Math 3 (V3020) — Exercise 9

1. Are the following sets equipped with the specified binary operations groups? Why / why not?

a) The even integers under addition?

Our set is $E = \{2k \mid k \in \mathbb{Z}\}$ and the binary operation $\oplus$ the standard arithmetic addition. Let us check if they satisfy the definition of a group.

i) Let $a = 2m$ and $b = 2n$, $m, n \in \mathbb{Z}$ be two elements in E. Now $a + b = 2(m+n) \in E$, meaning E is closed under addition. OK!

ii) Trivially associativity holds, i.e.
$a + (b+c) = (a+b) + c$ $\forall$ $a, b, c \in E$. OK!

iii) $0 \in E$ is a unique identity element, since $0 + a = a + 0 = a \quad \forall\ a \in E$. OK!

iv) For every $a = 2m \in E$, there is the inverse element $a^{-1} = 2(-m) \in E$, $m \in \mathbb{Z}$.
Here $a + a^{-1} = 2m + 2(-m) = 2(-m) + 2m$
$= a^{-1} + a = 0$ OK!

$\therefore (E, +)$ is a group.

b) The odd integers integers under addition?

The set is $D = \{2k+1 \mid k \in \mathbb{Z}\}$ and the binary operation the standard addition.

Let $a = 2m+1$, $b = 2n+1 \in D$. Now
$a + b = (2m+1) + (2n+1) = 2(m+n+1) \notin D$

Thus $(D, +)$ is not a groups.

2. Show that the set of elements a, b, c, e is a group when equipped with $\oplus$ that operates according to the following table.

$\oplus$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

The set being closed under $\oplus$ and e being the identity element are trivial.

From the table, we can see that the inverse elements are $e^{-1} = e$, $a^{-1} = a$, $b^{-1} = c$, $c^{-1} = b$, and that they are unique.

How about associativity? $\oplus$ is clearly commutative, so we don't have to check all "permutations".

Additionally

$$a \oplus (b \oplus c) = a \oplus e = a = (a \oplus b) \oplus c$$
$$e \oplus (a \oplus b) = e \oplus c = c = (e \oplus a) \oplus b$$
$$e \oplus (a \oplus c) = e \oplus b = b = (e \oplus a) \oplus c$$
$$e \oplus (b \oplus c) = e \oplus e = e = (e \oplus b) \oplus c$$

The rest of the possible "combinations" of elements obey associativity thanks to commutativity of $\oplus$.

$\therefore \{a, b, c, e\}$ with $\oplus$ is a group.

3. The set of complex numbers $\{1, -1, i, -i\}$ equipped with multiplication is a group. Here $i \cdot i = -1$.

Show that it is isomorphic to the group in Problem 2.

Let us establish the following correspondence

$e \longleftrightarrow 1$, $a \longleftrightarrow -1$, $b \longleftrightarrow i$, $c \longleftrightarrow -i$

With this, let us draw the table for operation results for both groups

$\oplus$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Performing the respective operation of the group for every pair of corresponding elements, yields

a one-to-one correspondence also after the operation is performed.

$\therefore$ The two groups are isomorphic.

(We also could have made the identification $b \leftrightarrow -i$ and $c \leftrightarrow i$.)

4. Claim: The set of all rational numbers $\mathbb{Q} = \{\frac{p}{q} \mid p \in \mathbb{Z}, q \in \mathbb{Z} \setminus \{0\}\}$ a field when equipped with the standard addition and multiplication operations.

Proof: First, let us briefly show that $(\mathbb{Q}, +)$ is a commutative group. Clearly, addition is commutative and associative.

$0 \in \mathbb{Q}$ is the identity element, since
$0 + x = x + 0 = x \quad \forall\, x \in \mathbb{Q}$

$(\mathbb{Q}, +)$ is closed, since $\forall\, x = \frac{p}{q}, y = \frac{m}{n} \in \mathbb{Q}$,
$x + y = \frac{p}{q} + \frac{x}{y} = \frac{py + xq}{qy} \in \mathbb{Q}$.

For all $x = \frac{p}{q} \in \mathbb{Q}$, there is $x^{-1} = \frac{-p}{q} \in \mathbb{Q}$,
s.t. $x + x^{-1} = x^{-1} + x = 0$.

$\therefore$ $(\mathbb{Q}, +)$ is a commutative group.

Next, we show that $(\mathbb{Q}, +, \cdot)$ is a ring.

$(\mathbb{Q}, +, \cdot)$ is closed under $\cdot$, since $\forall x = \frac{p}{q}, y = \frac{m}{n} \in \mathbb{Q}$, we have $x \cdot y = \frac{p}{q} \cdot \frac{m}{n} = \frac{p \cdot m}{q \cdot n} \in \mathbb{Q}$.

Clearly $\cdot$ is associative.

$\cdot$ is distributive w.r.t. $+$, since $\forall x, y, z \in \mathbb{Q}$,
$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ and
$(y + z) \cdot x = (y \cdot x) + (z \cdot x)$.

$\therefore (\mathbb{Q}, +, \cdot)$ is a ring and 0 is the zero of the ring.

Lastly, to show that $(\mathbb{Q}, +, \cdot)$ is a field, we establish $(\mathbb{Q} \setminus \{0\}, \cdot)$ is a commutative group.

$\forall x = \frac{p}{q}, y = \frac{m}{n} \in \mathbb{Q} \setminus \{0\}$, $x \cdot y = \frac{pm}{qn} \in \mathbb{Q} \setminus \{0\}$,
i.e. $\mathbb{Q} \setminus \{0\}$ is closed w.r.t. $\cdot$.

Clearly, $1 \in \mathbb{Q} \setminus \{0\}$ is the identity element, since $1 \cdot x = x \cdot 1 = x \quad \forall\, x \in \mathbb{Q} \setminus \{0\}$.

Trivially, $\cdot$ is associative and commutative.

For every $x = \frac{p}{q} \in \mathbb{Q} \setminus \{0\}$, $\exists\ x^{-1} = \frac{q}{p} \in \mathbb{Q} \setminus \{0\}$ with $x^{-1} \cdot x = x \cdot x^{-1} = 1$.

$\therefore (\mathbb{Q} \setminus \{0\}, \cdot)$ is a commutative group.

With all this, we've shown that $(\mathbb{Q}, +, \cdot)$ is a field.

5. Factorize 26149 using Pollard's $p-1$ method.

Let us choose $a=2$ and a bound $B=6$.

Now
$$a^{B!} = 2^{6!} \equiv 10924 \bmod 26149$$

Then the greatest common divisor
$$\begin{aligned}(a^{B!}-1, 26149) &= (2^{6!}-1, 26149) \\ &= (10924-1, 26149) \\ &= (10923, 26149) \\ &= 331 > 1\end{aligned}$$

One of the factors is 331 which is prime. Now easily $26149/331 = 79$ which is also prime.

$\therefore$ $26149 = 331 \cdot 79$, i.e. 331 and 79 are the prime factors of 26149.