Introduction to Ring Theory (MATH 228): Solutions to the Practice Problems – v 1.04

Paul Buckingham

1. (a) $\emptyset$

   (b) $\{1, 5\}$ (or one could answer simply Z in this case)

   (c) $\{1, 3, 4\}$

   (d) $\{1, 2\}$

2. (a) (*i*) $\emptyset$

   (*ii*) $\{1, 2, 3, 4\}$

   (*iii*) $\{1, 2, 4\}$

   (*iv*) $\{4, 5\}$

   (b) $(1, 3), (1, 4), (2, 3), (2, 4), (3, 3), (3, 4)$

3. $g = g \circ \mathbf{1}_Y = g \circ f \circ h = \mathbf{1}_X \circ h = h$.

4. (a) The map f is not injective, because $f(0) = f(-1)$.

   (b) The map g is injective, because if $x_1, x_2 \in \mathbb{Z}$, then

$$\begin{aligned} g(x_1) &= g(x_2) \\ \iff 2x_1^2 + x_1 + 1 &= 2x_2^2 + x_2 + 1 \\ \iff 2x_1^2 - 2x_2^2 + x_1 - x_2 &= 0 \\ \iff (x_1 - x_2)(2(x_1 + x_2) + 1) &= 0 \\ \iff x_1 - x_2 &= 0 \qquad (1) \\ \iff x_1 &= x_2. \end{aligned}$$

   The justification for the step at (1) is that $2(x_1 + x_2) + 1$ can never be zero, because $x_1 + x_2 \in \mathbb{Z}$.

5. Failure of injectivity is straightforward: $d(2) = d(11)$. To see that f is surjective, note that if m is any positive integer, then $m = d(n)$ where

$$n = \sum_{k=0}^{m-1} 10^k = \underbrace{1111 \cdots 1}_{m}.$$

6. (a) $1, 2, 5, 10, 17, 26, 37$

(b)

$$Y = \{1, 3, 5, 7, 9, 10, 12, \ldots\}$$
$$X \cap Y = \{1, 5, 10, 50, 65, 122, 197, \ldots\}$$

7. (a) Let $n \in \mathbb{Z}_{\geq 1}$. If n is odd, then $f(n) = n+1$ is even, so $f(f(n)) = f(n)-1 = n$. Similarly, if n is even, then $f(n) = n-1$ is odd, so $f(f(n)) = f(n)+1 = n$.

   (b) Because $f \circ f = \mathbf{1}_{\mathbb{Z}_{\geq 1}}$, Proposition 2.1 in Section I of the course notes shows that f is bijective. (Take $g = f$ in that proposition.)

8. (a) $y/|y|$ is equal to 1 when y is positive and is equal to -1 when y is negative, so $\text{Image}(g) = \{1, -1\}$.

   (b) If x is a fixed point of $g \circ f$, then $x = g(f(x)) \in \text{Image}(g) = \{1, -1\}$. Therefore, we have only to check 1 and -1. Since $g \circ f(1) = -1$ and $g \circ f(-1) = -1$, we see that -1 is the only fixed point of $g \circ f$.

   (c) For any $y \in \mathbb{Q} \smallsetminus \{0\}$, $(y/|y|)^2 = 1$, so $f \circ g(y) = (1-2)/(1+2) = -1/3$. Thus, $\text{Image}(f \circ g) = \{-1/3\}$.

9. We are to solve $(x+y)(x-y) = 77$. Because $77 = 7 \cdot 11$, and because x and y are assumed to be non-negative integers (so $x + y \geq 0$), uniqueness of factorization shows that one of the following possibilities for $(x+y, x-y)$ must hold:

$x+y$	$x-y$
77	1
11	7
7	11
1	77

   The first possibility, for example, gives the system

$$x + y = 77$$
$$x - y = \ \ 1$$

   of linear equations, which has the unique solution $x = 39$, $y = 38$. Similarly, the second possibility yields the solution $x = 9$, $y = 2$. The remaining two possibilities lead to solutions in which y is negative, so we ignore them. (Signs aside, they are the same solutions anyway.) Thus, the solutions $(x, y) \in \mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$ to $x^2 - y^2 = 77$ are $(x, y) = (39, 38)$ and $(x, y) = (9, 2)$.

10. (a) The given relation is not an equivalence relation, because symmetry fails: $0 \sim 1$, because $0 = 0 \cdot 1$, but $1 \not\sim 0$, because there is no $a \in \mathbb{Q}$ such that $1 = a \cdot 0$.

(b) The given relation is an equivalence relation. Reflexivity holds, because $x = 1 \cdot x$ for all $x \in \mathbb{R}$. Symmetry holds, because if $x = ay$ with $a \in \mathbb{Q} \smallsetminus \{0\}$, then $y = \frac{1}{a}x$, and $1/a \in \mathbb{Q} \smallsetminus \{0\}$. Finally, transitivity holds, because if $x = ay$ and $y = bz$, where $a, b \in \mathbb{Q} \smallsetminus \{0\}$, then $x = abz$, and ab is again in $\mathbb{Q} \smallsetminus \{0\}$.

11. (a) The given relation is not an equivalence relation, because transitivity fails:

$$\begin{aligned} 0 \sim 3/4, &\quad \text{because } |0 - 3/4| \leq 1, \\ \text{and} \quad 3/4 \sim 3/2, &\quad \text{because } |3/4 - 3/2| \leq 1, \\ \text{but} \quad 0 \not\sim 3/2, &\quad \text{because } |0 - 3/2| > 1. \end{aligned}$$

(b) The given relation is an equivalence relation. Reflexivity holds, because for all $X \in M_n(\mathbb{R})$, $\mathrm{Tr}(X - X) = 0 \in \mathbb{Z}$. Symmetry holds, because if $X \sim Y$, i.e., $\mathrm{Tr}(X - Y) \in \mathbb{Z}$, then $\mathrm{Tr}(Y - X) = -\mathrm{Tr}(X - Y) \in \mathbb{Z}$, so $Y \sim X$. Finally, transitivity holds, because if $X \sim Y$, i.e., $\mathrm{Tr}(X - Y) \in \mathbb{Z}$, and $Y \sim Z$, i.e., $\mathrm{Tr}(Y - Z) \in \mathbb{Z}$, then

$$\begin{aligned} \mathrm{Tr}(X - Z) &= \mathrm{Tr}((X - Y) + (Y - Z)) \\ &= \mathrm{Tr}(X - Y) + \mathrm{Tr}(Y - Z) \in \mathbb{Z}, \end{aligned}$$

the sum of two integers being again an integer. Thus, $X \sim Z$.

12. The relation is reflexive, because $\mathbf{u} \cdot \mathbf{u} \geq 0$ for all $\mathbf{u} \in \mathbb{R}^3$. It is symmetric because $\mathbf{u} \cdot \mathbf{v} = \mathbf{v} \cdot \mathbf{u}$, so $\mathbf{u} \cdot \mathbf{v} \geq 0$ if and only if $\mathbf{v} \cdot \mathbf{u} \geq 0$. However, the relation is not transitive. For example, if

$$\mathbf{u} = (1, 0, 0), \quad \mathbf{v} = (0, 1, 0), \quad \mathbf{w} = (-1, 0, 0),$$

then $\mathbf{u} \sim \mathbf{v}$ and $\mathbf{v} \sim \mathbf{w}$, but $\mathbf{u} \not\sim \mathbf{w}$.

13. The given relation is an equivalence relation. Reflexivity is immediate, because if $x \in \mathbb{Q} \smallsetminus \{0\}$, then $xx = x^2$ is the square of a rational number. Symmetry is also straightforward, because if $x, y \in \mathbb{Q} \smallsetminus \{0\}$, then $xy = yx$, so xy is the square of a rational number if and only if yx is. For transitivity, suppose that $x, y, z \in \mathbb{Q} \smallsetminus \{0\}$ satisfy $xy = r^2$ and $yz = s^2$, where $r, s \in \mathbb{Q}$. Then

$$xz = \frac{(xy)(yz)}{y^2} = \frac{r^2 s^2}{y^2} = \left(\frac{rs}{y}\right)^2,$$

so xz is the square of a rational number, namely, the rational number rs/y. (Note that y is non-zero by assumption.)

14. If $\mathbf{x} \in X$, then the vectors $\mathbf{y} \in X$ such that $\mathbf{y} \sim \mathbf{x}$ are those vectors of the form $c\mathbf{x}$ with $c \in \mathbb{R}_{>0}$. That is, the equivalence class of $\mathbf{x}$ is

$$[\mathbf{x}] = \{c\mathbf{x} \mid c \in \mathbb{R}_{>0}\},$$

which is the half line $L_{\mathbf{x}}$ beginning at (but not including) the origin and passing through $\mathbf{x}$. Each $L_{\mathbf{x}}$ contains a unique point on the unit circle S, and conversely each point on S is on a unique $L_{\mathbf{x}}$, so the equivalence classes are represented by the points of S, i.e., the points $(\cos(\theta), \sin(\theta))$ with $0 \leq \theta < 2\pi$.

Another possibility is to intersect the equivalence classes with the lines $x_1 = 1$ and $x_1 = -1$, if we give points in $\mathbb{R}^2$ the coordinates (x_1, x_2). Specifically, we have the class of $(1, x_2)$ and the class of $(-1, x_2)$ for each $x_2 \in \mathbb{R}$, and also two more classes, namely, the class of $(0, 1)$ and the class of $(0, -1)$, which are the two "vertical" classes.

15. To verify the case $n = 0$, we observe that the sum in this case is the empty sum and therefore equals zero, and also $(0 + 1)! - 1 = 1 - 1 = 0$.

Now assume that the equality holds for some $n \geq 0$. Then

$$\begin{aligned}\sum_{k=1}^{n+1} k(k!) &= \sum_{k=1}^{n} k(k!) + (n+1)(n+1)! \\ &= (n+1)! - 1 + (n+1)(n+1)! \quad \text{by the inductive hypothesis} \\ &= (n+2)(n+1)! - 1 \\ &= (n+2)! - 1,\end{aligned}$$

completing the induction.

16. The case $n = 0$ holds, because in that case the sum on the left is $0/(1!) = 0$, while the right-hand side is $1 - 1/(0!) = 0$. Now let $n \geq 0$, and assume that the equality holds for this n. Then

$$\begin{aligned}\sum_{k=0}^{n+1} \frac{k}{(k+1)!} &= \sum_{k=0}^{n} \frac{k}{(k+1)!} + \frac{n+1}{(n+2)!} \\ &= 1 - \frac{1}{(n+1)!} + \frac{n+1}{(n+2)!} \quad \text{by the inductive hypothesis} \\ &= 1 - \left(\frac{n+2}{(n+2)!} - \frac{n+1}{(n+2)!} \right) \\ &= 1 - \frac{1}{(n+2)!}.\end{aligned}$$

The induction is complete.

17. The base case, $n = 0$, holds because $3^{5 \cdot 0 + 3} + 5^0 = 27 + 1 = 28$, which is divisible by 7.

Now assume that the statement is true for some $n \geq 0$. Then there is $a \in \mathbb{Z}$ such that

$$3^{5n+3} + 5^n = 7a. \tag{2}$$

Hence,

$$\begin{aligned} 3^{5(n+1)+3} + 5^{n+1} &= 3^{5n+5+3} + 5^{n+1} \\ &= 3^5 \cdot 3^{5n+3} + 5^{n+1} \\ &= 3^5(7a - 5^n) + 5^{n+1} \quad \text{by (2)} \\ &= 3^5 \cdot 7a - 5^n(3^5 - 5) \\ &= 3^5 \cdot 7a - 5^n \cdot 7 \cdot 34 \\ &= 7(3^5 a - 5^n \cdot 34), \end{aligned}$$

which is divisible by 7. The induction is complete.

18. (a) By the binomial theorem,

$$\begin{aligned} (n+1)^3 - (n+1) &= n^3 + 3n^2 + 3n + 1 - n - 1 \\ &= (3n^2 + 3n) + (n^3 - n). \end{aligned}$$

(b) The case $n = 0$ holds, because $0^3 - 0 = 0$, which is divisible by 3. Now let $n \geq 0$, and assume that 3 divides $n^3 - n$, i.e., $n^3 - n = 3a$ for some $a \in \mathbb{Z}$. Then by part (a),

$$\begin{aligned} (n+1)^3 - (n+1) &= (3n^2 + 3n) + (n^3 - n) \\ &= 3(n^2 + n) + 3a \\ &= 3(n^2 + n + a), \end{aligned}$$

which is divisible by 3. This completes the induction.

(c) It remains to prove the statement for $n < 0$. In that case, $n = -m$ for some $m > 0$, and part (b) shows that 3 divides

$$m^3 - m = (-n)^3 - (-n) = -n^3 - (-n) = -(n^3 - n).$$

Therefore, 3 divides $n^3 - n$ as well.

19. By definition, there are $a, b \in \mathbb{Z}$ such that $s = ra$ and $t = sb$. Hence, $t = (ra)b = r(ab)$, so $r \mid t$.

20.

$$\begin{aligned} 14\,161 &= 11\,011 + 3150 \\ 11\,011 &= 3 \cdot 3150 + 1561 \\ 3150 &= 2 \cdot 1561 + 28 \\ 1561 &= 55 \cdot 28 + 21 \end{aligned}$$

$$28 = 21 + 7$$

Because $7 \mid 21$, we see that $\gcd(14\,161, 11\,011) = 7$. Further,

$$\begin{aligned}
7 &= 28 - 21 \\
&= 28 - (1561 - 55 \cdot 28) \\
&= 56 \cdot 28 - 1561 \\
&= 56(3150 - 2 \cdot 1561) - 1561 \\
&= 56 \cdot 3150 - 113 \cdot 1561 \\
&= 56 \cdot 3150 - 113(11\,011 - 3 \cdot 3150) \\
&= 395 \cdot 3150 - 113 \cdot 11\,011 \\
&= 395(14\,161 - 11\,011) - 113 \cdot 11\,011 \\
&= 395 \cdot 14\,161 - 508 \cdot 11\,011
\end{aligned}$$

21.

$$\begin{aligned}
5225 &= 4 \cdot 1183 + 493 \\
1183 &= 2 \cdot 493 + 197 \\
493 &= 2 \cdot 197 + 99 \\
197 &= 99 + 98 \\
99 &= 98 + 1
\end{aligned}$$

The greatest common divisor is therefore 1, and

$$\begin{aligned}
1 &= 99 - 98 \\
&= 99 - (197 - 99) \\
&= 2 \cdot 99 - 197 \\
&= 2(493 - 2 \cdot 197) - 197 \\
&= 2 \cdot 493 - 5 \cdot 197 \\
&= 2 \cdot 493 - 5(1183 - 2 \cdot 493) \\
&= 12 \cdot 493 - 5 \cdot 1183 \\
&= 12(5225 - 4 \cdot 1183) - 5 \cdot 1183 \\
&= 12 \cdot 5225 - 53 \cdot 1183
\end{aligned}$$

22. (a) Because a and b are coprime, there are integers m and n such that $1 = ma + nb$. Hence, $c = mac + nbc$. But the assumption $a \mid bc$ says that there is $d \in \mathbb{Z}$ such that $bc = ad$, so $c = mac + nad = a(mc + nd)$, and so $a \mid c$.

(b) Let $a = b = 2$ and $c = 1$. Then $a \mid bc$, but $a \nmid c$. Another possibility is $a = b = 0$, $c = 1$. In this case, $a \mid bc$ (because 0 divides 0), but $a \nmid c$.

23. (a) As in Question 22, let m and n be integers such that $1 = ma + nb$, and again multiply this equation by c to obtain $c = mac + nbc$. By the assumption that a and b divide c, there are integers a' and b' such that $c = aa'$ and $c = bb'$, so from the equation $c = mac + nbc$, we obtain

$$c = mabb' + nbaa' = ab(mb' + na').$$

Thus, $ab \mid c$.

(b) Let $a = b = c = 2$. Then $a \mid c$ and $b \mid c$, but $ab \nmid c$.

24. (a) Note that $1110 = 1111 - 1 = 101 \cdot 11 - 1$, so $1110 \equiv -1 \bmod 11$. Therefore,

$$\begin{aligned} 1110^{2021} &\equiv (-1)^{2021} \bmod 11 \\ &= -1 \\ &\equiv 10 \bmod 11, \end{aligned}$$

so the remainder is 10.

(b) This time,

$$\begin{aligned} 1110^{2022} &\equiv (-1)^{2022} \bmod 11 \\ &= 1, \end{aligned}$$

so the remainder is 1.

25. (a)

$$\begin{aligned} 35 &= 22 + 13 \\ 22 &= 13 + 9 \\ 13 &= 9 + 4 \\ 9 &= 2 \cdot 4 + 1, \end{aligned}$$

so

$$\begin{aligned} 1 &= 9 - 2 \cdot 4 \\ &= 9 - 2(13 - 9) = 3 \cdot 9 - 2 \cdot 13 \\ &= 3(22 - 13) - 2 \cdot 13 \\ &= 3 \cdot 22 - 5 \cdot 13 \\ &= 3 \cdot 22 - 5(35 - 22) = 8 \cdot 22 - 5 \cdot 35. \end{aligned}$$

Therefore, $22k \equiv 1 \bmod 35$ where $k = 8$.

(b)

$$\begin{aligned} & 66x + 4 \equiv 16 \bmod 105 \\ \iff & 66x \equiv 12 \bmod 105 \\ \iff & 22x \equiv 4 \bmod 35 \\ \iff & 8 \cdot 22x \equiv 8 \cdot 4 \bmod 35 \quad \text{because } \gcd(8, 35) = 1 \\ \iff & x \equiv 32 \bmod 35 \quad \text{by part (a).} \end{aligned}$$

26. (a)

$$\begin{aligned} & 100 \cdot 99 \cdot 98 \cdots 52 \cdot 51 \\ &= (101 - 1)(101 - 2)(101 - 3) \cdots (101 - 49)(101 - 50) \\ &\equiv (-1)(-2)(-3) \cdots (-49)(-50) \bmod 101 \\ &= (-1)^{50} \cdot 1 \cdot 2 \cdot 3 \cdots 49 \cdot 50 \\ &= 1 \cdot 2 \cdot 3 \cdots 49 \cdot 50. \end{aligned}$$

(b) If we multiply both sides of the congruence

$$100 \cdot 99 \cdot 98 \cdots 52 \cdot 51 \equiv 1 \cdot 2 \cdot 3 \cdots 49 \cdot 50 \bmod 101$$

by $50! = 50 \cdot 49 \cdots 2 \cdot 1$, then the left-hand side becomes $100!$ and the right $(50!)^2$.

27. (a) Because b and c are coprime, the G.C.D. Theorem says that there are $r, s \in \mathbb{Z}$ such that $1 = rb + sc$. Multiplying both sides of this equation by $a/(bc)$, we obtain

$$\frac{a}{bc} = \frac{k}{b} + \frac{l}{c}$$

where $k = as$ and $l = ar$.

(b) We may perform division with remainder to write $k = vb + m$ and $l = wc + n$ where $v, w, m, n \in \mathbb{Z}$, $0 \leq m < b$, and $0 \leq n < c$. Then

$$\frac{a}{bc} = u + \frac{m}{b} + \frac{n}{c}$$

where $u = v + w$.

28. (a)

$$\begin{aligned} 3375 &= 9 \cdot 343 + 288 \\ 343 &= 288 + 55 \end{aligned}$$

$$\begin{aligned} 288 &= 5 \cdot 55 + 13 \\ 55 &= 4 \cdot 13 + 3 \\ 13 &= 4 \cdot 3 + 1, \end{aligned}$$

so

$$\begin{aligned} 1 &= 13 - 4 \cdot 3 \\ &= 13 - 4(55 - 4 \cdot 13) = 17 \cdot 13 - 4 \cdot 55 \\ &= 17(288 - 5 \cdot 55) - 4 \cdot 55 = 17 \cdot 288 - 89 \cdot 55 \\ &= 17 \cdot 288 - 89(343 - 288) = 106 \cdot 288 - 89 \cdot 343 \\ &= 106(3375 - 9 \cdot 343) - 89 \cdot 343 = 106 \cdot 3375 - 1043 \cdot 343 \\ &= 106 \cdot 3^3 \cdot 5^3 - 1043 \cdot 7^3. \end{aligned}$$

(b)

$$\begin{aligned} 125 &= 4 \cdot 27 + 17 \\ 27 &= 17 + 10 \\ 17 &= 10 + 7 \\ 10 &= 7 + 3 \\ 7 &= 2 \cdot 3 + 1, \end{aligned}$$

so

$$\begin{aligned} 1 &= 7 - 2 \cdot 3 \\ &= 7 - 2(10 - 7) = 3 \cdot 7 - 2 \cdot 10 \\ &= 3(17 - 10) - 2 \cdot 10 = 3 \cdot 17 - 5 \cdot 10 \\ &= 3 \cdot 17 - 5(27 - 17) = 8 \cdot 17 - 5 \cdot 27 \\ &= 8(125 - 4 \cdot 27) - 5 \cdot 27 = 8 \cdot 125 - 37 \cdot 27 \\ &= -37 \cdot 3^3 + 8 \cdot 5^3. \end{aligned}$$

29. (a) Dividing both sides of the equation

$$1 = 106 \cdot 3^3 \cdot 5^3 - 1043 \cdot 7^3$$

by $3^3 \cdot 5^3 \cdot 7^3$, we obtain

$$\frac{1}{3^3 \cdot 5^3 \cdot 7^3} = -\frac{1043}{3^3 \cdot 5^3} + \frac{106}{7^3}.$$

(b) Dividing both sides of the equation

$$1 = -37 \cdot 3^3 + 8 \cdot 5^3$$

by $3^3 \cdot 5^3$, we obtain

$$\frac{1}{3^3 \cdot 5^3} = \frac{8}{3^3} - \frac{37}{5^3}.$$

(c)

$$\begin{aligned}
\frac{1}{105^3} &= -\frac{1043}{3^3 \cdot 5^3} + \frac{106}{7^3} \quad \text{by part (a)} \\
&= -1043\left(\frac{8}{3^3} - \frac{37}{5^3}\right) + \frac{106}{7^3} \quad \text{by part (b)} \\
&= -\frac{8344}{3^3} + \frac{38\,591}{5^3} + \frac{106}{7^3} \\
&= \frac{-310 \cdot 3^3 + 26}{3^3} + \frac{308 \cdot 5^3 + 91}{5^3} + \frac{106}{7^3} \\
&= -310 + \frac{26}{3^3} + 308 + \frac{91}{5^3} + \frac{106}{7^3} \\
&= -2 + \frac{26}{3^3} + \frac{91}{5^3} + \frac{106}{7^3}.
\end{aligned}$$

30. (a) We begin by replacing the first pair of congruences with a single congruence. Note that $1 = -19 + 20$, so a solution to the first two congruences is $13 \cdot 20 + 1(-19) = 241$. Hence, because $19 \cdot 20 = 380$, this pair of congruences is equivalent to the single congruence $x \equiv 241 \bmod 380$. We are now to solve

$$\begin{aligned}
x &\equiv 241 \mod 380 \\
x &\equiv 14 \mod 21
\end{aligned} \tag{3}$$

Let us perform the Euclidean algorithm on 380 and 21:

$$\begin{aligned}
380 &= 18 \cdot 21 + 2 \\
21 &= 10 \cdot 2 + 1
\end{aligned}$$

Hence,

$$1 = 21 - 10 \cdot 2 = 21 - 10(380 - 18 \cdot 21) = -10 \cdot 380 + 181 \cdot 21.$$

Therefore, a solution to the system of congruences in (3) is

$$241 \cdot 181 \cdot 21 + 14 \cdot (-10) \cdot 380 = 862\,841.$$

Because $380 \cdot 21 = 7980$, the system is equivalent to the single congruence

$$\begin{aligned}
&x \equiv 862\,841 \mod 7980, \\
\text{i.e.,} \quad &x \equiv 1001 \mod 7980.
\end{aligned}$$

The smallest solution is therefore 1001.

(b) The second smallest solution is $1001 + 7980 = 8981$.

31. Note that the three congruences are equivalent to

$$\begin{aligned} x &\equiv 3 && \mod 11 \\ x &\equiv 4 && \mod 13 \\ x &\equiv 16 && \mod 17 \end{aligned}$$

(a) Performing the Euclidean algorithm on 11 and 13, we find that $1 = 6{\cdot}11 - 5{\cdot}13$. Therefore, the first two congruences are equivalent to the single congruence

$$\begin{aligned} & x \equiv 3(-5) \cdot 13 + 4 \cdot 6 \cdot 11 && \mod 143 \\ \text{i.e.,} \quad & x \equiv 69 && \mod 143 \end{aligned}$$

Now we perform the Euclidean algorithm on 143 and 17. Because there are more steps this time, we will show them:

$$\begin{aligned} 143 &= 8 \cdot 17 + 7 \\ 17 &= 2 \cdot 7 + 3 \\ 7 &= 2 \cdot 3 + 1, \end{aligned}$$

so

$$\begin{aligned} 1 &= 7 - 2 \cdot 3 \\ &= 7 - 2(17 - 2 \cdot 7) = 5 \cdot 7 - 2 \cdot 17 \\ &= 5(143 - 8 \cdot 17) - 2 \cdot 17 = 5 \cdot 143 - 42 \cdot 17. \end{aligned}$$

Hence, we find that the three congruences combined are equivalent to

$$\begin{aligned} & x \equiv 69(-42) \cdot 17 + 16 \cdot 5 \cdot 143 && \mod 143 \cdot 17 \\ & \quad = -37\,826 \\ \text{i.e.,} \quad & x \equiv 1070 && \mod 2431 \end{aligned}$$

The least positive solution is therefore $x = 1070$.

(b) We subtract 2431 from the least positive solution: $1070 - 2431 = -1361$.

32. The equality $1 = 13 - 3 \cdot 4$ shows that -3 is inverse to 4 mod 13, so the first congruence is equivalent to

$$\begin{aligned} x &\equiv (-3) \cdot 2 && \mod 13 \\ &\equiv 7 && \mod 13 \end{aligned}$$

Similarly, the equality $1 = 21 - 4 \cdot 5$ shows that -4 is inverse to 5 mod 21, so the second congruence in the question is equivalent to

$$\begin{aligned} x &\equiv (-4) \cdot 6 && \mod 21 \\ &\equiv 18 && \mod 21 \end{aligned}$$

Hence, we solve the system

$$\begin{aligned} x &\equiv 7 && \mod 13 \\ x &\equiv 18 && \mod 21 \end{aligned}$$

The equality $1 = 5 \cdot 21 - 8 \cdot 13$ shows that this system is equivalent to

$$\begin{aligned} & x \equiv 7 \cdot 5 \cdot 21 + 18(-8) \cdot 13 && \mod 13 \cdot 21 \\ & \quad = -1137 \\ \text{i.e.,} \quad & x \equiv 228 && \mod 273 \end{aligned}$$

33. (a) According to the fact given at the beginning of the question, $93 \equiv 203^2 \mod 541$, so

$$\begin{aligned} & x^2 \equiv 93 \mod 541 \\ \iff\ & x^2 \equiv 203^2 \mod 541 \\ \iff\ & x^2 - 203^2 \equiv 0 \mod 541 \\ \iff\ & (x - 203)(x + 203) \equiv 0 \mod 541 \\ \iff\ & 541 \text{ divides } (x - 203)(x + 203) \\ \iff\ & 541 \text{ divides } x - 203 \text{ or } x + 203 \quad \text{(unique-factorization lemma)} \\ \iff\ & x \equiv 203 \mod 541 \text{ or } x \equiv -203 \mod 541. \end{aligned}$$

We were able to use the unique-factorization lemma in the above because 541 is prime.

To see why the primality of 541 was truly necessary in the above, consider the following situation. The congruence $x^2 \equiv 2^2 \mod 15$ appears, superficially, to be of the same kind as the congruence $x^2 \equiv 203^2 \mod 541$, but the solutions $x \equiv \pm 2 \mod 15$ are not the only ones. There are also the solutions $x \equiv \pm 7 \mod 15$.

(b) By part (a), x satisfies the given system of congruences if and only if it satisfies either system (4) or system (5):

$$\begin{aligned} x &= 203 && \mod 541 \\ x &= 3 && \mod 200 \end{aligned} \tag{4}$$

$$\begin{aligned} x &= -203 \qquad \mod 541 \\ x &= 3 \qquad\quad \mod 200 \end{aligned} \tag{5}$$

Let us handle system (5) first. For this, we apply the Euclidean algorithm to 541 and 200:

$$\begin{aligned} 541 &= 2 \cdot 200 + 141 \\ 200 &= 141 + 59 \\ 141 &= 2 \cdot 59 + 23 \\ 59 &= 2 \cdot 23 + 13 \\ 23 &= 13 + 10 \\ 13 &= 10 + 3 \\ 10 &= 3 \cdot 3 + 1, \end{aligned}$$

so

$$\begin{aligned} 1 &= 10 - 3 \cdot 3 \\ &= 10 - 3(13 - 10) = 4 \cdot 10 - 3 \cdot 13 \\ &= 4(23 - 13) - 3 \cdot 13 = 4 \cdot 23 - 7 \cdot 13 \\ &= 4 \cdot 23 - 7(59 - 2 \cdot 23) = 18 \cdot 23 - 7 \cdot 59 \\ &= 18(141 - 2 \cdot 59) - 7 \cdot 59 = 18 \cdot 141 - 43 \cdot 59 \\ &= 18 \cdot 141 - 43(200 - 141) = 61 \cdot 141 - 43 \cdot 200 \\ &= 61(541 - 2 \cdot 200) - 43 \cdot 200 = 61 \cdot 541 - 165 \cdot 200. \end{aligned}$$

Hence, system (5) is equivalent to

$$\begin{aligned} & x \equiv -203(-165) \cdot 200 + 3 \cdot 61 \cdot 541 \qquad \mod 541 \cdot 200 \\ & \quad = 6\,798\,003 \\ \text{i.e.,} \quad & x \equiv 89\,603 \qquad\qquad\qquad\qquad\qquad\quad \mod 108\,200 \end{aligned}$$

We could treat system (4) the same way, but there is a quicker solution in this case. Note that $3 \equiv 203 \bmod 200$, so the system is simply

$$\begin{aligned} x &= 203 \qquad \mod 541 \\ x &= 203 \qquad \mod 200 \end{aligned}$$

This system has the obvious solution $x = 203$, so its solution set is the set of all x satisfying $x \equiv 203 \bmod 108\,200$.

The first four positive solutions to the original pair of congruences are therefore

$$x_1 = 203$$

$$x_2 = 89\,603$$
$$x_3 = 203 + 108\,200 = 108\,403$$
$$x_4 = 89\,603 + 108\,200 = 197\,803$$

34. If $y = x - 4$, then the congruences say

$$\begin{aligned} y &\equiv 0 \mod 315 \\ y &\equiv 5 \mod 715 \end{aligned}$$

Thus, $5 \,|\, y$. For example, the first of these two congruences says that $315 \,|\, y$, so $5 \,|\, y$ as well. Therefore, we can let $z = y/5$ and divide through to obtain

$$\begin{aligned} z &\equiv 0 \mod 63 \\ z &\equiv 1 \mod 143 \end{aligned} \tag{6}$$

Hence, because

$$1 = 26 \cdot 143 - 59 \cdot 63 = -59 \cdot 63 + 26 \cdot 143,$$

a solution to (6) is

$$z = 0 \cdot 26 \cdot 143 + 1 \cdot (-59 \cdot 63) = -3717.$$

Thus, because $63 \cdot 143 = 9009$, we see that (6) is equivalent to

$$\begin{aligned} & z \equiv -3717 \mod 9009, \\ \text{i.e.,} \quad & z \equiv 5292 \mod 9009. \end{aligned}$$

In terms of $y = 5z$, the solution is $y \equiv 26\,460 \bmod 45\,045$, and in terms of the original variable $x = y + 4$, the solution is $x \equiv 26\,464 \bmod 45\,045$.

35. (a) (*i*) $s = -2$, $t = 1$. The inverse of 4 mod 9 is therefore -2 mod 9. The congruence in question is consequently $x \equiv -2 \cdot 5 \bmod 9$, i.e., $x \equiv -1 \bmod 9$.

(*ii*) $u = -7$, $v = 1$. The inverse of 3 mod 9 is therefore -7 mod 22. The congruence in question is consequently $x \equiv -7 \cdot 19 \bmod 22$, i.e., $x \equiv -133 \bmod 22$, i.e., $x \equiv -1 \bmod 22$.

(b) By part (a), the system of congruences to be solved is equivalent to

$$\begin{aligned} x &\equiv -1 \mod 9 \\ x &\equiv -1 \mod 22 \end{aligned}$$

A solution is $x = -1$, so because 9 and 22 are coprime and $9 \cdot 22 = 198$, the general solution is $x \equiv -1 \bmod 198$, i.e., $x \equiv 197 \bmod 198$.

36. Suppose that $x \in \mathbb{Z}$ satisfies $ax \equiv b \bmod n$, i.e., $n \,|\, ax - b$. Then because $d \,|\, n$, we conclude that $d \,|\, ax - b$. But then the assumption that $d \,|\, a$ implies that $d \,|\, b$, contradicting the further assumption that there is no integer greater than 1 dividing all three of a, b, and n.

37. (a) Let $f, g, h \in T$ and $x \in \mathbb{Z}$. Then

$$\begin{aligned}((g+h)\cdot f)(x) &= ((g+h)\circ f)(x) \quad \text{(def. of multiplication)}\\ &= (g+h)(f(x)) \quad \text{(def. of composition)}\\ &= g(f(x)) + h(f(x)) \quad \text{(def. of addition)}\\ &= (g\circ f)(x) + (h\circ f)(x) \quad \text{(def. of composition)}\\ &= ((g\circ f) + (h\circ f))(x) \quad \text{(def. of addition)}\\ &= (g\cdot f + h\cdot f)(x) \quad \text{(def. of multiplication)},\end{aligned}$$

so $(g+h)\cdot f = g\cdot f + h\cdot f$.

(b) Let $\mathbf{1} : \mathbb{Z} \to \mathbb{Z}$ be the constant function $x \mapsto 1$, let $f = \mathbf{1}$, and let g, h be any functions in T (for example, $g = h = \mathbf{1}$ again, but it does not matter). Then for $x \in \mathbb{Z}$,

$$\begin{aligned}(f\cdot(g+h))(x) &= (f\circ(g+h))(x)\\ &= \mathbf{1}((g+h)(x))\\ &= 1,\end{aligned}$$

$$\begin{aligned}\text{while}\quad (f\cdot g + f\cdot h)(x) &= ((f\circ g) + (f\circ h))(x)\\ &= (f\circ g)(x) + (f\circ h)(x)\\ &= \mathbf{1}(g(x)) + \mathbf{1}(h(x))\\ &= 2.\end{aligned}$$

38.

$$\begin{aligned}&\big((a,b)\cdot(c,d)\big)\cdot(e,f)\\ &= (ac-bd, ad+bc)\cdot(e,f)\\ &= ((ac-bd)e - (ad+bc)f, (ac-bd)f + (ad+bc)e)\\ &= (ace - bde - adf - bcf, acf - bdf + ade + bce),\end{aligned}$$

and

$$\begin{aligned}&(a,b)\cdot\big((c,d)\cdot(e,f)\big)\\ &= (a,b)\cdot(ce-df, cf+de)\\ &= (a(ce-df) - b(cf+de), a(cf+de) + b(ce-df))\end{aligned}$$

$$= (ace - adf - bcf - bde, acf + ade + bce - bdf).$$

Aside from the order of the terms in each entry, the two expressions are identical.

39. Let $a \in R$ be a unit. Then there is $b \in R$ such that $ab = 1$. Hence,

$$\begin{aligned} a^2 b &= a \\ \text{so} \quad ab &= a \quad \text{because } a^2 = a \\ \text{and so} \quad 1 &= a \quad \text{because } ab = 1. \end{aligned}$$

40. Suppose that $ca = 1$. Then

$$\begin{aligned} cab &= b, \\ \text{i.e.,} \quad c \cdot 0 &= b, \\ \text{i.e.,} \quad 0 &= b \quad \text{by Proposition 2.3 in Section IV,} \end{aligned}$$

contradicting the assumption that $b \neq 0$.

41. (a)

$$\begin{aligned} (1+1) \cdot (x+y) &= (1+1) \cdot x + (1+1) \cdot y \\ &= 1 \cdot x + 1 \cdot x + 1 \cdot y + 1 \cdot 1 \\ &= x + x + y + y. \end{aligned}$$

(b)

$$\begin{aligned} (1+1) \cdot (x+y) &= 1 \cdot (x+y) + 1 \cdot (x+y) \\ &= 1 \cdot x + 1 \cdot y + 1 \cdot x + 1 \cdot y \\ &= x + y + x + y. \end{aligned}$$

(c) By the above, $x + x + y + y = x + y + x + y$. Since the strengthened axiom A4 ensures that there are $a, b \in R$ such that $a + x = 0$ and $y + b = 0$, we may add a on the left and b on the right to obtain

$$\begin{aligned} a + x + x + y + y + b &= a + x + y + x + y + b, \\ \text{i.e.,} \quad 0 + x + y + 0 &= 0 + y + x + 0, \\ \text{i.e.,} \quad x + y &= y + x \quad \text{by the strengthened axiom A3.} \end{aligned}$$

42. If $a, b, c \in \mathbb{Z}$, then

$$([a][b])[c] = [ab][c] \quad \text{(def. of multiplication)}$$

$$
\begin{aligned}
&= [(ab)c] \quad \text{(def. of multiplication again)} \\
&= [a(bc)] \quad \text{(associativity of multiplication in } \mathbb{Z}) \\
&= [a][bc] \quad \text{(def. of multiplication again)} \\
&= [a]([b][c]) \quad \text{(def. of multiplication once more).}
\end{aligned}
$$

43. Suppose that $na = 0_R$, where n is a positive integer, and write $n = qm + r$ where $q, r \in \mathbb{Z}$ and $0 \leq r < m$. Then

$$
\begin{aligned}
0_R = na = (qm + r)a &= (qm)a + ra \\
&= q(ma) + ra \\
&= 0_R + ra \quad \text{because } ma = 0_R \\
&= ra.
\end{aligned}
$$

Therefore, because m is the least positive integer such that $ma = 0_R$, and because $0 \leq r < m$, we must have $r = 0$. Thus, $m \mid n$.

44. (a) (i) $2A = A + A = (A \cup A) \smallsetminus (A \cap A) = A \smallsetminus A = \emptyset = 0_{P(X)}$.

(ii) For brevity, we omit the dot for multiplication in this part.

$$
\begin{aligned}
(A + B)^2 &= (A + B)(A + B) \\
&= A(A + B) + B(A + B) \\
&= A^2 + AB + BA + B^2 \\
&= A^2 + AB + AB + B^2 \quad (P(X) \text{ is commutative}) \\
&= A^2 + 0_{P(X)} + B^2 \quad \text{by part } (i) \\
&= A^2 + B^2.
\end{aligned}
$$

(b) Let y, z be distinct elements of Y. Then $\{y\} \cdot \{z\} = \{y\} \cap \{z\} = \emptyset = 0_{P(Y)}$.

45. The sequences

$$
\begin{aligned}
e_1 &= (1, 0, 0, 1, 0, 0, 1, 0, 0, \ldots) \\
e_2 &= (0, 1, 0, 0, 1, 0, 0, 1, 0, \ldots) \\
e_3 &= (0, 0, 1, 0, 0, 1, 0, 0, 1, \ldots)
\end{aligned}
$$

have the required properties.

46. (a) $a = -1$, $b = 0$ (or the other way around).

(b) $a = 3/5$, $b = 4/5$, for example. There are infinitely many other possibilities, coming from Pythagorean triples.

(c) $a = \cos$, $b = \sin$ (or the other way around).

(d) $a = \{1\}$, $b = \{2, 3\}$, for example. (Remember that $A^2 = A$ for $A \in P(X)$.)

(e) $a = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $b = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, for example.

(f) $a = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $b = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, for example.

47. (a) In $\mathbb{Z}/n\mathbb{Z}$, $[a]$ is a unit if and only if n and a are coprime.

(b) $(\mathbb{Z}/21\mathbb{Z})^\times = \{[1], [2], [4], [5], [8], [10], [11], [13], [16], [17], [19], [20]\}$.

48. (a) If $x \in (\mathbb{Z}/7\mathbb{Z})^\times$, let n_x be the least positive integer n such that $x^n = [1]$. Then we have the following table:

x	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$
n_x	1	3	6	3	6	2

(b) For all $x \in (\mathbb{Z}/7\mathbb{Z})^\times$, n_x divides 6, the number of units in $\mathbb{Z}/7\mathbb{Z}$. This fact has an important generalization in group theory.

49. Let $\alpha = (a_n)_n$ be a unit in $\mathcal{S}(\mathbb{Z})$. Then there is $\beta = (b_n)_n \in \mathcal{S}(\mathbb{Z})$ such that $\alpha\beta = 1_{\mathcal{S}(\mathbb{Z})}$, i.e., $a_n b_n = 1$ for all $n \geq 0$. But then $a_n \in \mathbb{Z}^\times = \{1, -1\}$ for all n. Conversely, if $a_n \in \{1, -1\}$ for all n, then each a_n has an inverse b_n in $\mathbb{Z}$ (equal to a_n itself, in fact), and then the sequence $(b_n)_n$ is an inverse to $(a_n)_n$ in $\mathcal{S}(\mathbb{Z})$.

50. (a) We carry out the Euclidean algorithm on 455 and 11:

$$\begin{aligned} 455 &= 41 \cdot 11 + 4 \\ 11 &= 2 \cdot 4 + 3 \\ 4 &= 3 + 1, \end{aligned}$$

so

$$\begin{aligned} 1 &= 4 - 3 \\ &= 4 - (11 - 2 \cdot 4) = 3 \cdot 4 - 11 \\ &= 3(455 - 41 \cdot 11) - 11 = 3 \cdot 455 - 124 \cdot 11. \end{aligned}$$

Therefore,

$$[1] = [3 \cdot 455 - 124 \cdot 11] = [-124][11] = [331][11],$$

so $x^{-1} = [331]$.

(b) Observe that $455 = 5 \cdot 91$, so if $y = [5]$ and $z = [91]$, then y and z are non-zero and $yz = [5 \cdot 91] = [455] = 0$.

51. (a) (*i*) S is not closed under subtraction. For example, 1 and 10 are in S, but $1 - 10 = -9$ is congruent to 0 mod 9 and is therefore not in S.

(*ii*) Let $a, b \in S$. If either a or b is 0, then so is ab, so $ab \in S$ in that case. Hence, we may assume that a and b are both non-zero and therefore both congruent to 1 mod 9. Then $ab \equiv 1 \cdot 1 \bmod 9$, i.e., $ab \equiv 1 \bmod 9$, so $ab \in S$. Thus, S is closed under multiplication.

(*iii*) S is not a subring of R, because it is not closed under subtraction.

(b) (*i*) Let $a_1, b_1, a_2, b_2 \in \mathbb{Z}$ with b_1 and b_2 not divisible by 7. Then

$$\frac{a_1}{b_1} - \frac{a_2}{b_2} = \frac{a_1 b_2 - a_2 b_1}{b_1 b_2}. \tag{7}$$

Since 7 is prime, if it divided $b_1 b_2$ it would divide either b_1 or b_2, contrary to our assumption, so $7 \nmid b_1 b_2$. Thus, the rational number in (7) is in S, so S is closed under subtraction.

(*ii*) Again let $a_1, b_1, a_2, b_2 \in \mathbb{Z}$ with b_1 and b_2 not divisible by 7. Then

$$\frac{a_1}{b_1}\,\frac{a_2}{b_2} = \frac{a_1 a_2}{b_1 b_2},$$

which is in S by the same argument as above. Therefore, S is closed under multiplication.

(*iii*) S is non-empty: it contains $0 = 0/1$, because $7 \nmid 1$. Also, we have shown that S is closed under subtraction and multiplication, so S is a subring of R.

(c) (*i*) S is closed under subtraction, for if $a_1, a_2 \in \mathbb{Z}$, then

$$\frac{a_1}{2} - \frac{a_2}{2} = \frac{a_1 - a_2}{2} \in S.$$

(*ii*) S is not closed under multiplication. For example, $1/2 \in S$, but $(1/2)(1/2) = 1/4 \notin S$.

(*iii*) S is not a subring of $\mathbb{Q}$, because it is not closed under multiplication.

(d) (*i*) S is closed under subtraction. Indeed, let $A, B \in S$, which is to say that neither contains 0. Then

$$A - B = A + B \quad \text{by the hint}$$

$$= (A \smallsetminus B) \cup (B \smallsetminus A),$$

and this does not contain 0 either.

(*ii*) S is closed under multiplication, because if A and B do not contain 0, then neither does $A \cap B$.

(*iii*) S is a subring of $P(\mathbb{Z})$. It is non-empty because, for example, the empty set does not contain 0 and is therefore in S. Further, we have already seen that S is closed under subtraction and multiplication.

52. The set S is non-empty, because, of course, $\mathbb{Z} \in S$. It is also closed under multiplication, because if A and B both contain $\mathbb{Z}$, then so does their intersection, $A \cap B = A \cdot B$. However, S is not closed under subtraction. Indeed, let A be any element of S. Then $A - A = 0_{P(\mathbb{Q})} = \emptyset \notin S$. Therefore, S is not a subring of $P(\mathbb{Q})$.

53. (a) If $n(a, x) = (20, [3])$, then in particular $na = 20$, so $n \mid 20$. However, if $5 \mid n$, then $nx = [0] \neq [3]$, so there are no solutions in which $5 \mid n$. Thus, we are restricted to considering $n \in \{1, -1, 2, -2, 4, -4\}$. For each of these 6 values of n, there is a unique integer a such that $na = 20$, and a unique residue class x such that $nx = [3]$. To see the uniqueness of the residue class x, observe that $nx = [3]$ if and only if $[n]x = [3]$. But $[n]$ is invertible in $\mathbb{Z}/5\mathbb{Z}$ because $5 \nmid n$, so the unique x is $[n]^{-1}[3]$. Thus, the solutions are as follows:

n	a	x
1	20	[3]
-1	-20	[2]
2	10	[4]
-2	-10	[1]
4	5	[2]
-4	-5	[3]

(b) This time, we are restricted to considering integers n that divide 5, i.e., $n \in \{1, -1, 5, -5\}$. If $5 \nmid n$ (which in this case means simply $n \in \{1, -1\}$), then the equation $nx = [0]$ has the unique solution $x = [0]$. On the other hand, if $5 \mid n$ (i.e., if $n \in \{5, -5\}$), then every $x \in \mathbb{Z}/5\mathbb{Z}$ is a solution to $nx = [0]$. The solutions to $n(a, x) = (5, [0])$ are therefore the following:

n	a	x
1	5	[0]
−1	−5	[0]
5	1	[0]
5	1	[1]
5	1	[2]
5	1	[3]
5	1	[4]
−5	−1	[0]
−5	−1	[1]
−5	−1	[2]
−5	−1	[3]
−5	−1	[4]

54. (a) Let $A = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \in S$ and $B = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \in R$. Then $BA = B \notin S$. Therefore, S is not an ideal of R.

(b) Let $f \in S$ and $g \in R$. Then for all $x \in \mathbb{Z}$,

$$(g \cdot f)(x) = g(x)f(x) = g(x) \cdot 0 = 0,$$

so $g \cdot f \in S$. Thus, S is an ideal of R. (The ring R is commutative, so we do not need to check the condition $f \cdot g \in S$ separately.)

55. (a) The set S is not an ideal of $M_2(\mathbb{Z})$. Indeed, the identity matrix I is in S, but if A is any matrix in which the top-right entry is not divisible by n, then $AI = A \notin S$.

(b) The set S is a subring of $M_2(\mathbb{Z})$. We have already seen that it is non-empty. Now take integers $a, b, c, d, a', b', c', d'$ such that n divides b and b'. Then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} - \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a - a' & b - b' \\ c - c' & d - d' \end{pmatrix},$$

and $b - b'$ is divisible by n because both of b and b' are. Thus, S is closed under subtraction. Further, for the same two matrices,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix},$$

and again $ab' + bd'$ is divisible by n because b and b' are. The set S is therefore also closed under multiplication.

56. In our answer, we will let polynomials f and g have coefficients as follows:

$$f = \sum_{i=0}^{m} a_i x^i, \quad g = \sum_{j=0}^{n} b_j x^j.$$

We will then let fg have coefficients c_k, i.e.,

$$fg = \sum_{k=0}^{m+n} c_k x^k,$$

so that $c_0 = a_0 b_0$ and $c_1 = a_0 b_1 + a_1 b_0$.

(a) (*i*) S is an ideal of $\mathbb{Z}[x]$. Note that S is non-empty, because it contains the zero polynomial. It is closed under subtraction, because if n divides the coefficients a_0, a_1, b_0, b_1 in f and g, then it divides $a_0 - b_0$ and $a_1 - b_1$, the corresponding coefficients in $f - g$. As for multiplication by ring elements, we note that if g (but not necessarily f) is in S, so that n divides b_0 and b_1, then n also divides $a_0 b_0 = c_0$ and $a_0 b_1 + a_1 b_0 = c_1$, so $fg \in S$.

(*ii*) In this course, every ideal is a subring, so S is a subring of $\mathbb{Z}[x]$.

(b) (*i*) T is not an ideal of $\mathbb{Z}[x]$. For example, $1 \in T$ but $x \cdot 1 = x$ is not in T, because $n \geq 2$ does not divide the coefficient 1.

(*ii*) T is a subring of $\mathbb{Z}[x]$. We have already seen that it is non-empty. Now suppose that $f, g \in T$, so that n divides a_1, b_1. Then n also divides $a_1 - b_1$ and $a_0 b_1 + a_1 b_0 = c_1$. Thus, T is closed under subtraction and multiplication.

57. The set S is an ideal of $\mathcal{F}$. For brevity, let $h \in \mathcal{F}$ be the function $x \mapsto \sin(x^3)$. Then $S = \{f \in \mathcal{F} \mid hf = 0\}$. We know that S is non-empty, because the zero function (for example) is in S. Now suppose that $f, g \in S$, i.e., $hf = hg = 0$. Then $h(f - g) = hf - hg = 0 - 0 = 0$, so $f - g \in S$. Thus, S is closed under subtraction. Finally, if $f \in S$ and $g \in \mathcal{F}$, then

$$h \cdot (fg) = (hf) \cdot g = 0 \cdot g = 0,$$

so $fg \in S$. We do not need to show separately that $gf \in S$, because $\mathcal{F}$ is commutative.

58. Note that $g(1) = -1$. Therefore, if $f \in \mathbb{Z}[x]$, then $f + I = g + I$ if and only if $f - g \in I$, if and only if $(f - g)(1) = 0$, if and only if $f(1) - g(1) = 0$, if and only if $f(1) = -1$. Hence, from the table

f	$f(1)$
f_1	-1
f_2	1
f_3	2
f_4	-1

we see that $f_1 + I$ and $f_4 + I$ are equal to $g + I$, but $f_2 + I$ and $f_3 + I$ are not. In the case of f_4, another way to see that $f_4 + I = g + I$ is to observe that $f_4 = 6x^4(x-1) + g$.

59. (a) (i) $f(x) = (3x^2 - 5x + 7) \cdot x - 5 \cdot 2$.

(ii)

$$\begin{aligned} f(x) &= (3x^2 - 5x + 7)(3(x-4) - 2(x-6)) - 5((x-4) - (x-6)) \\ &= (9x^2 - 15x + 16)(x-4) + (-6x^2 + 10x - 9)(x-6). \end{aligned}$$

(b) An element of $(x-4, x-6)_{\mathbb{Z}[x]}$ takes the form $f_1(x)(x-4) + f_2(x)(x-6)$ with $f_1, f_2 \in \mathbb{Z}[x]$ and therefore has constant term $k_1(-4) + k_2(-6)$, where $k_1, k_2 \in \mathbb{Z}[x]$ are the constant terms of f_1 and f_2. But $k_1(-4) + k_2(-6)$ is even, whereas the constant term of $x^2 + 2x + 3$ is odd.

60. (a) The zero sequence is in I, because all of its terms are zero, so certainly the terms for $n < 5$ are zero. Therefore, I is non-empty. Now let $\alpha = (a_n)_n$ and $\beta = (b_n)_n$ be in I, i.e., $a_n = b_n = 0$ for $n < 5$. The nth term of $\alpha - \beta$ is $a_n - b_n$, and when $n < 5$, $a_n - b_n = 0 - 0 = 0$, so $\alpha - \beta \in I$. Finally, if $\alpha = (a_n)_n \in I$ and $\gamma = (c_n)_n$ is any sequence in $\mathcal{S}(\mathbb{R})$, then the nth term of $\gamma\alpha$ is $c_n a_n$, and when $n < 5$, $c_n a_n = c_n \cdot 0 = 0$, so $\gamma\alpha \in I$. Thus, I is an ideal of $\mathcal{S}(\mathbb{R})$.

(b) Let

$$\begin{aligned} \alpha' &= (2, -1, 1, 3, 6, 0, 0, 0, \ldots) \\ \beta' &= (-4, 3, 5, -6, 2, 0, 0, 0, \ldots) \end{aligned}$$

and observe that $\alpha + I = \alpha' + I$ and $\beta + I = \beta' + I$. Then

$$\begin{aligned} (\alpha + I) + (\beta + I) &= (\alpha' + I) + (\beta' + I) \\ &= (-2, 2, 6, -3, 8, 0, 0, 0, \ldots) + I, \end{aligned}$$

and

$$(\alpha + I)(\beta + I) = (\alpha' + I)(\beta' + I)$$

$$= (-8, -3, 5, -18, 12, 0, 0, 0, \ldots) + I.$$

61. We have $f + I = (-224x + 2) + I$ and $g + I = (312x + 1) + I$, so

$$\begin{aligned}(f + I) + (g + I) &= ((-224x + 2) + I) + ((312x + 1) + I) \\ &= (88x + 3) + I,\end{aligned}$$

$$\begin{aligned}\text{and} \quad (f + I)(g + I) &= ((-224x + 2) + I)((312x + 1) + I) \\ &= (-224x + 2)(312x + 1) + I \\ &= ((-224 \cdot 1 + 2 \cdot 312)x + 2 \cdot 1) + I \quad (x^2 \in I) \\ &= (400x + 2) + I.\end{aligned}$$

62. Note that if $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, then $f \in I$ if and only if 6 divides a_1 and a_0.

(a) Let $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. Every monomial $a_k x^k$ with $k \geq 2$ is in I because $6 \mid 0$, so

$$[f] = [a_1 x + a_0] = [a_1][x] + [a_0].$$

Further, if $r_1 \in \{0, \ldots, 5\}$ and $r_2 \in \{0, \ldots, 5\}$ are the remainders on dividing a_1 and a_0 (respectively) by 6, then 6 divides $a_1 - r_1$ and $a_0 - r_0$, so $[a_1] = [r_1]$ and $[a_0] = [r_0]$.

(b)

$$\begin{aligned}&([a][x] + [b])([c][x] + [d]) \\ &= [a][c][x^2] + ([a][d] + [b][c])[x] + [b][d] \\ &= ([a][d] + [b][c])[x] + [b][d] \quad \text{because } x^2 \in I \\ &= [ad + bc][x] + [bd].\end{aligned}$$

(c) We are to solve the equation $([a][x] + [b])([x] + [1]) = [1]$ for $a, b \in \{0, \ldots, 5\}$, i.e.,

$$[a + 1][x] + [b] = [1]$$

by the previous part. The equation obviously has the solution $b = 1$ and $a = 5$, so $[x] + [1]$ is a unit and has inverse $[5][x] + [1]$.

63. Note that the functions

$$x \mapsto \cos(3x) \ln((x^2 - 2x + 2)^2)$$
$$x \mapsto e^{3x} \sin((x^2 - 4x + 5)\pi)$$

both take the value 0 at $x = 1$ and are therefore both in I, so $f + I$ is represented by the polynomial $2x$, and $g + I$ by $3x^2 + 1$. Therefore, $(f + I) + (g + I) = h + I$ where $h(x) = 2x + (3x^2 + 1) = 3x^2 + 2x + 1$, and $(f + I)(g + I) = j + I$ where $j(x) = 2x(3x^2 + 1) = 6x^3 + 2x$.

64. (a) If $f = a_n x^n + \cdots + a_1 x + a_0$, then $f(0) = 0$ if and only if $a_0 = 0$. In this case, $f = a_n x^n + \cdots + a_1 x = x(a_n x^{n-1} + \cdots + a_1)$.

(b) (i) $f_1(0) = f(a) = 0$, so $f_1(x) = x f_2(x)$ for some $f_2 \in \mathbb{Q}[x]$ by part (a), and so

$$f(x) = f_1(x - a) = (x - a) f_2(x - a) = (x - a) f_3(x)$$

where $f_3(x) = f_2(x - a)$.

(ii) We have $0 = f(b) = (b - a) f_3(b)$ by part (i), so because $a \neq b$, we may cancel $b - a$ to leave $0 = f_3(b)$. Hence, applying the same argument as above but with f_3 in place of f, and b in place of a, we obtain $f_3(x) = (x - b)g(x)$ for some $g \in \mathbb{Q}[x]$. Combining this with $f(x) = (x - a) f_3(x)$, we arrive at $f(x) = (x - a)(x - b)g(x)$.

65. (a) Let $f = x^2 - 3x + 2 = (x - 1)(x - 2)$. If $g \in \mathbb{Z}[x]$, then $(gf)(1) = g(1)f(1) = g(1) \cdot 0 = 0$, and similarly $(gf)(2) = 0$. Conversely, suppose that $h \in \mathbb{Z}[x]$ satisfies $h(1) = h(2) = 0$. Then by Question 64, $h(x) = (x - 1)(x - 2)g(x)$ for some $g \in \mathbb{Z}[x]$, i.e., $h = fg = gf$, so $h \in I$.

(b) Note that $g(1) = 1/f(1)$ and $g(2) = 1/f(2)$, so the polynomial $fg - 1$ evaluates to 0 at 1 and 2 and therefore lies in I by part (a). Hence, $(f + I)(g + I) = fg + I = 1 + I$.

66. (a)

$$\begin{aligned}(A)_{P(X)} &= \{BA \mid B \in P(X)\} \\ &= \{B \cap A \mid B \in P(X)\} \\ &= \{C \in P(X) \mid C \subseteq A\},\end{aligned}$$

because $B \cap A \subseteq A$, and conversely every subset C of A can be expressed as $C = C \cap A$. Now just observe that $\{C \in P(X) \mid C \subseteq A\} = P(A)$.

(b)

$$\begin{aligned}B - BA &= B + BA \\ &= (B \cup (B \cap A)) \setminus (B \cap (B \cap A)) \\ &= B \setminus (B \cap A) = B \setminus A.\end{aligned}$$

(c) $B + P(A) = (B - BA) + P(A)$ because $BA \in P(A)$. But $B - BA \in P(B \setminus A)$ by the previous part.

67. (a) Let $a, b, c, d \in \mathbb{Q}$. Then

$$\begin{aligned}\varphi((a,b)+(c,d)) &= \varphi(a+c, b+d)\\ &= ((a+c)+(b+d), (a+c)-(b+d))\\ &= ((a+b)+(c+d), (a-b)+(c-d))\\ &= (a+b, a-b)+(c+d, c-d)\\ &= \varphi(a,b)+\varphi(c,d),\end{aligned}$$

and

$$\begin{aligned}\varphi((a,b)\cdot(c,d)) &= \varphi(ac+bd, ad+bc)\\ &= ((ac+bd)+(ad+bc), (ac+bd)-(ad+bc))\\ &= (ac+ad+bc+bd, ac-ad-bc+bd)\\ &= ((a+b)(c+d), (a-b)(c-d))\\ &= (a+b, a-b)(c+d, c-d)\\ &= \varphi(a,b)\varphi(c,d).\end{aligned}$$

Thus, φ respects both addition and multiplication and therefore is a ring homomorphism.

(b) If $(a+b, a-b) = (0,0)$, then $a+b = a-b = 0$, and the only solution to these simultaneous equations is $a = b = 0$. Thus, $\mathrm{Ker}(\varphi) = \{(0,0)\}$, so φ is injective.

(c) Let $(x,y) \in S$. We wish to show that the equation $\varphi(a,b) = (x,y)$ has a solution $(a,b) \in R$, and to express that solution in terms of x and y. Now, the equation says

$$(a+b, a-b) = (x,y),$$

i.e., $a+b = x$ and $a-b = y$, which has the unique solution

$$a = \frac{1}{2}(x+y), \quad b = \frac{1}{2}(x-y).$$

Thus, the unique element of R mapping to (x,y) is $(\frac{1}{2}(x+y), \frac{1}{2}(x-y))$.

(d) In S, it is easy to construct non-zero elements whose product is zero: Let $x, y \in \mathbb{Q} \setminus \{0\}$, and observe that $(x,0)(0,y) = (0,0)$. Therefore, $\varphi^{-1}(x,0) \cdot \varphi^{-1}(0,y)$ is zero in R, i.e.,

$$(\tfrac{1}{2}x, \tfrac{1}{2}x) \cdot (\tfrac{1}{2}y, -\tfrac{1}{2}y) = (0,0).$$

For example, $(1,1) \cdot (1,-1) = (0,0)$ in R (take $x = y = 2$).

68. (a) The map φ is not a ring homomorphism, because it does not respect multiplication. To see this, observe that

$$\varphi(1^2) = \varphi(1) = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

$$\text{while} \quad \varphi(1)^2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^2 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}.$$

Note, however, that φ does respect addition.

(b) The map ψ is a ring homomorphism. To see this, let $a, b \in \mathbb{Z}$. Then

$$\begin{aligned} \psi(a+b) &= \begin{pmatrix} 3(a+b) & -3(a+b) \\ 2(a+b) & -2(a+b) \end{pmatrix} \\ &= \begin{pmatrix} 3a & -3a \\ 2a & -2a \end{pmatrix} + \begin{pmatrix} 3b & -3b \\ 2b & -2b \end{pmatrix} \\ &= \psi(a) + \psi(b), \end{aligned}$$

so ψ respects addition. For multiplication, it is easier, in the case of this map, to begin with $\psi(a)\psi(b)$ rather than $\psi(ab)$. Thus,

$$\begin{aligned} \psi(a)\psi(b) &= \begin{pmatrix} 3a & -3a \\ 2a & -2a \end{pmatrix} \begin{pmatrix} 3b & -3b \\ 2b & -2b \end{pmatrix} \\ &= \begin{pmatrix} 9ab - 6ab & -9ab + 6ab \\ 6ab - 4ab & -6ab + 4ab \end{pmatrix} \\ &= \begin{pmatrix} 3ab & -3ab \\ 2ab & -2ab \end{pmatrix} \\ &= \psi(ab). \end{aligned}$$

69. The map φ does not respect addition. One way to see this is to observe that $\varphi(a) \leq 1$ for all $a \in \mathbb{Z}$. In particular, $\varphi(1+1) \leq 1 < 2 = \varphi(1) + \varphi(1)$, so $\varphi(1+1) \neq \varphi(1) + \varphi(1)$. Alternatively, one could consider $\varphi(1 + (-1))$. However, φ does respect multiplication, as we may see as follows. Let $a, b \in \mathbb{Z}$. If either a or b is zero, then

$$\varphi(ab) = \varphi(0) = 0 = \varphi(a)\varphi(b).$$

Assume, then, that a and b are both non-zero. Then letting $\lambda = \frac{1}{p}$ for brevity, we see that

$$\varphi(ab) = \lambda^{v_p(ab)} = \lambda^{v_p(a)+v_p(b)} = \lambda^{v_p(a)}\lambda^{v_p(b)} = \varphi(a)\varphi(b).$$

70. (a) If $f, g \in \mathcal{F}$, then

$$\varphi(f+g) = ((f+g)(n))_n \quad \text{(definition of } \varphi)$$

$$= (f(n) + g(n))_n \quad \text{(definition of addition in } \mathcal{F}\text{)}$$
$$= (f(n))_n + (g(n))_n \quad \text{(definition of addition in } \mathcal{S}(\mathbb{R})\text{)}$$
$$= \varphi(f) + \varphi(g) \quad \text{(definition of } \varphi\text{)},$$

and

$$\varphi(f \cdot g) = ((f \cdot g)(n))_n \quad \text{(definition of } \varphi\text{)}$$
$$= (f(n)g(n))_n \quad \text{(definition of multiplication in } \mathcal{F}\text{)}$$
$$= (f(n))_n (g(n))_n \quad \text{(definition of multiplication in } \mathcal{S}(\mathbb{R})\text{)}$$
$$= \varphi(f)\varphi(g) \quad \text{(definition of } \varphi\text{)}.$$

(b) Let us first show that φ is surjective. Given a sequence $(a_n)_n \in \mathcal{S}(\mathbb{R})$, we define $f \in \mathcal{F}$ by letting $f(n) = a_n$ if $n \in \mathbb{Z}_{\geq 0}$ and $f(x) = 0$ for all $x \in \mathbb{R} \smallsetminus \mathbb{Z}_{\geq 0}$. Then $\varphi(f) = (f(n))_n = (a_n)_n$.

Next,

$$\begin{aligned}\operatorname{Ker}(\varphi) &= \{f \in \mathcal{F} \mid \varphi(f) = (0, 0, 0, \ldots)\} \\ &= \{f \in \mathcal{F} \mid f(n) = 0 \text{ for all } n \in \mathbb{Z}_{\geq 0}\} \\ &= I.\end{aligned}$$

The First Isomorphism Theorem therefore gives us the desired isomorphism $\overline{\varphi} : \mathcal{F}/I \to \mathcal{S}(\mathbb{R})$.

(c) We simply need a non-constant function $f \in \mathcal{F}$ such that $f - \mathbf{1} \in I$. The condition $f - \mathbf{1} \in I$ holds if and only if $(f - \mathbf{1})(n) = 0$ for all $n \in \mathbb{Z}_{\geq 0}$, i.e., $f(n) = 1$ for all $n \in \mathbb{Z}_{\geq 0}$. There are many such functions. Here are two possibilities, the first continuous, the second not:

$$f : x \mapsto 1 + \sin(\pi x)$$

$$f : x \mapsto \begin{cases} 0 & \text{if } x = 1/2 \\ 1 & \text{otherwise} \end{cases}$$

71. (a) If $\alpha = (a_n)_n$ and $\beta = (b_n)_n$ are in $\mathcal{S}(\mathbb{R})$, then

$$\varphi(\alpha + \beta) = \varphi((a_n + b_n)_n) \quad \text{(definition of addition in } \mathcal{S}(\mathbb{R})\text{)}$$
$$= (a_{n+1} + b_{n+1})_n \quad \text{(definition of } \varphi\text{)}$$
$$= (a_{n+1})_n + (b_{n+1})_n \quad \text{(definition of addition in } \mathcal{S}(\mathbb{R})\text{)}$$
$$= \varphi(\alpha) + \varphi(\beta) \quad \text{(definition of } \varphi\text{)},$$

and

$$\varphi(\alpha\beta) = \varphi((a_n b_n)_n) \quad \text{(definition of multiplication in } \mathcal{S}(\mathbb{R})\text{)}$$

$$= (a_{n+1}b_{n+1})_n \quad \text{(definition of } \varphi\text{)}$$
$$= (a_{n+1})_n(b_{n+1})_n \quad \text{(definition of multiplication in } \mathcal{S}(\mathbb{R})\text{)}$$
$$= \varphi(\alpha)\varphi(\beta) \quad \text{(definition of } \varphi\text{)}.$$

(b) We first show that φ is surjective. Given a sequence $\beta = (b_n)_n \in \mathcal{S}(\mathbb{R})$, define $\alpha = (a_n)_n \in \mathcal{S}(\mathbb{R})$ by

$$a_n = \begin{cases} 0 & \text{if } n = 0 \\ b_{n-1} & \text{otherwise.} \end{cases}$$

Then $\varphi(\alpha) = (a_{n+1})_n = (b_n)_n = \beta$.

Next, observe that $\text{Ker}(\varphi)$ consists of the sequences $(a_n)_n \in \mathcal{S}(\mathbb{R})$ such that $a_n = 0$ if $n \geq 1$. In particular, the sequence $(1, 0, 0, 0, \ldots)$ is a non-zero sequence in the kernel. Therefore, the ideal $I = \text{Ker}(\varphi)$ is a non-zero ideal, and by the First Isomorphism Theorem, $\mathcal{S}(\mathbb{R})/I \cong \mathcal{S}(\mathbb{R})$.

72. (a) Let $f = x^2 + x - 20 = (x+5)(x-4)$, and note that $f(-5) = f(4) = 0$. If $g \in (f)_{\mathbb{Q}[x]} = f\mathbb{Q}[x]$, i.e., $g = fh$ where $h \in \mathbb{Q}[x]$, then $g(-5) = f(-5)h(-5) = 0$ and $g(4) = f(4)h(4) = 0$, so $g \in \text{Ker}(\varphi)$. Conversely, if $g \in \text{Ker}(\varphi)$, so that $g(-5) = g(4) = 0$, then by Question 64, $g = (x+5)(x-4)h$ for some $h \in \mathbb{Q}[x]$, i.e., $g = fh \in (f)_{\mathbb{Q}[x]}$.

(b) Observe that $\varphi(x-4) = (-9, 0)$ and $\varphi(x+5) = (0, 9)$, so $\varphi(-\frac{1}{9}(x-4)) = (1, 0)$ and $\varphi(\frac{1}{9}(x+5)) = (0, 1)$. Hence, if $a, b \in \mathbb{Q}$,

$$\varphi(-\tfrac{a}{9}(x-4) + \tfrac{b}{9}(x+5)) = (a, b).$$

(c) We have shown that φ is surjective and has kernel I, so by the First Isomorphism Theorem, $\mathbb{Q}[x]/I \cong \mathbb{Q}^2$.

73. (a) Let $x \in X$. Then

$$\begin{aligned} & x \in X_{f+g} \\ \iff & (f+g)(x) = [1] \\ \iff & f(x) + g(x) = [1] \\ \iff & \Big(f(x) = [1] \text{ and } g(x) = [0]\Big) \text{ or } \Big(f(x) = [0] \text{ and } g(x) = [1]\Big) \\ \iff & x \in X_f \smallsetminus X_g \text{ or } x \in X_g \smallsetminus X_f \\ \iff & x \in (X_f \smallsetminus X_g) \cup (X_g \smallsetminus X_f) = X_f + X_g. \end{aligned}$$

Also,

$$x \in X_{fg} \iff (fg)(x) = [1]$$

$$\begin{aligned}
&\iff f(x)g(x) = [1] \\
&\iff f(x) = [1] \text{ and } g(x) = [1] \\
&\iff x \in X_f \text{ and } x \in X_g \\
&\iff x \in X_f \cap X_g = X_f X_g.
\end{aligned}$$

(b) If $f \in \mathrm{Ker}(\varphi)$, then $X_f = \emptyset$, i.e., there are no $x \in X$ such that $f(x) = [1]$, i.e., $f(x) = [0]$ for all $x \in X$, which is to say that f is the zero function. Thus, φ is injective. For surjectivity, let $A \in P(X)$, and define

$$\begin{aligned}
f : X &\to \mathbb{Z}/2\mathbb{Z} \\
x &\mapsto \begin{cases} [1] & \text{if } x \in A, \\ [0] & \text{otherwise.} \end{cases}
\end{aligned}$$

Then

$$\varphi(f) = X_f = \{x \in X \mid f(x) = [1]\} = A.$$

74. Let $a, b, c, d \in \mathbb{Z}$. Then

$$\begin{aligned}
\varphi((a + b\sqrt{6}) + (c + d\sqrt{6})) &= \varphi((a + c) + (b + d)\sqrt{6}) \\
&= [(a + c) + 4(b + d)] \\
&= [(a + 4b) + (c + 4d)] \\
&= [a + 4b] + [c + 4d] \\
&= \varphi(a + b\sqrt{6}) + \varphi(c + d\sqrt{6}).
\end{aligned}$$

Also,

$$\begin{aligned}
\varphi((a + b\sqrt{6})(c + d\sqrt{6})) &= \varphi(ac + 6bd + (ad + bc)\sqrt{6}) \\
&= [ac + 6bd + 4ad + 4bc], \qquad (8) \\
\text{and} \quad \varphi(a + b\sqrt{6})\varphi(c + d\sqrt{6}) &= [a + 4b][c + 4d] \\
&= [ac + 4ad + 4bc + 16bd],
\end{aligned}$$

which is equal to the expression in (8) because $16 \equiv 6 \bmod 5$.

75. (a) $\varphi(1 + \sqrt{6}) = [1 + 4] = [5] = [0]$. Therefore, because $\mathrm{Ker}(\varphi)$ is an ideal, $y(1 + \sqrt{6}) \in \mathrm{Ker}(\varphi)$ for all $y \in \mathbb{Z}[\sqrt{6}]$.

(b) (*i*) Because $x \in \mathrm{Ker}(\varphi)$, $[a + 4b] = [0]$, so $5 \mid a + 4b$, i.e., $a + 4b = 5c$ for some $c \in \mathbb{Z}$, so $a = 5c - 4b$.

(*ii*) By part (*i*),

$$x = a + b\sqrt{6} = 5c - 4b + b\sqrt{6} = 5c - 5b + b + b\sqrt{6}$$

$$= 5d + b(1+\sqrt{6})$$

where $d = c - b$.

(*iii*) By part (*ii*) and the fact that $5 = (\sqrt{6}-1)(1+\sqrt{6})$,

$$\begin{aligned} x &= (\sqrt{6}-1)(1+\sqrt{6})d + b(1+\sqrt{6}) \\ &= ((\sqrt{6}-1)d + b)(1+\sqrt{6}) \\ &= y(1+\sqrt{6}) \end{aligned}$$

where $y = (\sqrt{6}-1)d + b$.

(c) Observe that φ is surjective, because if $a \in \mathbb{Z}$, then the element $[a]$ of $\mathbb{Z}/5\mathbb{Z}$ is equal to $\varphi(a)$. Further, we showed in parts (a) and (b) that $\mathrm{Ker}(\varphi) = I$. Therefore, by the First Isomorphism Theorem, $\mathbb{Z}[\sqrt{6}]/I \cong \mathbb{Z}/5\mathbb{Z}$.

76. (a) From the table

α	[0]	[1]	[2]	[3]	[4]
α^2	[0]	[1]	[4]	[4]	[1]

we see that α^2 is never equal to [2] or [3] = [−2].

(b) If $x^2 - 10y^2 = k$, then $x^2 \equiv k \bmod 5$, so in $\mathbb{Z}/5\mathbb{Z}$ we have $[x]^2 = [k] \in \{[2], [-2]\}$. But this contradicts part (a).

77. (a)

Case	$k \in A$	$k \in B$	$k \in (A \cup B) \setminus (A \cap B)$	$k \in A \cap B$
(i)	N	N	N	N
(ii)a	Y	N	Y	N
(ii)b	N	Y	Y	N
(iii)	Y	Y	N	Y

(b) A more insightful justification than the following can be given, one that allows us to generalize the situation, but we give this case-by-case argument for the sake of simplicity. Recall that addition in $P(\mathbb{Z})$ is given by $A + B = (A \cup B) \setminus (A \cap B)$, and multiplication by $AB = A \cap B$. Therefore, from the table we deduce the following:

Case (i): $\varphi(A) + \varphi(B) = [0] + [0] = [0] = \varphi(A + B)$

Case (ii)a: $\varphi(A) + \varphi(B) = [1] + [0] = [1] = \varphi(A + B)$

Case (ii)b: $\varphi(A) + \varphi(B) = [0] + [1] = [1] = \varphi(A + B)$

Case (iii): $\varphi(A) + \varphi(B) = [1] + [1] = [0] = \varphi(A + B)$

In all cases, $\varphi(A) + \varphi(B) = \varphi(A + B)$. Multiplication is verified similarly:

Case (i): $\varphi(A)\varphi(B) = [0][0] = [0] = \varphi(AB)$

Case (ii)a: $\varphi(A)\varphi(B) = [1][0] = [0] = \varphi(AB)$

Case (ii)b: $\varphi(A)\varphi(B) = [0][1] = [0] = \varphi(AB)$

Case (iii): $\varphi(A)\varphi(B) = [1][1] = [1] = \varphi(AB)$

Thus, $\varphi(A)\varphi(B) = \varphi(AB)$ for all A, B.

(c) The map φ is surjective, because $\varphi(\emptyset) = [0]$ and $\varphi(\{k\}) = [1]$. The kernel is

$$\{A \in P(\mathbb{Z}) \mid \varphi(A) = [0]\} = \{A \in P(\mathbb{Z}) \mid k \notin A\} = I,$$

so the First Isomorphism Theorem yields the desired isomorphism $\overline{\varphi} : P(\mathbb{Z})/I \to \mathbb{Z}/2\mathbb{Z}$.

78. (a) Note that neither $x+2$ nor $x-3$ is in the ideal $I = (x^2 - x + 6)_{\mathbb{Q}[x]}$, because every non-zero polynomial in I has degree at least 2, so $(x+2)+I$ and $(x-3)+I$ are both non-zero in $\mathbb{Q}[x]/I$. However, their product is $(x+2)(x-3)+I = (x^2 - x + 6) + I = I$, the zero element of $\mathbb{Q}[x]/I$. Thus, $\mathbb{Q}[x]/I$ is not an integral domain (and therefore not a field either).

(b) We saw in class that $\mathbb{Z}[x]/(x)_{\mathbb{Z}[x]} \cong \mathbb{Z}$. Therefore, because $\mathbb{Z}$ is an integral domain but not a field, the same is true of $\mathbb{Z}[x]/(x)_{\mathbb{Z}[x]}$.

(c) The ring $P(\mathbb{Z})$ is not an integral domain (and therefore not a field either), because if a, b are any two distinct integers, $\{a\} \cdot \{b\} = \{a\} \cap \{b\} = \emptyset$.

(d) For simplicity, let $I = I_p$. The ring $\mathbb{Z}[x]/I$ is a field. One way to see this is to observe that the map

$$\begin{aligned} \varphi : \mathbb{Z}[x] &\to \mathbb{Z}/p\mathbb{Z} \\ f &\mapsto [f(0)] \end{aligned}$$

is a surjective ring homomorphism with kernel I. That it respects addition and multiplication is a straightforward exercise, and surjectivity is clear because a residue class $[a]$ is the image of the constant polynomial a. Further, $\mathrm{Ker}(\varphi) = \{f \in \mathbb{Z}[x] \mid [f(0)] = [0]\} = I$. Hence, by the First Isomorphism Theorem, $\mathbb{Z}[x]/I \cong \mathbb{Z}/p\mathbb{Z}$. Therefore, because p is prime, $\mathbb{Z}/p\mathbb{Z}$ is a field, so the same is true of $\mathbb{Z}[x]/I$.

A direct proof that $\mathbb{Z}[x]/I$ is a field could go like this: Let $f + I$ be a non-zero element of $\mathbb{Z}[x]/I$, so p does not divide $f(0)$. Note that $f - f(0) \in I$, so $f + I = f(0) + I$. Now, because $p \nmid f(0)$ and p is prime, there is $b \in \mathbb{Z}$ such that $bf(0) \equiv 1 \bmod p$, so $bf(0) - 1 \in I$. Therefore,

$$(b + I)(f + I) = (b + I)(f(0) + I) = bf(0) + I = 1 + I.$$

(e) Note that R is an integral domain, because it is a non-zero unital subring of $\mathbb{R}$. However, it is not a field. To see this, we show that 2 has no multiplicative

inverse in R. Suppose it did, say $2(x + y\sqrt{2}) = 1$ (where $x, y \in \mathbb{Z}$). Then $2y\sqrt{2} = 1 - 2x$, so squaring both sides, we obtain $8y^2 = (1 - 2x)^2$. But the left-hand side of this equation is even, and the right-hand side odd, so we have arrived at a contradiction.

Another approach is to use the fact that $\sqrt{2}$ is not rational. This fact implies that if $x + y\sqrt{2} = 0$, where $x, y \in \mathbb{Z}$, then $x = y = 0$. So, if $m \in \mathbb{Z}$ is invertible in R, meaning that there are $x, y \in \mathbb{Z}$ such that $m(x + y\sqrt{2}) = 1$, then $mx + my\sqrt{2} = 1$, and so $mx = 1$ (and $my = 0$). Therefore, $m \in \{1, -1\}$. Thus, any integer m not equal to 1 or -1 has no multiplicative inverse in R.

Yet another approach (which again uses the fact that $\sqrt{2}$ is not rational) is to use the norm. We know from the notes that an element of R is a unit if and only if its norm is ± 1, so we have only to observe that R contains non-zero elements of norm other than ± 1, such as 2 (which has norm 4).

(f) The ring R is a field. To see this, suppose that $\alpha = x + y\sqrt{-3} \in R$, where $x, y \in \mathbb{Q}$, and assume that $\alpha \neq 0$ (so at least one of x and y is non-zero). Then

$$\alpha(x - y\sqrt{-3}) = (x + y\sqrt{-3})(x - y\sqrt{-3}) = x^2 + 3y^2,$$

so if $\nu = x^2 + 3y^2 \in \mathbb{Q}$ and $\beta = \frac{x}{\nu} - \frac{y}{\nu}\sqrt{-3} \in R$, then $\alpha\beta = 1$.

79. (a) $\mathcal{F}$ is not an integral domain. For example, define $f, g \in \mathcal{F}$ by

$$f(x) = \begin{cases} 1 & \text{if } x > 0 \\ 0 & \text{otherwise} \end{cases}$$

$$g(x) = \begin{cases} 1 & \text{if } x < 0 \\ 0 & \text{otherwise} \end{cases}$$

Then neither f nor g is the zero function in $\mathcal{F}$, but $f \cdot g$ is, because

$$(f \cdot g)(x) = \begin{cases} 0(g(x)) = 0 & \text{if } x \leq 0 \\ (f(x))0 = 0 & \text{if } x \geq 0 \end{cases}$$

(b) $\mathcal{F}/I$ is an integral domain. There are various ways to see this.

Solution 1: Suppose $f, g \in \mathcal{F}$ satisfy $(f + I)(g + I) = I$. Then $(fg) + I = I$, so $fg \in I$, and so $(fg)(1) = 0$. But this says that $f(1)g(1) = 0$. Hence, because $\mathbb{R}$ is an integral domain (a field, in fact), either $f(1) = 0$, in which case $f \in I$ so $f + I = I$, or $g(1) = 0$, in which case $g \in I$ so $g + I = I$.

Solution 2: This is almost the same as the first solution. Embedded in the first solution is a proof that I is a prime ideal. Therefore, by a result from the course, $\mathcal{F}/I$ is an integral domain.

Solution 3: The ideal I is the kernel of the ring homomorphism $\mathcal{F} \to \mathbb{R}$ that sends f to $f(1)$. Therefore, by the First Isomorphism Theorem, $\mathcal{F}/I$ is isomorphic to a subring of $\mathbb{R}$. All non-zero subrings of $\mathbb{R}$ are integral domains because $\mathbb{R}$ is, so we are done.

80. (a)

$$\begin{aligned}[a,b][c,d] &= \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} c & -d \\ d & c \end{pmatrix} \\ &= \begin{pmatrix} ac-bd & -ad-bc \\ ad+bc & ac-bd \end{pmatrix} \\ &= [ac-bd, ad+bc].\end{aligned}$$

(b)

$$\begin{aligned}[a,b][c,d] &= [ac-bd, ad+bc] \\ &= [ca-db, cb+da] \\ &= [c,d][a,b].\end{aligned}$$

Further,

$$[1,0][a,b] = [1a-0b, 1b+0a] = [a,b].$$

(We do not need to check the effect of multiplying by $[1,0]$ on the right, because we already know that F is commutative.)

(c)

$$\left[\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2}\right][a,b] = \left[\frac{a^2+b^2}{a^2+b^2}, \frac{ab-ba}{a^2+b^2}\right] = [1,0].$$

81. (a)

$$\begin{aligned}[a,b]+[c,d] &= \begin{pmatrix} a & -b \\ b & a \end{pmatrix} + \begin{pmatrix} c & -d \\ d & c \end{pmatrix} \\ &= \begin{pmatrix} a+c & -(b+d) \\ b+d & a+c \end{pmatrix} \\ &= [a+c, b+d].\end{aligned}$$

(b) If $a, b \in \mathbb{R}$, then

$$\begin{aligned}\varphi(a)+\varphi(b) &= [a,0]+[b,0] \\ &= [a+b,0] \quad \text{by part (a)} \\ &= \varphi(a+b),\end{aligned}$$

and

$$\begin{aligned}\varphi(a)\varphi(b) &= [a,0][b,0]\\ &= [ab - 0\cdot 0, a0 + 0b]\\ &= [ab, 0]\\ &= \varphi(ab).\end{aligned}$$

(c) Let $x = [a,b]$. Then

$$\begin{aligned}x^2 + \mathbf{1} = \mathbf{0} &\iff [a,b]^2 + [1,0] = [0,0]\\ &\iff [a^2 - b^2, 2ab] + [1,0] = [0,0]\\ &\iff [a^2 - b^2 + 1, 2ab] = [0,0]\\ &\iff a^2 - b^2 + 1 = 0 \text{ and } 2ab = 0\\ &\iff -b^2 + 1 = 0 \text{ and } a = 0 \quad \text{(see below)} \qquad (9)\\ &\iff b \in \{1,-1\} \text{ and } a = 0.\end{aligned}$$

Thus, the two solutions are $[0,1]$ and $[0,-1]$.

The justification for the step at (9) is that, if b were zero, then the condition $a^2 - b^2 + 1 = 0$ would become $a^2 + 1 = 0$, which is not possible for a real number a. Therefore, the conditions $a^2 - b^2 + 1 = 0$ and $2ab = 0$ together imply that $a = 0$ and $-b^2 + 1 = 0$.

82. (a) It is clear that φ has a two-sided inverse ψ, namely, $\psi([a,b]) = a + bi$. To show that φ respects addition and multiplication, let $\alpha = a + bi$ and $\beta = c + di$. Then

$$\begin{aligned}\varphi(\alpha + \beta) &= \varphi((a+c) + (b+d)i)\\ &= [a+c, b+d]\\ &= [a,b] + [c,d] \quad \text{by part (a) of Question 81}\\ &= \varphi(\alpha) + \varphi(\beta),\end{aligned}$$

$$\begin{aligned}\text{and} \quad \varphi(\alpha\beta) &= \varphi(ac - bd + (ad + bc)i)\\ &= [ac - bd, ad + bc]\\ &= [a,b][c,d] \quad \text{by part (a) of Question 80}\\ &= \varphi(\alpha)\varphi(\beta).\end{aligned}$$

(b) For brevity, let $\theta = \arg(\alpha) = \arg(a + bi)$. By definition of $\arg(a + bi)$, R_θ sends the vector $\begin{pmatrix}1\\0\end{pmatrix}$ to the unit vector in the same direction as $\begin{pmatrix}a\\b\end{pmatrix}$, i.e.,

$$R_\theta \begin{pmatrix}1\\0\end{pmatrix} = \frac{1}{\sqrt{a^2+b^2}} \begin{pmatrix}a\\b\end{pmatrix}.$$

There is only one rotation matrix having this effect on $\begin{pmatrix}1\\0\end{pmatrix}$, namely,

$$\frac{1}{\sqrt{a^2+b^2}}\begin{pmatrix}a & -b\\ b & a\end{pmatrix} = \frac{1}{\sqrt{a^2+b^2}}[a,b],$$

so $R_\theta = \frac{1}{\sqrt{a^2+b^2}}[a,b]$. Now just use the fact that $\sqrt{a^2+b^2} = |\alpha|$.

83. (a)

$$\begin{aligned}\zeta^5 = (\cos(\theta)+i\sin(\theta))^5 &= \cos(5\theta)+i\sin(5\theta)\\ &= \cos(2\pi)+i\sin(2\pi) = 1.\end{aligned}$$

(b) By part (a),

$$0 = \zeta^5 - 1 = (\zeta-1)(\zeta^4+\zeta^3+\zeta^2+\zeta+1),$$

so because $\zeta - 1 \neq 0$ and $\mathbb{C}$ is an integral domain (a field, in fact), $\zeta^4+\zeta^3+\zeta^2+\zeta+1 = 0$, i.e., $(\zeta+\zeta^{-1})+(\zeta^2+\zeta^{-2})+1 = 0$.

(c)

$$\begin{aligned}\gamma^2 = (\zeta+\zeta^{-1})^2 &= \zeta^2+2+\zeta^{-2}\\ &= 1-(\zeta+\zeta^{-1}) \quad \text{by part (b)}\\ &= 1-\gamma,\end{aligned}$$

so $\gamma^2+\gamma-1 = 0$.

(d) By the formula for the roots of a quadratic polynomial, $\gamma^2+\gamma-1 = 0$ if and only if $\gamma = \frac{1}{2}(-1\pm\sqrt{5})$.

(e)

$$\begin{aligned}\zeta^{-1} = (\cos(\theta)+i\sin(\theta))^{-1} &= \cos(-\theta)+i\sin(-\theta)\\ &= \cos(\theta)-i\sin(\theta).\end{aligned}$$

Hence, $\cos(\theta) = \frac{1}{2}(\zeta+\zeta^{-1}) = \frac{1}{2}\gamma = \frac{1}{4}(-1\pm\sqrt{5})$ by part (d). But $\cos(\theta) = \cos(2\pi/5) > 0$ because $0 < 2\pi/5 < \pi/2$, while $\frac{1}{4}(-1-\sqrt{5}) < 0$, so $\cos(\theta) = \frac{1}{4}(-1+\sqrt{5})$.

84. (a) If $x, y \in \mathbb{Z}$, then $N(x+y\alpha) = (x+y\alpha)(x-y\alpha) = x^2+5y^2$, so $x^2+5y^2 = m$ if and only if $N(x+y\alpha) = m$.

(b) If there is solution for some given m_1 and some given m_2, then there are $r_1, r_2 \in \mathbb{Z}[\alpha]$ such that $N(r_1) = m_1$ and $N(r_2) = m_2$. But N respects multiplication, so $N(r_1r_1) = N(r_1)N(r_2) = m_1m_2$, so there is a solution for m_1m_2 as well.

(c) We proceed by induction on $k \geq 0$. The case $k = 0$ holds, because in that case the equation is $x^2 + 5y^2 = 1$, which has the solutions $x = \pm 1$, $y = 0$. Next, let $k \geq 0$, and assume that the equation $x^2 + 5y^2 = 29^k$ has a solution with $x, y \in \mathbb{Z}$. Now, the equation $x^2 + 5y^2 = 29$ certainly has such a solution, one being $x = 3$, $y = 2$, so by part (b) and the inductive hypothesis, there is a solution to $x^2 + 5y^2 = 29^k \cdot 29 = 29^{k+1}$. The induction is complete.

85.

$$\begin{aligned}\frac{\alpha}{\beta} &= \frac{5 - 8\sqrt{2}}{3 + 4\sqrt{2}} \\ &= \frac{(5 - 8\sqrt{2})(3 - 4\sqrt{2})}{(3 + 4\sqrt{2})(3 - 4\sqrt{2})} \\ &= -\frac{79}{23} + \frac{44}{23}\sqrt{2}.\end{aligned}$$

Since $|-3 - (-\frac{79}{23})| \leq 1/2$ and $|2 - \frac{44}{23}| \leq 1/2$, we let $\gamma = -3 + 2\sqrt{2}$, and hence

$$\begin{aligned}\rho = \alpha - \gamma\beta &= (5 - 8\sqrt{2}) - (-3 + 2\sqrt{2})(3 + 4\sqrt{2}) \\ &= (5 - 8\sqrt{2}) - (7 - 6\sqrt{2}) = -2 - 2\sqrt{2}.\end{aligned}$$

Thus, $\alpha = \gamma\beta + \rho$ where $f(\rho) < f(\beta)$.

86. (a) $q = 3x^2 + 2x + 1$ and $r = 2x^2 + 2x + 8$:

$$\begin{array}{r|l} & 3x^2 + 2x + 1 \\ \hline x^3 - x^2 + 2x - 3 & 3x^5 - x^4 + 5x^3 - 4x^2 - 2x + 5 \\ & \underline{-3x^5 + 3x^4 - 6x^3 + 9x^2} \\ & 2x^4 - x^3 + 5x^2 - 2x \\ & \underline{-2x^4 + 2x^3 - 4x^2 + 6x} \\ & x^3 + x^2 + 4x + 5 \\ & \underline{-x^3 + x^2 - 2x + 3} \\ & 2x^2 + 2x + 8 \end{array}$$

(b) $q = 4x^2 - x - 3$ and $r = 7x^2 + 3x - 5$:

$$\begin{array}{r|l} & 4x^2 - x - 3 \\ \hline x^3 - 3x^2 + 2x - 4 & 4x^5 - 13x^4 + 8x^3 - 2x^2 + x + 7 \\ & \underline{-4x^5 + 12x^4 - 8x^3 + 16x^2} \\ & -x^4 + 14x^2 + x \\ & \underline{x^4 - 3x^3 + 2x^2 - 4x} \\ & -3x^3 + 16x^2 - 3x + 7 \\ & \underline{3x^3 - 9x^2 + 6x - 12} \\ & 7x^2 + 3x - 5 \end{array}$$

(c) $q = \frac{2}{3}x - \frac{13}{9}$ and $r = \frac{80}{9}x + \frac{23}{9}$:

$$\begin{array}{r|l} & \frac{2}{3}x - \frac{13}{9} \\ \hline 3x^2 + 5x - 1 & 2x^3 \quad - x^2 \quad + x \quad + 4 \\ & \underline{- 2x^3 - \frac{10}{3}x^2 \quad + \frac{2}{3}x} \\ & - \frac{13}{3}x^2 \quad + \frac{5}{3}x \quad + 4 \\ & \underline{\frac{13}{3}x^2 + \frac{65}{9}x - \frac{13}{9}} \\ & \frac{80}{9}x + \frac{23}{9} \end{array}$$

87. Suppose that g has the property that $g(x) = 0$ if and only if $x = 0$. Obviously, $g \in I$, so $(g)_{\mathcal{F}} \subseteq I$. Now let f be any function in I, and define $h \in \mathcal{F}$ by

$$h(x) = \begin{cases} 0 & \text{if } x = 0, \\ \frac{f(x)}{g(x)} & \text{otherwise.} \end{cases}$$

(Actually, the value of h at 0 does not matter.) Then $(hg)(0) = h(0)g(0) = h(0) \cdot 0 = 0 = f(0)$, and if $x \neq 0$, then $(hg)(x) = h(x)g(x) = f(x)$. Thus, $hg = f$, so $f \in (g)_{\mathcal{F}}$.

88. (a)

$$\frac{\alpha}{\beta} = \frac{7 - 4\sqrt{2}}{3 + \sqrt{2}} = \frac{(3 - \sqrt{2})(7 - 4\sqrt{2})}{(3 - \sqrt{2})(3 + \sqrt{2})} = \frac{(3 - \sqrt{2})(7 - 4\sqrt{2})}{7}$$
$$= \frac{29}{7} - \frac{19}{7}\sqrt{2}.$$

Therefore, if we take $\gamma = 4 - 3\sqrt{2}$ and let

$$\rho = \alpha - \gamma\beta = (7 - 4\sqrt{2}) - (4 - 3\sqrt{2})(3 + \sqrt{2}) = 1 + \sqrt{2},$$

then $\alpha = \gamma\beta + \rho$ and $f(\rho) < f(\beta)$.

(b) Observe that

$$\rho^{-1} = \frac{1}{1 + \sqrt{2}} = \frac{1 - \sqrt{2}}{(1 - \sqrt{2})(1 + \sqrt{2})} = -1 + \sqrt{2},$$

so the equation $\alpha - \gamma\beta = \rho$ yields

$$\begin{aligned} 1 &= (-1 + \sqrt{2})\alpha - (-1 + \sqrt{2})(4 - 3\sqrt{2})\beta \\ &= (-1 + \sqrt{2})\alpha + (10 - 7\sqrt{2})\beta. \end{aligned}$$

(c) According to the previous part,

$$1 + I = (10 - 7\sqrt{2})\beta + I = ((10 - 7\sqrt{2}) + I)(\beta + I),$$

so $\beta + I$ is invertible in $\mathbb{Z}[\sqrt{2}]/I$ and has inverse $(10 - 7\sqrt{2}) + I$.

89. (a)
$$\frac{\alpha}{\beta} = \frac{5+\sqrt{2}}{5-\sqrt{2}} = \frac{(5+\sqrt{2})^2}{23} = \frac{27}{23} + \frac{10}{23}\sqrt{2}.$$
Therefore, if we take $\gamma = 1$ and let
$$\rho = \alpha - \gamma\beta = (5+\sqrt{2}) - (5-\sqrt{2}) = 2\sqrt{2},$$
then $\alpha = \gamma\beta + \rho$ and $f(\rho) < f(\beta)$.

(b) This time, we calculate
$$\frac{\beta}{2\sqrt{2}} = \frac{\sqrt{2}\,\beta}{2(\sqrt{2})^2} = \frac{-2+5\sqrt{2}}{8} = -\frac{1}{4} + \frac{5}{8}\sqrt{2},$$
so we take $\gamma_2 = \sqrt{2}$ and $\rho_2 = \beta - \gamma_2 \cdot (2\sqrt{2}) = 1 - \sqrt{2}$. By construction, $f(\rho_2) < f(2\sqrt{2})$.

(c) In the previous two parts, we found two equations:
$$\alpha = \beta + 2\sqrt{2} \tag{10}$$
$$\beta = \sqrt{2} \cdot 2\sqrt{2} + (1 - \sqrt{2}) \tag{11}$$
Hence,
$$\begin{aligned} 1 - \sqrt{2} &= \beta - \sqrt{2} \cdot 2\sqrt{2} \quad \text{by (11)} \\ &= \beta - \sqrt{2}(\alpha - \beta) \quad \text{by (10)} \\ &= -\sqrt{2}\,\alpha + (1+\sqrt{2})\beta. \end{aligned}$$

90. (a) The (multiplicative) inverse of $1 - \sqrt{2}$ is $-(1+\sqrt{2})$, so
$$\begin{aligned} 1 &= (1+\sqrt{2})\sqrt{2}\,\alpha - (1+\sqrt{2})^2\beta \\ &= (2+\sqrt{2})\alpha - (3+2\sqrt{2})\beta. \end{aligned}$$

(b) Dividing through by $\alpha\beta = 23$, we obtain
$$\begin{aligned} \frac{1}{23} &= \frac{2+\sqrt{2}}{\beta} - \frac{3+2\sqrt{2}}{\alpha} \\ &= \frac{2+\sqrt{2}}{5-\sqrt{2}} - \frac{3+2\sqrt{2}}{5+\sqrt{2}} \\ &= \frac{(5-\sqrt{2}) - (3-2\sqrt{2})}{5-\sqrt{2}} - \frac{3+2\sqrt{2}}{5+\sqrt{2}} \\ &= 1 - \frac{3+2\sqrt{2}}{5+\sqrt{2}} - \frac{3-2\sqrt{2}}{5-\sqrt{2}}. \end{aligned}$$

Thus, we may take $u = 1$, $a = -3$, and $b = -2$.

Alternatively, we could have modified the second numerator:

$$\begin{aligned}\frac{1}{23} &= \frac{2+\sqrt{2}}{\beta} - \frac{3+2\sqrt{2}}{\alpha} \\ &= \frac{2+\sqrt{2}}{5-\sqrt{2}} - \frac{3+2\sqrt{2}}{5+\sqrt{2}} \\ &= \frac{2+\sqrt{2}}{5-\sqrt{2}} - \frac{(5+\sqrt{2})-(2-\sqrt{2})}{5+\sqrt{2}} \\ &= -1 + \frac{2-\sqrt{2}}{5+\sqrt{2}} + \frac{2+\sqrt{2}}{5-\sqrt{2}}.\end{aligned}$$

In this case, $u = -1$, $a = 2$, and $b = -1$.

91. (a) If $1 + \sqrt{-6} = \alpha\beta$, where $\alpha, \beta \in \mathbb{Z}[\sqrt{-6}]$, then

$$7 = N(1+\sqrt{-6}) = N(\alpha\beta) = N(\alpha)N(\beta),$$

so either $N(\alpha) = 1$, in which case α is a unit, or $N(\beta) = 1$, in which case β is a unit.

(b) If $5 = \alpha\beta$, then

$$25 = N(5) = N(\alpha\beta) = N(\alpha)N(\beta),$$

so $N(\alpha) \in \{1, 5, 25\}$. We cannot have $N(\alpha) = 5$, because in that case, if $\alpha = x + y\sqrt{-6}$, we would have $x^2 + 6y^2 = 5$, which has no solution $x, y \in \mathbb{Z}$. Therefore, either $N(\alpha) = 1$, in which case α is a unit, or $N(\alpha) = 25$, in which case $N(\beta) = 1$, so β is a unit.

(c) The equation $x^2 + 6y^2 = 31$ has the solution $x = 5$, $y = 1$ (for example), so $31 = \alpha\beta$ where $\alpha = 5 + \sqrt{-6}$ and $\beta = 5 - \sqrt{-6}$. Neither α nor β is a unit, because each has norm $31 > 1$, so 31 is not irreducible.

92. (a) This polynomial has an integer root, namely, 2, so it is not irreducible. (When looking for integer roots, if any exist, one can narrow down the search by using Proposition 7.2 in Section VI.)

(b) We use Proposition 7.2 in Section VI to look for rational roots, if any exist. According to the proposition, the only possible rational roots are $\pm 1, \pm 2, \pm 4$. If the polynomial in question is f, then we have the following table of values:

x	1	−1	2	−2	4	−4
$f(x)$	10	2	26	−2	112	−40

Therefore, f has no rational roots, so being cubic, it is irreducible. (Pay close attention to Proposition 7.3 in Section VI and the caveat that follows it.)

(c) The polynomial in question is irreducible by Eisenstein's Criterion with the prime $p = 3$. Indeed, 3 divides all the coefficients except for the leading coefficient, and $3^2 \nmid 51$.

(d) This polynomial is not irreducible, because it factorizes as

$$x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 - x + 1).$$

93. (a)

$$\begin{aligned} f(x^2) &= (x^2 - \alpha^2)(x^2 - \beta^2) \\ &= (x - \alpha)(x + \alpha)(x - \beta)(x + \beta) \\ &= (x - \alpha)(x - \beta)(x + \alpha)(x + \beta) \\ &= (x^2 - (\alpha + \beta)x + \alpha\beta)(x^2 + (\alpha + \beta)x + \alpha\beta). \end{aligned}$$

By the assumption on $\alpha + \beta$ and $\alpha\beta$ given in the question, the two quadratic polynomials in this factorization have rational coefficients.

(b) The polynomial in question is $f(x^2)$ where $f(x) = x^2 - 10x + 169$. The polynomial $f(x)$ has roots

$$\begin{aligned} \frac{1}{2}(10 \pm \sqrt{25 - 4 \cdot 169}) &= 5 \pm \sqrt{25 - 169} \\ &= 5 \pm \sqrt{-144} \\ &= 5 \pm 12i, \end{aligned}$$

i.e., has roots α^2 and β^2 where $\alpha = 3 + 2i$ and $\beta = 3 - 2i$. Therefore, since $\alpha + \beta = 6$ and $\alpha\beta = 13$, we have

$$\begin{aligned} f(x^2) &= (x^2 - (\alpha + \beta)x + \alpha\beta)(x^2 + (\alpha + \beta)x + \alpha\beta) \\ &= (x^2 - 6x + 13)(x^2 + 6x + 13). \end{aligned}$$

94. (a) The result we use is Proposition 7.2 in Section VI. If the polynomial $f = x^2 - 10$ had a root of the form $a = r/s$ where $r, s \in \mathbb{Z}$ and $s \neq 0$, then according to the proposition, we would have $r \mid 10$ and $s \mid 1$, so $a \in \{1, -1, 2, -2, 5, -5, 10, -10\}$. But none of these eight numbers is a root: $f(1) = f(-1) = -9$, $f(2) = f(-2) = -5$, $f(5) = f(-5) = 15$, and $f(10) = f(-10) = 90$. Therefore, $x^2 - 10$ has no rational roots.

Note that another solution uses Eisenstein's Criterion, but that result would be overkill in this case.

(b) Let $\alpha = \sqrt{3+\sqrt{5}} + \sqrt{3-\sqrt{5}}$. Then

$$\begin{aligned}\alpha^2 &= (3+\sqrt{5}) + 2\sqrt{(3+\sqrt{5})(3-\sqrt{5})} + (3-\sqrt{5}) \\ &= (3+\sqrt{5}) + 2\sqrt{4} + (3-\sqrt{5}) \\ &= 10.\end{aligned}$$

Hence, if α were rational, then $x^2 - 10$ would have a rational root, contradicting part (a).

95. For brevity, we will let $I = (7, 1+\sqrt{15})_R$ in our solution.

(a) Note that each of the generators 7 and $1+\sqrt{15}$ is in $\mathrm{Ker}(\varphi)$, because $[7-0]$ and $[1-1]$ are both zero. Therefore, $I \subseteq \mathrm{Ker}(\varphi)$. Conversely, suppose that $a + b\sqrt{15}$ is in $\mathrm{Ker}(\varphi)$, where $a, b \in \mathbb{Z}$. Then $a - b = 7c$ for some $c \in \mathbb{Z}$, i.e., $a = b + 7c$, so

$$a + b\sqrt{15} = (b+7c) + b\sqrt{15} = 7c + b(1+\sqrt{15}) \in I.$$

Thus, $\mathrm{Ker}(\varphi) = I$.

(b) The map φ is surjective, because for any $a \in \mathbb{Z}$, the residue class $[a]$ is equal to $\varphi(a)$. Therefore, by the First Isomorphism Theorem, together with part (a),

$$R/I = R/\mathrm{Ker}(\varphi) \cong \mathbb{Z}/7\mathbb{Z}.$$

Hence, because $\mathbb{Z}/7\mathbb{Z}$ is a field, 7 being prime, it follows that R/I is a field as well, so I is maximal by Proposition 9.1 in Section VI.

(c) (*i*) $\varphi(\alpha) = [a-b] \neq [0]$, so $\alpha \notin \mathrm{Ker}(\varphi)$, i.e., $\alpha \notin I$.

(*ii*) Because $a + b\sqrt{15} \notin I$, the ideal $J = (7, 1+\sqrt{15}, \alpha)_R$ satisfies $I \subsetneqq J \subseteq R$. But I is maximal, so $J = R$. In particular, $1 \in J$, so $1 = \beta \cdot 7 + \gamma(1+\sqrt{15}) + \delta\alpha$ for some $\beta, \gamma, \delta \in R$.

96. (a)

$$N(a)N(b) = N(ab) = N(7+\sqrt{10}) = 49 - 10 = 39.$$

Therefore, $N(a)$ divides 39 in $\mathbb{Z}$. The only divisors of $39 = 3 \cdot 13$ are those listed in the question.

(b) Let $a = x + y\sqrt{10}$, where $x, y \in \mathbb{Z}$. Then $N(a) = x^2 - 10y^2$. If $k \in \{\pm 3, \pm 13\}$, then $k \equiv \pm 2 \bmod 5$, so Question (a) shows that $x^2 - 10y^2$ cannot be equal to k, i.e., $N(a) \neq k$.

(c) We have shown that if $7 + \sqrt{10} = ab$ with $a, b \in \mathbb{Z}[\sqrt{10}]$, then $N(a)$ is one of $\pm 1, \pm 39$. If $N(a) = \pm 1$, then $(x + y\sqrt{10})(x - y\sqrt{10}) = \pm 1$, so $a = x + y\sqrt{10}$ is

a unit. If instead $N(a) = \pm 39$, then $N(b) = \pm 1$, and then b is a unit instead. Thus, $7 + \sqrt{10}$ is irreducible.

(d) If $3 = (7 + \sqrt{10})c$, where $c \in \mathbb{Z}[\sqrt{10}]$, then

$$3^2 = N(3) = N((7 + \sqrt{10})c) = N(7 + \sqrt{10})N(c) = 39N(c),$$

i.e., $3 = 13N(c)$. But this says that $13 \mid 3$, which is not the case.

If, on the other hand, $13 = (7 + \sqrt{10})c$ for some $c \in \mathbb{Z}[\sqrt{10}]$, then

$$13^2 = N(13) = N((7 + \sqrt{10})c) = N(7 + \sqrt{10})N(c) = 39N(c),$$

i.e., $13 = 3N(c)$. This time, we have arrived at $3 \mid 13$, which again is not the case.

97. (a) $N(\alpha)N(\beta) = N(\alpha\beta) = N(2 + \sqrt{-6}) = 10$, so $N(\alpha) \mid 10$. Note that, by definition, $N(\alpha)$ cannot be negative, so $N(\alpha)$ is equal to one of the positive divisors of 10, i.e., $1, 2, 5, 10$.

(b) Let $\alpha = x + y\sqrt{-6}$. Then $N(\alpha) = 2$ if and only if $x^2 + 6y^2 = 2$. This equation immediately forces y to be zero, but then we observe that the equation $x^2 = 2$ has no integer solution. Thus, $N(\alpha) \neq 2$. Exactly the same argument shows that $N(\alpha) \neq 5$.

(c) Part (a) shows that $N(\alpha)$ is one of $1, 2, 5, 10$, but part (b) shows that $N(\alpha)$ cannot be 2 or 5, so it must be 1 or 10. If 1, then α is a unit, and if 10, then $N(\beta) = 1$, so β is a unit. Thus, $2 + \sqrt{-6}$ is irreducible.

(d) Suppose that $2 = (2 + \sqrt{-6})\gamma$, where $\gamma \in \mathbb{Z}[\sqrt{-6}]$. Then

$$4 = N(2) = N((2 + \sqrt{-6})\gamma) = N(2 + \sqrt{-6})N(\gamma) = 10N(\gamma),$$

so $2 = 5N(\gamma)$, which is impossible, because $5 \nmid 2$. Similarly, if $5 = (2 + \sqrt{-6})\gamma$ for some $\gamma \in \mathbb{Z}[\sqrt{-6}]$, then

$$25 = N(5) = N((2 + \sqrt{-6})\gamma) = N(2 + \sqrt{-6})N(\gamma) = 10N(\gamma),$$

so $5 = 2N(\gamma)$. This contradicts the fact that $2 \nmid 5$.

98. (a) If x, y, k are integers such that $x^2 - 26y^2 = k$, then $[x]^2 = [k]$ in $\mathbb{Z}/13\mathbb{Z}$, and then the fact given in the question tells us that $[k]$ cannot be $[5]$ or $[-5]$.

(b) Suppose that $31 = \alpha\beta$, where $\alpha, \beta \in \mathbb{Z}[\sqrt{26}]$. Then $31^2 = N(31) = N(\alpha)N(\beta)$, so $N(\alpha) \in \{\pm 1, \pm 31, \pm 31^2\}$. If $N(\alpha) = \pm 31$, then letting $\alpha = x + y\sqrt{26}$, we would have $x^2 - 26y^2 = \pm 31$. But this contradicts part (a), because $31 \equiv 5 \bmod 13$. Therefore, $N(\alpha) \in \{\pm 1, \pm 31^2\}$. If $N(\alpha) = \pm 1$, then α is a unit, and if $N(\alpha) = \pm 31^2$, then $N(\beta) = \pm 1$, so β is a unit.

99. The last example in Section IV – 9 shows that $\mathbb{Z}[x]$ is not a principal ideal domain, so Proposition 5.1 in Section VI implies that it is not a Euclidean domain. It therefore has no Euclidean function.

100. (a) Note that $[\alpha][\alpha] = [\alpha^2] = [1 + \alpha]$, and

$$[\alpha][1 + \alpha] = [\alpha^2 + \alpha] = [\alpha + 1 + \alpha] = [1],$$

because $2\alpha \in I$. Also,

$$\begin{aligned}[1 + \alpha][1 + \alpha] &= [1 + 2\alpha + \alpha^2] \\ &= [1 + \alpha^2] \quad \text{because } 2\alpha \in I \\ &= [1 + \alpha + 1] \\ &= [\alpha] \quad \text{because } 2 \in I.\end{aligned}$$

Therefore, the multiplication table is

	$[0]$	$[1]$	$[\alpha]$	$[1 + \alpha]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[\alpha]$	$[1 + \alpha]$
$[\alpha]$	$[0]$	$[\alpha]$	$[1 + \alpha]$	$[1]$
$[1 + \alpha]$	$[0]$	$[1 + \alpha]$	$[1]$	$[\alpha]$

(b) Note that R/I is commutative and has identity $[1] \neq [0]$. Further, the multiplication table shows that, for every non-zero element $x \in R/I$, there is $y \in R/I$ such that $xy = [1]$. Therefore, R/I is a field, so I is a maximal ideal by a result in the course.