Groups 2C

1 a The order of a finite group is its number of elements, so the order of this group is 6.

b 1 has order 1.
To find the order of 2 compute: $2^2 = 4$, $2^3 = 8$, $2^4 = 7$, $2^5 = 5$, $2^6 = 1$, so the order of 2 is 6.
For 4: since $2^2 = 4, 2^6 = 4^3 = 1$, so the order of 4 is 3.
For 5: $5^2 = 7$, $5^3 = 8$, $5^4 = 4$, $5^5 = 2$, $5^6 = 1$, so the order of 5 is 6.
For 7: $7^2 = 4$, $7^3 = 1$, so the order of 7 is 3.
For 8: since $2^3 = 8, 2^6 = 8^2 = 1$ so the order of 8 is 2.

2 a It is clear from the Cayley table that e has order 1
The non-identity elements have order 2 as $a^2 = b^2 = c^2 = e$

b A group can only be cyclic if it has an element with the same order as the group. This group cannot be cyclic as every element has order 2 and the group has order 4.

3 a The order of the group is its number of elements, so this group has order 6.

b 0 has order 1.
1 is a generator so it has order 6.
For 2: $2+2=4$ and $4+2=0$, so the order of 2 is 3.
For 3: $3+3=0$ so 3 has order 2.
For 4: $4+4=2$ and $2+4=0$ so the order of 4 is 3.
For 5: $5+5=4$, $4+5=3$, $3+5=2$, $2+5=1$ and $1+5=0$, so 5 has order 6.

c From part **b**, {0, 2, 4} is closed under addition modulo 6, so it is a subgroup of order 3.

4 a i

$\circ$	**0**	**1**	**2**	**4**	**5**	**6**
0	0	1	2	4	5	6
1	1	4	0	6	2	5
2	2	0	5	1	6	4
4	4	6	1	5	0	2
5	5	2	6	0	4	1
6	6	5	4	2	1	0

ii From the Cayley table, the closure axiom holds, all entries are in H.
The identity element is 0.
Every element has an inverse: 0 and 6 are self-inverses and 2 and 5 are the inverses of 1 and 4 respectively.
As associativity is assumed, all axioms hold and so $(H, \circ)$ forms a group.

b i Consider 1: $1 \circ 1 = 4, 4 \circ 1 = 6, 6 \circ 1 = 5, 5 \circ 1 = 2, 2 \circ 1 = 0$
So 1 generates H.

ii A subgroup must contain 0, the identity element.
Consider 4 and 5: $4 \circ 4 = 5, 5 \circ 4 = 4 \circ 5 = 0$ and $5 \circ 5 = 4$
So {0, 4, 5} is closed under the operation $\circ$, so it is a subgroup of order 3.

4 b iii As 6 is self-inverse, $\{0, 6\}$ is a subgroup of order 2.

5 a The order of a finite group is its number of elements, so the order of this group is 10.
The order of a subgroup divides the order of the group, so the subgroups of U can have order 1, 2, 5 or 10.
However, to be a proper subgroup, the order of the subgroup must be less than the order of the group; so proper subgroups of U can have order 1, 2 or 5.

b Consider 2: $2^2 \equiv_{11} 4,\ 2^3 \equiv_{11} 8,\ 2^4 \equiv_{11} 5,\ 2^5 \equiv_{11} 10,\ 2^6 \equiv_{11} 9,\ 2^7 \equiv_{11} 7,\ 2^8 \equiv_{11} 3,\ 2^9 \equiv_{11} 6,\ 2^{10} \equiv_{11} 1$
So $(U, \times_{11})$ is a cyclic group.
Find values of n such that $\gcd(2^n, 10) = 1$. This gives the other generators: 6, 7, 8.

c From part **a**, proper subgroups must have an order 1, 2 or 5.
There is the trivial subgroup of order 1 given by $\{1\}$; one of order 2 generated by the element 2^5, $\{1, 10\}$; and a subgroup of order 5 generated by the element 2^2, $\{1, 3, 4, 5, 9\}$.
As $\{1, 3, 4, 5, 9\}$ is a cyclic group of order 5, all its elements are generators. Thus every non-identity element generates either $\{1, 10\}$ or $\{1, 3, 4, 5, 9\}$ and since cyclic groups only have cyclic subgroups these and $\{1\}$ must be the only proper subgroups.

6 a This is not a subgroup as it fails the inverse axiom.
For example, the inverse of 2 is –2 and $-2 \notin \mathbb{Z}^+$.

b This is closed under addition because the sum of even integers is even.
It contains the identity element 0.
The additive inverse of an even integer (2*k*) is an even integer (–2*k*).
The associativity axiom holds as addition is associative for all integers.
So this set is a subgroup of $(\mathbb{Z}, +)$.

c This is not a subgroup because $\mathbb{R} \not\subset \mathbb{Z}$.

d This is not a subgroup because it is not closed under addition (for example, $1 + 1 = 2$).

7 a The order of the group is 8, and by Lagrange's theorem the order of a subgroup must divide the order of the group, so there can't be any subgroup of order 3.

b 1 has order 1
For 3: $3^2 \equiv_{20} 9,\ 3^3 \equiv_{20} 7,\ 3^4 \equiv_{20} 1$, so 3 has order 4.
For 7: $7^2 \equiv_{20} 9,\ 7^3 \equiv_{20} 3,\ 7^4 \equiv_{20} 1$, so 7 has order 4.
For 9: $9^2 \equiv_{20} 1$, so 9 has order 2.
For 11: $11^2 \equiv_{20} 1$, so 11 has order 2.
For 13: $13^2 \equiv_{20} 9,\ 13^3 \equiv_{20} 17,\ 13^4 \equiv_{20} 1$, so 13 has order 4.
For 17: $17^2 \equiv_{20} 9,\ 17^3 \equiv_{20} 13,\ 17^4 \equiv_{20} 1$, so 17 has order 4.
For 19: $19^2 \equiv_{20} 1$, so 19 has order 2.

7 c From part **b**, two (cyclic) subgroups of order 4 are those generated by 3 (or 7) $\{1, 3, 7, 9\}$ and by 13 (or 17) $\{1, 9, 13, 17\}$ as these must be closed under multiplication modulo 20.
From part **b,** $9^2 \equiv_{20} 11^2 \equiv_{20} 19^2 \equiv_{20} 1$ and by calculation $9 \times_{20} 11 = 19$, $11 \times_{20} 19 = 9$, $9 \times_{20} 19 = 11$, so the set $\{1, 9, 11, 19\}$ is closed under multiplication modulo 20 is a subgroup of order 4.
So the solutions are $\{1, 3, 7, 9\}$, $\{1, 9, 13, 17\}$ and $\{1, 9, 11, 19\}$.

8 a Clearly, the closure axiom is satisfied. The element a is an identity because the corresponding row and column have the same elements as the headings. From the table, $b * c = c * b = a$, so the inverse axiom is satisfied. As associativity is assumed, {a, b, c} is a group.

b If $(S, *)$ is a finite group with $g \in S$, then |g| divides |S|. However the order of g is 3 and the order of S is 7, and 3 does not divide 7 so $(S, *)$ is not a group.

9 For any complex numbers z and w, $|zw| = |z||w|$, so in particular if two complex numbers have modulus 1 so does their product. Therefore this set is closed under multiplication.
The identity element is 1 and as $|1| = 1$, $1 \in S$.
If $|z| = 1$ then $\left|\frac{1}{z}\right| = \frac{1}{|z|} = 1$, so each element has an inverse that is $\in S$
As associativity is assume S is a subgroup of $\mathbb{C}_{\neq 0}$.

10 a $x^{10} = e \Rightarrow (x^2)^5 = e$. So x^2 has order 5.

b The order of y^2 is the same order of x^5.
$x^{10} = e \Rightarrow (x^5)^2 = e \Rightarrow |x^5| = |y^2| = 2$, so the order of y^2 is 2.

c As $|y^2| = 2 \Rightarrow |y| = 4$

d The order of y^3 must be the same as the order of y, because gcd(3, 4) = 1. So the order of y^3 is 4.

11 a The order of every element of G must be a divisor of p, so it is either 1 or p. Only the identity element can have order 1, so each non-identity element must have order p.
But then for any non-identity element g, $\{1, g, g^2, ..., g^{p-1}\}$ is a set of p distinct elements, so g generates the group, which is therefore cyclic.

b Since the argument in a does not depend on the choice of g, every element of G is a generator.

12 a False; x is not an identity, or its order would be 1.

b False; x can't be self-inverse, because if $x^2 = e$ the order of x would not be 4.

c True; $(x^2)^2 = x^4 = e$.

d False; x^3 is not self-inverse, because $(x^3)^2 = x^6 = x^4x^2 = ex^2 = x^2 \neq e$.

e True; the order of the group must be a multiple of 4 as there is an element of order 4.

f True; $\{e, x, x^2, x^3\}$ is closed under the operation of the group, so it is a subgroup of order 4.

12 g False; G could be the cyclic group generated by x.

h True; $x^8 = (x^4)^2 = e^2 = e$.

i True; $x^5 = x^1x^4 = xe = x$.

j True; $x^6 \neq e$ (part **d**) and $x^9 = x^5x^4 = xe = x$ and $x^{12} = (x^4)^3 = e^3 = e$.

k False: x^2 is self-inverse and is not the identity, so it has order 2.

13 a The order of a subgroup must be a divisor of the order of the group, so subgroups must have order 1, 2, 4 or 8. (Non-trivial, proper subgroups must have order 2 or 4.)

b The trivial cases are $\{0\}$ order 1 and $\{0, 1, 2, 3, 4, 5, 6, 7\}$ order 8.
The set $\{0, 4\}$ is closed under addition modulo 8 ($0 + 4 = 4 + 0 = 4$; $0 + 0 = 4$, $4 + 4 = 0$) so it is a subgroup of order 2.
The set of even numbers (0 is even) is also closed under addition modulo 8, so $\{0, 2, 4, 6\}$ is a subgroup of order 4.

14 Every non-identity element of G has order p or p^2.
If an element g has order p, then the cyclic group generated by g is a group of order p.
If g has order p^2 then g^2 has order p and generates a subgroup of order p.

15 a No; this set does not contain inverses (for example, the inverse of 2 is $\frac{1}{2}$ which is not an integer).

b Yes, this is a subgroup; the product of two positive rational numbers is a positive rational number, the identity element 1 is a positive rational number; the inverse of a positive rational is a positive rational and associativity holds on any subset of $\mathbb{Q}$.

c Yes: it can be seen from the Cayley table that this is a subgroup (it is closed, the identity is 1, and each element has an inverse):

×	**1**	**–1**
1	1	–1
–1	–1	1

d No; the set $\mathbb{R}_{\neq 0}$ is not a subset of the rational numbers.

e Yes; this is closed under multiplication as $3^h3^k = 3^{h+k}$, the identity is $1 = 3^0$, the inverse of 3^k is 3^{-k}, and it is associative by associativity of multiplication.

f Yes; this is the trivial subgroup. It is obviously closed, contains the identity and its inverse.

g No; this is not closed, as the product of two negative numbers is positive.

h No; this is not closed because the product of two negative numbers can be a positive number that is not 1.

16 Let $\mathbf{A} = \begin{pmatrix} 3 & 5 \\ -2 & -3 \end{pmatrix}$, then $\mathbf{A}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ and $\mathbf{A}^4 = \mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

So $\mathbf{A}$ generates a cyclic group $\{\mathbf{A}, \mathbf{A}^2, \mathbf{A}^3, \mathbf{A}^4\}$ of order 4 under matrix multiplication.
This is a finite subgroup of the set of real-valued non-singular matrices under matrix multiplication.

17 a Denote the given permutation by σ, then:

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} \quad \sigma^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

As σ^3 is the identity permutation, $S = \{\sigma, \sigma^2, \sigma^3\}$ is a closed subset of all possible permutations of 4 elements under the operation of composition. So it is a subgroup of this group of order 3.

b Just take a permutation of order 2, for example:

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

As τ^2 is an identity, τ generates a cyclic group $S = \{\tau, \tau^2\}$ of order 2, which is a subgroup of all possible permutations of 4 elements under the operation of composition.

18 a The element p is a symmetry so it is self-inverse. Therefore it has order 2.
The element q has order 6 as it must be composed 6 times with itself to form a complete rotation of 360°.

b The element p has order 2, so its Cayley table is:

$\circ$	e	p
e	e	p
p	p	e

c The composition q^2 is an anticlockwise rotation of 120°.
Therefore, the subgroup generated by q^2 is $\{e, q^2, q^4\}$.

Challenge

1 Suppose H has n elements, let $a \in H$.
As H is closed under the group of operation of G the set $\{a, a^2, ..., a^{n+1}\}$ these all belong to H.
But since H only has n elements, there are i and j such that $a^i = a^j$.
Assuming without loss of generality $j > i$, this implies that $a^{j-i} = e$; therefore, $e \in H$.
To show that H contains inverses, suppose a is any element of H, then find $j > i$ such that $a^{j-i} = e$.
But $aa^{j-i-1} = e \Rightarrow a^{j-i-1} = a^{-1}$, i.e. $a^{j-i-1} = a^{-1}$.
Associativity holds as $H \subseteq G$.
So H is a subgroup of G.

2 a As $(x^{-1})^n = x^{-n} = (x^n)^{-1} = e$, so the order of x^{-1} is at most n.
Suppose there is $m < n$ such that $(x^{-1})^m = e$; then, $(x^m)^{-1} = e$. But this would imply that $x^m = e$, which is a contradiction. So the order of x^{-1} is n.

Challenge

2 b Use induction on n. For $n=1$, it is trivial: $y=z^{-1}xz$. Now assume it is true for n, then:

$y^{n+1}=y^n y=z^{-1}x^n z(z^{-1}xz)=z^{-1}x^n(zz^{-1})xz=z^{-1}x^n exz=z^{-1}x^{n+1}z$

So if the result holds for n it holds for $n+1$.

So $y^{n+1}=z^{-1}x^{n+1}z$ for all $n\in\mathbb{Z}^+$.