Groups 2D

1 a $e_H = \mathrm{f}(e_G) = \mathrm{f}(a * a^{-1}) = \mathrm{f}(a) \circ \mathrm{f}(a^{-1})$

Similarly $e_H = \mathrm{f}(e_G) = \mathrm{f}(a^{-1} * a) = \mathrm{f}(a^{-1}) \circ \mathrm{f}(a)$

By uniqueness of the inverse $\Rightarrow (\mathrm{f}(a))^{-1} = \mathrm{f}(a^{-1})$

b We use induction on n. For $n = 1$ it is trivial, $\mathrm{f}(a^1) = \mathrm{f}(a) = (\mathrm{f}(a))^1$

Assuming it is true for n then:

$$\begin{aligned}\mathrm{f}(a^{n+1}) &= \mathrm{f}(a^n * a) = \mathrm{f}(a^n) \circ \mathrm{f}(a) \\ &= (\mathrm{f}(a))^n \circ \mathrm{f}(a) \qquad \text{by induction hypothesis;} \\ &= (\mathrm{f}(a))^{n+1}\end{aligned}$$

So if the statement is true for n it is true for $n+1$.

Therefore $\mathrm{f}(a^{n+1}) = (\mathrm{f}(a))^{n+1}$ for all $n \in \mathbb{Z}^+$.

2 a The Cayley table for G is:

$\times$	**1**	**–1**	**i**	**–i**
1	1	–1	i	–i
–1	–1	1	–i	i
i	i	–i	–1	1
–i	–i	i	1	–1

The Cayley table for H is:

$+_4$	**0**	**1**	**2**	**3**
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

b Both these groups are cyclic: i generates G and 1 generates H.

Therefore, consider the mapping function defined as $\mathrm{f}(\mathrm{i}^k) = k \pmod 4$ for $k = 0, 1, 2, 3$.

As $\mathrm{f}(1) = \mathrm{f}(\mathrm{i}^0) = 0$, $\mathrm{f}(-1) = \mathrm{f}(\mathrm{i}^2) = 2$, $\mathrm{f}(\mathrm{i}) = \mathrm{f}(\mathrm{i}^1) = 1$, $\mathrm{f}(-\mathrm{i}) = \mathrm{f}(\mathrm{i}^3) = 3$ all elements of G map on to all elements of H

One-to-one: assume $\mathrm{f}(\mathrm{i}^m) = \mathrm{f}(\mathrm{i}^n)$. Then $m \equiv n \pmod 4 \Rightarrow m = n + 4p$ for some $p \in \mathbb{Z}$

Then $\mathrm{i}^m = \mathrm{i}^{n+4p} = (\mathrm{i}^n)(\mathrm{i}^{4p}) = (\mathrm{i}^n)(\mathrm{i}^4)^p = \mathrm{i}^n$, so f is one-to-one.

Preserves structure: $\mathrm{f}(\mathrm{i}^m \times \mathrm{i}^n) = \mathrm{f}(\mathrm{i}^{m+n}) = m + n \pmod 4 = \mathrm{f}(\mathrm{i}^m) +_4 \mathrm{f}(\mathrm{i}^n)$

So f is an isomorphism from G onto H and $G \cong H$.

3 a The Cayley table is:

$\times_8$	**1**	**3**	**5**	**7**
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

This shows that the set is closed under the operation and that the identity (= 1) and inverse (each element is a self-inverse) axioms hold. Associativity follows by associativity of normal multiplication. So $(G, \times_8)$ is a group.

b As $3^{-1} = 3$, the equation is equivalent to $7 \times_8 x = y \times_8 3$.
The solutions to this equation can be found from the Cayley table.
For example, as $7 \times_8 1 = 7$ look for $y \times_8 3 = 7$, which is solved by 5, $5 \times_8 3 = 7$, so a solution is (1, 5). The full list of solutions are (1, 5), (3, 7), (5, 1) and (7, 3).

c As $5 \times_{10} a = 5$ for all $a \in H$, 5 does not have an inverse. Therefore H can't be a group.

d Removing 5 from H to produce a set $K = \{1, 3, 7, 9\}$. The Cayley table of K under $\times_{10}$ is:

$\times_{10}$	**1**	**3**	**7**	**9**
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

This is a group as the set is closed under the operation and that the identity (= 1) and inverse (1 and 9 are self-inverses and 3 is the inverse of 7 and vice verse) axioms hold. Associativity follows by associativity of normal multiplication.

e These groups cannot be isomorphic because K has elements of order 4 ($3^2 = 9$, $3^2 = 7$ and $3^4 = 1$) while all the elements of G have order 1 or 2 (each element is a self inverse). So order is not preserved.

4 a Suppose $a = ab$. As G is a group, a has an inverse so this give $a^{-1}a = a^{-1}ab \Rightarrow e = b$ but b is distinct from e, so $a \neq ab$. The argument to show $b \neq ab$ is the same.

4 b Two possible Cayley tables are:

∘	***e***	***a***	***b***	***c***
e	*e*	*a*	*b*	*c*
a	*a*	*e*	*c*	*b*
b	*b*	*c*	*e*	*a*
c	*c*	*b*	*a*	*e*

∘	***e***	***a***	***b***	***c***
e	*e*	*a*	*b*	*c*
a	*a*	*c*	*e*	*b*
b	*b*	*e*	*c*	*a*
c	*c*	*b*	*a*	*e*

These tables obtained by following the rule that each row and each column of the table must contain each element of the group exactly once. Note that the groups are not isomorphic, as the first one only has elements of order 1 or 2 (each element is a self-inverse) and the second group has some element of order 4 ($a^2 = c$, $a^3 = b$, $a^4 = e$).

c H has two elements of order 4 (i and –i), for example $i^2 = -1$, $i^3 = -i$, $i^4 = 1$.
So H is isomorphic to the second (lower) group above.
Both groups are cyclic, so one possible isomorphism maps a^n to i^n, for $n = 0,1,2,3$.

5 a 1 has order 1.
For 7: $7^2 \equiv_{30} 19$, $7^3 \equiv_{30} 13$, $7^4 \equiv_{30} 1$, so 7 has order 4 and 19 has order 2.
For 11: $11^2 \equiv_{30} 1$, so 11 has order 2.
For 13: $13^2 \equiv_{30} 19$ and as 19 has order 2, 13 has order 4.
For 17: $17^2 \equiv_{30} 19$ and as 19 has order 2, 17 has order 4.
For 23: $23^2 \equiv_{30} 19$ and as 19 has order 2, 23 has order 4.
For 29: $29^2 \equiv_{30} 1$, so 11 has order 2.

b The element 7 generates a cyclic group: {1, 7, 19, 13}.
Similarly, 17 generates a cyclic group: {1, 17, 19, 23}.
The set {1, 11, 19, 29} is a Klein four-group: all the elements have order 2
This Klein four-group is closed as $11 \times_{30} 19 = 29$, $19 \times_{30} 29 = 11$ and $29 \times_{30} 11 = 19$.

c In D_8 there are 4 reflection: the horizontal and vertical ones and the two diagonal ones.
Each of these has order 2.
In G there are only 3 elements of order 2 (11, 19 and 29).
So D_8 and G cannot be isomorphic.

6 a 1 has order 1.

For 2: $2^2 \equiv_7 4,\ 2^3 \equiv_7 1$, so 2 has order 3.

For 3: $3^2 \equiv_7 2,\ 3^3 \equiv_7 6,\ 3^4 \equiv_7 4,\ 3^5 \equiv_7 5,\ 3^6 \equiv_7 1$, so 3 has order 6.

For 4: $4^2 \equiv_7 2,\ 4^3 \equiv_7 1$, so 4 has order 3.

For 5: $5^2 \equiv_7 4,\ 5^3 \equiv_7 6,\ 5^4 \equiv_7 2,\ 5^5 \equiv_7 3,\ 5^6 \equiv_7 1$, so 5 has order 6.

For 6: $6^2 \equiv_7 1$, so 6 has order 2.

G is a cyclic group generated by 3 and 5.

b G is a cyclic group of order 6, so it has two non-trivial proper subgroups: $\{1, 6\}$ of order 2 and $\{1, 2, 4\}$ of order 3. Both are obviously cyclic. The other proper subgroup is the trivial group $\{1\}$.

c Find a generator for H: $5^2 \equiv_{18} 7,\ 5^3 \equiv_{18} 17,\ 5^4 \equiv_{18} 13,\ 5^5 \equiv_{18} 11,\ 5^6 \equiv_{18} 1$, so 5 is a generator of H.

So an isomorphism is $\mathrm{f}: G \to H$ such that $\mathrm{f}(3^k) = 5^k$ for $k \in \mathbb{Z}$.

7 a The order of each element of the group must be a divisor of the order of the group, so if G has order p all its non-identity elements must have order p.

So there exists an element $g \in G$ such that $g^p = e$, i.e g has order p.

Therefore g is a generator and the group is cyclic.

b As $7^2 \equiv_{29} 20,\ 7^3 \equiv_{29} 24,\ 7^4 \equiv_{29} 23,\ 7^5 \equiv_{29} 16,\ 7^6 \equiv_{29} 25,\ 7^7 \equiv_{29} 1$, so 7 is a generator of G.

As $e^{\pi i} = -1$ (Euler's equation), then $(e^{\frac{2\pi i}{7}})^7 = (e^{2\pi i}) = (e^{\pi i})^2 = (-1)^2 = 1$, so $e^{\frac{2\pi i}{7}}$ is a generator of G.

So an isomorphism is $\mathrm{f}: G \to H$ such that $\mathrm{f}(7^k) = e^{\frac{2k\pi i}{7}}$ for $k \in \{0, 1, 2, 3, 4, 5, 6\}$

8 As $e^{\pi i} = -1$ (Euler's equation), then $(e^{\frac{\pi i}{4}})^8 = (e^{2\pi i}) = (e^{\pi i})^2 = (-1)^2 = 1$, so $e^{\frac{\pi i}{4}}$ is a generator of G.

Look for a generator for H.

For 3: $3^2 \equiv_{32} 9,\ 3^3 \equiv_{32} 27,\ 3^4 \equiv_{32} 1$, so 3 has order 4.

For 9: $9^2 \equiv_{32} 1$, so 9 has order 1.

For 11: $11^2 \equiv_{32} 25,\ 11^3 \equiv_{32} 19,\ 11^4 \equiv_{32} 17,\ 11^5 \equiv_{32} 27,\ 11^6 \equiv_{32} 9,\ 11^7 \equiv_{32} 3,\ 11^8 \equiv_{32} 1$, so 11 has order 8.

Hence 11 is a generator of H.

So an isomorphism is $\mathrm{f}: G \to H$ such that $\mathrm{f}(e^{\frac{k\pi i}{4}}) = 11^k \pmod{32}$ for $k \in \{0, 1, 2, 3, 4, 5, 6, 7\}$

9 G has elements that are order 4. For example:

$$\begin{pmatrix} -1 & -2 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} -1 & -2 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

However, $5^2 \equiv_{12} 1,\ 7^2 \equiv_{12} 1,\ 11^2 \equiv_{12} 1$ so 5, 7 and 11 are all self-inverse modulo 12

Therefore, every non-identity element of H has order 2.

So G and H cannot be isomorphic.

10 a The identity matrix obviously has order 1.

The matrix $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ is self-inverse, so it has order 2.

For any other matrix $\mathbf{A} \in G$, $\mathbf{A}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, so they all have order 4.

b The Klein four-group has three elements of order 2, while G only has one. Therefore, G cannot have any subgroup isomorphic to the Klein four-group, because if it did then it would have three distinct non-identity elements and at least two of these would have to be order 4.

c As $9^2 \equiv_{20} 1$, $11^2 \equiv_{20} 1$, $19^2 \equiv_{20} 1$, the elements 9, 11 and 19 all have order 2 in H, while G only has one element of order 2. Therefore, these groups are not isomorphic.

Challenge

a i The elements of S are:

$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

ii The set is closed under matrix multiplication because the determinant of the product of two matrices is the product of the determinants.

The identity matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is obviously an identity.

For the inverse axiom

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

The other four matrices are easily verified to be self-inverse.

Associativity is assumed, so all four axioms are satisfied and S forms a group under $\times_2$.

iii Another group of order 6 with three elements of order 2 and two elements of order 3 that are inverses is the group S_3 of permutations of three objects.

b i Consider the matrix:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

There three possibilities for a_{11}.

If $a_{11} = 0$, then a_{22} can take any value while the other two entries cannot be zero, so there are 12 possible matrices.

If $a_{11} = 1$, then consider a_{22}: if it is 0 then there are 4 possible matrices, if it is 1 then there are 7 possible matrices, as these matrices

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

have determinant 0, and 7 more if it 2, so in total 18 possibilities.

If $a_{11} = 2$, by a similar argument, there are 18 possibilities.

So there are in total $12 + 18 + 18 = 48$ possible matrices.

The order of the group is 48.

Challenge

b ii For a general matrix

$$\begin{pmatrix}1 & 2\\ 1 & 1\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix}=\begin{pmatrix}a+2c & b+2d\\ a+c & b+d\end{pmatrix}$$

For this to be the identity, $a+c=0$ and $a+2c=1$, so $a=2$ and $c=1$, and $b+d=1$ and $b+2d=0$, so $b=2$ and $d=2$.
Therefore, the inverse is:

$$\begin{pmatrix}2 & 2\\ 1 & 2\end{pmatrix}$$