Problem 1 (7.3.24 (from HW 5)). a) We will give a direct proof first, and a more elegant proof after.

Fix $J \subset S$ an ideal and consider the preimage $\varphi^{-1}(J) \subset R$ under $\varphi$. Let $a_1, a_2$ be in $\varphi^{-1}(J)$, so that $\varphi(a_1) = j_1, \varphi(a_2) = j_2 \in J$. Then we have

$$\varphi(a_1 + a_2) = \varphi(a_1) + \varphi(a_2) = j_1 + j_2 \in J$$

since $J$ is an ideal. Therefore, $(a_1 + a_2) \in \varphi^{-1}(J)$ which proves that $\varphi^{-1}(J)$ is an additive subgroup of $R$.

Then, take $a \in \varphi^{-1}(J)$ and $r \in R$. Then $\varphi(a) = j \in J$, and we have

$$\varphi(ar) = \varphi(a)\varphi(r) = j\varphi(r) \in J$$

since $J$ is an ideal. Therefore, $(ar) \in \varphi^{-1}(J)$ which proves that $\varphi^{-1}(J)$ is an ideal.

Now for the more elegant proof: let’s take a step back and consider a more general ring homomorphism $\psi: S \longrightarrow T$, with kernel $\ker(\psi) = J$. We can consider the composition of $\varphi$ and $\psi$ to obtain

$$\psi \circ \varphi: R \longrightarrow T;$$

we will look at its kernel.

We have

$$\ker(\psi \circ \varphi) = \{r \in R \mid 0 = \psi(\varphi(r))\},$$

but $\psi(\varphi(r)) = 0$ if and only if $\varphi(r) \in J = \ker(\psi)$, and the latter is equivalent to $r \in \varphi^{-1}(J)$. Therefore,

$$\ker(\psi \circ \varphi) = \varphi^{-1}(\ker \psi).$$

Now back to our particular case: we can consider the quotient map $\pi: S \longrightarrow S/J = T$, which has obviously kernel $J$. Therefore, $\ker(\pi \circ \varphi) = \varphi^{-1}(J)$ is also an ideal.

Let’s consider now the special case where $\varphi: R \hookrightarrow S$ is the inclusion homomorphism of the subring $R$ into $S$. Then we have

$$\varphi^{-1}(J) = \{r \in R \mid r = \varphi(r) \in J\} = \{r \in R \mid r \in J\} = R \cap J,$$

and thus by the previous proof $R \cap J = \varphi^{-1}(J)$ is an ideal of $R$ for every ideal $J$ of $S$. 
b) Assume now that \( \varphi : R \rightarrow S \) is a surjective homomorphism of rings, and that \( I \subset R \) is an ideal. Let \( a_1 = \varphi(i_1), a_2 = \varphi(i_2) \in \varphi(I) \), then

\[
a_1 + a_2 = \varphi(i_1) + \varphi(i_2) = \varphi(i_1 + i_2),
\]

and since \( i_1 + i_2 \in I \) since \( I \) is an ideal, we get \( a_1 + a_2 \in \varphi(I) \) - so that \( \varphi(I) \) is an additive subgroup of \( S \).

Let now \( \varphi(i) = a \in \varphi(I) \) and \( s \in S \). By surjectivity, there exists some \( r \in R \) with \( \varphi(r) = s \), and then

\[
sa = \varphi(r)\varphi(i) = \varphi(ri) \in \varphi(I)
\]

since \( ri \in I \) because \( I \) is an ideal. Therefore, \( sa \in \varphi(I) \) which proves that \( \varphi(I) \) also is an ideal.

To give a counterexample when \( \varphi \) is not surjective, consider the inclusion \( \mathbb{Z} \hookrightarrow \mathbb{Q} \). Then the ideal of even numbers \( 2\mathbb{Z} \subset \mathbb{Z} \) maps to the set of even integers \( 2\mathbb{Z} \subset \mathbb{Q} \), but this is not an ideal - since the only ideals of \( \mathbb{Q} \) are 0 and itself, being a field.

**Problem 2** (7.4.13). a) Since \( P \) is a prime ideal, by definition \( S/P \) is an integral domain, and it comes with the projection map \( \pi : S \rightarrow S/P \) with kernel \( P \). Now we compose \( \pi \circ \varphi : R \rightarrow T = S/P \) and by the discussion in the previous problem, we have \( \varphi^{-1}(P) = \ker (\pi \circ \varphi) \).

The isomorphism theorem for rings applied to the map \( \pi \circ \varphi \) gives then

\[
R/\ker (\pi \circ \varphi) \cong \text{Im} (\pi \circ \varphi).
\]

Suppose \( \varphi^{-1}(P) = \ker (\pi \circ \varphi) \neq R \), so that the quotient above is a ring (with 0 and 1 distinct elements), and through the isomorphism theorem we get that the image \( \text{Im} (\pi \circ \varphi) \) is a subring of the integral domain \( S/P \), so it is itself an integral domain. In particular, \( R/\varphi^{-1}(P) \) is an integral domain, which means that \( \varphi^{-1}(P) \) is a prime ideal.

Consider now the special case where \( R \) is a subring of \( S \) and \( \varphi : R \hookrightarrow S \) is the inclusion homomorphism: exactly like in the previous problem we have that \( \varphi^{-1}(P) = P \cap R \), so the above argument proves that either \( P \cap R = R \), or \( P \cap R \) is a prime ideal of \( R \).

b) Suppose now that \( \varphi : R \rightarrow S \) is a surjective homomorphism of rings and \( M \subset S \) a maximal ideal. By proposition 12, this means that \( S/M = F \) is a field, and it comes with a quotient map \( \pi : S \rightarrow S/M \) of kernel \( M \).

Composing with \( \varphi \), we obtain a surjective map \( \pi \circ \varphi : R \rightarrow F \) with kernel \( \ker (\pi \circ \varphi) = \varphi^{-1}(\ker \pi) = \varphi^{-1}(M) \). Applying the isomorphism theorem for rings to the map \( \pi \circ \varphi \) yields that

\[
R/\ker (\pi \circ \varphi) \cong \text{Im} (\pi \circ \varphi) = F.
\]

where the last equality holds by surjectivity of \( \pi \circ \varphi \). Thus, \( R/\varphi^{-1}(M) \cong F \) is a field, which means that \( \varphi^{-1}(M) \) is a maximal ideal.

For a counterexample when \( \varphi \) is not surjective, consider again the inclusion map \( \varphi : \mathbb{Z} \hookrightarrow \mathbb{Q} \). As \( \mathbb{Q} \) is a field, the only proper ideal is \( (0) \), which therefore is maximal. Since \( \varphi \) is injective, \( \varphi^{-1}(0) = (0) \), but this is not a maximal ideal of \( \mathbb{Z} \), as \( \mathbb{Z}/(0) \cong \mathbb{Z} \) is not a field. [In terms of the previous paragraph, the point is that the image of \( \pi \circ \varphi \) is in general only a subring of the field \( F \). This is a domain (as we proved on HW5), so \( \varphi^{-1}(P) \) is prime, but it does not have to be a field.]
**Problem 3 (Q1).** a) By definition, we are looking for prime ideals $P \subset \mathbb{Z}/300\mathbb{Z}$. Theorem 8.3 (the lattice isomorphism theorem for rings) says that given a general ring $R$ and an ideal $I$, there is a bijection between ideals of $R/I$ and ideals of $R$ containing the ideal $I$. Indeed the bijection is given as in the first problem of this handout, by using the surjective homomorphism $R \rightarrow R/I$ and saying that the ideal $J \subset R$ containing $I$ corresponds to the ideal $J/I$ of $R/I$, and that any ideal $J' \subset R/I$ is of this form for some $J \subset R$.

Moreover, by problem 2 of this handout, every prime ideal of $R/I$ corresponds to a prime ideal of $R$.

Now let’s come back to the setting of this problem. By example 2 at page 243, the only ideals of $\mathbb{Z}$ are of the form $n\mathbb{Z}$, i.e. the set of integers multiple of a fixed $n$. It is immediate that an ideal $n\mathbb{Z}$ is a prime ideal if and only if $n$ is a prime number; for if $n = ab$ is composite, then the ideal being prime means that either $a$ or $b$ are in $n\mathbb{Z}$. But having $1 < |a|, |b| < n$ yields a contradiction, since neither $a$ nor $b$ can be multiples of $n$.

Therefore, we are looking for ideals $p\mathbb{Z}$ of $\mathbb{Z}$ with $p$ prime and containing $300\mathbb{Z}$. This means of course that the prime number $p$ must divide 300, and hence we have $p \in \{2, 3, 5\}$. The corresponding prime ideals of $\mathbb{Z}/300\mathbb{Z}$ are then the images of $2\mathbb{Z}, 3\mathbb{Z}$ and $5\mathbb{Z}$. We conclude

$$\text{PrimeSpace}(\mathbb{Z}/300\mathbb{Z}) = \{2\mathbb{Z}/300\mathbb{Z}, 3\mathbb{Z}/300\mathbb{Z}, 5\mathbb{Z}/300\mathbb{Z}\}.$$  

b) We are now looking for prime ideals $P \subset \mathbb{R}[t]$ such that $\mathbb{R}[t]/P \cong \mathbb{R}$. In other words, we are looking for surjective homomorphisms $\varphi: \mathbb{R}[t] \rightarrow \mathbb{R}$, and then $\ker \varphi$ will be our prime ideal $P$, by the first isomorphism theorem.

Suppose we have such a map $\varphi$, and that $\varphi(t) = a \in \mathbb{R}$. This determines the value of $\varphi$ on each polynomial $f(t)$, since $\varphi$ is a ring homomorphism and hence goes through addition and multiplication of monomials.

On the other hand, any value $a \in \mathbb{R}$ gives us a ring homomorphism $\varphi_a: \mathbb{R}[t] \rightarrow \mathbb{R}$ by defining $\varphi_a(t) = a$: indeed the map $\varphi_a$ can be described as the “evaluation map at $a$”, i.e. $f(t) \mapsto f(a)$, and this is clearly a ring homomorphism.

We conclude that the family of surjective ring homomorphism $\varphi: \mathbb{R}[t] \rightarrow \mathbb{R}$ coincides with the family of evaluation maps $f(t) \mapsto f(a)$. Call $\varphi_a$ the map “evaluation at $a$”. Then we have

$$\ker(\varphi_a) = \{f(t) \in \mathbb{R}[t] \mid f(a) = 0\}$$
$$= \{f(t) \in \mathbb{R}[t] \mid a \text{ is a root of } f\}$$
$$= \{f(t) \in \mathbb{R}[t] \mid (t - a) \text{ divides } f(t)\}$$
$$= (t - a).$$

Therefore we obtain

$$\mathbb{R}\text{-points of } \text{PrimeSpace}(\mathbb{R}[t]) = \{(t - a) \mid a \in \mathbb{R}\}.$$

Now we want to find a non $\mathbb{R}$-point of $\text{PrimeSpace}(\mathbb{R}[t])$, i.e. a prime ideal $P \subset \mathbb{R}[t]$ such that $\mathbb{R}[t]/P \not\cong \mathbb{R}$. We take $P = (t^2 + 1)$: this is a prime ideal because $\mathbb{R}[t]$ is a unique factorization domain, and the polynomial $t^2 + 1$ is irreducible in $\mathbb{R}[t]$.

On the other hand, the ring $S = \mathbb{R}[t]/(t^2 + 1)$ is not isomorphic to $\mathbb{R}$. Indeed, the equation $x^2 = -1$ has no solution in $\mathbb{R}$, but the coset $\bar{t} = t + (t^2 + 1) \in \mathbb{R}[t]/(t^2 + 1)$ is a solution in $S$! If
we had a ring isomorphism \( \varphi: S \xrightarrow{\cong} \mathbb{R} \), this would force \( \varphi(\bar{t}) \) to be a solution of \( x^2 = -1 \) in \( \mathbb{R} \), which cannot be. [TC: indeed, we saw in class that \( \mathbb{R}[t]/(t^2 + 1) \) is isomorphic to the complex numbers \( \mathbb{C} \).

c) Since \( \mathbb{R}[t] \) is a PID, every prime ideal \( P \subset \mathbb{R}[t] \) is principal. Since PIDs are UFDs, we know that a nonzero principal ideal \( (f(t)) \) is prime if and only if \( f(t) \) is an irreducible polynomial. Therefore, the nonzero prime ideals of \( \mathbb{R}[t] \) coincide with the ideals generated by irreducible polynomials.

By the fundamental theorem of algebra, we know that every irreducible polynomial in \( \mathbb{R}[t] \) is either linear, or quadratic with negative discriminant, i.e. \( f(t) = at^2 + bt + c \) with \( \Delta(f) = b^2 - 4ac < 0 \).

Notice that every polynomial in \( \mathbb{R}[t] \) generates the same ideal as its unique associated monic polynomial: indeed if the leading coefficient of a polynomial \( f(t) \) is \( c \neq 0 \in \mathbb{R} \), then \( \frac{1}{c}f(t) \) is a monic polynomial that is associate to \( f(t) \) [and thus generates the same principal ideal.

We conclude
\[
\text{PrimeSpace}(\mathbb{R}[t]) = (0) \cup \{(f) \mid f(t) \in \mathbb{R}[t] \text{ is irreducible } \}
\]
\[
= (0) \cup \{(t - a) \mid a \in \mathbb{R} \} \cup \{(t^2 + bt + c) \mid b^2 - 4c < 0 \}.
\]

d) We need to describe all \( \mathbb{R} \)-points of \( \text{PrimeSpace}(\mathbb{R}[s,t]/(s^2 + t^2 - 1)) \), or in other words all prime ideals \( P \subset \mathbb{R}[s,t]/(s^2 + t^2 - 1) \) such that \( \mathbb{R}[s,t]/(s^2 + t^2 - 1)/P \cong \mathbb{R} \). Every such prime ideal corresponds bijectively to a surjection \( \mathbb{R}[s,t]/(s^2 + t^2 - 1) \twoheadrightarrow \mathbb{R} \), and hence we focus on describing these surjections.

Let now \( \varphi: \mathbb{R}[s,t]/(s^2 + t^2 - 1) \twoheadrightarrow \mathbb{R} \) be one such surjective ring homomorphism. Precomposing with the quotient map \( \pi: \mathbb{R}[s,t] \twoheadrightarrow \mathbb{R}[s,t]/(s^2 + t^2 - 1) \) yields a ring homomorphism
\[
\varphi \circ \pi: \mathbb{R}[s,t] \twoheadrightarrow \mathbb{R}
\]
which is obviously still surjective, and moreover \( (\varphi \circ \pi)(s^2 + t^2 - 1) = \varphi(\pi(s^2 + t^2 - 1)) = \varphi(0) = 0 \), so \( s^2 + t^2 - 1 \in \ker(\varphi \circ \pi) \), in other words, every such composition \( \varphi \circ \pi \) has the polynomial \( s^2 + t^2 - 1 \) in its kernel.

On the other hand, suppose that we have a surjection \( \psi: \mathbb{R}[s,t] \twoheadrightarrow \mathbb{R} \) with kernel containing \( s^2 + t^2 - 1 \). Then the map \( \psi \) can be seen as a composition
\[
\mathbb{R}[s,t] \xrightarrow{\pi} \mathbb{R}[s,t]/(s^2 + t^2 - 1) \xrightarrow{\psi} \mathbb{R}[s,t]/\ker(\psi) \cong \text{Im}\psi = \mathbb{R}
\]
where the last equality holds by surjectivity, and the previous one by the first isomorphism theorem for rings.

We have just shown that every surjection \( \varphi: \mathbb{R}[s,t]/(s^2 + t^2 - 1) \twoheadrightarrow \mathbb{R} \) corresponds to a surjection \( \psi: \mathbb{R}[s,t] \twoheadrightarrow \mathbb{R} \) whose kernel \( \ker \psi \) contains \( s^2 + t^2 - 1 \). We will describe this last family of ring homomorphism, and then follow the steps above in the opposite direction to obtain \( \text{PrimeSpace}(\mathbb{R}[s,t]/(s^2 + t^2 - 1)) \).

Suppose than that we have one such surjection \( \psi: \mathbb{R}[s,t] \twoheadrightarrow \mathbb{R} \) with \( s^2 + t^2 - 1 \) in its kernel. Since the only ring homomorphism between \( \mathbb{R} \) and \( \mathbb{R} \) is the identity, \( \psi \) must fix all constants, and hence \( \psi \) is completely determined by the image of the two indeterminates \( s \) and \( t \). Indeed once
such images are chosen, we have that $\psi(p(s, t)) = p(\psi(s), \psi(t))$ for every polynomial $p(s, t) \in \mathbb{R}[s, t]$, as $\psi$ is a ring homomorphism and must "commute" with addition and multiplication.

So what real numbers can $\psi(s) = a$ and $\psi(t) = b$ be? Well, by assumption $s^2 + t^2 - 1$ is in the kernel, so we must have

$$0 = \psi(s^2 + t^2 - 1) = \psi(s)^2 + \psi(t)^2 - 1 = a^2 + b^2 - 1$$

or in other words

$$a^2 + b^2 = 1,$$

so that the images $(a, b) = (\psi(a), \psi(b))$ define a point on the unit circle on the Euclidean plane $\mathbb{R}^2$. It is easy to see that any point $(a, b)$ on the circle gives rise to a ring homomorphism in the family we are studying, by setting $\psi(s) = a$ and $\psi(t) = b$.

Therefore we found the family of surjective ring maps $\mathbb{R}[s, t] \twoheadrightarrow \mathbb{R}$ with kernel containing $s^2 + t^2 - 1$ and retracing our steps we get that all surjections

$$\varphi: \mathbb{R}[s, t]/(s^2 + t^2 - 1) \twoheadrightarrow \mathbb{R}$$

are obtained by sending $\bar{s} \mapsto a$ and $\bar{t} \mapsto b$ for some point $(a, b)$ on the unit circle.

Recall that what we ultimately want is the prime ideal $P = \ker \varphi$. It is immediate to see that the polynomials $\bar{s} - a$ and $\bar{t} - b$ belongs to $\ker \varphi$, and thus we get $P = \ker \varphi \supseteq (\bar{s} - a, \bar{t} - b)$.

On the other hand, we see that

$$(s - a, t - b) = \pi^{-1} ( (\bar{s} - a, \bar{t} - b) ) = \pi^* (\bar{s} - a, \bar{t} - b)$$

is exactly the kernel of the "evaluation at $(a, b)$" map $\mathbb{R}[s, t] \twoheadrightarrow \mathbb{R}$, and as such it is a maximal ideal, because quotienting $\mathbb{R}[s, t]$ by it yields the field $\mathbb{R}$.

Using again the lattice isomorphism theorem for rings - in particular the crucial fact that it preserves inclusions of ideals - we see that in the quotient map $\mathbb{R}[s, t] \twoheadrightarrow \mathbb{R}[s, t]/(s^2 + t^2 - 1)$ the maximal ideal $(s - a, t - b) \subset \mathbb{R}[s, t]$ corresponds to the prime ideal $(\bar{s} - a, \bar{t} - b)$ contained in $P$, so what ideal can $P$ correspond to in $\mathbb{R}[s, t]$? Not the entire ring, thus $\pi^{-1}(P) = (s - a, t - b)$ as well - but since the correspondence between ideals is bijective we must have $P = (\bar{s} - a, \bar{t} - b)$.

Finally, we conclude

$$\text{PrimeSpace} \left( \mathbb{R}[s, t]/(s^2 + t^2 - 1) \right) = \{ (\bar{s} - a, \bar{t} - b) \mid a^2 + b^2 = 1 \}.$$

e) [Answers only] Recall that for the ring $R = \mathbb{Z}/10\infty\mathbb{Z}$ of the HW4, we found two "unexpected" zero-divisors that were also nontrivial solutions of $t^2 = t$, i.e. $x = \ldots 625$ and $y = 1 - x = \ldots 376$. Two of our prime ideals will be $(x)$ and $(y)$, notice indeed that in order to get a surjective map $R \twoheadrightarrow R/P$ into a domain, we must send at least one of these two zero-divisors to zero.

The other two prime ideals are those generated by the integers 2 and 5, so we conclude

$$\text{PrimeSpace}(R) = \{ (x), (y), (2), (5) \}.$$

Notice that $(2) \supset (y)$ and $(5) \supset (x)$, so that we have successive surjections $R \twoheadrightarrow R/(x) \twoheadrightarrow R/(5)$: it is easy to see that $R/(5) \cong \mathbb{Z}/5\mathbb{Z}$ is the field with 5 elements, and as we saw when we covered the Chinese Remainder Theorem, $\mathbb{Z}/10\infty\mathbb{Z}/(x)$ is isomorphic to $\mathbb{Z}/5\mathbb{Z}$.

Similarly, we have successive surjections $R \twoheadrightarrow R/(y) \twoheadrightarrow R/(2)$: it is easy to see that $R/(2) \cong \mathbb{Z}/2\mathbb{Z}$ is the field with 2 element, and $R/(y) \cong \mathbb{Z}/2\mathbb{Z}$. 

5
**Problem 4 (Q2).** a) Since $\mathbb{Q}$ is a field, the only prime ideal is $(0)$. Indeed, $(0)$ is the only proper ideal, so it is in fact maximal, and a fortiori prime. Therefore, to describe the map $f^*: \text{PrimeSpace}(\mathbb{Q}) \to \text{PrimeSpace}(\mathbb{Z})$ we only need to describe the image of the single element $(0) \in \text{PrimeSpace}(\mathbb{Q})$.

By definition, $f^* ( x_{(0)} ) = x_{f^{-1}((0))}$, which is a prime ideal of $\mathbb{Z}$ by exercise 7.4.13. Since $f: \mathbb{Z} \hookrightarrow \mathbb{Q}$ is the inclusion, the preimage of $(0)$ is simply $f^{-1} ((0)) = (0) \cap \mathbb{Z} = (0)_\mathbb{Z}$, the zero ideal in $\mathbb{Z}$. Therefore, $f^* ( x_{(0)} ) = x_{(0)_\mathbb{Z}} \in \text{PrimeSpace}(\mathbb{Z})$.

This is also the image of $f^*$, as $\text{PrimeSpace}(\mathbb{Q})$ consists of the single element $(0)$.

b) We follow a reasoning extremely similar to the one we did in Question 1a. The lattice isomorphism theorem for rings gives a bijection between ideals of the quotient ring $R/I$ and ideals of $R$ containing $I$. Moreover, by problem 7.4.13 this bijection sends a prime ideal $P/I \subset R/I$ to a prime ideal $P \subset R$.

By example 2 at page 243 of the textbook, the ideals of $\mathbb{Z}$ are exactly those subsets of the form $n\mathbb{Z}$ for nonnegative integers $n \in \mathbb{N}$, and such ideals are prime exactly when $n = p$ is a prime number. On the other hand, in our particular instance we are looking for ideals $n\mathbb{Z} \supset 20\mathbb{Z}$, so we need our prime number $p$ to divide 20. We conclude that

$$\text{PrimeSpace}(\mathbb{Z}/20\mathbb{Z}) = \{ 2\mathbb{Z}/20\mathbb{Z}, 5\mathbb{Z}/20\mathbb{Z} \}.$$  

Let’s start with $P = 2\mathbb{Z}/20\mathbb{Z}$, and by definition

$$g^* ( 2\mathbb{Z}/20\mathbb{Z} ) = g^{-1} ( 2\mathbb{Z}/20\mathbb{Z} ) = 2\mathbb{Z},$$

since the preimage $g^{-1} ( 2\mathbb{Z}/20\mathbb{Z} )$ consists of those integers which have even residue class modulo 20, and these are exactly the even integers.

Similarly, taking $P = 5\mathbb{Z}/20\mathbb{Z}$, we have by definition

$$g^* ( 5\mathbb{Z}/20\mathbb{Z} ) = g^{-1} ( 5\mathbb{Z}/20\mathbb{Z} ) = 5\mathbb{Z},$$

since the preimage $g^{-1} ( 5\mathbb{Z}/20\mathbb{Z} )$ consists of those integers which have residue class modulo 20 divisible by 5, and these are exactly the integers divisible by 5.

Thus we conclude

$$g^* ( 2\mathbb{Z}/20\mathbb{Z} ) = 2\mathbb{Z}, \; g^* ( 5\mathbb{Z}/20\mathbb{Z} ) = 5\mathbb{Z}, \; \text{Im}(g^*) = \{ 2\mathbb{Z}, 5\mathbb{Z} \}.$$  

c) Since $\varphi: R \to S$ is surjective, the first isomorphism theorem for rings tells us that $S \cong R/\ker \varphi$, so once we denote $\ker \varphi = I$, we can assume that $\varphi: R \to R/I$ is the ring homomorphism, and the corresponding map is

$$\varphi^*: \text{PrimeSpace}(R/I) \to \text{PrimeSpace}(R).$$

Now theorem 8.3 at page 246, the lattice isomorphism theorem for rings, tells us that there is a bijection

$$\{ \text{ideals of } R \text{ containing } I \} \leftrightarrow \{ \text{ideals of } R/I \}.$$
given by \( J \mapsto J/I \) (an ideal of \( R/I \)) in one direction, and by \( R/I \supset J' \mapsto \varphi^{-1}(J') \subset R \) in the opposite direction. In particular, for every ideal \( J \subset R \) containing \( I \), there is only one ideal \( J' \subset R/I \) such that \( \varphi^{-1}(J') = J \).

Suppose then that we have two prime ideals \( P_1, P_2 \subset R/I \) such that
\[
\varphi^{-1}(P_1) = \varphi^*(P_1) = \varphi^*(P_2) = \varphi^{-1}(P_2),
\]
and call \( P \) this prime ideal of \( R \). Since \( P_1 \) is an ideal of \( R/I \), the ideal \( P \subset R \) to which it corresponds contains \( I \). But then by the above considerations, the ideal \( P \) corresponds to a unique ideal \( P/I \) of \( R/I \), therefore \( P_1 = P_2 \), which proves injectivity of \( \varphi^* \).

d) Consider the inclusion \( \varphi : \mathbb{Z} \hookrightarrow \mathbb{Z}[i] \), and the map between prime spaces in opposite direction

\[
\varphi^* : \text{PrimeSpace}(\mathbb{Z}[i]) \rightarrow \text{PrimeSpace}(\mathbb{Z}).
\]

We want to find an element \( x_P \in \text{PrimeSpace}(\mathbb{Z}[i]) \) which maps to \( x_{(2)} \in \text{PrimeSpace}(\mathbb{Z}) \) under \( \varphi^* \), i.e. a prime ideal \( P \subset \mathbb{Z}[i] \) such that
\[
(2) = \varphi^*(P) = \varphi^{-1}(P).
\]

As in problem 7.4.13, since \( \varphi \) is an injection we have that \( \varphi^{-1}(P) = P \cap \mathbb{Z} \): therefore what we are looking for is a prime ideal \( P \subset \mathbb{Z}[i] \) such that \( P \cap \mathbb{Z} = (2) \).

Now we may try to choose \( P = (2) \), the ideal generated by 2 in \( \mathbb{Z}[i] \): unfortunately, this is not a prime ideal anymore! Indeed, \( 2 = (1 + i)(1 - i) \) in \( \mathbb{Z}[i] \), and on the other hand neither \((1 + i)\) nor \((1 - i)\) are in the ideal generated by 2 (because \( 2(a + bi) = 2a + (2b)i \), which means that every Gaussian integer in the ideal \((2)\) has even real and imaginary parts), so that the containment \((1 + i) \supset (2)\) is strict.

So what to do? Well, we can try to choose \( P = (1 + i) \): this is a proper ideal, because the Norm
\[
\text{Norm} : \mathbb{Z}[i] \rightarrow \mathbb{N} \quad (a + bi) \mapsto a^2 + b^2
\]
is multiplicative, and on the other hand \( \text{Norm}(1 + i) = 2 \), so there can be no Gaussian integer \((a + bi)\) such that \( 1 = (a + bi)(1 + i) \), or else \( \text{Norm}(a + bi) = \frac{1}{2} \).

Moreover, \( P \) certainly contains 2, so that \( P \cap \mathbb{Z} \supset (2) \). On the other hand, \( P \cap \mathbb{Z} \neq \mathbb{Z} \), because otherwise \( P \) would contain 1, which we just proved does not happen. Thus
\[
(2) \subseteq P \cap \mathbb{Z} \subsetneq \mathbb{Z}
\]
forces \((2) = P \cap \mathbb{Z}\).

It remains to prove that \( P \) is a prime ideal of \( \mathbb{Z}[i] \): we do that by studying the quotient \( \mathbb{Z}[i]/P \) and showing that it is a domain. The elements of \((1 + i)\), i.e. the multiples of \(1 + i\), are the elements \((a + bi)(1 + i) = (a - b) + (a + b)i\). Any number \( c + di \) with \( c + d \) divisible by 2 can be written in this form (set \( a = \frac{d-c}{2} \) and \( b = \frac{d+c}{2} \)). Therefore
\[
(1 + i) = \{ c + di \mid c + d \text{ is even} \}.
\]

\[^1\text{see also pages 229-230 of the textbook}\]
As an additive subgroup of \((1 + i)\), the ideal \((1 + i)\) is a subgroup of index 2. Therefore \(\mathbb{Z}[i]/(1 + i)\) is some ring with 2 elements. We cannot have \(0 = 1\) (because the zero ring has only one element), so the two elements must be 0 and 1. Then all the additions and multiplications of these two elements are forced on us by the ring axioms. In short, the only ring with two elements is \(\mathbb{Z}/2\mathbb{Z}\). In particular, \(\mathbb{Z}[i]/(1 + i)\) is isomorphic to \(\mathbb{Z}/2\mathbb{Z}\).

f) [Answers only] We have

\[
(\varphi^*)^{-1}(x_{(2)}) = \{\text{prime ideals } P \subset \mathbb{Z}[i] \mid P \cap \mathbb{Z} = (2)\} = \{(1 + i)\};
\]

\[
(\varphi^*)^{-1}(x_{(3)}) = \{\text{prime ideals } P \subset \mathbb{Z}[i] \mid P \cap \mathbb{Z} = (3)\} = \{(3) = 3\mathbb{Z}[i]\};
\]

\[
(\varphi^*)^{-1}(x_{(5)}) = \{\text{prime ideals } P \subset \mathbb{Z}[i] \mid P \cap \mathbb{Z} = (5)\} = \{(i - 2), (i + 2)\};
\]

Consider the quotients \(\mathbb{Z}[i]/P\) for each of the prime ideals above. If \(P = (y)\), the division algorithm explained in class tells us that the coset representatives \(x + P \in \mathbb{Z}[i]/P\) can be chosen so that \(\text{Norm}(x) < \text{Norm}(y)\). But there are only finitely many elements of \(\mathbb{Z}[i]\) with \(\text{Norm}(x)\) less than a fixed constant, because this means we are looking for points on the integer lattice that lie inside the circle of some fixed radius. We conclude that the quotient ring \(\mathbb{Z}[i]/P\) has finitely many element, because there are only finitely many Gaussian integers of norm bounded above by the generator of \(P\). On the other hand, corollary 3 at page 228 tells us that any finite domain is a field, thus each \(\mathbb{Z}[i]/P\) is a finite field.

More explicitly, we have that \(\mathbb{Z}[i]/(1 + i) \cong \mathbb{Z}/2\mathbb{Z}\) is the finite field with two elements (we generally; denote that by \(F_2\)), as seen in question 2d.

With similar considerations, one can conclude that \(\mathbb{Z}[i]/(i - 2) \cong F_5\) and \(\mathbb{Z}[i]/(i + 2) \cong F_5\) are both ring-isomorphic to the field with 5 elements - which turns out to be \(\mathbb{Z}/5\mathbb{Z}\).

Finally, we get that \(\mathbb{Z}[i]/3\mathbb{Z}[i]\) is some field with 9 elements. Be careful, this is NOT \(\mathbb{Z}/9\mathbb{Z}\)!

Indeed, \(\mathbb{Z}/9\mathbb{Z}\) is not even a domain, because \(3 \cdot 3 = 0\).