

1 FUNCTIONS. Say which of the following rules successfully define functions, giving reasons. For each one which is a function, say whether it is injective, surjective, both or neither, again giving reasons.

- (a) $f : \mathbb{N} \rightarrow \mathbb{N}$ given by $f(n) = n^2 + n + 41$.
- (b) $f : \mathbb{Q} \rightarrow \mathbb{Z}$ given by $f(a/b) = a + b$.
- (c) $f : \mathbb{Q} \times \mathbb{Q} \rightarrow \mathbb{Q}$ given by $f(a/b, c/d) = (2ad - bc)/bd$.
- (d) $f : \mathbb{R} \rightarrow \{0, 1\}$ given by $f(x) = 0$ if $x \in \mathbb{Q}$ and $f(x) = 1$ otherwise.
- (e) $f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Q}$ given by $f(a, b) = a/b$.

2 OPERATIONS. Say which of the following successfully define binary operations on the set A , giving your reasons. For each one which is a binary operation, say whether it is associative, commutative, both or neither, again giving reasons.

- (a) $A = \mathbb{N}$, $m \circ n = \frac{m}{n}$ if $m, n \in A$. Here $\mathbb{N} = \{1, 2, 3, \dots\}$ denotes the natural numbers.
- (b) $A = \mathbb{Z}$, $m \circ n = m - n$ if $m, n \in A$. Here \mathbb{Z} denotes the integers.
- (c) $A = \mathbb{R}$, $x \circ y = x^y$ if $x, y \in A$. Here \mathbb{R} denotes the real numbers.
- (d) $A = \mathbb{C}$, $w \circ z = w + iz$ if $w, z \in \mathbb{C}$. Here \mathbb{C} denotes the complex numbers and $i = \sqrt{-1}$.
- (e) $A = P(U)$, i.e., the set of all subsets of U , where U is a given non-empty set, and $X \circ Y = |X \cap Y|$ if $X, Y \in A$. Here $|X|$ denotes the cardinality of a subset X .

3 Say which of the following successfully define binary operations, giving your reasons.

(a) $A = \mathbb{Q}$, $x \circ y = \frac{x}{y}$ if $x, y \in A$.

(b) $A = \{m \in \mathbb{N} \mid m \geq 3\}$, $m \circ n = mn - (m + n)$ if $m, n \in A$.

(c) $A = \mathbb{C}$ and if $x, y \in \mathbb{C}$, $x \circ y$ solves the equation $Z^2 + xZ + y = 0$ for Z .

4 Let $A = P(U)$, the set of subsets of a given set U and $X \circ Y = X \Delta Y$, the symmetric difference, if $X, Y \in A$. Using Venn diagrams, or otherwise, show that \circ is an *associative* binary operation on A .

5 Let $B \subseteq A$ be closed under a binary operation \circ on A and let \circ_B on B be as in lectures.

(a) Prove that if A has an identity element e with respect to \circ and if $e \in B$ then e is an identity element with respect to \circ_B .

(b) Let $A = M_2(\mathbb{Z})$ and $B = M_2(2\mathbb{Z})$ (where the matrix entries are even). Show that $B \subseteq A$ is closed under the binary operation \circ of matrix multiplication in A .

(c) Does \circ_B in the example of part (b) have an identity element? Justify your answer briefly.

6 Let \circ be a binary operation on a set A and let \circ be associative and have an identity element e in A .

(a) State what it means for an element of A to be invertible with respect to \circ .

(b) Let a be an invertible element of A with inverse a^{-1} . Prove that a and a^{-1} commute with each other.

(c) Show in part (b) that a^n defined as $a \circ a \circ \dots \circ a$ (n times) is invertible and find its inverse. Here $n \in \mathbb{N} = \{1, 2, \dots\}$.

7 RELATIONS. Say which of the following successfully define (binary) relations on the set A , giving your reasons. For those which are relations, say which of the following properties it has, and which it does not have: reflexive, irreflexive, symmetric, anti-symmetric, transitive. For those which are equivalence relations, describe the equivalence classes.

- (a) $A = \mathbb{Z}$, and $a \sim b$ whenever $a + b$ is a prime number. (Note: 0 and 1 are not prime numbers.)
- (b) $A = \mathbb{R}$, and $a \sim b$ whenever $\sin a = \cos b$.
- (c) $A = \{1, 2, 3, 4, 5\}$ and $R = \{(1, 2), (2, 3), (3, 4), (4, 5)\}$.
- (d) $A = \{1, 2, 3, 4\}$ and $R = \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 2), (2, 1)\}$.
- (e) $A = \mathbb{C}$, and $z \sim w$ whenever $|z| = |w|$.

8 HARDER.

- (a) Define the relation \sim on the set \mathbb{R} of real numbers by $a \sim b$ whenever $a - b \in \mathbb{Q}$. Prove that \sim is an equivalence relation.
 - (b) Prove that if $a \sim a'$ then $a + b \sim a' + b$. Hence show that the rule $[a] \oplus [b] = [a + b]$ defines a binary operation \oplus on the set of equivalence classes. Show that this operation is associative and commutative.
 - (c) Do the same for the rule $[a] \otimes [b] = [ab]$.
 - (d) Show that the rule $\ominus[a] = [-a]$ defines a unary operation on the set of equivalence classes, and prove that $[a] \oplus (\ominus[a]) = [0]$.
- 9**
- (a) Define $f : \mathbb{Z} \rightarrow \mathbb{Z}$ by $f(n) = n$ if n is even and $f(n) = -n$ if n is odd. Decide whether f is injective, surjective, both or neither (with reasons).
 - (b) Prove carefully that the symmetric difference operation is associative, that is $(A \Delta B) \Delta C = A \Delta (B \Delta C)$ for any sets A, B, C .
 - (c) Define a relation \sim on $P(\mathbb{N})$ (i.e. the set of all sets of natural numbers) by $A \sim B$ whenever $|A| = |B|$. Show that \sim is an equivalence relation, and describe the equivalence classes.

10 CHALLENGE QUESTION. Ternary operations are functions $f : A \times A \times A \rightarrow A$, and there are a number of useful ones which you may have come across, for example:

- (a) $A = \mathbb{R}$ (or \mathbb{Z} or \mathbb{Q} , etc.) and $f(a, b, c) = ab + c$.
- (b) $A = \mathbb{R}^3$ and $f(\mathbf{u}, \mathbf{v}, \mathbf{w}) = (\mathbf{u} \times \mathbf{v}) \cdot \mathbf{w}$.

There are various interesting properties which ternary relations may or may not have, such as *symmetry*: f is *cyclically symmetric* if $f(a, b, c) = f(b, c, a)$, and *totally symmetric* if also $f(a, b, c) = f(a, c, b)$. Show that (b) is cyclically symmetric but not totally symmetric. Investigate other ternary relations and other useful properties they may have.

11 For each set A and binary operation \circ on A listed below answer the following questions giving reasons for your answer.

- (i) Is \circ associative ?
- (ii) Is \circ commutative ?
- (iii) Is there an identity element for \circ in A ? If so, what is it ?
- (iv) If the answer to (iii) is yes, which elements of A have an inverse under \circ in A ?

- (a) $A = \mathbb{Z}$; if $m, n \in A$ then $m \circ n$ is defined to be $(m + n)^2$.
- (b) $A = \mathbb{Z}$; if $m, n \in A$ then $m \circ n$ is defined to be $m + n - mn$.
- (c) $A = S(2)$ the set of permutations of two objects, with \circ composition of permutations.

12 If $B \subseteq A$ is closed under a binary operation \circ on A , define as in the lectures $a \circ_B b = a \circ b$ for all $a, b \in B$.

- (a) Explain why \circ_B is associative if \circ is.
- (b) Explain why \circ_B is commutative if \circ is.
- (c) Let $A = M_2(\mathbb{R})$ and $B = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{R} \right\}$. Show that B is closed under matrix multiplication and \circ_B is commutative. Show that \circ_B has an identity element by finding it.
- (d) In the example of part (c), which elements of B are invertible with respect to \circ_B in B ? Which, if any, of the elements invertible with respect to \circ_B in B are invertible with respect to \circ in A ?

13 RINGS. Say which of the following rules successfully define rings, giving reasons. For each one which is a ring, say whether it is commutative, whether it has an identity element, and whether it is a division ring, again giving reasons.

- (a) \mathbb{Z} , with the usual addition and multiplication.

- (b) \mathbb{Z} , with the usual addition, and multiplication defined by $a \times b = ab/2$.
- (c) $\mathbb{Z} \times \mathbb{Z}$, with addition $(a, b) + (c, d) = (a+c, b+d)$ and multiplication $(a, b) \cdot (c, d) = (ac, bd)$.
- (d) $\mathbb{R} \times \mathbb{R}$, with the same operations.
- (e) $\mathbb{Z} \times \mathbb{N}$ with addition $(a, b) + (c, d) = (ad+bc, bd)$ and multiplication $(a, b) \cdot (c, d) = (ac, bd)$, where $\mathbb{N} = \{1, 2, 3, \dots\}$.
- (f) $\{a, b, c, d\}$ with addition and multiplication defined by

$+$	a	b	c	d	\times	a	b	c	d
a	a	b	c	d	a	a	a	a	a
b	b	a	d	c	b	a	b	c	d
c	c	d	a	b	c	a	c	d	b
d	d	c	b	a	d	a	d	b	c

- (g) The set of polynomials with real coefficients, with the usual addition, and multiplication \circ defined by $(f \circ g)(x) = f(g(x))$.

14 Let R be a ring with identity (written 1) and write the zero as 0. Say which of the following statements are *true* and which are *false*, justifying your answer.

- (a) $0 \cdot 0 = 0$.
- (b) $(-1) \cdot 1 = -1$.
- (c) $1 + 1 \neq 0$.

15 Let R be a ring with identity (written 1 and different from 0).

- (a) Show that if R has only two elements, it must be a Boolean ring.
- (b) Show that if R has only three elements, it must be commutative.
- (c) Show that in both parts (a) and (b), R must be a field. You may assume without proof that $(-1) \cdot (-1) = 1$. (Hint: in part (b) if the elements are $0, 1, x$, what values could $1 + x$ have and hence what must x be?)

16 If R is any ring, it can be shown that $M_2(R)$ (i.e., 2×2 matrices with entries in R) is also a ring. You are *not* asked to prove this.

- (a) If R is a ring with identity, show that $M_2(R)$ is necessarily a ring *with identity* and find the identity element.
- (b) If R is a division ring, is $M_2(R)$ necessarily a division ring? Justify your answer.
- (c) If R is commutative, is $M_2(R)$ necessarily commutative? Justify your answer.

17 Let $R = \mathbb{Z}/3\mathbb{Z}$ denote the integers modulo 3 with elements $[0], [1], [2]$, where $[i]$ denotes the integer i modulo 3. The addition and multiplication modulo 3 are defined by the corresponding operations for integers: $[i] + [j] = [i + j]$ and $[i] \times [j] = [ij]$ (you may assume without proof that these define associative binary operations on R). Show that $+, \times$ make R into a ring.

18 POWER SET. Let A be any set, and let $X = \mathcal{P}(A)$ be the set of all subsets of A , that is

$$\mathcal{P}(A) = \{B \mid B \subseteq A\}.$$

Define addition on X by $B + C = B \cup C$, and define multiplication by $B.C = B \cap C$.

Show that X satisfies all the axioms of a ring except the existence of additive inverses.

19 PROPERTIES OF RINGS. Let R be a ring with identity.

- (a) Prove that the identity element is unique.
- (b) Prove that if R is a division ring then inverses are unique.
- (c) Prove that if $0 = 1$ then $R = \{0\}$.

20 EXAMPLES. Construct examples of rings R with the following properties.

- (a) R is commutative but has no identity element.
- (b) R is non-commutative and has no identity element.
- (c) R is non-commutative and has an identity element, but is not a division ring.
- (d) $x.x = x$ for all $x \in R$.

21 Let A be any set, and let $X = \mathcal{P}(A)$ be the set of all subsets of A , that is

$$\mathcal{P}(A) = \{B \mid B \subseteq A\}.$$

Define addition on X by $B + C = B \Delta C$, and define multiplication by $B.C = B \cap C$.

- (a) Show that X is a ring.
- (b) What is the zero element of this ring?
- (c) Does X have an identity? If so, what is it?
- (d) Is X a division ring?

[Justify all your answers.]

22 EXTENSION QUESTION. Investigate which axioms of a ring can be dropped. On the one hand, by commutativity of addition, $0 + x = x$ is equivalent to $x + 0 = x$, so one of these is redundant. On the other hand, we have seen examples of objects which satisfy all the ring axioms except one. For example, can you give examples of sets with two binary operations which

- (a) satisfy all the ring axioms except one of the distributive laws?
- (b) satisfy all the ring axioms except the associative law of multiplication?

What about a ring with identity? Or a division ring?

23 MATRIX RINGS.

- (a) In any ring with identity, an element a is called *invertible* if there is an element x such that $ax = xa = 1$. This element x is called the *inverse* of a , and is denoted a^{-1} . Prove that if a and b are invertible, then so is ab , and $(ab)^{-1} = b^{-1}a^{-1}$.
- (b) Let R be the ring of 2×2 matrices with entries in $\mathbb{Z}/2\mathbb{Z}$ (that is, integers modulo 2).
 - (i) How many elements does R have?
 - (ii) Write down the zero and one of R .
 - (iii) Write down all the invertible elements of R , with their inverses.
 - (iv) Explain why the other elements of R are not invertible.

24 POLYNOMIAL RINGS. Let R be the ring of polynomials with coefficients in $\mathbb{Z}/4\mathbb{Z}$.

- (a) Calculate $(3x^2 + 2x + 1).(x + 1)$ in this ring. (Here 3 is shorthand for the coset $[3]_4$, i.e. the congruence class of 3 modulo 4, etc.)
- (b) Show that in this ring $(x + 1)^2 = (x + 3)^2$. Does this worry you? Should it worry you?

25 SUBRINGS. In each case use a suitable subring test to determine whether or not S is a subring of R .

- (a) $R = \mathbb{Z}$, S the subset of odd integers.
- (b) $R = \mathbb{Z}$, $S = 5\mathbb{Z}$.
- (c) $R = \mathbb{C}$, $S = \{a + bi \mid a, b \in \mathbb{Z}\}$.
- (d) $R = \mathbb{R}$, $S = \{a + b2^{1/3} \mid a, b \in \mathbb{Q}\}$.
- (e) $R = M_2(\mathbb{Z})$, $S = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid c \equiv 0 \pmod{n} \right\}$.
- (f) $R = \mathbb{Q}[x]$, the ring of polynomials (in the dummy variable x) with rational coefficients, S the subset of polynomials of even degree.
- (g) $R = \mathbb{Q}[x]$, S the subset of polynomials with constant term 0.
- (h) R any ring with identity, and S the subset of invertible elements.

26 Using the subring test, determine which of the following subsets S are *subrings* of the stated ring R , giving your reasons.

- (a) $S = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{R} \right\} \subseteq R = M_2(\mathbb{R})$.
- (b) $S = P(V) \subseteq R = P(U)$ where $V \subseteq U$ are sets and $P(U)$ is the ring of subsets of U with the operations of Δ and \cap , similarly for $P(V)$.
- (c) $S = \{f(X) \mid f(1) = 0\} \subseteq R = \mathbb{Z}[X]$.

27 Let $S = \mathbb{Z}$ be viewed as a subring of $R = \mathbb{R}$. Describe the distinct cosets of S in R in terms of the real number line and briefly describe how they partition R .

28 Explain what it means for two groups to be *isomorphic*. Show that

- (a) $U(\mathbb{Z}/4\mathbb{Z})$ is isomorphic to the additive group of $\mathbb{Z}/2\mathbb{Z}$.
- (b) $U(\mathbb{Z}/8\mathbb{Z})$ is isomorphic to the Klein 4-group described in lectures.

29 COSETS. For each case when S is a subring of R in Q25, say how many cosets of S in R there are, and describe the cosets of S as clearly as you can.

30 Let A be the ring $\mathbb{Z}/5\mathbb{Z}$ of integers modulo 5, and let R be the ring $M_2(A)$ of 2×2 matrices with entries from A . Let

$$S = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in R \mid c = 0 \right\}.$$

- (a) Prove that S is a subring of R .
- (b) List the cosets of S in R .
- (c) Pick any coset C of S other than S itself, and for every coset D_i of S find two elements x_i, y_i in C whose product $x_i \cdot y_i$ is in D_i .

31 EXTENSION QUESTION. Let $R = M_2(\mathbb{C})$, and let

$$S = \left\{ \begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix} \mid z, w \in \mathbb{C} \right\}.$$

Show that S is a subring of R .

Show that S is a 4-dimensional real vector space, with basis

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Write down the multiplication table for these basis elements.

Can you do a similar thing with other rings besides \mathbb{C} ? For example $\{a + bi \mid a, b \in \mathbb{Z}\}$? Or $\{a + bi \mid a, b \in \mathbb{Z}/3\mathbb{Z}\}$?

32 HOMOMORPHISMS. Which of the following define ring homomorphisms $f : R \rightarrow S$? In each case which is a ring homomorphism, calculate the image and the kernel.

- (a) $R = \mathbb{Z}, S = \mathbb{Z}, f(n) = 2n$.
- (b) $R = \mathbb{Z}, S = \mathbb{Z}, f(n) = n^2$.
- (c) $R = S = \mathbb{Z}, f(n) = n + 1$.
- (d) $R = S = \mathbb{Q}, f(x) = 2x$.
- (e) $R = M_2(\mathbb{R}), S = \mathbb{R}, f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = a$.

$$(f) R = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, b, d \in \mathbb{R} \right\}, S = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a, d \in \mathbb{R} \right\}, \text{ and } f\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\right) = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}.$$

33 IDEALS. Which of the following subsets S of the ring R are ideals? (Justify your answers.) In each case which is an ideal, construct the quotient ring R/S .

(a) $R = \mathbb{Q}, S = \mathbb{Z}$.

(b) $R = \mathbb{Z}, S = \mathbb{N}$.

(c) $R = \mathbb{Z}, S = 4\mathbb{Z}$.

(d) $R = \mathbb{C}, S = \mathbb{R}$.

(e) $R = \mathbb{R}, S = \{0\}$.

(f) $R = \mathbb{Z}[x]$, the ring of polynomials with integer coefficients, and the subset $S = \{(2x + 1)f(x) \mid f(x) \in R\}$.

(g) $R = M_2(\mathbb{Q}), S = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a \in \mathbb{Q} \right\}$.

34 (a) In the ring $\mathbb{Z}[X]$ show that the set I of polynomials for which the constant term is a multiple of 5 is an ideal. (So elts of I are of the form $5a_0 + a_1X + \dots + a_nX^n$ with $a_0, \dots, a_n \in \mathbb{Z}$.) Show that there is *no* polynomial $g(X) \in \mathbb{Z}[X]$ such that $I = (g)$.

(b) Deduce from part (a) and theory in the lectures that $\mathbb{Z}[X]$ is not a Euclidean domain.

(c) Let $I = \{a + ib \mid a, b \in \mathbb{Z}, a + b \text{ is even}\} \subseteq J$ an ideal. Find an element $z \in J$ such that $I = (z)$. (Hint: z will have minimal $|z|^2$ among elements of I . You might want to draw a picture on the complex plane to help choose z , then check it works.)

35 (a) Let R be a ring and $I \subseteq R$ an ideal. Define the quotient ring R/I stating its ring operations.

(b) State the 1st isomorphism theorem for $\theta : R_1 \rightarrow R_2$ a ring homomorphism between two rings.

- (c) Let $\theta : J \rightarrow \mathbb{Z}/2\mathbb{Z}$ be $(a + ib)\theta = [a + b] \pmod{2}$. Let I be the ideal in Q34(c). Noting that $I = \ker(\theta)$, deduce that J/I is isomorphic to the field $\mathbb{Z}/2\mathbb{Z}$.

36 State in each case whether the statement is true or false. You are *not* asked to justify your answer.

- (a) Let $I, I' \subseteq R$ be ideals in a ring R and $I \subseteq I'$, and let $\theta : R/I \rightarrow R/I'$ be $(x + I)\theta = x + I'$ for all $x \in R$. Then θ is a ring homomorphism.
- (b) In \mathbb{Z} , $(15) \subseteq (5)$.
- (c) in \mathbb{Z} , $(5) \subseteq (15)$.
- (d) In $K = \{a + b\sqrt{-6} \mid a, b \in \mathbb{Z}\}$, $I = \{a + b\sqrt{-6} \in K \mid a \text{ even}\}$ is an ideal.
- (e) In a Euclidean domain R , if $a \in R$ is irreducible and $I \subseteq R$ is an ideal with $(a) \subseteq I \subseteq R$ then $I = (a)$ or $I = R$.

37 ISOMORPHISM THEOREM. Let $R = \mathbb{Z}_9$, the ring of integers mod 9, that is $R = \{[0], [1], [2], \dots, [8]\}$ under addition and multiplication mod 9. If you like, you may write i for $[i]$.

- (a) Let S be the subset $\{[x] \mid x = 3n, n \in \mathbb{Z}\}$ of R . Prove that S is a subring of R . Show that the subring has all products zero.
- (b) Find the cosets of S in R . Show that there are 3 distinct cosets.
- (c) Define the sum and product of cosets in part (b) by the same operations in R on representative elements. Show that these operations are well-defined in this example.
- (d) Show that this ring is isomorphic to the ring \mathbb{Z}_3 .

38 (a) Let $R = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, b, d \in \mathbb{R} \right\}$, $S = \mathbb{R}$, and $f\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\right) = a$. Show that f is a ring homomorphism, and compute its kernel and image.

- (b) Let $R = \mathbb{R}[x]$, the ring of polynomials with real coefficients, and define the subset $I = \{(x^2 + 1)f(x) \mid f(x) \in R\}$. Show that I is an ideal in R , and construct the quotient ring R/I . Show that R/I is isomorphic to \mathbb{C} .

39 ISOMORPHISM THEOREMS.

- (a) Let $f : \mathbb{C} \rightarrow M_2(\mathbb{R})$ be defined by $f(a + bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$. Show that f is a ring homomorphism. What is its kernel?
- (b) Let $f : \mathbb{Q}[x] \rightarrow \mathbb{R}$ be defined by $f(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) = a_0 + a_1\sqrt{2} + a_2 \cdot 2 + \cdots + a_n(\sqrt{2})^n$. Show that f is a ring homomorphism. What is its kernel? What is its image? What does the first isomorphism theorem tell you about this situation?

40 (a) State the 2nd isomorphism theorem for rings.

- (b) Using (a), find all the ideals of $\mathbb{Z}/18\mathbb{Z}$.
- (c) Which of the ideals I of $\mathbb{Z}/18\mathbb{Z}$ in (b) are maximal? Identify $(\mathbb{Z}/18\mathbb{Z})/I$ obtained in these cases.
- (d) We saw that 11 and $1+4i$ are irreducible in \mathbb{Z} . Are the ideals (11) and $(1+4i)$ maximal? Justify your answer.
- (e) Are $\mathbb{Z}/(11)$ and $\mathbb{Z}/(1+4i)$ fields? Justify your answer.

41 Let $F = \mathbb{Z}/2\mathbb{Z}$ with elements 0,1 (and working modulo 2).

- (a) Find an irreducible polynomial $g(X) \in F[X]$ of degree 2. (Hint, g will have to be of the form $X^2 + aX + b$ for $a, b \in F$ and not vanish at $X = 0, 1$, as otherwise $X, X - 1$ respectively would be factors.)
- (b) From lectures we know that $F[X]/(g)$ is a field. How many elements does it have? Justify your answer.
- (c) Write out the addition and multiplication tables for $F[X]/(g)$. You do *not* need to show your working for the tables.
- (d) State which standard groups appear in part (c) as isomorphic to $F[X]/(g)$ under addition and $(F[X]/(g)) \setminus \{0\}$ under multiplication.

42 (a) State what it means for a subgroup $H \subset G$ of a group G to be *normal*

- (b) Which of the following subgroups are normal. Briefly justify your answers.
- (i) $S_3 \subset S_4$ as the permutations that leave 4 unchanged.
- (ii) $\{(e, (123), (132))\} \subset S_3$
- (iii) $\{A \in GL_2(\mathbb{Z}) \mid \det(A) = 1\} \subset GL_2(\mathbb{Z})$

43 ZERO DIVISORS.

- (a) List all the zero divisors in $\mathbb{Z}/16\mathbb{Z}$, the integers mod 16.
- (b) Let $\mathcal{P}(U) = \{X \mid X \subseteq U\}$ be the power set of U , with addition and multiplication defined by $X + Y = X \Delta Y$ and $X.Y = X \cap Y$. Show that every element X of the ring $\mathcal{P}(U)$ with $X \neq \emptyset, U$ is a zero divisor.
- (c) Let $R = \mathbb{Z}/8\mathbb{Z}$, and let S be the ring of polynomials with coefficients in R . Show that R has zero-divisors of degree n , for every n .
- (d) Let $R = M_2(\mathbb{C})$. Find (with justification) a zero-divisor in R .

44 UNITS.

- (a) For each ring in (a), (b) or (c) of the previous question, list the units.
- (b) Let $R = \{a + bi \mid a, b \in \mathbb{Z}\}$ be the ring of Gaussian integers. List the units in R , and the associates of $2 + i$.
- (c) Find a ring in which every element is either 0, or a unit, or a zero-divisor.
- (d) Find a ring which has exactly one unit, and no zero-divisors.

- 45** (a) Show that every element in $M_2(\mathbb{R})$ is either zero, a unit, or a zero-divisor.
- (b) Give an example to show that the same is not true in $M_2(\mathbb{Z})$.

The Gaussian integers Let J , or $\mathbb{Z}[i]$, denote the ring of Gaussian integers, that is $\{a + bi \mid a, b \in \mathbb{Z}\}$. This is a subring of the ring \mathbb{C} of complex numbers, with operations inherited from the arithmetic operations on the complex numbers. We shall also write $|z|^2 = z\bar{z}$ for the square of the absolute value of a complex number. Thus if $z = x + yi$ we have $|z|^2 = x^2 + y^2$.

46 UNIQUE FACTORISATION DOMAINS.

- (a) Show that for every non-zero $z \in J$, we have $|z|^2 \in \mathbb{N} = \{1, 2, 3, \dots\}$.
- (b) Show that $z \in J$ is a unit if and only if $|z| = 1$. List the units in J .
- (c) Show that $1 + i$ and $2 + i$ are irreducible in J . Write down all irreducibles in J which have absolute value $\sqrt{2}$ or $\sqrt{5}$, separated into associate classes.
- (d) Factorise each of 2, 3, 4, 5, 6 as products of irreducibles in J .

- (e) Prove that every element z of J , except 0 and the units, can be factorised as a product of irreducible elements.

47 MODULO 3.

- (a) Construct the quotient ring $J/3J$: write down its addition and multiplication tables.
- (b) Show that $J/3J$ is an integral domain.
- (c) Show that $J/3J$ is a field.

48 MODULO 2.

- (a) Construct the quotient ring $J/2J$: write down its addition and multiplication tables.
- (b) Show that $J/2J$ is not an integral domain.
- (c) Is $J/2J$ a field?

49 PRINCIPAL IDEAL DOMAINS.

- (a) Show that if z is any complex number then there is an element q of J such that $|z - q| < 1$.
- (b) By applying this to tw^{-1} show that if t, w are any non-zero elements of J then $t = wq + r$ for some $q, r \in J$ with $|r| < |w|$.
- (c) Now suppose that I is an ideal in J , and let w be an element of $I \setminus \{0\}$ which has absolute value as small as possible. Show that $wz \in I$ for all $z \in J$.
- (d) With this same value of w , show that if $t \in I$ then $t = wq$ for some $q \in J$.
- (e) Hence show that J is a principal ideal domain.

50 (a) Let R be the ring $\{a + b\sqrt{-2} \mid a, b \in \mathbb{Z}\}$. Prove that R is a principal ideal domain.

- (b) Let S be the ring $\{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$. Show that the subset of all elements $a + b\sqrt{-5}$ of S for which $a + b$ is even is an ideal of S , but is not of the form $(x + y\sqrt{-5})S$ for any $x + y\sqrt{-5} \in S$.

51 EXTENSION QUESTION. You saw in Question 46 that some primes in \mathbb{Z} are irreducible in $\mathbb{Z}[i]$, and some are not.

- (a) Can you find a simple rule which distinguishes the two cases?
- (b) Can you prove it?

Notation If R is any ring, then $R[x]$ denotes the ring of all polynomials with coefficients in R .

If x is replaced by a constant α , such as i or $\sqrt{2}$ or $\sqrt{-3}$, then $R[\alpha]$ denotes the image of $R[x]$ under the map $x \mapsto \alpha$. For example $\mathbb{Q}[\sqrt{-2}] = \{x + y\sqrt{-2} \mid x, y \in \mathbb{Q}\}$.

We shall also write $|z|^2 = z\bar{z}$ for the square of the absolute value of a complex number. Thus if $z = x + yi$ we have $|z|^2 = x^2 + y^2$.

Euclidean domains The correct definition of a Euclidean domain is as follows:

An integral domain R is a *Euclidean domain* if there is a function $d : R \setminus \{0\} \rightarrow \mathbb{N} = \{0, 1, 2, 3, \dots\}$ satisfying

- (a) $d(ab) \geq d(a)$ whenever a, b are non-zero;
- (b) if $a, b \in R$ and $b \neq 0$, there exist $q, r \in R$ with (i) $a = bq + r$ and (ii) either $d(r) < d(b)$ or $r = 0$.

52 EUCLIDEAN DOMAINS. Which of the following are Euclidean domains, with Euclidean function d ? Give brief justifications.

- (a) \mathbb{Z} , with $d(n) = n^2$.
- (b) $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$, with $d(a + bi) = |a + bi|^2 = a^2 + b^2$.
- (c) $\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$, with $d(z) = |z|^2$.
- (d) $\mathbb{Q}[x]$, with $d(f) = \deg(f)$.
- (e) $\mathbb{Z}[x]$, with $d(f) = \deg(f)$.

53 A COUNTEREXAMPLE.

- (a) Let $\tau = (1 + \sqrt{5})/2$, and let $R = \mathbb{Z}[\tau] = \{a + b\tau \mid a, b \in \mathbb{Z}\}$. Show that τ is a unit in R , and deduce that R contains infinitely many units.
- (b) Let I be a non-zero ideal in $R = \mathbb{Z}[\tau]$. Show that I contains elements arbitrarily close to 0.

54 Explain what is meant by an *integral domain*. Determine which of the following are integral domains, giving your reasons

- (a) $\mathbb{Z}/15\mathbb{Z}$
- (b) $M_2(\mathbb{C})$
- (c) $J[X]$ where J is the Gaussian integers (which you can assume is an integral domain).

55 Let R be a commutative ring with identity and $a, b \in R$. We can define that a is an associate of b if $a = bu$ for some $u \in U(R)$. Show that in this case b is a zero divisor if and only if a is.

56 In the Gaussian integers J , say which of the following z are irreducible in J , giving your reasons, and if z is not irreducible, express it as product of two or more irreducible elements of J .

$$(a) z = 11, \quad (b) z = 1 + 3i, \quad (c) z = -3 + i, \quad (d) z = 1 + 4i$$

57 State a Euclidean function d on each of the following integral domains R , and for the given $a, b \in R$ find q, r obeying the condition (ii) for a Euclidean function:

(a) $R = J$ and $a = 5 + 2i, b = 2 + 3i$.

(b) $R = F[X]$ where $F = \mathbb{Z}/3\mathbb{Z}$ and $a = X^6 + X^2 - 1, b = X^4 + 2$.

(c) $R = \mathbb{Z}/7\mathbb{Z}$ and $a = [2], b = [3]$.

58 FIELDS.

(a) Let $R = \mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} \mid a, b \in \mathbb{Z}\}$, and let I be the ideal $(1 + \sqrt{-2})R$. Using the first isomorphism theorem, or otherwise, prove that $R/I \cong \mathbb{Z}_3$, the field of integers modulo 3.

(b) Let $R = \mathbb{Q}[x]$ and let $I = (x^2 + 2)F$. Show that $x^2 + 2$ is irreducible in R . Show that R/I consists of the cosets $I + f(x)$, where $\deg(f) \leq 1$, together with the identity coset I . Show that $(I + x).(I + x) = I - 2$. Find the inverse in R/I of the element $I + (ax + b)$.

(c) Let $F = \mathbb{Z}/2\mathbb{Z}$, the field of order 2. Let $R = F[x]$, the ring of polynomials with coefficients in F . Show that $x^3 + x + 1$ is irreducible in R . Deduce that $F[x]/\langle x^3 + x + 1 \rangle$ is a field. How many elements does it have? Write down its addition and multiplication tables.

59 Which of the following are Euclidean domains? Justify your answers. [\mathbb{Z}_n denotes the ring of integers modulo n .]

(a) $\mathbb{C}[x]$ with $d(f) = \deg(f)$.

(b) \mathbb{Z} with $d(n) = |n| + 1$.

(c) $\mathbb{Z}_5[x]$ with $d(f) = 2 \deg(f)$.

(d) $\mathbb{Z}_6[x]$ with $d(f) = \deg(f)$.

(e) $\mathbb{Z}[\omega]$, where $\omega = (1 + \sqrt{-3})/2$, with $d(z) = |z|^2$.

60 (a) State the unique factorisation theorem for Euclidean domains.

(b) In the integral domain $K = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$, factorise 4 into irreducibles in two different ways and hence show that K is not a Euclidean domain.

61 Define the notion of a ring homomorphism from a ring R_1 to R_2 . For each of the following rings R_1, R_2 and maps $\theta : R_1 \rightarrow R_2$, state whether θ is (i) a ring homomorphism (ii) 1-1 (iii) onto.

(a) $R_1 = M_2(\mathbb{Z}), R_2 = M_2(\mathbb{R}), x\theta = x$ for all $x \in R_1$.

(b) $R_1 = \mathbb{Z}/15\mathbb{Z}, R_2 = \mathbb{Z}/5\mathbb{Z}, [a]\theta = [a]$ for all $[a] \in R_1$ (here θ maps $a \bmod 15$ to $a \bmod 5$).

(c) $R_1 = J, R_2 = \mathbb{Z}, (a + ib)\theta = a + b$.

Note that you are *not* asked to justify your 9 answers to this question.

62 Define the image and kernel of a ring homomorphism $\theta : R_1 \rightarrow R_2$. Let $R_1 = (\mathbb{Z}/2\mathbb{Z})[X], R_2 = \mathbb{Z}/2\mathbb{Z}$ and $f\theta = f(1)$ for all $f \in (\mathbb{Z}/2\mathbb{Z})[X]$.

(a) Find $\text{image}(\theta)$.

(b) Show that $\text{kernel}(\theta)$ consists precisely of polynomials in $(\mathbb{Z}/2\mathbb{Z})[X]$ with an even number of terms.

63 Define what it means for a subset $I \subseteq R$ of a ring to be an *ideal*. Let $R = J$ and $I = \{a + ib \mid a + b \text{ is even}\} \subset J$. Is this an ideal? Justify your answer.

64 GROUPS. Which of the following are groups? Which ones are Abelian? Justify your answers.

(a) \mathbb{R} with the operation $+$.

(b) $\mathbb{R} \setminus \{0\}$ with multiplication.

(c) $\{x \in \mathbb{R} \mid x > 0\}$ with multiplication.

(d) $\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Q}, ad - bc = 1 \right\}$ with matrix multiplication.

(e) $\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}$ with matrix multiplication.

(f) $G \times H$, where G and H are groups, with the operation $(g_1, h_1) \circ (g_2, h_2) = (g_1g_2, h_1h_2)$.

- (g) $\left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\}$ with matrix multiplication.
- (h) $\{z \in \mathbb{C} \mid |z| = 1\}$ under multiplication.
- (i) $\{[k]_n \in \mathbb{Z}_n \mid \gcd(k, n) = 1\}$ under multiplication of integers modulo n .
- (j) the set of non-zero polynomials over \mathbb{Q} , under multiplication.

65 SUBGROUPS OF S_n . Which of the following subsets of S_n are subgroups?

- (a) H consisting of all permutations which have no fixed points.
- (b) H consisting of all permutations which have at least one fixed point.
- (c) H consisting of all permutations which fix the point n .

66 SUBGROUPS of $\mathbb{C} \setminus \{0\}$. Which of the following subsets of \mathbb{C} are subgroups of the multiplicative group of units?

- (a) H consisting of all z with $|z| \geq 1$.
- (b) H consisting of all non-zero z with $|z| \in \mathbb{Q}$.
- (c) H consisting of all non-zero $x + iy$ with $x, y \in \mathbb{Q}$.

67 SUBGROUPS OF $GL_2(\mathbb{R})$. Which of the following subsets of $GL_2(\mathbb{R})$ are subgroups, under matrix multiplication?

- (a) H consisting of all matrices A with trace zero.
- (b) H consisting of all matrices A with determinant 2^n (for some $n \in \mathbb{Z}$).
- (c) H consisting of all matrices $A = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ for some $a, b, d \in \mathbb{R}$.

68 Using the subgroup test, or otherwise, determine which of the following subsets H are subgroups of the stated group G , giving your reasons.

- (a) $H = \{e, (12), (23), (13)\} \subseteq G = S_3$
- (b) $H = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{Q}, a^2 + b^2 = 1 \right\} \subseteq G = GL_2(\mathbb{Q})$.
- (c) $H = \{1, x, x^2, \dots, x^7\} \subseteq G = \{1, x, x^2, \dots, x^8\}$, the cyclic group of order 9.

(d) $H = \{A \mid \det A \in \mathbb{Z}\} \subseteq G = GL_3(\mathbb{R})$.

(e) $H = \{[k] \mid k \text{ even}\} \subseteq G = \mathbb{Z}/13\mathbb{Z}$ with group operation being addition.

69 Using the subgroup test, determine which of the following subsets H are *subgroups* of the stated group G , giving your reasons.

(a) $H = \{e, (12), (23), (13)\} \subseteq G = S_3$.

(b) $H = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{Q}, a^2 + b^2 = 1 \right\} \subseteq G = GL_2(\mathbb{Q})$.

(c) $H = \{e, x, x^2, \dots, x^7\} \subseteq G = \{e, x, x^2, \dots, x^8\}$, the cyclic group of order 9.

70 COSETS.

(a) Suppose that S is a subring of the ring R . Show that S is a subgroup of the additive group of R . Show that the (left or right) cosets of S as a subgroup of R are the same as the cosets of S as a subring of R .

(b) Let G be the group

$$\{1, (1, 2, 3, 4), (1, 3)(2, 4), (1, 4, 3, 2), (1, 2)(3, 4), (1, 4)(2, 3), (1, 3), (2, 4)\}.$$

(This is called the *dihedral group* of order 8, written D_8 .) Compute the left cosets of $H = \{1, (1, 2, 3, 4), (1, 3)(2, 4), (1, 4, 3, 2)\}$ and of $K = \{1, (1, 3)\}$. Compute also the right cosets. What do you notice?

71 LAGRANGE'S THEOREM.

(a) Use Lagrange's Theorem to list all the subgroups of S_3 .

(b) Find all the subgroups of the group $\{1, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$ (which is itself a subgroup of S_4).

(c) Check that the set

$$G = \{1, (a, b)(c, d), (a, b, c) \mid a, b, c, d \text{ are distinct elements of } \{1, 2, 3, 4\}\}$$

is a subgroup of order 12 in S_4 . Use Lagrange's Theorem to help you find all the subgroups of G . What does this tell you about the converse of Lagrange's Theorem?

72 Let $G = \{(a, b) \mid a, b \in \mathbb{Z}/2\mathbb{Z}\}$ with group operation $+$ defined by

$$(a, b) + (c, d) = (a + c, b + d),$$

in other words, the addition as vectors with entries in $\mathbb{Z}/2\mathbb{Z}$. You are *not* asked to show that this is a group. Show that G is isomorphic to the Klein 4-group.

73 (a) Find the order of the group $G = GL_3(\mathbb{Z}/2\mathbb{Z})$. You may assume that two nonzero row vectors with entries in $\mathbb{Z}/2\mathbb{Z}$ are linearly independent iff they are not equal, and three of them are linearly independent iff no two of them are equal and one is not the sum of the other two.

(b) Show that $H = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{Z}/2\mathbb{Z} \right\}$ is a subgroup of G .

(c) State Lagrange's theorem and check that it holds for H in (b).

(d) How many distinct cosets of H in G above are there?

74 (a) Show that $H = \{e, (23)\}$ is a subgroup of $G = S_3$.

(b) Find all the cosets of H in G above, listing their members.

(c) In the group S_9 , find

$$o((123)), \quad o((12)(34)), \quad o((12)(234)).$$

75 Let $0 \neq [a] \in \mathbb{Z}/m\mathbb{Z}$ where $m \in \mathbb{N}$ and $a \in \{1, \dots, m-1\}$. Let $d = o([a])$ in the group $\mathbb{Z}/m\mathbb{Z}$ under *addition*.

(a) Explain why m divides ad .

(b) Explain why $\frac{m}{d}$ is always an integer and why $\frac{m}{d}$ divides a .

(c) Deduce from (b) that if $\gcd(a, m) = 1$ then $d = m$ and hence that $\langle [a] \rangle = \mathbb{Z}/m\mathbb{Z}$.

(d) Deduce from (c) that in this case $[a]$ is invertible under *multiplication* in the ring $\mathbb{Z}/m\mathbb{Z}$.

76 (a) Let G be a group that contains distinct elements $x, y, z \neq e$ obeying $x^2 = y^2 = z^2 = e$ and $xy = z$. Here e denotes the group identity element. Show that $H = \{e, x, y, z\}$ is a subgroup of G with the group table that we gave in lectures for

the Klein four group. (Hint: look at $(xy)^{-1}$ to deduce that $yx = z$ and look at xz to deduce that $xz = y$. The rest can be deduced, or argued similarly.)

(b) Using part (a), deduce that if G is any group of order ≥ 4 for which all elements other than the group identity have order 2, then G contains the Klein four group as a subgroup.

77 Let G be the ‘quaternion group’ defined by $G = \{e, -e, I, -I, J, -J, K, -K\}$ where

$$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

and the group product is given by matrix multiplication. Do not prove that G is a group.

(a) Show that

$$I^2 = J^2 = K^2 = -e, \quad IJ = K.$$

(b) Is G abelian? Justify your answer.

(c) Find all possible order 2 subgroups of G . (Hint: a subgroup must contain e . Which choices for the other element work?)

(d) Show that every subgroup of G is normal. (Hint: what are potential values for the order of the subgroup? Come up with an argument for each potential case.)

(e) Find three distinct subgroups of G of order 4.

78 (a) Define the notion of a group homomorphism.

(b) Let $K = \{e, x, y, z\}$ be the ‘Klein four group’ with group table as in Q76. Find a surjective group homomorphism $\theta : G \rightarrow K$ where G is the ‘quaternion group’ in Q77. You are *not* asked to prove in detail that θ is a group homomorphism. (Hint: compare $xy = z$ in K with part (a) of Q77).

(c) Find $\ker \theta$ for θ in part (b).

79 HOMOMORPHISMS. Which of the following functions $f : G \rightarrow H$ are homomorphisms? Which are isomorphisms? In each case which is a homomorphism, find the kernel and the image.

(a) $G = C_6 = \langle g \rangle$, $H = C_2 = \langle h \rangle$, $f(g^k) = h^k$ for every integer k .

(b) $G = C_7 = \langle g \rangle$, $H = C_3 = \langle h \rangle$, $f(g^k) = h^k$.

(c) $G = C_n = \langle g \rangle$, $H = G$, $f(g^k) = g^{2k}$.

(d) $G = H$ any Abelian group, $f(x) = x^2$.

(e) $G = H = S_3$, $f(x) = x^2$.

80 NORMAL SUBGROUPS. Which of the following sets H are normal subgroups of the group G ? Justify your answers.

- (a) $G = C_8 = \langle g \rangle$, $H = \{1, g^2, g^4, g^6\}$.
- (b) $G = S_3$, $H = \{1, (1, 2)\}$.
- (c) $G = S_3$, $H = \{1, (1, 2, 3), (1, 3, 2)\}$.
- (d) $G = S_4$, $H = \{1, (1, 2, 3, 4), (1, 3)(2, 4), (1, 4, 3, 2)\}$.

81 (a) Suppose G is an Abelian group, and let $f : G \rightarrow G$ be the function defined by $f(x) = x^3$.

- (i) Show that f is a group homomorphism.
 - (ii) Show that f is an isomorphism if $|G|$ is not divisible by 3.
- (b) Give an example to show that $f : x \mapsto x^3$ need not be a homomorphism if G is non-Abelian.
- (c) Suppose that G is a group in which $x^2 = e$ for all $x \in G$. Prove that G is Abelian.

82 EXTENSION QUESTION. Finite Abelian groups.

- (a) Show that the direct product of Abelian groups is Abelian. Deduce that the direct product of any number of cyclic groups is Abelian.
- (b) For finite groups, the converse is also true, but harder to prove: if A is any finite Abelian group, pick $x \in A$ of largest possible order, and let $C = \langle x \rangle$. Then show that $A \cong C \times B$ for some subgroup B of A .

Hence the result follows by induction on the order of A .

- (c) In this way we find that $A = C_a \times C_b \times C_c \times \cdots$, and we have that a is a multiple of b , b is a multiple of c , and so on. It is not obvious that different choices of x give us the same sequence of numbers a, b, c, \dots . To prove this, show that different sequences a_1, b_1, c_1, \dots and a_2, b_2, c_2, \dots give rise to non-isomorphic groups.

83 (a) State the definition of a quotient group G/N where $N \subseteq G$ is a normal subgroup.

- (b) State the first isomorphism theorem for groups.

(c) Let R be a commutative ring with 1 and let

$$G = GL_2(R) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in R, ad - bc \in U(R) \right\}.$$

You may assume that this is a group. Let $f : G \rightarrow U(R)$ be given by $f(A) = \det A$. Is this necessarily a group homomorphism? Briefly justify your answer.

(d) Compute the kernel and image of f in part (c).

(e) Deduce that $G/\ker f$ in the case $R = J = \mathbb{Z}[i]$ (the Gaussian integers) is isomorphic to the cyclic group of order 4 defined by $\langle i \rangle$ where $i = \sqrt{-1}$.

(f) Find an element of $G/\ker f$ corresponding to $-1 \in \langle i \rangle$ in part (e).

84 (a) State the 2nd isomorphism theorem for groups.

(b) Let $G = GL_2(J)$ as in Q83(e),(f) and $N = \ker f$ there. Find all subgroups of G/N in this case.

(c) Find all subgroups $K \subseteq G$ containing N . (Hint: use the construction in the proof of (a) and use Q1(f).)

85 Let G be the ‘quaternion group’ defined by $G = \{e, -e, I, -I, J, -J, K, -K\}$ where

$$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

and the group product is given by matrix multiplication. Do not prove that G is a group.

(a) Show that

$$I^2 = J^2 = K^2 = -e, \quad IJ = K.$$

(b) Is G abelian? Justify your answer.

(c) Find all possible order 2 subgroups of G . (Hint: a subgroup must contain e . Which choices for the other element work?)

(d) Show that every subgroup of G is normal. (Hint: what are potential values for the order of the subgroup? Come up with an argument for each potential case.)

(e) Find three distinct subgroups of G of order 4.

86 In S_5 the number of elements of various ‘cycle shape’ are

$$|\{2 - \text{cycles}\}| = 10, \quad |\{3 - \text{cycles}\}| = 20, \quad |\{4 - \text{cycles}\}| = 30$$

$$|\{5 - \text{cycles}\}| = 24, \quad |\{2 - 2 - \text{cycles}\}| = 15, \quad |\{2 - 3 - \text{cycles}\}| = 20$$

and there is one other possibility, e (consisting of 1-cycles).

Let $N \subseteq S_5$ be a normal subgroup and $\{e\} \neq N$. We know from (7.5) that N must contain all elements of a given shape if it contains any element of that shape, and $|N|$ must divide $|S_5| = 120$.

(a) Noting that 1 plus any nonzero multiple of 10 cannot divide 120, deduce that N must contain 2-2-cycles or 5-cycles.

(b) Deduce furthermore that N must contain both 2-2-cycles *and* 5-cycles.

(c) Show that N must contain 3-cycles. (Hint: consider $(12345)(12)(34)$.)

(d) Deduce that $N = \{e, 3 - \text{cycles}, 2 - 2 - \text{cycles}, 5 - \text{cycles}\} = A_5$ or $N = S_5$.

87 (a) State the definition of a quotient group G/N where $N \subseteq G$ is a normal subgroup.

(b) State the first isomorphism theorem for groups.

(c) Let R be a commutative ring with 1 and let $G = GL_2(R) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in R, ad - bc \in U(R) \right\}$. You may assume that this is a group. Let $\theta : G \rightarrow U(R)$ be given by $A\theta = \det A$. Is this necessarily a group homomorphism? Briefly justify your answer.

(d) Compute the kernel and image of θ in part (c).

(e) Deduce that $G/\ker \theta$ in the case $R = J$ is isomorphic to the cyclic group of order 4 defined by $\langle i \rangle$ where $i = \sqrt{-1}$.

(f) Find an element of $G/\ker \theta$ corresponding to $-1 \in \langle i \rangle$ in part (e).

88 (a) State the 2nd isomorphism theorem for groups.

(b) Let $G = GL_2(J)$ as in Q87(e),(f) and $N = \ker \theta$ there. Find all subgroups of G/N in this case.

(c) Find all subgroups $K \subseteq G$ containing N . (Hint: use the construction in the proof of (a) and use part (f) of the previous question.)