1.

1.

Consider D_{2k}:

$$\forall x \in D_{2k} : \exists i \in \{1, 2, \ldots, n\}, j \in \{0, 1\} : x = r^i s^j$$

If $j = 0$ then

$$x^m = (r^i)^m = r^{im} = 1 = r^{kn} \text{ where } k \in \mathbb{N} \iff im \text{ is a multiply of } n$$

If $j = 1$ then

$$\begin{aligned} x^2 &= (r^i s)^2 = r^{i-1} \cdot r \cdot s \cdot r^i s = r^{i-1} \cdot s \cdot r^{-1} \cdot r^i s = (r^{i-1})^2 \\ &= r^{i-2} \cdot r \cdot s \cdot r^{i-1} \cdot s = r^{i-2} \cdot s \cdot r^{-1} \cdot r^{i-1} \cdot s = (r^{i-2})^2 \\ &\ldots \\ &= (rs)^2 = 1 \end{aligned}$$

Therefore,
In D_6:

$$\operatorname{ord}(1) = 1, \operatorname{ord}(r) = 3, \operatorname{ord}(r^2) = 3$$
$$\operatorname{ord}(rs) = 2, \operatorname{ord}(r^2 s) = 2, \operatorname{ord}(r^3 s) = 2$$

In D_8:

$$\operatorname{ord}(1) = 1, \operatorname{ord}(r) = 4, \operatorname{ord}(r^2) = 2, \operatorname{ord}(r^3) = 4$$
$$\operatorname{ord}(s) = 2, \operatorname{ord}(rs) = 2, \operatorname{ord}(r^2 s) = 2, \operatorname{ord}(r^3 s) = 2$$

In D_{10}:

$$\operatorname{ord}(1) = 1, \operatorname{ord}(r) = 5, \operatorname{ord}(r^2) = 5, \operatorname{ord}(r^3) = 5, \operatorname{ord}(r^4) = 5$$

$$\operatorname{ord}(s) = 2, \operatorname{ord}(sr) = 2, \operatorname{ord}(sr^2) = 2, \operatorname{ord}(sr^3) = 2, \operatorname{ord}(sr^4) = 2$$

2.

Since i is an integer, there exists $t \in \mathbb{Z}$ such that: $i = mt + j$ where $0 \leq j < m$, therefore

$$\sigma = (a_1, a_2, \ldots, a_m)$$
$$\implies \sigma^i = \sigma^{mt} \cdot \sigma^j = \sigma^j = (a_{j+1}, a_{j+2}, \ldots, a_m, a_1, a_2, \ldots, a_i)$$

As $j \equiv i \bmod m, j + k \equiv i + k \bmod m$ and therefore, $r \equiv j + k \bmod m$

$$\implies \sigma^i(a_k) = a_{j+k} = a_r$$

3.

For S_3, all the cycles are
order 1: $()$
order 2: $(1,2),(1,3),(2,3)$
order 3: $(1,2,3),(1.3,2)$
For S_4, all the cycles are
order 1: $()$
order 2: $(1,2),(2,3),(3,4),(1,4)$
order 3: $(2,3,4),(2,4,3),(1,3,4),(1,4,3),(1,2,4),(1,4,2),(1,2,4),(1,4,2)$
order 4: $(1,2,3,4),(1,2,4,3),(1,3,4,2),(1,3,2,4),(1,4,2,3),(1,4,2,3)$
order 2: $(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)$

2.

1.

If a and b are central elements of a group G, then

$$\forall h \in G : h \cdot (a \cdot b) = (h \cdot a) \cdot b = (a \cdot h) \cdot b = a \cdot (h \cdot b) = a \cdot (b \cdot h) = (a \cdot b) \cdot h$$

which proves that $a \cdot b$ is also a central element.

2.

If a is a central elements of a group G, then

$$\forall h \in G : h \cdot a = a \cdot h \implies a^{-1} \cdot h \cdot a \cdot a^{-1} = a^{-1} \cdot a \cdot h \cdot a^{-1} \implies a^{-1} \cdot h = h \cdot a^{-1}$$

which proves that a^{-1} is also a central element.

3.

1 is obviously a central element: $\forall g \in G : 1 \cdot g = g \cdot 1$ the product of central elements are also central element. the inverse of a central element is a central elements.
Therefore, the centre of G is a subgroup of G.

4.

The centre of S_4 is $\{()\}$: Consider an arbitary cycle $\sigma \in Z(S_4)$, then $\sigma(a, b) = (a, b)\sigma \implies \sigma^{-1}(a, b)\sigma = (a, b)$ but $\sigma^{-1}(a, b)\sigma = (\sigma(a), \sigma(b))$ which means that σ either keep the location of a and b or swap the location of a and b.
If it swaps the location of a and b then $\sigma^{-1}(abc)\sigma = (\sigma(b)\sigma(c)\sigma(a)) = (a\sigma(c)b) \neq (abc)$ which is a contradiction, therefore σ keeps the location of a and b. Since a and b are arbitary, σ must keep the location of everything and every cycle can be break up into a. Which means that () must be the only identity.

Since $\forall a \in Q_8 : (-1) \cdot a = a \cdot (-1)$, -1 is a central element.
We have, $a \in Q_8 \iff -a \in Q_8$ and $\forall a \in Q_8 : (-1)(-1) \cdot a \cdot (-1) = (-1) \cdot a \cdot (-1)(-1) \implies 1 \cdot (-a) = (-a) \cdot 1$, which means that 1 is also a central element.
Since $i \cdot j = -j \cdot i = (-1) \cdot j \cdot i \neq j \cdot i$, i and j is not central element and since -i and -j is the inverse of i and j because $-i^2 = -j^2 = 1$. Also, $k \cdot (-j) = i \cdot j \cdot (-j) \implies k \cdot (-j) = i$ and $(-j) \cdot k = (-j) \cdot (-j) \cdot i = (-1) \cdot j \cdot (-j) \cdot i = (-1) \cdot i = -i \neq i$, which means that k is not a central element and as -k is the inverse of $k : -k^2 = 1$.

Let $x = r^i s^j \in D_{2n}$ where $i \in \{0, 1, \ldots, n-1\}$ and $j \in \{0, 1\}$ be an element in the central group $Z(D_{2n})$. Then

$$\begin{aligned}
& r^i \cdot s^j \cdot r = r \cdot r^i \cdot s^j \\
\implies & r^i \cdot s^j \cdot r = r^{i+1} \cdot s^j \\
\implies & r^{n-i} \cdot r^i \cdot s^j \cdot r = r^{n-i} \cdot r^{i+1} \cdot s^j \\
\implies & s^j \cdot r = r \cdot s^j
\end{aligned}$$

If $j = 1$ then $sr = rs = sr^{-1}$ which means that $ssr = ssr^{-1}$ and hence $r = r^{-1}$ which means that r has order 2 and hence is a contradiction in $D_{2n}\, \forall n \geq 3$.
Thenefore $j = 0$ and we get $x = r^i$ and get the following

$$\begin{aligned}
& r^i \cdot s = s \cdot r^i \\
\implies & r^i \cdot s = r^{n-i} \cdot s \\
\implies & r^i \cdot s \cdot s = r^{n-i} \cdot s \cdot s \\
\implies & r^i = r^{n-i} \\
\implies & r^i \cdot r^i = r^{n-i} \cdot r^i \\
\implies & r^{2i} = 1
\end{aligned}$$

If $r^i s = sr^i$, then consider an arbitary element $y = s^n r^m \in D_{2n}$
If $n = 0$, then obviously $r^i \cdot r^m = r^m \cdot r^i$
If $n = 1$, then $r^i \cdot s \cdot r^m = s \cdot r^i \cdot r^m = s \cdot r^m \cdot r^i$
Therefore, any element r^i satisfy r^{2i} is a central element, which means that for odd n, the only central element is 1 and for even n, there is 2 central elments 1 and $r^{n/2}$.

3.

Since φ is homomorphism, we have

$$\varphi(1) = \varphi(1 \cdot 1) = \varphi^2(1) \implies \varphi(1) = 1 \vee \varphi(1) = 0$$

If $\varphi(1) = 0$, then $\forall g \in G : \varphi(g) = \varphi(g) \cdot \varphi(1) = 0$. Therefore, $\forall a \in \mathbb{Z} : \varphi(g^a) = 0 = \varphi^a(g)$

If $\varphi(1) = 1$, then we use induction to prove that

$$\forall g \in G \, \forall a \in \mathbb{Z}^+ \cup \{0\} : \varphi(g^a) = \varphi(g)^a$$

Base case: $a = 0$

$$\varphi(g^0) = \varphi(1) = 1 = (\varphi(g))^0$$

Inductive step: Suppose $\varphi(g^a) = \varphi(g)^a$, prove that $\varphi(g^{a+1}) = \varphi(g)^{a+1}$

$$\varphi(g^{a+1}) = \varphi(g^a \cdot g) = \varphi(g^a) \cdot \varphi(g) = \varphi(g)^a \cdot \varphi(g) = \varphi(g)^{a+1}$$

We also have that since G is a group,

$$1 = \varphi(1) = \varphi(g \cdot g^{-1}) = \varphi(g) \cdot \varphi(g^{-1}) \implies \varphi(g)^{-1} = \varphi(g^{-1})$$

And

$$\forall g \in G \, \forall a \in \mathbb{Z}^- : \varphi(g^a) = \varphi((g^{-1})^{-a}) = \varphi(g^{-1})^{-a} = (\varphi(g)^{-1})^{-a} = \varphi(g)^a$$

Therefore, $\forall g \in G \, \forall a \in \mathbb{Z} : \varphi(g^a) = \varphi(g)^a$

4.

1.

Since S_3 and D_6 has the same order(6), they are isomorphic

2.

Since S_4 has order 8 and D_{24} has order 24, they are not isomorphic

3.

Consider $f : G \times H \to H \times G, \qquad (g, h) \to (h, g)$
$\forall (h, g) \in H \times G : g \in G \wedge h \in H$
$\implies (g, h) \in G \times H$
$\implies f(g, h) = (h, g)$
which proves that f is surjective. If $exists(g_1, h_1), (g_2, h_2) \in G \times H$ such that $f(g_1, h_1) = f(g_2, h_2)$ then $(h_1, g_1) = (h_2, g_2)$ which means that $h_1 = h_2$ and $g_1 = g_2$ and hence $(g_1, h_1) = (g_2, h_2)$. Therefore, f is injective and there $G \times H$ is isomorphic to $H \times G$.

4.

Consider the function $id : G \to G, \qquad g \to g$
$\forall g \in G : id(g) = g$.
$\forall g_1, g_2 \in G$ such that $id(g_1) = id(g_2) \implies g_1 = g_2$.
Hence, id is bijective. It is also obvious that $\forall g_1, g_2 \in G : id(g_1 \cdot g_2) = g_1 \cdot g_2 = id(g_1) \cdot id(g_2)$. Therefore, id is isomorphic.
$\forall f \in \text{Aut}(G) : G \to G, \qquad g \to h$:
$f \circ id(g) = f(g) = id(f(g)) = id \circ f(g)$.
Therefore, id is the identity.
$\forall f \in \text{Aut}(G) : G \to G, \qquad g \to h$
$\exists f^{-1} : G \to G, \qquad h \to g$ such that $f \circ f^{-1} = f^{-1} \circ f = id$
$\forall h_1, h_2 \in G$ such that $f^{-1}(h_1) = f^{-1}(h_2)$ then
$f \circ f^{-1}(h_1) = f \circ f^{-1}(h_2) \implies h_1 = h_2$
$\forall g \in G : f(g) = h$ and therefore, $g = f^{-1} \circ f(g) = f^{-1}(h)$.
Therefore, f^{-1} is bijective.
$\forall h_1, h_2 \in G : \exists g_1, g_2 \in G$ such that $f^{-1}(g_1) = h_1, f^{-1}(g_2) = h_2$, then

$$f^{-1}(h_1 \cdot h_2) = f^{-1}(f(g_1) \cdot f(g_2)) = f^{-1}(f(g_1 + g_2)) = g_1 + g_2 = f^{-1}(h_1) + f^{-2}(h_2)$$

therefore f^{-1} is an isomorphism and hence each function in $\text{Aut}(G)$ has an inverse also in $\text{Aut}(G)$ Function composition is associative. Therefore, $\text{Aut}(G)$ is a group.

5.

G and H are isomorphic, there exists $g : G \to H$ and $g^{-1} : H \to G$.
Consider $F : \text{Aut}(G) \to \text{Aut }(H), \qquad f \to g \circ f \circ g^{-1}$

Since there is an obvious inverse of $F : \mathrm{Aut}(H) \to \mathrm{Aut}\ (G)$, $\qquad h \to g^{-1} \circ h \circ g$:

$$(F \circ F^{-1})(f) = F(g^{-1} \circ f \circ g) = g \circ g^{-1} \circ f \circ g \circ g^{-1} = f$$

Therefore, F is bijective. $F(f_1 \circ f_2) = g \circ f_1 \circ f_2 \circ g^{-1} = g \circ f_1 \circ g^{-1} \circ g \circ f_2 \circ g^{-1} = F(f_1) \circ F(f_2)$. Hence, F is isomorphic, which means that $\mathrm{Aut}(G)$ is isomorphic to $\mathrm{Aut}(H)$

6.

1.

$$\forall a, b \in \mathbb{R} : (a + ia)(b + ib) = ab - ab + 2abi = 2abi \neq 1$$

Therefore, there don't exists an inverse for all elements in the set $\{a + i \cdot a \,|a \in \mathbb{R}\}$ and hence is not a subgroup.

2.

Consider $x = 1, y = -1 \in \{z \in \mathbb{C} \wedge \|z\| = 1\}$ $x + y = 0 \notin \{z \in \mathbb{C} \wedge \|z\| = 1\}$
Hence $\{z \in \mathbb{C} \wedge \|z\| = 1\}$ is not a subgroup

3.

Magnitude stay the same after $\cdot, g \cdot h \in$ the set
$\forall x \in \mathbb{C}\backslash\{0\} : \exists! z = \dfrac{x_1 - ix_2}{x_1^2 + x_2^2}$ (since $x_1^2 + x_2^2 = 0$ if and only if $x_1 = x_2 = 0$ which means that $x = 0 + 0i$) such that

$$x \cdot z = \left(x_1 \cdot \frac{x_1}{x_1^2 + x_2^2} - x_2 \cdot \frac{-x_2}{x_1^2 + x_2^2}\right) + i\left(x_1 \cdot \frac{-x_2}{x_1^2 + x_2^2} + x_2 \cdot \frac{x_1}{x_1^2 + x_2^2}\right) = 1 + 0i$$

inverse exists as: is a subgroup

4.

Let the set be A.
$(1, 2), (1, 3) \in A$, but $(1, 2)(1, 3) = (1, 3, 2) \notin A$. Therefore, the set is not closed and not a subgroup.

5.

Let the set be A.
$\forall a = sr^i \in A : sr \cdot sr^i = r^{n-1}s \cdot sr^i = r^{n-1+i} \notin A$. Therefore, the set is not closed and not a subgroup.

6.

Let the set be A.
If it is a subgroup, then as 0 is the identity in $\mathbb{Z}$ is an element of A, but 0 is even, which is a contradiction.

7.

For $n \in \mathbb{N}$, let $A_n \subset \mathbb{Z}$ be the set contains integers which are divisible by n that is $a \equiv 0 \bmod n$. We have
If $a, b \in A_n : a \equiv 0 \bmod n \wedge b \equiv 0 \bmod n \implies a + b \equiv 0 \bmod n$ and hence

$a + b \in A_n$
0 is a multiply of n, and hence $0 \in A_n$. Also $\forall a \in A_n : a{+}0 = a$, which means that 0 is the identity. $\forall a \in A_n : a \equiv 0 \bmod n \implies -a \equiv 0 \bmod n \implies -a \in A_n$ and a+(-a) = 0 Therefore, for any natural number n, A_n satisfies all the conditions to be a group, that is closed, there is an identity and every element has an inverse.

8.

Because of $r^4 = 1, s^2 = 1, rs^2 = sr^2, sr^2 = r^2 s$ and 1 is the identity, we have the following table:

$\cdot$	1	r^2	s	sr^2
1	1	r^2	s	sr^2
r^2	r^2	1	sr^2	s
s	s	sr^2	1	r^2
sr^2	sr^2	sr	r^2	1

From the table, we can see that it satisfies all the conditions to be a group, that is closed, there is an identity and every element has an inverse.

9.

Because of $r^4 = 1, s^2 = 1, rs = sr^3, sr = r^3 s$ and 1 is the identity, we have the following table:

$\cdot$	1	r^2	sr	sr^3
1	1	r^2	sr	sr^3
r^2	1	1	sr^3	sr
sr	sr	sr^3	1	r^2
sr^3	sr^3	sr	r^2	1

From the table, we can see that it satisfies all the conditions to be a group, that is closed, there is an identity and every element has an inverse.

10.

Let A be the set. $sr^2 \cdot s = r^3 s \cdot s = r^3 \cdot s^2 = r^3 \notin A$. Hence A is not closed and not a subgroup.

11.

Let A be the set. $sr^3 \cdot r^2 = sr^5 = s \notin A$. Hence A is not closed and not a subgroup.

12.

Let the set be A. We have that $i \cdot i = -1 \notin A$ Hence A is not closed and not a subgroup.

13.

Because of $i^2 = 1, -i = -1 \cdot i, -1 \cdot (-1) = 1$ and 1 is the identity, we have the following table:

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

From the table, we can see that it satisfies all the conditions to be a group, that is closed, there is an identity and every element has an inverse.

14.

Let the set be A. A contains all cycles of length 2 (as stated in the first question of the assignment). Since $\forall \sigma \in A, \exists a, b, c, d \in \{1, 2, 3, 4\} : \sigma = (a, b)(c, d)$. Therefore, all cycles in A has even order as the identity can be written as 0 transposition. And since $\forall \sigma_1, \sigma_2 \in A \subset S_4 :$

$$\sigma_1\sigma_2 \text{ is even and } \sigma_1\sigma_2 \in S_4 \text{ which has order} \leq 4$$

Therefore, $\forall \sigma_1, \sigma_2 \in A : \sigma_1\sigma_2 \in A$
A has the identity element.
$\forall \sigma \in A \subset S_4 : \exists \sigma^{-1} \in S_4 : \sigma\sigma^{-1} = 1$ As $\sigma$and 1 are two known even cycle, $\sigma^{-1} \in S_4$ also has even cycle and therefore is an element of A
Therefore, A is a subgroup.