Problem 1. Let $f : R \longrightarrow S$ be a homomorphism of commutative unital rings.

a) Prove that if P is a prime ideal of S then $f^{-1}(P)$ is a prime ideal of R.

b) Find an example when P is a maximal ideal of S but $f^{-1}(P)$ is not maximal in R.

c) Prove that if f is onto and Q is a prime ideal of R such that $\ker f \subseteq Q$ then $f(Q)$ is a prime ideal of S.

d) Suppose that f is surjective. Prove that if P is a maximal ideal of S then $f^{-1}(P)$ is maximal in R. Prove that if Q is a maximal ideal of R then $f(Q)$ is either S or it is a maximal ideal of S. Show by example that a similar statement for prime ideals is false.

e) Find all prime ideals of $\mathbb{Z}/36\mathbb{Z}$.

Solution: a) Suppose that $a, b \in R$ are such that $ab \in f^{-1}(P)$. Then $f(ab) = f(a)f(b) \in P$. Since P is prime, we have either $f(a) \in P$ or $f(b) \in P$. In the former case, we get $a \in f^{-1}(P)$ and in the latter case we get $b \in f^{-1}(P)$. Thus, either $a \in f^{-1}(P)$ or $b \in f^{-1}(P)$, which proves that P is a prime ideal.

b) Let $R = \mathbb{Z}$, $S = \mathbb{Q}$ and let f be the identity map $f(m) = m$. Let $P = \{0\}$ be the ideal of S. Since S is a field, P is maximal. But $f^{-1}(P) = \{0\}$ is not maximal as an ideal of R.

c) Let $x, y \in S$ be such that $xy \in f(Q)$. Since f is surjective, there are $a, b \in R$ such that $x = f(a)$ and $y = f(b)$. Thus $xy = f(ab) \in f(Q)$. This means that there is $q \in Q$ such that $f(ab) = f(q)$. In other words $ab - q \in \ker f$. Since $\ker f \subseteq Q$, we see that both $ab - q$ and q are in Q, and therefore $ab = (ab - q) + q \in Q$. But Q is a prime ideal, so either $a \in Q$ or $b \in Q$ and consequently either $f(a) = x \in f(Q)$ or $f(b) = y \in f(Q)$. This proves that $f(Q)$ is a prime ideal.

Another argument: Since Q contains the kernel of f, we have R/Q and $S/f(Q)$ are isomorphic by the second isomorphism theorem (as discussed in class). Thus R/Q is a domain iff $S/f(Q)$ is a domain. It follows that if Q is prime then so is $f(Q)$.

Remark: Note that c) and a) (or our second argument for c)) imply that in the correspondence theorem prime ideals correspond to prime ideals.

d) If J is an ideal of R which contains $f^{-1}(P)$ then J contains $\ker f$ and $f(J)$ is an ideal of S containing P. Since P is maximal, we have either $f(J) = P$ or $f(J) = S$. Since J contains the kernel of f, we have $J = f^{-1}(P)$ or $J = f^{-1}(S) = R$. This proves that $f^{-1}(P)$ is maximal.

Another argument: We have $R/f^{-1}(P)$ and S/P are isomorphic by the second isomorphism theorem (as discussed in class). Thus $R/f^{-1}(P)$ is a field iff S/P is a field. It follows that $f^{-1}(P)$ is maximal iff P is.

Suppose now that Q is maximal in R. If Q contains the kernel of f then $f^{-1}(f(Q)) = Q$ (correspondence theorem). If $f(Q)$ is contained in and ideal I then Q is containce id the ideal $f^{-1}(I)$. Since Q is maximal, either $f^{-1}(I) = Q$ of $f^{-1}(I) = R$. In the former case we have $I = f(Q)$ and in the latter case $I = f(R) = S$. This shows that $f(Q)$ is maximal. This also follows from our second argument above, since R/Q and $S/f(Q)$ are isomorphic.

If Q does not contain $\ker f$ then $Q + \ker f$ is an ideal larger that Q, so we must have $Q + \ker f = R$ (since Q is maximal). Thus $S = f(R) = f(Q + \ker f) = f(Q) + f(\ker f) = f(Q)$.

To see that the statement is not always true for prime ideals consider the canonical homomorphism $f : \mathbb{Z} \longrightarrow \mathbb{Z}/6\mathbb{Z}$. Note that $\{0\} = Q$ is a prime ideal in $\mathbb{Z}$ but $f(Q) = \{0\}$ is not prime in $\mathbb{Z}/6\mathbb{Z}$ since $\mathbb{Z}/6\mathbb{Z}$ is not a domain.

Remark: Note that we proved in particular that in the correspondence theorem maximal ideals correspond to maximal ideals.

e) By correspondence theorem, ideals of $\mathbb{Z}/36\mathbb{Z}$ are in bijective correspondence with ideals $m\mathbb{Z}$ of $\mathbb{Z}$ which contain $36\mathbb{Z}$, i.e. such that $m|36$. Also, by the remark to our solution to c), in the correspondence theorem prime ideals correspond to prime ideals. Prime ideals in $\mathbb{Z}$ are $\{0\}$ and $p\mathbb{Z}$, p a prime. Among these ideals only $2\mathbb{Z}$ and $3\mathbb{Z}$ contain $36\mathbb{Z}$. Thus $\mathbb{Z}/36\mathbb{Z}$ has two prime ideals, namely $2\mathbb{Z}/36\mathbb{Z}$ and $3\mathbb{Z}/36\mathbb{Z}$.

Problem 2. Let R be a commutative unital ring.

a) Prove that R is a domain iff $\{0\}$ is a prime ideal of R.

b) Prove that if P is a prime ideal and $r \in R$ is nilpotent then $r \in P$.

c) Prove that if R is finite then every prime ideal of R is maximal.

Solution: a) Since R and $R/\{0\}$ are isomorphic, we see that R is a domain iff $R/\{0\}$ is a domain iff $\{0\}$ is a prime ideal.

Alternatively, if for any a, b in R we have $ab \in \{0\}$ iff $ab = 0$. If R is a domain and $ab \in \{0\}$, this means that $ab = 0$ and therefore $a = 0$ or $b = 0$. This shows that $a \in \{0\}$ or $b \in \{0\}$, i.e. $\{0\}$ is prime. Conversely, if $\{0\}$ is prime and $ab = 0 \in \{0\}$, then either $a \in \{0\}$ or $b \in \{0\}$, i.e. either $a = 0$ or $b = 0$. This proves that R is a domain.

b) Suppose that P is prime and r is nilpotent. This means that $r^k = 0$ for some $k > 0$. In particular, $r^k \in P$. Let m be smallest positive integer such that $r^m \in P$. If $m = 1$ then $r \in P$. Otherwise, $r^m = r \cdot r^{m-1} \in P$, so either $r \in P$ or $r^{m-1} \in P$. This however contradicts our choice of m, so $m > 1$ is not possible. Thus $r \in P$.

c) Let I be a prime ideal of R. Thus R/I is a domain and it is a finite ring. But we proved that a finite domain is a field, so R/I is a filed and therefore I is maximal.