Problem 1. An element a of a ring R is called **nilpotent** if $a^m = 0$ for some $m > 0$.

a) Prove that in a commutative ring R the set N of all nilpotent elements of R is an ideal. This ideal is called the **nilradical** of R. Prove that 0 is the only nilpotent element of R/N.

b) Let R be a commutative ring and let $a_1, ..., a_n \in R$ be nilpotent. Set I for the ideal $< a_1, ..., a_n >$ generated by $a_1, ..., a_n$. Prove that there is a positive integer N such that $x_1 x_2 ... x_N = 0$ for any $x_1, ..., x_N$ in I (i.e. that $I^N = 0$).

c) Prove that the set of all nilpotent elements in the ring $M_2(\mathbb{R})$ is not an ideal.

d) Prove that if p is a prime and $m > 0$ then every element of $\mathbb{Z}/p^m\mathbb{Z}$ is either nilpotent or invertible.

e) Find the nilradical of $\mathbb{Z}/36\mathbb{Z}$ (by correspondence theorem, it is equal to $n\mathbb{Z}/36\mathbb{Z}$ for some n).

Solution:a) Suppose that $a, b \in N$ and $r \in R$. Thus $a^n = 0$ and $b^m = 0$ for some positive integers m, n. By the Newton's binomial formula we have

$$(a-b)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n}{i} a^i (-b)^{m+n-i}. \quad (1)$$

Note that, for every $i \in \{1, 2, ..., m+n\}$, either $i \geq n$ or $m+n-i \geq m$ and therefore either $a^i = 0$ or $(-b)^{m+n-i} = 0$. It follows that every summand in the sum (1) is 0, so $(a-b)^{m+n} = 0$. Thus $a - b \in N$. Clearly $(ra)^n = r^n a^n = 0$, so N is an ideal. If $(r + N)$ is nilpotent in R/N then $(r+N)^k = r^k + N = 0 + N$ for some $k > 0$, i.e. $r^k \in N$. But then $(r^k)^m = 0$ for some m, i.e. $r^{km} = 0$ so $r \in N$. This shows that $r + N = 0 + N$.

b) Suppose that $a_i^{k_i} = 0$ for $i = 1, ..., n$. Let $N = k_1 + ... + k_n$. Consider $x_1, ..., x_N \in I$. Then $x_i = r_{i,1}a_1 + r_{i,2}a_2 + ... + r_{i,n}a_n$ for some $r_{i,1}, ..., +r_{i,n} \in R$. The product $x_1 ... x_N$ is a sum of expressions of the form $r_{i,j_i} a_{j_1} r_{i,j_2} a_{j_2} ... r_{i,j_N} a_{j_N}$ for some sequence $j_1, ..., j_N$ consisting of elements from $\{1, 2, ..., n\}$. It suffices to show that each such product is 0. Since $N = k_1 + ... + k_n$, there is $i \in \{1, 2, ..., n\}$ which occurs in the sequence $j_1, ..., j_N$ et least k_i times (otherwise, if 1 occurred less than k_1 times, 2 occurred less than k_2 times,..., n occurred less than k_n times, the length of the sequence would be less than $N = k_1 + ... + k_n$). But then the product $r_{i,j_i}a_{j_1}r_{i,j_2}a_{j_2}...r_{i,j_N}a_{j_N}$ contains at least k_i factors equal to a_i. Since $a_i^{k_i} = 0$, we have $r_{i,j_i}a_{j_1}r_{i,j_2}a_{j_2}...r_{i,j_N}a_{j_N} = 0$.

c) Note that

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

so both matrices $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$ are nilpotent but their sum $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ is not nilpotent (it is invertible). Thus nilpotent elements of $M_2(\mathbb{R})$ do not form an ideal.

d) Note that if $p|x$ then $p^m|x^m$ so $(x + p^m\mathbb{Z})^m = x^m + p^m\mathbb{Z} = 0 + p^m\mathbb{Z}$, so $x + p^m\mathbb{Z}$ is nilpotent. If $p \nmid x$, then x is relatively prime to p^m and therefore $x + p^m\mathbb{Z}$ is invertible. This proves our claim. Note that our argument shows that the nilradical of $\mathbb{Z}/p^m\mathbb{Z}$ is equal to $p\mathbb{Z}/p^m\mathbb{Z}$.

e) An element $a + 36\mathbb{Z}$ is nilpotent iff $(a + 36\mathbb{Z})^k = 0 + 36\mathbb{Z}$ for some k. This is equivalent to $a^k \in 36\mathbb{Z}$, i.e. $36|a^k$. It follows that $2|a^k$ and $3|a^k$ so also $2|a$ and $3|a$, i.e. $6|a$. Conversely, if $6|a$ then $36|a^2$ and therefore $a + 36\mathbb{Z}$ is nilpotent. This shows that $a + 36\mathbb{Z}$ is nilpotent iff $6|a$. In other words, the nilradical of $\mathbb{Z}/36\mathbb{Z}$ equals $6\mathbb{Z}/36\mathbb{Z}$.

Problem 2. Let R be a commutative ring. For an ideal I of R define

$$\sqrt{I} = \{x \in R : x^n \in I \text{ for some } n > 0\}.$$

a) Prove that $\sqrt{I}$ is an ideal. It is called the **radical** of I.

b) Prove that $\sqrt{\{0\}}$ is the nilradical of R.

c) Consider a surjective homomorphism $f : R \longrightarrow S$. Prove that in the correspondence theorem the nilradical of S corresponds to $\sqrt{\ker f}$.

d) Prove that $R/\sqrt{I}$ has trivial nilradical.

Solution: It is easy to prove a) and b) directly, but we will show that they follow from c) and then prove c).

To see that a) follows from c), consider the canonical homomorphsim $f : R \longrightarrow R/I$. We have $I = kerf$ so by c) the radical $\sqrt{I}$ is an ideal of R. To see that

b) follows from c) take $I = \{0\}$ so $R/I = R$ and $f : R \longrightarrow R/I$ is the identity. The correspondence in this case is the same as equality, so $\sqrt{\{0\}} = \sqrt{\ker f}$ is the nilradical of R.

It remains to prove c). Let N be the nilradical of S. Note that $f(x) \in N$ iff $f(x)^k = 0$ for some $k > 0$, iff $f(x^k) = 0$ for some $k > 0$, iff $x^k \in \ker f$ for some $k > 0$, iff $x \in \sqrt{\ker f}$. This shows that $f^{-1}(N) = \sqrt{\ker f}$, i.e. $\sqrt{\ker f}$ corresponds to N.

d) Again this is easy to check directly, but we will use a) of Problem 1. By c) applied to the canonical homomorphsim $f : R \longrightarrow R/I$ we see that the nilradical of R/I is $\sqrt{I}/I$. By a) of Problem 1, the ring $(R/I)/(\sqrt{I}/I)$ has trivial nilradical and by the second isomorphism theorem this ring is isomorphic to $R/\sqrt{I}$. This shows that $R/\sqrt{I}$ has trivial nilradical.

Problem 3. Let R be a commutative ring. Let $I =< a_1, ..., a_n >$, $J =< b_1, ..., b_m >$. Prove that IJ is generated by the mn elements $a_i b_j$, $i = 1, 2, ..., n$, $j = 1, 2, ..., m$.

Solution: Let K be the ideal generated by the mn elements $a_i b_j$, $i = 1, 2, ..., n$, $j = 1, 2, ..., m$. Since IJ contains all the products $a_i b_j$, we have $K \subseteq IJ$. Conversely, let $x \in I$ and $y \in J$. Then $x = r_1 a_1 + ... + r_n a_n$ and $y = s_1 b_1 + ... + s_m b_m$ for some $r_1, ..., r_n, s_1, ..., s_m \in R$. It follows that xy is a sum of products of the form $r_i a_i s_j b_j = r_i s_j a_i b_j$. Each such product is in K, so $xy \in K$. Any element of IJ is a sum of elements of the form xy (with $x \in I$, $y \in J$) and we have just proved that all such products are in K, hence their sums are in K as well. This shows that $IJ \subseteq K$ and therefore $IJ = K$.