5^3$.

(c) Prove that $\mathbb{F}_7[X]/(X^2 + 2)$ and $\mathbb{F}_7[X]/(X^2 + X + 3)$ are both finite fields of size 49. Show that these fields are isomorphic by exhibiting an explicit isomorphism between them.

**Solution:** Both $X^2 + X + 3$ and $X^2 + 2$ are monic irreducibles in $\mathbb{F}_7[X]$. Any ring map $\varphi : \mathbb{F}_7[X] \to \mathbb{F}_7[Y]/(Y^2 + Y + 3)$ has the form

\[
X \mapsto aY + b,
\]

so $X^2 + 2$ maps to

\[
(aY + b)^2 + 2 = a^2Y^2 + 2abY + b^2 + 2 = a^2(Y^2 + 3) + 2abY + b^2 + 2 = -(a^2 - 2ab)Y + b^2 + 2 - 3a^2
\]

so since $1, Y$ is an $\mathbb{F}_7$-basis of the target, if $X^2 + 2$ is to map to zero we must have $a^2 = 2ab$ and $b^2 = 3a^2 + 2 = 0$. If $a = 0$ then $\varphi$ would not be surjective, so we must have $a \neq 0$. Then $a = 2b$ and $b^2 = 4$ so $b = \pm 2$. Taking $b = 2$ and $a = 4$ gives the map $X \mapsto 4Y + 2$ which by our calculation induces a nonzero map of fields $\mathbb{F}_7[X]/(X^2 + 2) \to \mathbb{F}_7[Y]/(Y^2 + Y + 3)$ which must therefore be an isomorphism.

4. Let $R$ be a ring with $1 \neq 0$ and $M$ an $R$-module. Show that if $N_1 \subseteq N_2 \subseteq \cdots$ is an ascending chain of submodules of $M$ then $\cup_{i \geq 1} N_i$ is a submodule of $N$. Show by way of counterexample that modules over a ring need not have maximal proper submodules (in contrast to the special case of ideals in a ring with 1).
Solution: The argument is identical to that for the special case of ideals. For a counterexample, consider \( \mathbb{Q} \) as a \( \mathbb{Z} \)-module.

5. Let \( R \) be any commutative ring with \( 1 \neq 0 \) and \( M \) and \( R \)-module. Show that the canonical map 

\[
\text{Hom}_R(R, M) \to M
\]

sending \( \varphi \) to \( \varphi(1) \) is an isomorphism of \( R \)-modules.

Solution: One must first check that the given map really is a map of \( R \)-modules; as this is straightforward and tedious, we omit it. For \( m \in M \) let \( \varphi_m : R \to M \) be the map defined by \( \varphi_m(r) := rm \). It is easy to see that this is an \( R \)-module homomorphism and is inverse to the canonical map \( \text{Hom}_R(R, M) \to M \).

6. Let \( F = \mathbb{R} \) and let \( V = \mathbb{R}^3 \). Consider the linear map \( \varphi : V \to V \) given by rotation through an angle of \( \pi/2 \) about the \( z \)-axis. Consider \( V \) as an \( F[X] \)-module by defining

\[
(a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0) v := (a_n \varphi^n + a_{n-1} \varphi^{n-1} + \cdots + a_1 \varphi + a_0) v,
\]

where \( \varphi^i \) is the composition of \( \varphi \) with itself \( i \)-times.

(a) What are the \( F[X] \)-submodules of \( V \)?

Solution: The \( F[X] \)-submodules are precisely that \( F \)-subspaces of the vector space \( \mathbb{R}^3 \) which are stable under multiplication by \( X \), i.e. the subspaces preserved by \( \varphi \). Thinking geometrically, these are the \( x - y \) plane and the \( z \)-axis.

(b) Show that \( V \) is naturally a module over the quotient ring \( F[X]/(X^3 - X^2 + X - 1) \).

Solution: Thinking geometrically, \( \varphi \) has eigenvalues 1 (the \( z \)-axis is an eigenvector) and \( \pm i \) (the restriction of \( \varphi \) to the \( x - y \) plane is rotation through \( \pi/2 \), whose characteristic polynomial is clearly \( X^2 + 1 \)). We conclude that the characteristic polynomial of \( \varphi \) is

\[
(X - 1)(X^2 + 1) = (X^3 - X^2 + X - 1)
\]

and hence that this element of \( F[X] \) acts trivially on \( V \) by the Cayley-Hamilton theorem. Thus, \( V \) is a module over the quotient ring \( F[X]/(X^3 - X^2 + X - 1) \).

7. Let \( R \) be a ring with \( 1 \neq 0 \).

(a) For a left ideal \( I \) of \( R \) and an \( R \)-module \( M \), define

\[
IM := \{ r_1 m_1 + r_2 m_2 + \cdots + r_k m_k : r_i \in R, m_i \in M, k \in \mathbb{Z}_{\geq 0} \}
\]

Show that \( IM \) is an \( R \)-submodule of \( M \).

Solution: Obvious.

(b) Prove that for any ideal \( I \) of \( R \) and any positive integer \( n \), there is a canonical isomorphism of \( R \)-modules

\[
R^n/IR^n \cong R/IR \times R/IR \times \cdots \times R/IR
\]
with \( n \)-factors in the product on the right.

**Solution:** The map 
\[
R^n \cong R/IR \times R/IR \times \cdots \times R/IR
\]
defined by \((r_1, \ldots, r_n) \mapsto (r_1 + I, \ldots, r_n + I)\) is a well-defined and surjective \( R \)-module homomorphism. The kernel consists of exactly those \((r_1, \ldots, r_n)\) with \( r_i \in I \) for all \( I \), which is easily seen to be the ideal \( IR^n \).

(c) Suppose now that \( R \) is commutative and that \( R^n \cong R^m \) as \( R \)-modules. Show that \( m = n \).

**Hint:** reduce to the case of finite dimensional vector spaces over a field by applying (??) with \( I \) a maximal ideal of \( R \).

**Solution:** Let \( I \) be a maximal ideal of \( R \) so \( F := R/IR \) is a field. By (??), we deduce that \( F^m \cong R^m/IR^m \cong R^n/IR^n \cong F^n \) which forces \( m = n \) since all bases of a finite dimensional vector space have the same cardinality (i.e. dimension is well-defined).

(d) If \( R \) is commutative and \( A \) is any finite set of cardinality \( n \), show that \( F(A) \cong R^n \) as \( R \)-modules (Hint: Show that \( R^n \) satisfies the same universal mapping property as \( F(A) \) and deduce from this that one has maps in both directions whose composition in either order must be the identity). Conclude that the rank of a free module over a commutative ring is well-defined if it is finite.

**Solution:** Let \( E := \{e_i\}_{i=1}^n \) be the standard basis of \( R^n \) and suppose given a map of sets \( \psi : E \to M \) for an \( R \)-module \( M \). We extend \( \psi \) to an \( R \)-module homomorphism \( R^n \to M \) by the rule
\[
\sum r_i e_i \mapsto \sum r_i \psi(e_i).
\]
This is well-defined because \( \{e_i\} \) is a basis of \( R^n \), so every element of \( R^n \) has a unique representation as a sum \( \sum r_i e_i \). Moreover, this map is obviously a homomorphism of \( R \)-modules, and is uniquely determined by \( \psi \) (because \( \{e_i\} \) spans \( R^n \)). Thus, \( R^n \) with the set \( E \) satisfies the same universal property as \( F(E) \) so the two must be isomorphic as \( R \)-modules. As \( F(E) \cong F(A) \) (because \( A \) and \( E \) are in bijection as sets) we conclude as desired.

8. Let \( R \) be a ring with \( 1 \neq 0 \) and \( M \) an \( R \)-module. We say that \( M \) is irreducible if \( M \neq 0 \) and the only submodules of \( M \) are \( 0 \) and \( M \).

(a) Show that \( M \) is irreducible if and only if \( M \) is a nonzero cyclic \( R \)-module.

**Solution:** Let \( m \in M \) be any nonzero element. Then \( Rm \) is a nonzero cyclic submodule of \( M \) (since it contains \( m \)) and by irreducibility of \( M \) we must have \( Rm = M \). The converse is false in general (example \( 2\mathbb{Z} \subseteq \mathbb{Z} \)), and we must require the additional phrase “with any nonzero element as a generator” to get the desired equivalence. Suppose that \( M \) is a nonzero cyclic \( R \)-module with any nonzero element as a generator. If \( N \subseteq M \) is a submodule which is nonzero, then any nonzero \( n \in N \) generates \( M \) as an \( R \)-module so \( N = M \) and \( M \) is irreducible.
(b) If $R$ is commutative, show that $M$ is irreducible if and only if $M \simeq R/I$ as $R$-modules for some maximal ideal $I$ of $R$.

**Solution:** By part (a), if $M$ is irreducible then there is a natural surjective map of $R$-modules $\varphi : R \to M$ given by $r \mapsto rm$ for any (fixed) nonzero $m \in M$. The kernel of this map is a submodule of $R$, i.e. an ideal $I$ of $R$. Since the submodules of $M \simeq R/\ker(\varphi)$ are those ideals of $R$ containing $\ker(\varphi)$, by irreducibility of $M$ we conclude that $I$ must be maximal.

(c) Prove Schur’s lemma: if $M_1$ and $M_2$ are irreducible $R$-modules then any nonzero $R$-module homomorphism $\varphi : M_1 \to M_2$ is an isomorphism.

**Solution:** The kernel of $\varphi$ is a submodule of $M_1$ so by irreducibility of $M_1$ must be zero (as $\varphi$ is not the zero map). Since $M_1$ is nonzero (definition of irreducible) we conclude that $M_1$ is isomorphic to a nonzero submodule of $M_2$ and hence $\varphi$ is an isomorphism by irreducibility of $M_2$. 