Solution to Problem 8: Recall, that in order to prove that a subset I of a ring R is an ideal we must verify that for any $a, b \in I$ and any $r \in R$ the elements $a - b, ar, ra$ belong to R.

i) Let $a, b \in I \cap J$ and $r \in R$. Since I is an ideal and $a, b \in I$, the elements $a-b, ra, ar$ are in I. Similarly, since J is an ideal and $a, b \in J$, the elements $a - b, ra, ar$ are in J. It follows that $a - b, ar, ra$ belong to both I and J, i.e. to $I \cap J$. This proves that $I \cap J$ is an ideal.

ii) Let $a, b \in I + J$ and $r \in R$. By the definition of $I + J$, we have $a = i + j$, $b = i_1 + j_1$ for some $i, i_1 \in I$ and $j, j_1 \in J$. Thus $a - b = (i - i_1) + (j - j_1)$. Since I, J are ideals, we have $i - i_1 \in I$ and $j - j_1 \in J$ and therefore $a - b \in I + J$. Similarly, $ra = ri + rj$ and $ar = ir + jr$. Since I, J are ideals, we have $ri, ir \in I$ and $rj, jr \in J$, hence $ra, ar \in I + J$. It follows that $I + J$ is an ideal.

iii) An element x belongs to IJ iff there is $n > 0$ and elements $a_1, ..., a_n \in I$, $b_1, ..., b_n \in J$ such that $x = a_1 b_1 + a_2 b_2 + ... + a_n b_n$.

Suppose that $a, b \in IJ$ and $r \in R$. Thus there exist positive integers m, n and elements $a_1, ..., a_m, c_1, ..., c_n \in I$, $b_1, ..., b_m, d_1, .., d_n \in J$ such that

$$a = a_1 b_1 + ... + a_m b_m, \ b = c_1 d_1 + ... + c_n d_n.$$

Thus

$$a - b = a_1 b_1 + ... + a_m b_m + (-c_1) d_1 + ... + (-c_n) d_n \in IJ,$$

$$ra = (ra_1) b_1 + ... + (ra_m) b_m \in IJ$$

(since $ra_i \in I$ for all i) and similarly

$$ar = a_1 (b_1 r) + ... + a_m (b_m r) \in IJ.$$

This proves that IJ is an ideal.

iv) Note that if $a \in I$ and $b \in J$ then $ab \in I$ (since $ar \in I$ for any $r \in R$) and similarly $ab \in J$ so $ab \in I \cap J$. If $a = a_1 b_1 + a_2 b_2 + ... + a_n b_n$ is an element of IJ (so $a_1, ..., a_n \in I$ and $b_1, ..., b_n \in J$) then $a_i b_i \in I \cap J$ for all i. Since $I \cap J$ is an ideal (so it is closed under addition), we have $x \in I \cap J$. This proves that $IJ \subseteq I \cap J$.

Consider now $R = \mathbb{Z}$ and let $I = J$ be the ideal of all even numbers (i.e. $I = J = 2\mathbb{Z}$). Then $I \cap J = 2\mathbb{Z}$ consists of all even numbers and $IJ = 4\mathbb{Z}$ consists of all numbers divisible by 4.)

v) In general, the subset $\{ab : a \in I, b \in J\}$ is not an ideal.

Solution to Problem 9: Let I be the union of the ideals $I_1 \subseteq I_2 \subseteq ....$ If a, b are in I and $r \in R$ then there are m, n such that $a \in I_m$, $b \in I_n$. Without loss of generality we may assume that $m \leq n$. Then $I_m \subseteq I_n$, so $a, b \in I_n$. Since I_n is an ideal, we have $a - b, ra, ar \in I_n \subseteq I$, so I is indeed an ideal.

Suppose now that $R = \mathbb{Z}$, $I = 2\mathbb{Z}$ cosists of even numbers and $J = 3\mathbb{Z}$ consists of multiples of 3. Then $I \cup J$ is not an ideal. In fact, $2, 3 \in I \cup J$ but $5 = 2 + 3 \notin I \cup J$.

Problem 1. Let R be a ring.

a) Let $f : \mathbb{Z} \longrightarrow R$ be a homomorphism and let $r = f(1)$. Prove that $r^2 = r$.

b) Let $r \in R$ be such that $r^2 = r$ (such elements are called **idempotents**). Prove that there is unique homomorphism $f : \mathbb{Z} \longrightarrow R$ such that $f(1) = r$.

c) Suppose that R is a domain and $r \in R$ is an idempotent. Prove that either $r = 0$ or R is unital and $r = 1$. Conclude that if R is a unital domain, there exist unique homomorphisms $f : \mathbb{Z} \longrightarrow R$ which is not identically 0.

Solution: a) Since f is a homomorphism, we have

$$r = f(1) = f(1 \cdot 1) = f(1) \cdot f(1) = r \cdot r = r^2.$$

b) Note that if f exists then it is unique since if $n > 0$ then $n = 1 + 1 + ... + 1$ (1 is added n times) so

$$f(n) = f(1 + 1 + ... + 1) = f(1) + f(1) + ... + f(1) = r + r + ... + r = nr$$

and if $n < 0$ then $-n > 0$ and

$$f(n) = f(-(-n)) = -f(-n) = -((-n)r) = nr.$$

Thus if f exists then it is given by $f(n) = nr$. It suffices now to check that this formula indeded defines a homomorphism if r is an idempotent:

$$f(m + n) = (m + n)r = mr + nr = f(m) + f(n),$$

$$f(mn) = (mn)r = mnr^2 = (mr)(nr) = f(m)f(n).$$

c) Let r be an idempotent, so $r^2 = r$. Suppose that R is a domain and $r \neq 0$. For any $s \in R$ we have $r(rs - s) = r^2 s - rs = rs - rs = 0$ and $(sr - s)r = sr^2 - sr = 0$. Since R is a domain and $r \neq 0$, we must have $rs - s = 0 = sr - s$, i.e. $sr = s = rs$ This proves that r is the identity element of R.

Now by a) and b), the homomorphisms from $\mathbb{Z}$ to R are in bijective correspondence with idempotents of R. The idempotent 0 corresponds to the homomoprhism which maps all integers to 0. Since 1 is the only non zero idempotent of R, there is unique non-zero homomorphism from $\mathbb{Z}$ to R and it maps $1 \in \mathbb{Z}$ to $1 \in R$.