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

Paul Buckingham

1. If $X = \{1, 2, 3, 4\}$, $Y = \{3, 4, 5\}$, and $Z = \{1, 5\}$, find the following sets:

   (a) $X \cap Y \cap Z$

   (b) $(X \cup Y) \cap Z$

   (c) $X \cap (Y \cup Z)$

   (d) $X \smallsetminus Y$

2. Let $X = \{1, 2, 4, 5\}$, $Y = \{1, 2, 3\}$, and $Z = \{3, 4\}$.

   (a) Find the following sets, writing the elements of each set in increasing numerical order:

   (*i*) $X \cap Y \cap Z$

   (*ii*) $(X \cap Y) \cup Z$

   (*iii*) $X \cap (Y \cup Z)$

   (*iv*) $X \smallsetminus Y$

   (b) Write down all the elements of the set $Y \times Z$.

3. Let X and Y be sets, and suppose that $f : X \to Y$, $g : Y \to X$, and $h : Y \to X$ are functions such that $g \circ f = \mathbf{1}_X$ and $f \circ h = \mathbf{1}_Y$. Show that $g = h$. *Hint: Observe that* $g = g \circ \mathbf{1}_Y$.

4. For each of the following functions, decide whether it is injective. If the function is injective, prove carefully that it is. If the function is not injective, exhibit two distinct elements of the domain that map to the same element in the codomain.

   (a)
   $$\begin{array}{rcl} f : \mathbb{Z} & \to & \mathbb{Z} \\ x & \mapsto & x^2 + x - 3 \end{array}$$

   (b)
   $$\begin{array}{rcl} g : \mathbb{Z} & \to & \mathbb{Z} \\ x & \mapsto & 2x^2 + x + 1 \end{array}$$

5. Consider $\mathbb{Z}_{\geq 1}$, the set of positive integers, and define a map $d : \mathbb{Z}_{\geq 1} \to \mathbb{Z}_{\geq 1}$ by letting $d(n)$ be the sum of the decimal digits of n. For example, $d(172) = 1+7+2 = 10$. Show that d is surjective but not injective.

6. A *square number* is a number of the form b^2 where $b \in \mathbb{Z}$. Recall also the digit sum $d(n)$ from Question 5. Define

$$X = \{n \in \mathbb{Z} \mid n-1 \text{ is a square number}\}$$
$$Y = \{n \in \mathbb{Z}_{\geq 1} \mid d(n) \text{ is odd}\}$$

(a) Write down the first 7 elements of X in increasing numerical order.

(b) Do the same for Y and $X \cap Y$.

7. Consider the following function:

$$\begin{array}{rcl} f : \mathbb{Z}_{\geq 1} & \to & \mathbb{Z}_{\geq 1} \\ n & \mapsto & \begin{cases} n-1 & \text{if } n \text{ is even} \\ n+1 & \text{if } n \text{ is odd.} \end{cases} \end{array}$$

(a) Show that $f \circ f = \mathbf{1}_{\mathbb{Z}_{\geq 1}}$.

(b) Deduce that f is bijective by using a result from the course notes.

8. Consider the following functions:

$$\begin{array}{rcl} f : \mathbb{Z} & \to & \mathbb{Q} \smallsetminus \{0\} \\ x & \mapsto & \dfrac{x^2-2}{x^2+2} \end{array}$$

$$\begin{array}{rcl} g : \mathbb{Q} \smallsetminus \{0\} & \to & \mathbb{Z} \\ y & \mapsto & \dfrac{y}{|y|} \end{array}$$

(a) Find Image(g), briefly explaining your answer.

(b) Show that $g \circ f$ has a unique fixed point, i.e., a unique integer x such that $g \circ f(x) = x$. What is x?

(c) Find Image($f \circ g$), explaining your answer.

9. By considering uniqueness of factorization of integers, find all pairs $(x, y) \in \mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$ such that $x^2 - y^2 = 77$. *Hint: Consider the identity* $x^2 - y^2 = (x+y)(x-y)$.

10. For each of the following sets A and binary relations $\sim$, decide whether $\sim$ defines an equivalence relation on A. Justify your answer in each case.

(a) Set: $A = \mathbb{R}$
Relation: $x \sim y$ if $x = ay$ for some $a \in \mathbb{Q}$

(b) Set: $A = \mathbb{R}$
Relation: $x \sim y$ if $x = ay$ for some $a \in \mathbb{Q} \setminus \{0\}$

11. For each of the following sets B and binary relations $\sim$, decide whether $\sim$ defines an equivalence relation on B. Justify your answer in each case.

(a) Set: $B = \mathbb{R}$
Relation: $x \sim y$ if $|x - y| \leq 1$

(b) Set: $B = M_n(\mathbb{R})$, the set of $n \times n$ matrices with real entries, where n is some fixed positive integer
Relation: $X \sim Y$ if $\mathrm{Tr}(X - Y) \in \mathbb{Z}$

(Here, $\mathrm{Tr}(X)$ denotes the trace of a matrix $X \in M_n(\mathbb{R})$.)

12. Recall the dot product $\mathbf{u} \cdot \mathbf{v}$ defined for vectors $\mathbf{u} = (a_1, a_2, a_3)$ and $\mathbf{v} = (b_1, b_2, b_3)$ in $\mathbb{R}^3$ by

$$\mathbf{u} \cdot \mathbf{v} = a_1 b_1 + a_2 b_2 + a_3 b_3.$$

Define a relation $\sim$ on the vector space $\mathbb{R}^3$ by declaring that $\mathbf{u} \sim \mathbf{v}$ if $\mathbf{u} \cdot \mathbf{v} \geq 0$. Decide, with justification in each case, which of the three properties of an equivalence relation (reflexivity, symmetry, and transitivity) the relation R satisfies.

13. Define a relation $\sim$ on $\mathbb{Q} \setminus \{0\}$ by declaring that $x \sim y$ if xy is the square of a rational number, i.e., if $xy = r^2$ for some $r \in \mathbb{Q}$. Decide, with justification, whether $\sim$ is an equivalence relation. If it is, prove so. Otherwise, explain why not with the aid of a counterexample.

14. Consider the vector space $\mathbb{R}^2$, and let $X = \mathbb{R}^2 \setminus \{(0, 0)\}$. Define a relation $\sim$ on X by declaring that $\mathbf{x} \sim \mathbf{y}$ if there is a positive scalar $c \in \mathbb{R}_{>0}$ such that $\mathbf{x} = c\mathbf{y}$. This relation is an equivalence relation. Find a representative for each equivalence class. *Hint: It may help you develop the right intuition for this problem if you first draw yourself a diagram illustrating all the vectors that are related to a given vector.*

15. Recall the factorial of a non-negative integer n:

$$n! = \prod_{m=1}^{n} m.$$

Prove by induction that $\sum_{k=1}^{n} k(k!) = (n + 1)! - 1$ for every non-negative integer n.

16. Show by induction that

$$\sum_{k=0}^{n} \frac{k}{(k+1)!} = 1 - \frac{1}{(n+1)!} \quad \text{for all } n \geq 0.$$

17. Prove by induction that 7 divides $3^{5n+3} + 5^n$ for every non-negative integer n.

18. (a) Show that if $n \in \mathbb{Z}$, then $(n+1)^3 - (n+1) = (3n^2 + 3n) + (n^3 - n)$.

    (b) Using part (a), show by induction that 3 divides $n^3 - n$ for all non-negative integers n.

    (c) Without any further induction, deduce from part (b) that 3 divides $n^3 - n$ for *all* integers n.

19. Using the definition of divisibility given at the beginning of Section II–1 of the course notes, show that if r, s, t are integers such that $r \mid s$ and $s \mid t$, then $r \mid t$.

20. Using the Euclidean algorithm, find the greatest common divisor of $a = 14\,161$ and $b = 11\,011$, and express the greatest common divisor in the form $ma + nb$ with $m, n \in \mathbb{Z}$.

21. Repeat Question 20 for the integers $a = 5225$ and $b = 1183$.

22. (a) Let a, b, c be integers such that a and b are coprime. Show that if $a \mid bc$, then $a \mid c$. *Hint: Adopt the strategy of the proof of the unique-factorization lemma in the notes.*

    (b) Show by counterexample that the assertion in part (a) would be false if the assumption that a and b be coprime were removed.

23. (a) Let a, b, c be integers such that a and b are coprime. Show that if $a \mid c$ and $b \mid c$, then $ab \mid c$.

    (b) Show by counterexample that the assertion in part (a) would be false if the assumption that a and b be coprime were removed.

24. (a) Find the remainder on dividing 1110^{2021} by 11.

    (b) Find the remainder on dividing 1110^{2022} by 11.

25. (a) Use the Euclidean algorithm to find an integer k such that $22k \equiv 1 \bmod 35$. Choose k so that $0 < k < 35$.

    (b) Solve the congruence $66x + 4 \equiv 16 \bmod 105$, expressing your answer in the form $x \equiv a \bmod n$ for an appropriate positive integer n and an appropriate integer $a \in \{0, \ldots, n-1\}$.

26. (a) Show that

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

Hint: $100 = 101 - 1$, $99 = 101 - 2$.

(b) Deduce that $100! \equiv (50!)^2 \bmod 101$.

27. Let a be an integer, let b and c be positive integers, and assume that $\gcd(b, c) = 1$.

(a) Show that there are integers k and l such that

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

Hint: Use the G.C.D. Theorem.

(b) Deduce that there are integers u, m, n, where $0 \leq m < b$ and $0 \leq n < c$, such that

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

28. (a) Perform the Euclidean algorithm on $a = 3^3 \cdot 5^3 = 3375$ and $b = 7^3 = 343$ to express 1 in the form $ma + nb$, where $m, n \in \mathbb{Z}$.

(b) Do the same for $a = 3^3 = 27$ and $b = 5^3 = 125$.

29. Before attempting this question, make sure that your answers to Question 28 are correct.

(a) Use your answer to part (a) of Question 28 to write $1/(3^3 \cdot 5^3 \cdot 7^3)$ in the form

$$\frac{x_1}{3^3 \cdot 5^3} + \frac{x_2}{7^3},$$

where $x_1, x_2 \in \mathbb{Z}$.

(b) Use your answer to part (b) of Question 28 to write $1/(3^3 \cdot 5^3)$ in the form

$$\frac{y_1}{3^3} + \frac{y_2}{5^3},$$

where $y_1, y_2 \in \mathbb{Z}$.

(c) Hence, find integers u, z_1, z_2, z_3 with $0 < z_1 < 3^3$, $0 < z_2 < 5^3$, and $0 < z_3 < 7^3$ such that

$$\frac{1}{105^3} = u + \frac{z_1}{3^3} + \frac{z_2}{5^3} + \frac{z_3}{7^3}.$$

(Note that $105 = 3 \cdot 5 \cdot 7$.) Check your answer by adding together the four terms on the right and ensuring that they sum to $1/105^3$.

30. (a) Find the smallest positive integer x satisfying the simultaneous congruences

$$\begin{aligned} x &\equiv 13 \mod 19 \\ x &\equiv 1 \mod 20 \\ x &\equiv 14 \mod 21 \end{aligned}$$

(b) What is the second smallest positive solution?

31. (a) Find the smallest positive integer x that simultaneously satisfies all of the following:

$$\begin{aligned} x &\equiv 17^2 \mod 11 \\ x &\equiv 11^2 \mod 13 \\ x &\equiv 13^2 \mod 17 \end{aligned}$$

(b) Find the greatest negative integer satisfying the same congruences.

32. Solve the following system of simultaneous congruences:

$$\begin{aligned} 4x &\equiv 2 \mod 13 \\ 5x &\equiv 6 \mod 21 \end{aligned}$$

Give your answer in the form $x \equiv a \bmod n$ for an appropriate positive integer n and an appropriate integer $a \in \{0, \ldots, n-1\}$. You may use the following equalities:

$$1 = 13 - 3 \cdot 4, \quad 1 = 21 - 4 \cdot 5, \quad 1 = 5 \cdot 21 - 8 \cdot 13.$$

33. In this question, you may use the fact that $541 \mid 203^2 - 93$.

(a) Let $x \in \mathbb{Z}$. Using the fact that 541 is prime, show that

$$\begin{gathered} x^2 \equiv 93 \bmod 541 \\ \iff \\ x \equiv 203 \bmod 541 \quad \text{or} \quad x \equiv -203 \bmod 541 \end{gathered}$$

That is, show that x satisfies the first congruence if and only if it satisfies the second or the third. You should make it clear how you use the primality of 541. *Hint: Take the* 93 *over to the other side of the congruence.*

(b) Find the first four positive integers x satisfying the simultaneous congruences

$$\begin{aligned} x^2 &\equiv 93 \mod 541 \\ x &\equiv 3 \mod 200 \end{aligned}$$

Do not adopt a brute-force approach.

34. Find all solutions to the simultaneous congruences

$$\begin{aligned} x &\equiv 4 \mod 315 \\ x &\equiv 9 \mod 715 \end{aligned}$$

Give your answer as a single congruence $x \equiv a \bmod n$ for an appropriate positive integer n and an appropriate integer $a \in \{0, \ldots, n-1\}$. You may use the fact that $1 = 26 \cdot 143 - 59 \cdot 63$. *Hint: Let $y = x - 4$, show that y must be divisible by 5, and then divide the congruences through by 5.*

35. (a) (*i*) Without using the Euclidean algorithm, write down integers s, t such that $1 = 4s + 9t$, and use your answer to find the inverse of 4 mod 9. Hence, replace the congruence $4x \equiv 5 \bmod 9$ with one of the form $x \equiv a \bmod 9$.

(*ii*) Without using the Euclidean algorithm, write down integers u, v such that $1 = 3u + 22v$, and use your answer to find the inverse of 3 mod 22. Hence, replace the congruence $3x \equiv 19 \bmod 22$ with one of the form $x \equiv b \bmod 22$.

(b) Use your answers to part (a) to solve the simultaneous congruences

$$\begin{aligned} 4x &\equiv 5 \mod 9 \\ 3x &\equiv 19 \mod 22 \end{aligned}$$

Give your answer as a single congruence $x \equiv c \bmod n$ for an appropriate positive integer n and an appropriate integer $c \in \{0, \ldots, n-1\}$.

36. Let a and b be integers and n a positive integer. Assume also that a and n have a common divisor $d > 1$, but that the only positive integer dividing all three of a, b, and n is 1. Show that the congruence $ax \equiv b \bmod n$ has no solutions.

37. Let T be the set of all functions $f : \mathbb{Z} \to \mathbb{Z}$, and define operations of addition and multiplication on T as follows:

$$\begin{aligned} (f + g)(x) &= f(x) + g(x) \quad \text{for all } x \in \mathbb{Z} \\ f \cdot g &= f \circ g \end{aligned}$$

(a) Show that $(g + h) \cdot f = g \cdot f + h \cdot f$ for all $f, g, h \in T$.

(b) Exhibit functions $f, g, h \in T$ such that $f \cdot (g + h) \neq f \cdot g + f \cdot h$, and show carefully that $f \cdot (g + h)$ is indeed different from $f \cdot g + f \cdot h$. (This part of the question shows that T is not a ring with the above operations.)

38. Let $S = \mathbb{R} \times \mathbb{R}$, and define a multiplication operation on S by

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc).$$

Verify that this operation is associative by showing that

$$\big((a, b) \cdot (c, d)\big) \cdot (e, f) = (a, b) \cdot \big((c, d) \cdot (e, f)\big)$$

for all real numbers a, b, c, d, e, f.

39. Let R be a ring such that $a^2 = a$ for all $a \in R$, and assume that R has an identity. Show that the only unit in R is 1.

40. Let R be a unital ring. Let $a \in R$, and suppose that there is $b \in R \setminus \{0\}$ such that $ab = 0$. Show that there is no $c \in R$ such that $ca = 1$.

41. Suppose that a non-empty set R together with binary operations $+$ (addition) and $\cdot$ (multiplication) satisfies all the axioms of a ring except possibly axiom A2, commutativity of addition. In this case, we strengthen axiom A3 to say that $a + 0 = 0 + a = a$ for all $a \in R$, and also strengthen axiom A4 to say that, for all $a \in R$, there is $b \in R$ such that $a + b = b + a = 0$. Assume also that R has a multiplicative identity, i.e., an element 1 such that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$.

    (a) Use the two distributivity axioms in one order to show that

    $$(1 + 1) \cdot (x + y) = x + x + y + y.$$

    for all $x, y \in R$. (Do not assume commutativity of addition.)

    (b) Now use the distributivity axioms in the opposite order to show that

    $$(1 + 1) \cdot (x + y) = x + y + x + y$$

    for all $x, y \in R$. (Do not assume commutativity of addition.)

    (c) Deduce from parts (a) and (b) that addition is commutative in R. *Hint: Use the strengthened axioms A3 and A4 described above.*

42. Let n be a positive integer. Prove that multiplication in $\mathbb{Z}/n\mathbb{Z}$ is associative. If you use the associativity of multiplication in another ring, state clearly where you use it.

43. Let R be a ring and $a \in R$. Suppose that there is a positive integer n such that $na = 0_R$. In that case, there is a least such n; let it be m. Show that if n is any positive integer such that $na = 0_R$, then m divides n. *Hint: Divide m into n with*

remainder. What can you deduce about the remainder? The proof of the G.C.D. Theorem may help you.

44. (a) Let X be a set.

    (i) Show that $2A = 0$ for all $A \in P(X)$.

    (ii) Deduce that $(A + B)^2 = A^2 + B^2$ for all $A, B \in P(X)$. (Remember that $P(X)$ is a commutative ring.)

    (b) Let Y be a set with at least two elements. Show that there are non-zero elements A and B of $P(Y)$ such that $A \cdot B = 0$.

45. Let R be a unital ring. Show that the ring $S = \mathcal{S}(R)$ has elements e_1, e_2, e_3 satisfying

$$\begin{aligned} e_i^2 &= e_i \quad (i = 1, 2, 3) \\ e_i e_j &= 0_S \quad (i \neq j) \\ e_1 + e_2 + e_3 &= 1_S \end{aligned}$$

46. Find a solution to the equation $a^2 + b^2 = 1_R$ in each of the following unital rings R. That is, exhibit an explicit element $a \in R$ and an explicit element $b \in R$ satisfying the equation. If you are given any restrictions on a and b, adhere to those restrictions.

    (a) $R = \mathbb{Z}$. Choose a and b to be non-positive.

    (b) $R = \mathbb{Q}$. Choose a and b so that neither is an integer. *Hint: If the two shorter sides of a right-angled triangle have lengths* 3 *and* 4*, how long is the hypotenuse?*

    (c) $R = \mathcal{F}$. Choose the functions a and b such that both are continuous and neither is constant. *Hint: Think of a well-known identity from trigonometry.*

    (d) $R = P(X)$, where $X = \{1, 2, 3\}$. Choose a and b so that neither is zero.

    (e) $R = M_2(\mathbb{Z})$, the ring of 2×2 matrices with integer entries. Choose the two matrices so that both are diagonal and neither matrix is zero.

    (f) $R = M_2(\mathbb{Z})$ again. This time, choose the two matrices so that at least one of them is not diagonal. *Hint: Can you think of a non-zero matrix $B \in M_2(\mathbb{Z})$ such that $B^2 = 0$?*

47. (a) If n is a positive integer and $a \in \mathbb{Z}$, what is the condition on a for $[a]$ to be a unit in $\mathbb{Z}/n\mathbb{Z}$?

(b) Find $(\mathbb{Z}/21\mathbb{Z})^\times$.

48. (a) For each $x \in (\mathbb{Z}/7\mathbb{Z})^\times$, find the least positive integer n such that $x^n = [1]$.

(b) What do you notice about these integers n in relation to the number of units in $\mathbb{Z}/7\mathbb{Z}$?

49. Characterize the units in $\mathcal{S}(\mathbb{Z})$. That is, if $\alpha = (a_n)_n \in \mathcal{S}(\mathbb{Z})$, what is the condition on the terms a_n for α to be a unit in $\mathcal{S}(\mathbb{Z})$. Explain your answer.

50. (a) If $x = [11] \in \mathbb{Z}/455\mathbb{Z}$, find x^{-1}. Express your answer in the form $x^{-1} = [a]$ where a is the least non-negative representative of x^{-1}.

(b) Find non-zero elements y and z in $\mathbb{Z}/455\mathbb{Z}$ such that $yz = 0$. Justify your answer. Make sure that y and z are non-zero elements of the ring.

51. (a) Let $R = \mathbb{Z}$ and $S = \{a \in \mathbb{Z} \mid a \equiv 1 \bmod 9\} \cup \{0\}$.

(*i*) Decide whether S is closed under subtraction. If it is, prove so. Otherwise, explain why not with the aid of a counterexample.

(*ii*) Decide whether S is closed under multiplication. If it is, prove so. Otherwise, explain why not with the aid of a counterexample.

(*iii*) Is S a subring of R?

(b) Repeat part (a) with the ring $R = \mathbb{Q}$ and the set

$$S = \{a/b \in \mathbb{Q} \mid a, b \in \mathbb{Z} \text{ and } 7 \nmid b\}.$$

(c) Repeat part (a) with the ring $R = \mathbb{Q}$ and the set

$$S = \{a/2 \in \mathbb{Q} \mid a \in \mathbb{Z}\}.$$

(d) Repeat part (a) with the ring $R = P(\mathbb{Z})$ and the set

$$S = \{A \in P(\mathbb{Z}) \mid 0 \notin A\}.$$

Hint: If $A \in P(\mathbb{Z})$, then $-A = A$. This will help when you are considering closure under subtraction.

52. Let $S = \{A \in P(\mathbb{Q}) \mid \mathbb{Z} \subseteq A\}$. Is S a subring of $P(\mathbb{Q})$? Which of the properties (i), (ii), and (iii) of Proposition 8.1 in Section IV hold and which fail? Justify your answers.

53. Let $R = \mathbb{Z} \times (\mathbb{Z}/5\mathbb{Z})$, the product of the rings $\mathbb{Z}$ and $\mathbb{Z}/5\mathbb{Z}$. Find all integers n and all elements $(a, x) \in R$ such that

(a) $n(a, x) = (20, [3])$.

(b) $n(a, x) = (5, [0])$.

In each part, show your solutions in a table indicating the values of n, a, and x for each solution, like this:

(a)

n	a	x
1	20	[3]
$\vdots$	$\vdots$	$\vdots$

Explain how you arrived at your solutions. Do not use simply trial and error.

Note: $n(a, x) = (na, nx)$ if $n \in \mathbb{Z}$.

54. In each of the following, R is a ring and S is a non-empty subset of R that is closed under subtraction. Given this information, decide whether S is an ideal of R. If it is, prove so. Otherwise, explain why not with the aid of a counterexample.

(a) $R = M_2(\mathbb{Z})$, S is the set of upper-triangular matrices in R.

(b) $R = \mathcal{F}$, $S = \{f \in R \mid f(x) = 0 \text{ for all } x \in \mathbb{Z}\}$.

55. Let $n \geq 2$ be an integer, and let

$$S = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) \;\middle|\; n \text{ divides } b \right\}.$$

(a) Is S an ideal of $M_2(\mathbb{Z})$? Justify your answer.

(b) Is S a subring of $M_2(\mathbb{Z})$? Justify your answer.

56. Let $n \geq 2$ be an integer.

(a) Define

$$S = \{f \in \mathbb{Z}[x] \mid n \text{ divides both } f(0) \text{ and the coefficient of } x \text{ in } f\}.$$

(*i*) Is S an ideal of $\mathbb{Z}[x]$? Justify your answer.

(*ii*) Is S a subring of $\mathbb{Z}[x]$? Justify your answer.

(b) Repeat part (a) for the set

$$T = \{f \in \mathbb{Z}[x] \mid n \text{ divides the coefficient of } x \text{ in } f\}.$$

57. Let $S = \{f \in \mathcal{F} \mid \sin(x^3)f(x) = 0 \text{ for all } x \in \mathbb{R}\}$. Decide whether S is an ideal of $\mathcal{F}$, justifying your answer either way.

58. Let $I = (x-1)_{\mathbb{Z}[x]} = (x-1)\mathbb{Z}[x]$, and let $g = x^3 + 2x^2 - x - 3$. Which of the following polynomials f_j are in the same coset of I as g, i.e., satisfy $f_j + I = g + I$?

$$f_1 = x^3 + 3x^2 - 5 \qquad f_2 = 2x^3 + x - 2$$
$$f_3 = x^4 + 2x^2 - 4x + 3 \qquad f_4 = 6x^5 - 6x^4 + x^3 + 2x^2 - x - 3$$

Briefly explain your answers. You may use the fact that a polynomial $f \in \mathbb{Z}[x]$ is in I if and only if $f(1) = 0$.

59. (a) Let $f(x) = 3x^3 - 5x^2 + 7x - 10$.

(*i*) Express $f(x)$ in the form $g(x) \cdot x + k \cdot 2$ where $g \in \mathbb{Z}[x]$ and $k \in \mathbb{Z}$.

(*ii*) Using part (*i*) and the equalities $x = 3(x-4) - 2(x-6)$ and $2 = (x-4) - (x-6)$, express $f(x)$ in the form $h(x)(x-4) + j(x)(x-6)$ where $h, j \in \mathbb{Z}[x]$.

(b) Explain why the polynomial $x^2 + 2x + 3$ is not in the ideal $(x-4, x-6)_{\mathbb{Z}[x]}$. *Hint: Think about even and odd integers.*

60. Let $I = \{(a_n)_n \in \mathcal{S}(\mathbb{R}) \mid a_n = 0 \text{ for all } n < 5\}$.

(a) Show that I is an ideal of $\mathcal{S}(\mathbb{R})$.

(b) Suppose that $\alpha, \beta \in \mathcal{S}(\mathbb{R})$ begin

$$\alpha = (2, -1, 1, 3, 6, 2\,462\,465\,426, \tfrac{531\,441}{16\,807}, \ldots)$$
$$\beta = (-4, 3, 5, -6, 2, \tfrac{15\,625}{14\,641}, 1\,508\,975\,315, \ldots)$$

Without using a calculator, compute $(\alpha + I) + (\beta + I)$ and $(\alpha + I)(\beta + I)$ in the quotient ring $\mathcal{S}(\mathbb{R})/I$. Express each answer in the form $\gamma + I$ for a suitable $\gamma \in \mathcal{S}(\mathbb{R})$.

61. Let $I = (x^2)_{\mathbb{Q}[x]}$, the principal ideal in $\mathbb{Q}[x]$ generated by x^2, and let

$$f(x) = 8\,306\,843\,612x^{15} - \frac{72\,609\,182}{356\,109}x^8 - 224x + 2$$
$$g(x) = \frac{60\,587\,954}{121\,611}x^{22} + 958\,486\,254\,731x^{13} + 312x + 1$$

Without using a calculator, compute $(f+I)+(g+I)$ and $(f+I)(g+I)$ in the quotient ring $\mathbb{Q}[x]/I$. Express each answer in the form $h+I$ for a suitable $h \in \mathbb{Q}[x]$.

62. Let $I = \{f \in \mathbb{Z}[x] \mid 6 \text{ divides both } f(0) \text{ and the coefficient of } x \text{ in } f\}$, and note that I is an ideal of $\mathbb{Z}[x]$ by part (a) of Question 56. For brevity, if $f \in \mathbb{Z}[x]$, let $[f] = f + I$.

    (a) Show that every element of $\mathbb{Z}[x]/I$ may be expressed in the form $\alpha = [a][x] + [b]$, where $a, b \in \{0, \ldots, 5\}$.

    (b) If $a, b, c, d \in \mathbb{Z}$, express $([a][x] + [b])([c][x] + [d])$ in the form $[s][x] + [t]$ for suitable integers s and t given in terms of a, b, c, d.

    (c) Show that $[x]+[1]$ is a unit in $\mathbb{Z}[x]/I$, and find its inverse in the form $[a][x]+[b]$ with $a, b \in \{0, \ldots, 5\}$.

63. Let $I = \{f \in \mathcal{F} \mid f(1) = 0\}$, an ideal of $\mathcal{F}$, and let $f, g \in \mathcal{F}$ be defined by

$$f(x) = \cos(3x)\ln((x^2 - 2x + 2)^2) + 2x$$
$$g(x) = 3x^2 + e^{3x}\sin((x^2 - 4x + 5)\pi) + 1$$

    Find polynomials h and j such that $(f+I)+(g+I) = h+I$ and $(f+I)(g+I) = j+I$. Explain your answers.

64. This exercise gives an ad hoc way to show that if $f \in \mathbb{Q}[x]$ and a, b are *distinct* rational numbers such that $f(a) = f(b) = 0$, then $f(x) = (x-a)(x-b)g(x)$ for some $g \in \mathbb{Q}[x]$. Another approach is via division-with-remainder in the ring $\mathbb{Q}[x]$, which is encountered later in the course.

    (a) Suppose that $f \in \mathbb{Q}[x]$. Show that if $f(0) = 0$, then $f(x) = xh(x)$ for some $h \in \mathbb{Q}[x]$. *Hint: Consider the coefficients of f and what the equality $f(0) = 0$ means for one of those coefficients.*

    (b) Now suppose that $f \in \mathbb{Q}[x]$ and that there are rational numbers $a \neq b$ satisfying $f(a) = f(b) = 0$.

        (i) Show that if $f_1(x) = f(x + a)$, then $f_1(x) = xf_2(x)$ for some $f_2 \in \mathbb{Q}[x]$. Deduce that $f(x) = (x - a)f_3(x)$ for some $f_3 \in \mathbb{Q}[x]$.

        (ii) Show that $f_3(b) = 0$. (Be careful; state what assumption you are using.) Deduce that $f_3(x) = (x - b)g(x)$ for some $g \in \mathbb{Q}[x]$. Thus, $f(x) = (x - a)(x - b)g(x)$.

65. Let $I = (x^2 - 3x + 2)_{\mathbb{Q}[x]}$.

(a) Using Question 64, show that $I = \{f \in \mathbb{Q}[x] \mid f(1) = f(2) = 0\}$. Be careful to show both directions, i.e., that each set is contained in the other.

(b) Suppose that $f \in \mathbb{Q}[x]$ is such that both $f(1)$ and $f(2)$ are non-zero. By considering the polynomial

$$g(x) = \frac{1}{f(2)}(x-1) - \frac{1}{f(1)}(x-2),$$

show that $f + I$ is a unit in $\mathbb{Q}[x]/I$. *Hint: Use part (a).*

66. Let X be a set and $A \in P(X)$.

(a) Show that $(A)_{P(X)} = P(A)$.

(b) Show that if $B \in P(X)$, then $B - BA \in P(B \setminus A)$. *Hint: Remember that $C = -C$ for all $C \in P(X)$.*

(c) Show that $B + P(A)$ may be expressed in the form $D + P(A)$, where $D \in P(B \setminus A)$. *Hint: Use the previous part.*

67. Let R be the cartesian product $\mathbb{Q} \times \mathbb{Q}$ together with operations of addition and multiplication defined by

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

You may assume that R is a ring with respect to these operations. Also, let S be the product ring $\mathbb{Q} \times \mathbb{Q}$ with the usual operations of addition and multiplication. In particular, $(a,b)(c,d) = (ac,bd)$ in S. Note that R and S have the same addition operations but different multiplication operations.

Now consider the map

$$\begin{aligned}\varphi : R &\to S\\ (a,b) &\mapsto (a+b, a-b).\end{aligned}$$

(a) Show that φ is a ring homomorphism.

(b) Show that φ is injective.

(c) Show that φ is surjective. If $(x,y) \in S$, what is the unique element (a,b) of R such that $\varphi(a,b) = (x,y)$?

(d) The above shows that φ is a ring isomorphism. Explain how to use the ring S and the isomorphism φ to construct non-zero elements $\alpha, \beta \in R$ such that $\alpha \cdot \beta = 0_R$. Write down such a pair of elements α and β.

68. (a) Decide whether the map

$$\begin{aligned} \varphi : \mathbb{Z} &\to M_2(\mathbb{Z}) \\ a &\mapsto \begin{pmatrix} a & a \\ a & -a \end{pmatrix} \end{aligned}$$

is a ring homomorphism, justifying your answer either way.

(b) Repeat part (a) for the map

$$\begin{aligned} \psi : \mathbb{Z} &\to M_2(\mathbb{Z}) \\ a &\mapsto \begin{pmatrix} 3a & -3a \\ 2a & -2a \end{pmatrix}. \end{aligned}$$

69. If $a \in \mathbb{Z} \smallsetminus \{0\}$ and p is a prime number, let $v_p(a)$ be the highest power of p dividing a. For example, if $a = 3^2 \cdot 5^6 \cdot 7^4$, then $v_3(a) = 2$, $v_5(a) = 6$, $v_7(a) = 4$, and $v_p(a) = 0$ if p is a prime not equal to 3, 5, or 7.

Now fix a prime p. Decide whether the map

$$\begin{aligned} \varphi : \mathbb{Z} &\to \mathbb{Q} \\ a &\mapsto \begin{cases} \left(\frac{1}{p}\right)^{v_p(a)} & \text{if } a \neq 0 \\ 0 & \text{if } a = 0 \end{cases} \end{aligned}$$

respects addition, multiplication, both, or neither, justifying your answers carefully. (If a property fails, provide a counterexample.) You may use the fact that if a and b are non-zero integers, then $v_p(ab) = v_p(a) + v_p(b)$.

70. Define

$$\begin{aligned} \varphi : \mathcal{F} &\to \mathcal{S}(\mathbb{R}) \\ f &\mapsto (f(n))_n. \end{aligned}$$

(a) Show that φ is a ring homomorphism.

(b) Use the First Isomorphism Theorem to show that there is a well-defined ring isomorphism $\overline{\varphi} : \mathcal{F}/I \to \mathcal{S}(\mathbb{R})$ satisfying $\overline{\varphi}(f + I) = (f(n))_n$ for all $f \in \mathcal{F}$, where $I = \{f \in \mathcal{F} \mid f(n) = 0 \text{ for all } n \in \mathbb{Z}_{\geq 0}\}$.

(c) Let $\mathbf{1} \in \mathcal{F}$ be the constant function $\mathbf{1} : x \mapsto 1$. Find a non-constant function $f \in \mathcal{F}$ such that $f + I = \mathbf{1} + I$.

71. Define

$$\begin{aligned} \varphi : \mathcal{S}(\mathbb{R}) &\to \mathcal{S}(\mathbb{R}) \\ (a_n)_{n\geq 0} &\mapsto (a_{n+1})_{n\geq 0}, \end{aligned}$$

that is, $\varphi(a_0, a_1, a_2, a_3, \ldots) = (a_1, a_2, a_3, \ldots)$.

(a) Show that φ is a ring homomorphism.

(b) Show that there is a non-zero ideal I of $\mathcal{S}(\mathbb{R})$ such that $\mathcal{S}(\mathbb{R})/I \cong \mathcal{S}(\mathbb{R})$. (Use the First Isomorphism Theorem.)

72. Consider the ring homomorphism

$$\begin{aligned} \varphi : \mathbb{Q}[x] &\to \mathbb{Q}^2 \\ f &\mapsto (f(-5), f(4)). \end{aligned}$$

(a) Using Question 64, show that $\mathrm{Ker}(\varphi) = I$ where $I = (x^2 + x - 20)_{\mathbb{Q}[x]}$. Be careful to show both inclusions, i.e., not only that $I \subseteq \mathrm{Ker}(\varphi)$, but also that $\mathrm{Ker}(\varphi) \subseteq I$.

(b) By considering $\varphi(x-4)$ and $\varphi(x+5)$, or otherwise, show that φ is surjective.

(c) Deduce that $\mathbb{Q}[x]/I \cong \mathbb{Q}^2$. What result from the course are you using?

73. Let X be a non-empty set, and let R be the set of maps $f : X \to \mathbb{Z}/2\mathbb{Z}$. The operations of addition and multiplication on R defined by

$$\begin{aligned} (f+g)(x) &= f(x) + g(x) \\ (fg)(x) &= f(x)g(x) \end{aligned}$$

make R a ring. If $f \in R$, let $X_f = \{x \in X \mid f(x) = [1]\}$, and view X_f as an element of $P(X)$.

(a) Show that $X_{f+g} = X_f + X_g$ and $X_{fg} = X_f X_g$ in the ring $P(X)$.

(b) Part (a) shows that the map

$$\begin{aligned} \varphi : R &\to P(X) \\ f &\mapsto X_f \end{aligned}$$

is a ring homomorphism. Show that it is both injective and surjective and therefore an isomorphism. *Hint: For surjectivity, if $A \subseteq X$, consider the function $f \in R$ that satisfies $f(x) = [1]$ if $x \in A$ and $f(x) = [0]$ otherwise.*

74. Consider the map

$$\begin{aligned} \varphi : \mathbb{Z}[\sqrt{6}] &\to \mathbb{Z}/5\mathbb{Z} \\ a + b\sqrt{6} &\mapsto [a + 4b]. \end{aligned}$$

(Note: If $a, b, a', b' \in \mathbb{Z}$, then $a + b\sqrt{6} = a' + b'\sqrt{6}$ if and only if $a = a'$ and $b = b'$, so the map is well defined.) Show that φ is a ring homomorphism.

75. Consider again the ring homomorphism

$$\begin{aligned} \varphi : \mathbb{Z}[\sqrt{6}] &\to \mathbb{Z}/5\mathbb{Z} \\ a + b\sqrt{6} &\mapsto [a + 4b] \end{aligned}$$

encountered in Question 74.

(a) Show that $1 + \sqrt{6} \in \mathrm{Ker}(\varphi)$, and deduce that $y(1 + \sqrt{6}) \in \mathrm{Ker}(\varphi)$ for all $y \in \mathbb{Z}[\sqrt{6}]$.

(b) Now let $x \in \mathrm{Ker}(\varphi)$, and write $x = a + b\sqrt{6}$ with $a, b \in \mathbb{Z}$.

(i) Show that $a = 5c - 4b$ for some $c \in \mathbb{Z}$.

(ii) Using part (i), show that $x = 5d + b(1 + \sqrt{6})$ for some $d \in \mathbb{Z}$.

(iii) Using the fact that $5 = (\sqrt{6} - 1)(1 + \sqrt{6})$, deduce from part ($ii$) that $x = y(1 + \sqrt{6})$ for some $y \in \mathbb{Z}[\sqrt{6}]$.

(c) Conclude that $\mathbb{Z}[\sqrt{6}]/I \cong \mathbb{Z}/5\mathbb{Z}$, where $I = (1 + \sqrt{6})_{\mathbb{Z}[\sqrt{6}]}$.

76. (a) Let $\alpha \in \mathbb{Z}/5\mathbb{Z}$. Show, by testing all five possibilities for α, that $\alpha^2 \notin \{[2], [-2]\}$.

(b) Deduce that if k is an integer such that $k \equiv \pm 2 \bmod 5$, then the equation $x^2 - 10y^2 = k$ has no solutions $x, y \in \mathbb{Z}$. *Hint: The given equation yields the congruence* $x^2 - 10y^2 \equiv k \bmod 5$.

77. Consider $P(\mathbb{Z})$, the power set of $\mathbb{Z}$. Fix $k \in \mathbb{Z}$, and define

$$\begin{aligned} \varphi : P(\mathbb{Z}) &\to \mathbb{Z}/2\mathbb{Z} \\ A &\mapsto \begin{cases} [0] & \text{if } k \notin A \\ [1] & \text{if } k \in A \end{cases} \end{aligned}$$

(For example, $\varphi(\{k-1, k+1, k+2\}) = [0]$, while $\varphi(\{k-1, k, k+1, k+2\}) = [1]$.)

(a) Let $A, B \in P(\mathbb{Z})$. Complete the last two columns of the following table, where Y means "Yes" and N means "No".

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

(b) Using the table in part (a), show that the map φ is a ring homomorphism.

(c) Show that if $I = \{A \in P(\mathbb{Z}) \mid k \notin A\}$, then there is a well-defined ring

isomorphism

$$\begin{aligned} \overline{\varphi} : P(\mathbb{Z})/I &\to \mathbb{Z}/2\mathbb{Z} \\ A + I &\mapsto \begin{cases} [0] & \text{if } k \notin A \\ [1] & \text{if } k \in A \end{cases} \end{aligned}$$

(Incidentally, observe that $I = P(\mathbb{Z} \setminus \{k\})$, although this fact need not play any role in your answer.)

78. Each of the following rings R is commutative with a non-zero identity. In each case, decide whether it is a field, an integral domain that is not a field, or neither. Remember that every field is an integral domain.

(a) $R = \mathbb{Q}[x]/(x^2 - x - 6)_{\mathbb{Q}[x]}$.

(b) $R = \mathbb{Z}[x]/(x)_{\mathbb{Z}[x]}$. You may refer to an example done in class.

(c) $R = P(\mathbb{Z})$.

(d) $R = \mathbb{Z}[x]/I_p$, where p is a prime and $I_p = \{f \in \mathbb{Z}[x] \mid p \text{ divides } f(0)\}$.

(e) $R = \{x + y\sqrt{2} \in \mathbb{R} \mid x, y \in \mathbb{Z}\}$.

(f) $R = \{x + y\sqrt{-3} \in \mathbb{C} \mid x, y \in \mathbb{Q}\}$.

79. For each of the following rings R, decide whether it is an integral domain. If it is, prove so. Otherwise, explain why not with the aid of a counterexample.

(a) $R = \mathcal{F}$.

(b) $R = \mathcal{F}/I$, where $I = \{f \in \mathcal{F} \mid f(1) = 0\}$.

80. For brevity, given $a, b \in \mathbb{R}$, let

$$[a, b] = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in M_2(\mathbb{R}).$$

Now define $F = \{[a, b] \in M_2(\mathbb{R}) \mid a, b \in \mathbb{R}\}$. You may assume that F is a ring. This exercise proves that F is a field.

(a) Show that $[a, b][c, d] = [ac - bd, ad + bc]$ for all $a, b, c, d \in \mathbb{R}$.

(b) Show that F is commutative and has the identity element $[1, 0]$.

(c) Show that if a and b are not both zero, then

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

81. We continue with the ring F of Question 80. Recall that we showed F to be a field in that question.

(a) Show that $[a,b]+[c,d]=[a+c,b+d]$ for all $a,b,c,d\in\mathbb{R}$.

(b) Show that the map

$$\begin{aligned}\varphi:\mathbb{R} &\to F\\ a &\mapsto [a,0]\end{aligned}$$

is an injective ring homomorphism.

(c) If $\mathbf{0}=[0,0]$, the zero element of F, and $\mathbf{1}=[1,0]$, the identity element, show that the equation $x^2+\mathbf{1}=\mathbf{0}$ has exactly two solutions $x\in F$.

82. Let F be as in Question 80.

(a) Show that the map

$$\begin{aligned}\varphi:\mathbb{C} &\to F\\ a+bi &\mapsto [a,b]\end{aligned}$$

is a ring isomorphism.

(b) If we view $\mathbb{C}$ as a plane, so that a complex number $\alpha=a+bi$ corresponds to the point (a,b) in the plane, then as long as α is non-zero, the line segment $L_{(a,b)}$ from the origin to (a,b) forms an angle $\theta\in[0,2\pi)$ with the line segment $L_{(1,0)}$ from the origin to $(1,0)$, where θ is measured anticlockwise from $L_{(1,0)}$. This angle is called the *argument* of α, denoted $\arg(\alpha)$.

Show that if $\alpha\in\mathbb{C}\smallsetminus\{0\}$, then the matrix $\varphi(\alpha)\in F$ is equal to $|\alpha|R_{\arg(\alpha)}$, where $R_{\arg(\alpha)}$ is the rotation matrix with angle $\arg(\alpha)$.

83. This exercise uses complex numbers to show that $\cos(2\pi/5)=\frac{1}{4}(-1+\sqrt{5})$. You may use the following equation, which holds for any real number ϕ and any integer n:

$$(\cos(\phi)+i\sin(\phi))^n=\cos(n\phi)+i\sin(n\phi). \tag{1}$$

(a) Let $\theta=2\pi/5$ and $\zeta=\cos(\theta)+i\sin(\theta)$. Use (1) to show that $\zeta^5=1$, and therefore $\zeta^4=\zeta^{-1}$ and $\zeta^3=\zeta^{-2}$.

(b) Using the fact that $\zeta\neq 1$, deduce from (a) that

$$0=\zeta^4+\zeta^3+\zeta^2+\zeta+1=(\zeta+\zeta^{-1})+(\zeta^2+\zeta^{-2})+1.$$

(c) Let $\gamma=\zeta+\zeta^{-1}$. Deduce from (b) that $\gamma^2+\gamma-1=0$. *Hint: Handle* γ^2 *by expanding out* $(\zeta+\zeta^{-1})^2$.

(d) Solve the equation $\gamma^2 + \gamma - 1 = 0$ to find the two possibilities for γ.

(e) Use (1) to show that $\zeta^{-1} = \cos(\theta) - i\sin(\theta)$, and hence use (d) to show that $\cos(\theta) = \frac{1}{4}(-1 + \sqrt{5})$. Take care to explain the choice of sign in front of $\sqrt{5}$.

84. Let $\alpha \in \mathbb{C}$ be a square root of -5 (i.e., $\alpha^2 = -5$), and consider the ring

$$\mathbb{Z}[\alpha] = \{x + y\alpha \in \mathbb{C} \mid x, y \in \mathbb{Z}\}$$

and the norm map

$$\begin{aligned} N : \mathbb{Z}[\alpha] &\to \mathbb{Z} \\ x + y\alpha &\mapsto (x + y\alpha)(x - y\alpha). \end{aligned}$$

Note that N respects multiplication.

(a) Show that if $m \in \mathbb{Z}$, then the equation $x^2 + 5y^2 = m$ has a solution with $x, y \in \mathbb{Z}$ if and only if there is $r \in \mathbb{Z}[\alpha]$ such that $N(r) = m$.

(b) Using part (a), show that if $m_1, m_2 \in \mathbb{Z}$ and there exist $x_1, y_1, x_2, y_2 \in \mathbb{Z}$ such that $x_1^2 + 5y_1^2 = m_1$ and $x_2^2 + 5y_2^2 = m_2$, then there exist $x_3, y_3 \in \mathbb{Z}$ such that $x_3^2 + 5y_3^2 = m_1 m_2$.

(c) Via an induction argument, deduce that for every non-negative integer k, the equation $x^2 + 5y^2 = 29^k$ has a solution with $x, y \in \mathbb{Z}$.

85. Recall that the map $f : x + y\sqrt{2} \mapsto |x^2 - 2y^2|$ is a Euclidean function on $\mathbb{Z}[\sqrt{2}]$. If $\alpha = 5 - 8\sqrt{2}$ and $\beta = 3 + 4\sqrt{2}$, find $\gamma, \rho \in \mathbb{Z}[\sqrt{2}]$ such that $\alpha = \gamma\beta + \rho$ and $f(\rho) < f(\beta)$.

86. For each of the following pairs of polynomials $f, g \in \mathbb{Q}[x]$, find $q, r \in \mathbb{Q}[x]$ such that $f = qg + r$ and $\deg(r) < \deg(g)$.

(a) $f = 3x^5 - x^4 + 5x^3 - 4x^2 - 2x + 5$, $g = x^3 - x^2 + 2x - 3$.

(b) $f = 4x^5 - 13x^4 + 8x^3 - 2x^2 + x + 7$, $g = x^3 - 3x^2 + 2x - 4$.

(c) $f = 2x^3 - x^2 + x + 4$, $g = 3x^2 + 5x - 1$.

87. Let $I = \{f \in \mathcal{F} \mid f(0) = 0\}$, an ideal of $\mathcal{F}$. Show that I is a principal ideal. *Hint: Suppose that $g \in \mathcal{F}$ has the property that $g(x) = 0$ if and only if $x = 0$. Show that $I = (g)_{\mathcal{F}}$.*

88. Recall that the map $f : x + y\sqrt{2} \mapsto |x^2 - 2y^2|$ is a Euclidean function on $\mathbb{Z}[\sqrt{2}]$.

(a) If $\alpha = 7 - 4\sqrt{2}$ and $\beta = 3 + \sqrt{2}$, find $\gamma, \rho \in \mathbb{Z}[\sqrt{2}]$ such that $\alpha = \gamma\beta + \rho$ and $f(\rho) < f(\beta)$.

(b) In part (a), if you followed exactly the algorithm given in the course, then you should have found that $\rho \in \mathbb{Z}[\sqrt{2}]^\times$. Multiply both sides of the equation $\alpha - \gamma\beta = \rho$ by ρ^{-1} to find $\mu, \nu \in \mathbb{Z}[\sqrt{2}]$ such that $1 = \mu\alpha + \nu\beta$ with $\mu, \nu \in \mathbb{Z}[\sqrt{2}]$. Make sure that each of your elements μ, ν is expressed in the form $a + b\sqrt{2}$ with $a, b \in \mathbb{Z}$.

(c) Let $I = (\alpha)_{\mathbb{Z}[\sqrt{2}]}$. Use your answer to part (b) to show that $\beta + I$ is invertible in $\mathbb{Z}[\sqrt{2}]/I$ and to find $(\beta + I)^{-1}$.

89. (a) Repeat part (a) of Question 88 for the elements $\alpha = 5 + \sqrt{2}$ and $\beta = 5 - \sqrt{2}$. Follow the steps to perform division with remainder in this ring, as outlined in the course notes.

(b) The outcome of performing division with remainder in the previous part should have resulted in $\alpha = \beta + 2\sqrt{2}$. Now perform division with remainder again to express β as $\gamma_2 \cdot 2\sqrt{2} + \rho_2$ with $\gamma_2, \rho_2 \in \mathbb{Z}[\sqrt{2}]$ and $f(\rho_2) < f(2\sqrt{2})$.

(c) This time, the outcome of division with remainder should have been $\beta = \sqrt{2} \cdot 2\sqrt{2} + (1 - \sqrt{2})$. Use this equation together with $\alpha = \beta + 2\sqrt{2}$ to express $1 - \sqrt{2}$ in the form $\mu\alpha + \nu\beta$ with $\mu, \nu \in \mathbb{Z}[\sqrt{2}]$.

90. This question is a continuation of Question 89, which showed that $1 - \sqrt{2} = -\sqrt{2}\,\alpha + (1 + \sqrt{2})\beta$ where $\alpha = 5 + \sqrt{2}$ and $\beta = 5 - \sqrt{2}$.

(a) Using the fact that $1 - \sqrt{2} \in \mathbb{Z}[\sqrt{2}]^\times$, find $\mu', \nu' \in \mathbb{Z}[\sqrt{2}]$ such that $1 = \mu'\alpha + \nu'\beta$.

(b) By dividing through by $\alpha\beta$ and making a suitable modification to one of the numerators, find $u, a, b \in \mathbb{Z}$ such that

$$\frac{1}{23} = u + \frac{a + b\sqrt{2}}{5 + \sqrt{2}} + \frac{a - b\sqrt{2}}{5 - \sqrt{2}}.$$

91. (a) Show that the element $1 + \sqrt{-6} \in \mathbb{Z}[\sqrt{-6}]$ is irreducible. (Consider a factorization and take norms.)

(b) Show that the element $5 \in \mathbb{Z}[\sqrt{-6}]$ is irreducible. (Consider a factorization and take norms.)

(c) Show that the element $31 \in \mathbb{Z}[\sqrt{-6}]$ is not irreducible. (Consider the equation $x^2 + 6y^2 = 31$.)

92. Decide which of the following polynomials are irreducible in $\mathbb{Q}[x]$. Explain your answers.

(a) $x^4 - 6x^3 + 10x^2 - 10x + 12$

(b) $x^3 + 2x^2 + 3x + 4$

(c) $x^4 - 45x^2 + 51$

(d) $x^4 + x^2 + 1$

93. (a) Suppose that $f(x) \in \mathbb{Q}[x]$ is a monic quadratic polynomial whose roots in $\mathbb{C}$ are α^2 and β^2, where α and β are complex numbers such that $\alpha + \beta$ and $\alpha\beta$ are both rational. Show that $f(x^2)$ factorizes as a product of two quadratic polynomials in $\mathbb{Q}[x]$ (so is not irreducible). *Hint: Note that* $f(x) = (x - \alpha^2)(x - \beta^2)$.

(b) By observing that $5 + 12i = (3 + 2i)^2$, use the above idea to factorize $x^4 - 10x^2 + 169$ in $\mathbb{Q}[x]$.

94. (a) Apply a result from the course to show that the polynomial $x^2 - 10$ has no rational roots. Specify which result you are using.

(b) Deduce that $\sqrt{3 + \sqrt{5}} + \sqrt{3 - \sqrt{5}}$ is not rational. *Hint: Consider its square.*

95. Let $R = \mathbb{Z}[\sqrt{15}]$, and consider the map

$$\begin{aligned} \varphi : R &\to \mathbb{Z}/7\mathbb{Z} \\ a + b\sqrt{15} &\mapsto [a - b], \end{aligned}$$

which is in fact a ring homomorphism.

(a) Show that $\mathrm{Ker}(\varphi) = (7, 1 + \sqrt{15})_R$, the ideal generated by 7 and $1 + \sqrt{15}$.

(b) Deduce that $(7, 1 + \sqrt{15})_R$ is a maximal ideal.

(c) Suppose that a and b are integers such that $a \not\equiv b \bmod 7$, and let $\alpha = a + b\sqrt{15}$.

(i) Show that $\alpha \notin (7, 1 + \sqrt{15})_R$. *Hint: Consider* $\varphi(\alpha)$.

(ii) Hence, or otherwise, show that there are $\beta, \gamma, \delta \in R$ such that $1 = \beta \cdot 7 + \gamma(1 + \sqrt{15}) + \delta\alpha$.

96. Recall the norm map

$$\begin{aligned} N : \mathbb{Z}[\sqrt{10}] &\to \mathbb{Z} \\ x + y\sqrt{10} &\mapsto x^2 - 10y^2 = (x + y\sqrt{10})(x - y\sqrt{10}). \end{aligned}$$

In the following, you may use the fact that $N(ab) = N(a)N(b)$ for all $a, b \in \mathbb{Z}[\sqrt{10}]$.

(a) Suppose that $7+\sqrt{10} = ab$ where $a, b \in \mathbb{Z}[\sqrt{10}]$. Show that $N(a)$ divides 39 in $\mathbb{Z}$ and is therefore equal to one of $\pm 1, \pm 3, \pm 13, \pm 39$.

(b) Show that $N(a)$ is not equal to any of $\pm 3, \pm 13$. *Hint: Let $a = x + y\sqrt{10}$, and use Question 76.*

(c) Deduce that $7+\sqrt{10}$ is irreducible in $\mathbb{Z}[\sqrt{10}]$.

(d) The equality $(7+\sqrt{10})(7-\sqrt{10}) = 3 \cdot 13$ shows that $7+\sqrt{10}$ divides the product $3 \cdot 13$ in $\mathbb{Z}[\sqrt{10}]$. Show, however, that $7+\sqrt{10}$ divides neither 3 nor 13 in $\mathbb{Z}[\sqrt{10}]$. *Hint: Assume that $3 = (7+\sqrt{10})c$ for some $c \in \mathbb{Z}[\sqrt{10}]$ and apply N to both sides.*

The significance of the above exercise is that it shows that $7+\sqrt{10}$ is an irreducible element of $\mathbb{Z}[\sqrt{10}]$ but not a prime element, so $\mathbb{Z}[\sqrt{10}]$ does not have uniqueness of factorization.

97. In this exercise, $\sqrt{-6}$ denotes a fixed square root of -6 in $\mathbb{C}$. (We could adopt the choice of square root made in the course notes, but the choice does not matter.)

Recall the norm map

$$\begin{array}{rcl} N : \mathbb{Z}[\sqrt{-6}] & \to & \mathbb{Z} \\ x + y\sqrt{-6} & \mapsto & x^2 + 6y^2 = (x+y\sqrt{-6})(x-y\sqrt{-6}). \end{array}$$

(a) Suppose that $2+\sqrt{-6} = \alpha\beta$ where $\alpha, \beta \in \mathbb{Z}[\sqrt{-6}]$. Show that $N(\alpha)$ divides 10 in $\mathbb{Z}$ and is therefore equal to one of $1, 2, 5, 10$.

(b) Show that $N(\alpha)$ is not equal to either 2 or 5.

(c) Deduce that $2+\sqrt{-6}$ is irreducible in $\mathbb{Z}[\sqrt{-6}]$.

(d) The equality $(2+\sqrt{-6})(2-\sqrt{-6}) = 2 \cdot 5$ shows that $2+\sqrt{-6}$ divides the product $2 \cdot 5$ in $\mathbb{Z}[\sqrt{-6}]$. Show, however, that $2+\sqrt{-6}$ divides neither 2 nor 5 in $\mathbb{Z}[\sqrt{-6}]$. *Hint: Assume that $2 = (2+\sqrt{-6})\gamma$ for some $\gamma \in \mathbb{Z}[\sqrt{-6}]$ and apply N to both sides.*

The significance of the above exercise is that it shows that $2+\sqrt{-6}$ is an irreducible element of $\mathbb{Z}[\sqrt{-6}]$ but not a prime element, so $\mathbb{Z}[\sqrt{-6}]$ does not have uniqueness of factorization.

98. (a) It is a fact that if $t \in \mathbb{Z}/13\mathbb{Z}$, then $t^2 \notin \{[5], [-5]\}$. (You may verify this, if you wish.) Using this fact, show that if k is an integer such that $k \equiv \pm 5 \bmod 13$, then the equation $x^2 - 26y^2 = k$ has no solutions $x, y \in \mathbb{Z}$. See Question 76 if you need some help.

(b) Use your answer to part (a) to show that 31 is irreducible in $\mathbb{Z}[\sqrt{26}]$. See Question 96 or Question 97 if you need some help.

99. Show that there is no Euclidean function on $\mathbb{Z}[x]$. **Caution:** It is not enough to show that there is no Euclidean function defined in terms of the degree. It has to be shown that there are no Euclidean functions whatsoever on $\mathbb{Z}[x]$. The last example in Section IV – 9 of the course notes will help.

100. Let $\alpha \in \mathbb{R}$ satisfy $\alpha^2 = 1 + \alpha$, let $R = \{x + y\alpha \in \mathbb{R} \mid x, y \in \mathbb{Z}\}$, and let $I = (2)_R = 2R$. If $x + y\alpha \in R$, abbreviate the coset $(x + y\alpha) + I$ by $[x + y\alpha]$.

(a) The quotient ring R/I consists of the four elements $[0], [1], [\alpha], [1 + \alpha]$. Compute the multiplication table for R/I.

(b) In light of your answer to part (a), decide whether I is a maximal ideal of R, giving your reasoning.