Problem (8.2.3). Let $R$ be a P.I.D. and $P$ a prime ideal. If $P = (0)$, then $R/(0) \cong R$ is a P.I.D. by assumption, so it remains to handle nonzero $P$.

By proposition 7 in chapter 8.2 of the textbook, $P$ is a maximal ideal, and therefore $R/P$ is a field. In particular, the only ideals in $R/P$ are the zero ideal $(0)$ and the entire ring $(1)$. Since both are principal, $R/P$ is a P.I.D. and this concludes the proof.

Problem (Q1). Notice that $\mathbb{OD} \subset \mathbb{Q}$ is a subring of $\mathbb{Q}$ because multiplying and summing two fractions with odd denominators yields again fractions with odd denominators. In particular $\mathbb{OD}$ is a domain, since $\mathbb{Q}$ is.

Let $I$ be an ideal of $\mathbb{OD}$, we will prove that $I$ is principal. In fact, we can show something stronger: in fact every ideal $I$ is generated by a single integer: $I = (n)$, where

$$n = \min \left\{ p \mid \frac{p}{q} \in I, p, q > 0 \right\}$$

is the smallest positive numerator appearing in a fraction in $I$. (This is well-defined since $I$ is a nonzero additive subgroup of $\mathbb{OD}$, hence it contains some positive fraction.)

Notice moreover that $n$ is even, since if it were odd we would have $\frac{n}{p} \in I$ for some $p > 0$, but as $\frac{n}{p} \in \mathbb{OD}$ we would get $1 = \frac{n}{p} \cdot \frac{p}{n} \in I$, against the assumption that $I$ is proper. We claim that $I = (n)$: the inclusion $\supset$ is obvious, since $n = \frac{n}{q} \cdot q$ for that fraction $\frac{n}{q} \in I$, which exists by definition of $n$.

Take then $\frac{n}{q} \in I$, where WLOG we can assume $p, q > 0$. If $n$ divides $p$, then $\frac{p}{q} = n \cdot \frac{p/n}{q} \in (n)$ as claimed.

Arguing by contradiction, suppose $n$ does not divide $p$. Then we can write $p = an + b$ for $a \geq 1$ (since $n$ is minimal by choice), and $0 < r < n$. But then

$$\frac{b}{q} = \frac{p}{q} - \frac{a}{q} \cdot n \in I,$$

which is a contradiction by minimality of $n$. This concludes the proof, since we showed that $I$ is principal.

Problem (Q2). a) We use the Norm function, as in the hint:

$$\text{Norm}(a + b\sqrt{-5}) = a^2 + 5b^2,$$

which is multiplicative, i.e. $\text{Norm}(xy) = \text{Norm}(x)(y)$ for all $x, y, \in \mathbb{Z}\left[\sqrt{-5}\right]$.

We compute

$$\text{Norm}(2) = 2^2 = 4, \text{Norm}(3) = 3^2 = 9,$$
Norm\(1 + \sqrt{-5}\) = 1^2 + 5 \cdot 1^2 = 6, \text{ Norm}(1 - \sqrt{-5}) = 1^2 + 5 \cdot (-1)^2 = 6.

Notice also that Norm\(x\) = 1 if and only if \(x = \pm 1\), and in both cases \(\pm 1 \in \mathbb{Z}[\sqrt{-5}]^\times\) is a unit in \(\mathbb{Z}[\sqrt{-5}]\).

Suppose then that \(xy = 2\), then we know that

\[
4 = \text{Norm}(2) = \text{Norm}(xy) = \text{Norm}(x)\text{Norm}(y),
\]

and since no element \(a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]\) has \(\text{Norm}(a + b\sqrt{-5}) = a^2 + 5b^2\) equal to 2, one between \(\text{Norm}(x)\) and \(\text{Norm}(y)\) must be equal to 1, which means that either \(x\) or \(y\) is a unit. We conclude

\[
\mathbb{Z}[\sqrt{-5}]^\times = \{\pm 1\}.
\]

Therefore, two different irreducibles \(x, y\) are associate if and only if \(x = \pm y\). This is not the case for any two of the four we found.

b) Arguing by contradiction, suppose there exists \(a + b\sqrt{-5}, c + d\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]\) such that

\[
1 = 2 \cdot (a + b\sqrt{-5}) + (1 + \sqrt{-5}) \cdot (c + d\sqrt{-5}) = (2a + c - 5d) + (2b + d + c)\sqrt{-5}.
\]

We get then the two equations

\[
1 = 2a + c - 5d \text{ and } 2b + d + c = 0.
\]

Solving for \(c\) in the second equation, we get \(c = -2b - d\) which we plug in into the first equation, to obtain

\[
1 = 2a + (-2b - d) - 5d = 2a - 2b - 6d.
\]

The right hand side is thus even, but the left hand side is 1. This contradiction completes the proof.

c) Arguing by contradiction, suppose that \(I_2 = (x)\) is a principal ideal. As \(2 \in I_2\), there exists \(y \in \mathbb{Z}[\sqrt{-5}]\) such that \(2 = xy\), and hence \(4 = \text{Norm}(2) = \text{Norm}(x)\cdot\text{Norm}(y)\), in particular \(\text{Norm}(x)\) divides 4. Similarly, since \(1 + \sqrt{-5} \in I_2\) we get that \(\text{Norm}(x)\) divides \(\text{Norm}(1 + \sqrt{-5}) = 6\).

Therefore, \(\text{Norm}(x)\) divides the greatest common divisor \(\gcd(4, 6) = 2\), and in particular \(\text{Norm}(x) \leq 2\). On the other hand, we have seen that \(\mathbb{Z}[\sqrt{-5}]\) has no elements of Norm exactly 2, thus \(\text{Norm}(x) = 1\).

This means that \(x\) must be a unit, and hence \(I_2 = \mathbb{Z}[\sqrt{-5}]\), but this contradicts the conclusion of the Q2b, where we showed that \(I_2\) is proper. This concludes the proof that \(I_2\) is not a principal ideal.
d) Let’s start by noticing that

\[(1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}) - 2 \cdot 2 = 6 - 4 = 2\]

and hence \(2 \in I_2 \cdot I_2\), so that \((2) \subset I_2 \cdot I_2\).

Now let \(I, J, L\) be three ideals of a ring \(R\). Recall that the product of two ideals is defined as

\[I \cdot J = \left\{ \sum_{k} i_k \cdot j_k \mid i_k \in I, j_k \in J \right\},\]

thus to show that \(I \cdot J\) is contained in \(L\) it suffices to show that the single summand \(i_k \cdot j_k\) is in \(L\).

Let then \(2 \cdot a + (1 + \sqrt{-5}) \cdot b\) and \(2 \cdot c + (1 + \sqrt{-5}) \cdot d\) be two elements of \(I_2\). We have

\[
(2 \cdot a + (1 + \sqrt{-5}) \cdot b) \cdot (2 \cdot c + (1 + \sqrt{-5}) \cdot d) = \\
4ac + 2 (1 - \sqrt{-5}) ad + 2 (1 + \sqrt{-5}) bc + (1 + \sqrt{-5}) (1 - \sqrt{-5}) bd = \\
4ac + 2 (1 - \sqrt{-5}) ad + 2 (1 + \sqrt{-5}) bc + 6bd
\]

which is visibly in the ideal generated by 2 since each summand is a \(\mathbb{Z}[\sqrt{-5}]\)-multiple of 2.

This shows the inclusion \(I_2 \cdot I_2 \subset (2)\) and completes the proof.

**Problem (Q3).** We have a domain \(R\) and an element \(d \in R\) and we want to construct a ring \(R_d\) together with the map \(\varphi : R \rightarrow R_d\) such that \(\text{PrimeSpace}(R_d)\) maps onto \(U_d \subset \text{PrimeSpace}(R)\).

This means that in \(R_d\), the image \(\varphi(d)\) must not contained in any prime ideal, in particular in any maximal ideal. On the other hand, every proper ideal is contained in some maximal ideal. Since \(\varphi(d)\) is always contained in the principal ideal \((\varphi(d))\), this means that this principal ideal cannot be proper, so we must have \((\varphi(d)) = R_d\). From class, we know this is equivalent to \(\varphi(d)\) being a unit in \(R_d\).

To sum up, what we need to do when constructing \(R_d\) is “force” \(d\) to have a multiplicative inverse. We can do this simply adjoining the element \(\frac{1}{d}\), or something that behaves like it.

We’ll give two constructions of \(R_d\) (but they give the same ring).

**First construction:** we want to adjoin to \(R\) an element which formally behaves like \(\frac{1}{d}\). So let’s take the quotient of the polynomial ring \(R[x]\) by \((xd - 1)\) to get the ring

\[R_d \overset{\text{def}}{=} R[x]/(xd - 1)\]

with the map \(\varphi\) being the composition

\[\varphi : R \leftrightarrow R[x] \rightarrow R[x]/(xd - 1) = R_d.\]

If \(y \in R_d\) is the image of \(x \in R[x]\), then by definition we have \(yd = 1\). Therefore \(d\) is a unit in \(R_d\), and \(y\) plays the role of \(\frac{1}{d}\) in \(R_d\). We clearly have \(\varphi(d) = d \in \mathbb{R}[x]/(xd - 1)\) has inverse the class of \(x: \varphi\), as \(x \cdot d = 1\) in this quotient.

**Second construction:** We know that \(R\) is a domain and so has a field of fractions

\[K = \left\{ \frac{a}{b} \mid a, b \in R, b \neq 0 \right\}\]
and we set
\[ R_d \overset{\text{def}}{=} \left\{ \frac{a}{d^k} \middle| a \in R, k \in \mathbb{N} \right\} \subset K. \]

We notice that \( R_k \) is indeed a subring of \( K \), because addition and multiplication of fractions with denominator powers of \( d \) still gives fractions with denominator some power of \( d \); in this case, the map \( \varphi : R \hookrightarrow R_d \) is just the obvious map
\[ \varphi : R \hookrightarrow R_d \quad a \mapsto \frac{a}{1}. \]

It is not hard to see that the two constructions given above for \( R_d \) produce indeed the same ring; there is a canonical isomorphism from the first to the second, given by:
\[ \psi : R[x]/(xd - 1) \rightarrow R \left[ \frac{1}{d} \right] \] defined by \( \psi(a) = \frac{a}{1} \forall a \in R \) and \( \psi(y) = \frac{1}{d} \).

The usual notation for this ring is \( R[\frac{1}{d}] \), but I couldn’t call it that without giving away the answer.

Finally, we take the second construction and we show that the map
\[ \varphi^* : \text{PrimeSpace} (R_d) \rightarrow \text{PrimeSpace} (R) \]
has indeed image exactly the subset \( U_d \) of prime ideals of \( R \) not containing \( d \).

Note that a prime ideal \( P' \subset R_d \) can never contain \( d \), because a prime ideal can never contain a unit. If we think of \( R \) as a subring of \( R_d \), for any prime ideal \( P' \subset R_d \) we have \( \varphi^{-1}(P') = P' \cap R \). We know that \( P' \cap R \) cannot ever contain \( d \), by the first sentence. Therefore \( \varphi^{-1}(P') \) never contains \( d \). This shows that \( \text{Im}(\varphi^*) \subset U_d \).

Vice versa, let \( P \subset R \) be a prime ideal not containing \( d \). Define
\[ P_d \overset{\text{def}}{=} \left\{ \frac{p}{d^k} \middle| p \in P, k \in \mathbb{N} \right\} \subset R_d. \]

There are three things to check: (a) \( P_d \) is an ideal of \( R_d \); (b) \( P_d \) is a prime ideal of \( R_d \); (c) \( P_d \cap R = P \).

(a): Consider \( \frac{p}{d^m}, \frac{q}{d^n} \in P_d \) and \( \frac{r}{d^p} \in P_d \). We have
\[ \frac{p}{d^k} + \frac{q}{d^m} = \frac{pd^m + qd^k}{d^{k+m}} \]
which is in \( P_d \) because \( pd^m + qd^k \) is in \( P \) since \( P \) is an ideal. Similarly
\[ \frac{p}{d^k} \cdot \frac{r}{d^p} = \frac{pr}{d^{k+p}} \]
which is in \( P_d \) because \( pr \) is in \( P \) since \( P \) is an ideal. This shows that \( P_d \) is an ideal of \( R_d \).

(b) Let \( \frac{a}{d^m}, \frac{b}{d^n} \in R_d \) and suppose their product \( \frac{ab}{d^{n+m}} \) is in \( P_d \). We have then \( ab \in P \), by definition of \( P_d \), and since \( P \) is a prime ideal of \( R \) this means that either \( a \in P \) or \( b \in P \). In particular, either \( \frac{a}{d^m} \) or \( \frac{b}{d^n} \) is in \( P_d \), which concludes our proof.

(c) If \( x \in P_d \cap R \) then \( x = \frac{p}{d^k} \) for some \( p \in P \) and \( x = \frac{a}{d} \) for some \( a \in R \). By definition, \( \frac{p}{d^k} = \frac{a}{d} \) holds if and only if \( p \cdot 1 = a \cdot d^k \). Since \( p \in P \) and \( P \) is prime, we know either \( a \in P \) or \( d^k \notin P \). Since \( d \notin P \), by induction we know \( d^k \notin P \). Therefore \( x = \frac{a}{d} \) for some \( a \in P \). This shows that \( P_d \cap R = P \).

(An alternate proof of (b) and (c) would be to show that the composition \( R \hookrightarrow R_d \rightarrow R_d/P_d \) descends to an isomorphism \( (R/P)[\frac{1}{d}] \cong R_d/P_d = R[\frac{1}{d}]/(P[\frac{1}{d}]) \).

We conclude that \( \varphi^*(x_{P_d}) = x_P \in U_d \), so \( x_P \) is in the image of \( \varphi^* \). This shows the inclusion \( \text{Im}(\varphi^*) \supset U_d \), completing the proof.
Problem (Q4). a) We use the second description given in Q3, so that

\[ R_d = \mathbb{Z} \left[ \frac{1}{6} \right] = \left\{ \frac{a}{6^k} \mid a \in \mathbb{Z}, k \in \mathbb{N} \right\} = \left\{ \frac{p}{2^n 3^m} \text{ in lowest terms} \mid p \in \mathbb{Z}, n, m \in \mathbb{N} \right\}. \]

A rational number in lowest terms \( \frac{p}{2^n 3^m} \) is invertible in \( \mathbb{Z}[\frac{1}{6}] \) if and only its inverse \( \frac{2^n 3^m}{p} \in \mathbb{Q} \) is also in \( \mathbb{Z}[\frac{1}{6}] \), that is, if and only if \( p \) is also of the form \( \pm 2^n 3^b \). Putting the fraction into reduced form yields then that the units are exactly the integer powers of 2 times integer powers of 3, up to a sign:

\[ \mathbb{Z}[\frac{1}{6}]^\times = \{ \pm 2^x 3^y \mid x, y \in \mathbb{Z} \}. \]

b) Using again the second description from Q3, we have that

\[ \mathbb{Z}[x]_x = \mathbb{Z}[x] \left[ \frac{1}{x} \right] = \left\{ \frac{p(x)}{x^k} \mid p(x) \in \mathbb{Z}[x], k \in \mathbb{N} \right\} = \left\{ a_{-k} x^{-k} + \cdots + a_{-1} x^{-1} + a_0 + a_1 x + \cdots + a_n x^n \right\} \]

is the ring of “Laurent polynomials”, i.e. a polynomial in \( x \) plus a polynomial in \( x^{-1} \). Thinking of this as a subring of the rational functions \( \mathbb{Z}(x) \), this consists of those functions whose denominator is a power of \( x \).

Therefore, the element \( \frac{p(x)}{x^k} \) is invertible in \( \mathbb{Z}[x]_x \) if and only if its inverse \( \frac{x^k}{p(x)} \) in \( \mathbb{Z}(x) \) is also in \( \mathbb{Z}[x]_x \), that is, if and only if \( \pm p(x) \) is also a power of \( x \), say \( x^m \). But then we can simplify numerator and denominator to get an integer power of \( x \), up to a sign. We conclude

\[ (\mathbb{Z}[x]_x)^\times = \{ \pm x^n \mid n \in \mathbb{Z} \}. \]

c) As usual we consider the second description from Q3 and we have that

\[ \mathbb{Z}[x]_{2x} = \mathbb{Z}[x] \left[ \frac{1}{2x} \right] = \left\{ \frac{p(x)}{(2x)^k} \mid p(x) \in \mathbb{Z}[x], k \in \mathbb{N} \right\}. \]

We notice that since \( \frac{p(x)}{2^n x^k} = \frac{p(x)2^b x^n}{(2x)^{k+b}} \), this subring of \( \mathbb{Z}(x) \) consists of all the rational functions whose denominator is divisible only by 2 and \( x \) (among all the irreducibles of \( \mathbb{Z}[x] \)) - and not just of the ones whose denominator is divisible by powers of \( (2x) \), as it appeared at a first glance.

Suppose that the nonzero element \( \frac{p(x)}{2^n x^b} \) is invertible in \( \mathbb{Z}[x]_{2x} \), and WLOG assume that it is in reduced form, i.e. if \( x \) divides \( p(x) \) then \( b = 0 \), and similarly if \( 2 \) divides \( p(x) \) then \( a = 0 \).

As we are assuming that the element is invertible in \( \mathbb{Z}[x]_{2x} \) we have its inverse \( \frac{2^n x^b}{p(x)} \in \mathbb{Z}[x]_{2x} \), so that only powers of 2 and/or \( x \) divides \( p(x) \).

We have then the following possibilities:

- \( p(x) \) is not divisible by 2 nor \( x \). Then \( p(x) \in \mathbb{Z}[x]^\times = \{ \pm 1 \} \), so that \( \frac{p(x)}{2^n x^b} = \pm \frac{1}{2^n x^b} \).
- \( p(x) \) is divisible by 2, and hence \( a = 0 \). Therefore, our invertible element is \( \pm 2^n \).
- \( p(x) \) is divisible by \( x \), and hence \( b = 0 \). Therefore, our invertible element is \( \pm \frac{x^m}{2^n} \).

\[ ^1 \text{this is the fraction field of the domain } \mathbb{Z}[x], \text{ whose elements are the quotients of two polynomials with integer coefficients} \]
• \(p(x)\) is divisible by both 2 and \(x\), and hence \(a = b = 0\). Therefore, our invertible element is \(\pm 2^n x^m\).

We conclude that
\[
(Z[x]_{2x})^\times \cong \{\pm 2^n x^m \mid n, m \in \mathbb{Z}\}.
\]

d) We consider now the ring \(R = \mathbb{Z}/5\infty\mathbb{Z}\) of left-infinite sequences in base 5, with addition and multiplication being “column by column”, again in base 5. In other words, 5 is the element \(\ldots 00010\), 7 is the element \(\ldots 00012\) and so on.

Something different compared to our previous friend, the ring \(\mathbb{Z}/10\infty\mathbb{Z}\), is that \(R\) is now a domain. This is not too hard to see, and eventually it boils down to the fact that 5 is prime while 10 was composite.

We want then to describe \(R_5\), i.e. the ring we obtain from \(R\) when we force 5 to be an invertible element.

As a reality check, notice that 5 = \(\ldots 00010\) is not a unit in \(R\), because as for \(\mathbb{Z}/10\infty\mathbb{Z}\), the rightmost digit of a product \(a \cdot b\) in \(R\) is given by the product of the rightmost digits of \(a\) and \(b\) (all in base 5), and since the rightmost digit of 5 = \(\ldots 00010\) is zero, there can be no \(b\) whose rightmost digit can multiply 0 into 1.

We now proceed to describe an equivalent way to represent elements of the ring \(\mathbb{Z}/5\infty\mathbb{Z}\).

Note that the base 5 representation for a natural number \(n\) is simply obtained by

1) finding the largest \(k \geq 0\) such that \(5^{k+1} > n \geq 5^k\),
2) dividing \(n\) by \(5^k\) to obtain \(n = a_k5^k + r\) where \(0 \leq a_k < 5\) and \(r < 5^k\) and then
3) iterating from step 1 with \(r\) in place of \(n\).

This algorithm obviously finishes because at each iteration the possible \(k\) we choose in step 1 is strictly decreasing.

The representation of \(n\) in base 5 is then

\[
n = \ldots a_{k+1}a_k \ldots a_2a_1a_0
\]

where we filled in with zeros in case our algorithm did not produce \(a_k\) for a specific \(k\).

Revisiting this argument we notice that the digits \(a_k\) we found are precisely the unique choices of coefficients \(b_k\) between 0 and 5 – 1 = 4 that give

\[
n = b_0 + b_1 \cdot 5 + b_2 \cdot 5^2 + \ldots = \sum_{k=0}^{\infty} b_k5^k.
\]

With a leap of faith, we see that we can think of elements of \(R\) as a sort of “power series” in 5:

\[
R = \{\ldots a_{k+1}a_k \ldots a_1a_0 \mid 0 \leq a_i < 5\} = \left\{ \sum_{k=0}^{\infty} a_k5^k \mid 0 \leq a_k < 5 \right\},
\]

except that the addition and multiplication can carry over to the next place.
Now we are finally ready to understand what happens when we invert \( d = 5 \). Using the second description from Q3, elements of \( R_5 = R \left[ \frac{1}{5} \right] \) are polynomials in \( \frac{1}{5} \) with coefficients in \( R \), that is to say, finite sums of terms of the type

\[
\left( \sum_{k=0}^{\infty} a_k 5^k \right) \cdot \left( \frac{1}{5} \right)^n = \sum_{k=0}^{\infty} a_k 5^{k-n} = \sum_{k=-n}^{\infty} a_{k+n} 5^k,
\]

which are "doubly-infinite" power series with only finitely many negative terms: more generally we denote them by

\[
\sum_{m \gg -\infty} a_m 5^m
\]

where \( m \gg -\infty \) means that \( m \) is greater than some negative integer (depending on the series in question) - so that only finitely many \( m \)'s are negative.

With this description of elements of \( R_5 \), it turns out that every nonzero element is invertible! Indeed, take a series

\[
x = \sum_{m \geq M} a_m 5^m
\]

in \( R_5 \), where \( M \) is the smallest integer \( k \in \mathbb{Z} \) such that \( a_k \neq 0 \). Then

\[
x \cdot 5^{-M} = \sum_{m \geq M} a_m 5^m \cdot 5^{-M} = \sum_{m \geq M} a_m 5^{m-M} = \sum_{m' \geq 0} a_{m'+M} 5^{m'},
\]

We now use the following lemma, which we basically proved on HW4.

**Lemma 1.** Let \( y = \ldots a_{k+1}a_k \ldots a_1a_0 \in R \) have nonzero \( a_0 \). Then \( y \) is invertible in \( R \).

Using this lemma, our element \( x \cdot 5^{-M} \) is invertible in \( R \), since \( a_M \neq 0 \) is the coefficient of \( 5^0 \) - i.e. the rightmost digit in our original interpretation of the elements of \( R \).

Denote then by \( z \) the inverse of \( x \cdot 5^{-M} \) in \( R \), we obtain that

\[
1 = (x \cdot 5^{-M}) \cdot z = x \cdot (5^{-M} \cdot z)
\]

so that \( 5^{-M} \cdot z \in R_5 \) is an inverse to \( x \).

We conclude that \( R_5 \) is a field, and thus every nonzero element is invertible.

g) We use the description of \( R_d \) as subring of the field of fraction \( K \) of \( R \), i.e. the second construction given in Question 3.

Let then \( I \subset R_d \) be an ideal, and consider \( \varphi^{-1}(I) = I \cap R \), which is an ideal of \( R \) by problem 7.3.24 from HW 5. Since \( R \) is a PID, we obtain that \( I \cap R = (r) \) for some \( r \in R \). We will prove that

\[
I = \left( \frac{r}{1} \right) \text{ inside } R_d.
\]

Notice that the inclusion \( I \supset \left( \frac{r}{1} \right) \) is immediate, since \( r \in \varphi^{-1}(I) \) and hence \( \varphi(r) = \frac{r}{1} \in I \).

Consider then \( \frac{i}{d^k} \in I \). We have then

\[
i = \frac{i}{d^k} \cdot d^k \in I
\]

and thus \( i \in I \cap R = (r) \). There exists then \( a \in R \) such that \( i = r \cdot a \) and we conclude

\[
\frac{i}{d^k} = \frac{r}{d^k} = \frac{r}{1} \cdot \frac{a}{d^k} \in \left( \frac{r}{1} \right),
\]

hence proving the opposite inclusion. Note: this was basically our proof of Question 1!