1. (DF7.3.29) Let R be a commutative ring. Recall that an element $x \in R$ is nilpotent if $x^n = 0$ for some $n \in \mathbb{Z}^+$. Prove that the set of nilpotent elements form an ideal — called the *nilradical* of R and denoted by $\mathfrak{N}(R)$. [Use the Binomial Theorem to show $\mathfrak{N}(R)$ is closed under addition.]

Proof. Let R be a commutative ring.

We check that the nilradical $\mathfrak{N}(R)$ is a subring of R. Observe that $0^1 = 0$, so that $0 \in \mathfrak{N}(R)$ and $\mathfrak{N}(R)$ is a nonempty subset of R. Let $x, y \in R$ such that $x^n = 0$ and $y^m = 0$. By properties of the multiplication in a ring and induction it follows that $-y$ is nilpotent:

$$(-y)^m = \begin{cases} y^m = 0 & \text{if } m \text{ is even} \\ -(y^m) = 0 & \text{if } m \text{ is odd} \end{cases}.$$

Since R is commutative, it follows that

$$\begin{aligned} (x-y)^{n+m} &= \sum_{k=0}^{n+m} \binom{n+m}{k} x^k (-y)^{n+m-k} \\ &= \sum_{k=0}^{n-1} \binom{n+m}{k} x^k (-y)^{n+m-k} + \sum_{k=n}^{n+m} \binom{n+m}{k} x^k (-y)^{n+m-k}. \end{aligned}$$

Each sum must vanish due to the exponent on either x or $(-y)$ for each term being large enough to cause the term to vanish. Specifically,

$$\begin{aligned} (-y)^{n+m-k} = (-y)^{n-k}(-y)^m = (-y)^{n-k}0 = 0 &\quad \text{for } k < n \\ x^k = x^n x^{k-n} = 0(x^{k-n}) = 0 &\quad \text{for } k \geq n, \end{aligned}$$

so that the terms in each sum vanish. It follows that $(x-y)^{n+m} = 0$, so that $x - y$ is nilpotent and $\mathfrak{N}(R)$ is a subgroup of R. Closure under multiplication is also easy to check since R is a commutative ring. The element xy is nilpotent since $(xy)^{nm} = x^{nm}y^{nm} = (x^n)^m(y^m)^n = (0)(0) = 0$, so $\mathfrak{N}(R)$ is closed under multiplication and hence is a subring of R.

It follows in a similar manner that $\mathfrak{N}(R)$ is an ideal. For any element $r \in R$ and $x \in \mathfrak{N}(R)$ with $x^n = 0$, we have that

$$\begin{aligned} (rx)^n &= r^n x^n = r^n 0 = 0 \\ (xr)^n &= x^n r^n = 0 r^n = 0. \end{aligned}$$

Thus xr, rx are nilpotent and it follows that R is an ideal. □

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

2. (DF7.4.1) Let L_j be the left ideal of $M_n(R)$ consisting of arbitrary elements in the j^{th} column and zero in all other entries and let E_{ij} be the element of $M_n(R)$ whose i, j entry is 1 and whose other entries are all 0. Prove that $L_j = M_n(R)E_{ij}$ for any i.

Proof. Let n be a positive integer and let i be any integer from 1 to n. It is clear that L_j is a left ideal since it is an additive subgroup and is closed under multiplication by matrices from $M_n(R)$ on the left: For any element $A \in L_j$ and $M \in M_n(R)$, we have

$$(MA)_{rs} = \sum_{k=1}^{n} M_{rk}A_{ks} = \begin{cases} 0 & \text{if } s \neq j \\ \sum_{k=1}^{n} M_{rk}A_{kj} & \text{if } s = j, \end{cases}$$

meaning that only the j-th column of the resulting matrix survives in the product.

Any element L of L_j may be written as ME_{ij}, where $M \in M_n(R)$ and E_{ij} is the matrix whose entries are zero except for the i, j-th entry being $1 \in R$. Let $L_{ij} = \ell_i \in R$ for $1 \leq i \leq n$ (and all other entries of L are zero). Then choose M to be the matrix whose entries are zero except for its i-th column being the j-th column of L; that is, $M_{ri} = L_{rj}$ for $1 \leq r \leq n$. It follows that

$$(ME_{ij})_{rs} = \sum_{k=1}^{n} M_{rk}(E_{ij})_{ks} = M_{ri}(E_{ij})_{is} = L_{rj}(E_{ij})_{is} = \begin{cases} 0 & \text{if } s \neq j \\ L_{rs}(1) = \ell_r & \text{if } s = j \end{cases} = L_{rs},$$

and since i was arbitrary, it follows that $L_j \subseteq M_n(R)E_{ij}$.

The reverse inclusion is checked similarly. Any matrix M in $M_n(R)$ multiplied by E_{ij} on the right has the form we desire. Note also that because matrix multiplication distributes, we only need to check that the product of one matrix M with E_{ij} has the form needed to be an element of L_j. We have that

$$(ME_{ij})_{rs} = \sum_{k=1}^{n} M_{rk}(E_{ij})_{ks} = M_{ri}(E_{ij})_{is} = \begin{cases} 0 & \text{if } s \neq j \\ M_{ri}(1) = M_{ri} & \text{if } s = j, \end{cases}$$

meaning the resulting matrix is the matrix with zeros in all entries except for the j-th column whose entries are taken from the i-th column of M. Since i was arbitrary, it follows that $M_n(R)E_{ij} \subseteq L_j$.

Hence $L_j = M_n(R)E_{ij}$ for any i. □

3. Lemma. The preimage of a subring under a ring homomorphism is a subring, and the preimage of an ideal is an ideal.

Proof. Let $\varphi\colon R \to S$ be a homomorphism of rings. Let T be a subring of S, and let $a, b \in \varphi^{-1}(T)$. Note $\varphi(0_R) = 0_S \in T$, so $\varphi^{-1}(T)$ contains 0_R and hence is a nonempty subset of R. Then $\varphi(a-b) = \varphi(a)-\varphi(b) \in T$ since T is an additive group, and $\varphi(ab) = \varphi(a)\varphi(b) \in T$ since T is a ring. Hence $a - b, ab \in \varphi^{-1}(T)$, so $\varphi^{-1}(T)$ is a subring of R.

If T is an ideal of S, then we check that the preimage under φ is an ideal of R: By the above argument, we know that the preimage $\varphi^{-1}(T)$ is a subring of R. Then let $r \in R$ and $a \in \varphi^{-1}(T)$. We have $\varphi(ra) = \varphi(r)\varphi(a) \in T$ and $\varphi(ar) = \varphi(a)\varphi(r) \in T$ since T is an ideal in S. Hence $\varphi^{-1}(T)$ is closed under multiplication on the left and right by elements of R, so it is an ideal. □

4. (DF7.4.13) Let $\varphi\colon R \to S$ be a homomorphism of commutative rings.

(a) Prove that if P is a prime ideal of S then either $\varphi^{-1}(P) = R$ or $\varphi^{-1}(P)$ is a prime ideal of R. Apply this to the special case when R is a subring of S and φ is the inclusion homomorphism to deduce that if P is a prime ideal of S then $P \cap R$ is either R or a prime ideal of R.

Proof. By the previous lemma, we know that $\varphi^{-1}(P)$ is an ideal of R. If $ab \in \varphi^{-1}(P)$, then $\varphi(ab) = \varphi(a)\varphi(b) \in P$. Because R, S are commutative rings, we can take without loss of generality that $\varphi(a) \in P$. What remains is to determine what happens if $\varphi(b)$ is in P or not. We have $b \in \varphi^{-1}(P)$ if $\varphi(b) \in P$. Otherwise, if $\varphi(b) \notin P$, then $b \notin \varphi^{-1}(P)$. It follows that $\varphi^{-1}(P)$ is a prime ideal of R if it is properly contained in R, since at least one of a, b is in $\varphi^{-1}(P)$ whenever $ab \in \varphi^{-1}(P)$. But it is also possible for $\varphi^{-1}(P)$ to contain 1_R and thus be equivalent to R.

When φ is the inclusion homomorphism, it follows that $\varphi^{-1}(P) = P \cap R$ (since $P \cap R$ contains all of the elements of R which map into P under φ). By the previous result, it follows that $P \cap R$ is either R or is a prime ideal of R. □

(b) Prove that if M is a maximal ideal of S and φ is surjective then $\varphi^{-1}(M)$ is a maximal ideal of R. Give an example to show that this need not be the case if φ is not surjective.

Proof. Let $\pi\colon S \to S/M$ be the projection map, which is surjective. Then the composition $\pi \circ \varphi\colon R \to S/M$ is surjective since both π, φ are surjective. The kernel of $\pi \circ \varphi$ is found by investigating which elements $r \in R$ are mapped to $0_S + M$ in S/M: If $\pi(\varphi(r)) = 0_S + M$, it follows that $\varphi(r) \in M$, so that $r \in \varphi^{-1}(M)$. Hence $\ker(\pi \circ \varphi) = \varphi^{-1}(M)$, and by the first isomorphism theorem we have that

$$\frac{R}{\varphi^{-1}(M)} \cong \frac{S}{M}.$$

Since M is a maximal ideal in S, the quotient ring S/M is a field, so that $R/\varphi^{-1}(M)$ is also a field. It follows from the lattice isomorphism theorem that $\varphi^{-1}(M)$ is a maximal ideal of R (since there are no ideals outside of $R/\varphi^{-1}(M)$ and the trivial ideal in $R/\varphi^{-1}(M)$, it follows that there are no proper ideals of R containing $\varphi^{-1}(M)$ outside of $\varphi^{-1}(M)$). □

5. (DF7.4.25) Assume R is commutative and for each $a \in R$ there is an integer $n > 1$ (depending on a) such that $a^n = a$. Prove that every prime ideal of R is a maximal ideal.

Proof. Let R be a commutative ring with the property that for every $a \in R$ there is an $n \in \mathbb{Z}^+$ depending on a such that $a^n = a$.

We show that for any prime ideal P of R, that R/P is a field (so that by the lattice isomorphism theorem P is a maximal ideal of R.) Suppose by way of contradiction that there is a proper nontrivial ideal $\overline{J}$ of R/P. Then for some nontrivial element $j + P \in \overline{J}$ (so $j \notin P$), we can find $n \in \mathbb{Z}^+$ depending on j such that $(j + P)^n = j^n + P = j + P$, from which it follows that $j^n - j = j(j^{n-1} - 1_R) \in P$. Since P is a prime ideal and $j \notin P$, it follows that $j^{n-1} - 1_R \in P$. Equivalently, $j^{n-1} + P = 1_R + P$, so that by taking the product

$(j^{n-2}+P)(j+P) = j^{n-1}+P = 1_R+P$, it follows from $\overline{J}$ being an ideal of R/P that $\overline{J}$ contains the identity element 1_R+P. By closure under multiplication by elements of R/P, it follows that $\overline{J}$ contains R/P so that $\overline{J} = R/P$, which contradicts the assumption that $\overline{J}$ was a proper nontrivial ideal of R/P.

Hence the ideals of R/P are only R/P and the trivial ideal, meaning R/P is a field. Since P was arbitrary, every prime ideal of R is a maximal ideal of R. $\square$