0.3.11) If \( \bar{a}, \bar{b} \in (\mathbb{Z}/n\mathbb{Z})^* \), then \( \gcd(a, n) = \gcd(b, n) = 1 \).

\( \Rightarrow a, b \) have no prime factors in common with \( n \).
Any prime factor of \( ab \) is a factor of either \( a \) or \( b \),
so \( ab \) has no prime factors in common with \( n \).

\( \therefore \gcd(ab, n) = 1 \)
\( \therefore \bar{a} \bar{b} \in (\mathbb{Z}/n\mathbb{Z})^* \) (Proposition 4 again)
by definition of multiplication in \( \mathbb{Z}/n\mathbb{Z} \), \( \bar{a} \bar{b} = \bar{ab} \).
\( \therefore \bar{a} \bar{b} \in \mathbb{Z}/n\mathbb{Z} \), as required.

1.1.5) We will show that for \( n > 1 \), the element \( \bar{0} \) of \( \mathbb{Z}/n\mathbb{Z} \) does not have an inverse.

Assume that the element \( a \) of \( \mathbb{Z}/n\mathbb{Z} \) was a multiplicative inverse of \( \bar{0} \). That is, \( a \bar{0} = \bar{0} a = \bar{1} \) (It is easily checked that \( \bar{1} \) is the only possibility for the identity of \( \mathbb{Z}/n\mathbb{Z} \) as a multiplicative group).

Then: \( a \bar{0} = \bar{1} \), but also \( a \bar{0} = a(\bar{0} \cdot \bar{0}) = \underbrace{a(\bar{0} \cdot \bar{0}) \cdot \bar{0}}_\text{by definition of multiplication in } \mathbb{Z}/n\mathbb{Z} \cdot \bar{0} = \bar{1} \cdot \bar{0} \cdot \bar{0} = \bar{0} \).

\( \therefore \bar{1} = \bar{0} \), a contradiction as \( n > 2 \).

\( \therefore \) The element \( \bar{0} \) of \( \mathbb{Z}/n\mathbb{Z} \) does not have a multiplicative inverse.
\( \therefore \mathbb{Z}/n\mathbb{Z} \) under multiplication is not a group.

1.1.2b) Note first that for some \( y \in G \), \( y \) is the identity \( \bar{1} \) if and only if \( y^{-1} \) is the identity \( \bar{1} \),\( \Rightarrow y = \bar{1} \) ( \( \Rightarrow \) \( y^{-1} = \bar{1} \) and the reverse implication is similar).

Now, for each \( n \in \mathbb{Z}^+ \), \( x^n(x^{-1})^n = x^{-n}(x^{-1})^n(x^{-1})^{n-1} \)
\( = x^{-n}(x^{-1})^{n-1} \)
\( = x x^{-1} = \bar{1} \).
Likewise, \((x^{-1})^n x^n = (x^{-1})^{n-1}(x^{-1}x)x^{n-1}\)
\[= (x^{-1})^{n-1}x^{n-1}\]
\[= x^{-1}x\]
\[= 1_a\]

\[\therefore \] \(x^n\) and \((x^{-1})^n\) are inverses.

\[\therefore\] By our initial remark, \(x^n = 1_a\) if and only if \((x^{-1})^n = 1_a\).

\[\therefore\] The smallest \(n \in \mathbb{Z}^+\) with \(x^n = 1_a\) is the same as the smallest \(n \in \mathbb{Z}^+\) with \((x^{-1})^n = 1_a\). (If many such integers exist)

But this is the definition of the order of \(x\) and of \(x^{-1}\). (If no such integers exist, then both \(x\) and \(x^{-1}\) have infinite order)

\[\therefore \] \(x\) and \(x^{-1}\) have the same order.

1.122) As with the previous question, it suffices to show that \(x^n = 1_a\) if and only if \((g^{-1}xg)^n = 1_a\), for each \(n \in \mathbb{Z}^+\):

\[(g^{-1}xg)^n = g^{-1}xg g^{-1}xg \cdots g^{-1}xg\]

\[= g^{-1}x(gg^{-1})x(gg^{-1})x \cdots x(gg^{-1})xg\]

\[= g^{-1}x^1 a x^1 a \cdots x^1 a x g\]

\[= g^{-1}x^a g\]

Now, if \(x^n = 1_a\) then \(g^{-1}x^a g = g^{-1}g = 1_a\) (left-multiply by \(g^{-1}\) and right-multiply by \(g\)).

Likewise, if \(g^{-1}x^a g = 1_a\), then \(gg^{-1}x^a gg^{-1} = gg^{-1} = 1_a\) by \(g\)

\[\therefore x^n = 1_a\]
\[ x^n = e \text{ if and only if } (g^{-1}xg)^n = e. \]
\[ |x| = |g^{-1}xg| \text{ for each } g, x \in G. \] (See argument in 1.1.20, preceding page)

For any \( a, b \in G \), let \( x = ab \) and \( y = a. \)

\[ |x| = |g^{-1}xg|, \text{ so } |ab| = |a^{-1}aba| = |bab| = |bal|, \text{ as required.} \]

1.1.28) In this question, if \( a, a' \) are elements of \( A \) we will use \( aa' \) to denote \( a \ast a' \). Likewise, if \( b, b' \) are elements of \( B \), then \( bb' = b \circ b' \).

a) Consider three arbitrary elements \((a_1, b_1), (a_2, b_2), \text{ and } (a_3, b_3)\) of \( A \times B\)

\[
(a_1, b_1)(a_2, b_2)(a_3, b_3) = (a_1, b_1)(a_2a_3, b_2b_3) \] (Definition of multiplication in the direct product)

\[ = (a_1, a_2a_3, b_1, b_2b_3) \] (""")

\[ = (a, a_2a_3, b_1b_2b_3) \] (Multiplication in \( A \) or \( B \) is associative)

\[ = (a, a_2, b_1b_2)(a_3, b_3) \] (Multiplication in \( A \times B \))

\[ = (a_1, b_1)(a_2, b_2)(a_3, b_3) \] ("")

Hence multiplication in \( A \times B \) is associative.

b) Consider an arbitrary element \((a, b)\) of \( A \times B\).

\[
(1_A, 1_B)(a, b) = (1_A, a, 1_B, b) = (a, b), \quad (1_A, 1_B \text{ are the identities of } A, B) \]

\[
(a, b)(1_A, 1_B) = (a, b, 1_B, 1_B) = (a, b, b), \]

\[
(1_A, 1_B) \text{ is the identity of } A \times B. \]
c) Consider an arbitrary element \((a, b)\) of \(A \times B\).
\[
\begin{align*}
(a^{-1}, b^{-1})(a, b) &= (a^{-1}a, b^{-1}b) = (1_A, 1_B) = 1_{A \times B}, \\
(a, b)(a^{-1}, b^{-1}) &= (aa^{-1}, bb^{-1}) = (1_A, 1_B) = 1_{A \times B}
\end{align*}
\]
Because \(a^{-1}a = a, b^{-1}b = b\) and \(a, b \in A \times B\).
\[
\therefore (a^{-1}, b^{-1}) \text{ is the inverse of } (a, b).
\]

1.1.32) Let \(x \in G\) have order \(n < \infty\).

Assume, for the sake of a contradiction, that two of the elements \(1_A, x, x^2, \ldots, x^{n-1}\) are equal.

Let \(x^k = x^l\), for \(k \neq l\) and \(k, l \in \{0, 1, 2, \ldots, n-1\}\). Assume also that \(k > l\) (WLOG).

\[
x^k = x^l, \text{ so } x^{-l}x^k = x^{-l}x^l \\
\therefore x^{k-l} = x^0 = 1_G.
\]

\[
\therefore x^{k-l} = 1_G \text{ and } k-l \text{ is a positive integer less than } n \text{ (as both } k \text{ and } l \text{ are in } \{0, 1, \ldots, n-1\} \text{ and } k > l)\]

This contradicts the fact that the order of \(x\) is \(n\).

\[
\therefore \text{No two of } 1_A, x, x^2, \ldots, x^{n-1} \text{ are equal.}
\]

Each of these are elements of \(G\), so \(G\) contains at least \(n\) distinct elements.

\[
\therefore \text{For any } x \in G, \text{ } G \text{ contains at least } |x| \text{ elements. That is, } |x| \leq |G|.
\]
1.2.3) $D_n$ is generated by the elements $r$ and $s$, so any element $g$ of $D_n$ is equal to the product of some sequence of $r$s and $s$s.

Because $rs = sr^{-1}$, we may move any $r$ on the left of an $s$ to the right, changing it to an $r^{-1}$. Repeating this will give $g = s^i r^j$, for $i,j \in \mathbb{Z}$.

For example, take $sr s r^2 s$

$= ss r^{-1} r^2 s$
$= ss r s$
$= ss s r^{-1}$
$= s^3 r^{-1}$.

Now, $r^n = s^2 = 1$, so we may write $g$ as $g = s^i r^j$ with $0 \leq i \leq n$ and $0 \leq j \leq n-1$.

Any element of $D_n$ is one of the following:

$\{1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1} \}$

(We have not shown that these are distinct. Is it possible that $r^2 = sr^3$ or something?)

Now we are asked about the elements of $D_n$ which are not the powers of $r$.
These are $\{s, sr, sr^2, \ldots, sr^{n-1} \}$

Consider $(sr^i)^2 = sr^i sr^i$

$= sr^{i-1} sr^{-1} r^i$ (rs = sr^{-1})
$= sr^{i-2} sr^{-2} r^i$
$\vdots$
$= s^2 r^{-i} r^i = 1.$
Each element \((sr^i)\) has order 2, as required.

(This corresponds to the reflections of the \(n\)-gon, while the elements \(r^i\) are rotations.)

\(D_n\) is generated by \(s\) and \(r\) and the element \(r\) can be written as \(s\cdot sr^i\).

\(D_n\) is generated by \(s\) and \(sr^i\), and each of these has order two.

(s and \(sr^i\) correspond to adjacent reflections of the \(n\)-gon. Convince yourself that composing them produces a rotation. What if you compose them in the other order?)

1.3.11) The permutation \(σ^i\) is either an \(m\)-cycle or the product of a number of smaller cycles. By symmetry, each of these cycles must have the same length (because the cycles \((1, 2, 3, \ldots, m)\) and \((2, 3, 4, \ldots, m, 1)\) represent the same permutation).

Hence either \(σ^i\) is an \(m\)-cycle or the product of \(k\) \(\frac{m}{k}\)-cycles.

\(σ^i\) is an \(m\)-cycle if and only if the order of \(σ^i\) is no less than \(m\).

\[
\Rightarrow (σ^i)^n \neq 1 \quad \text{for all} \quad n < m.
\]

\[
\Leftrightarrow \text{mf in} \quad \text{for all} \quad n < m \quad (σ \text{ has order } m)
\]

\[
\Leftrightarrow \gcd(m, i) = 1 \quad (\text{examine } n = \frac{m}{\gcd(i, m)})
\]

\(σ^i\) is an \(m\)-cycle if and only if \(\gcd(i, m) = 1\).
6.4) The multiplicative group \( C - \mathbb{Z}03 \) has elements of any positive order, while any element of \( \mathbb{R} - \mathbb{Z}03 \) has order 1, 2 or \( \infty \). To see why this means the groups cannot be isomorphic, assume that there is an isomorphism \( \phi: C - \mathbb{Z}03 \to \mathbb{R} - \mathbb{Z}03 \).

\[ \phi(1) = 1, \] as 1 is the identity of both groups.

Let \( \phi(w) = e^{i\frac{2\pi}{3}} = \frac{1 - \sqrt{3}i}{2} \).

\[ w^3 = 1, \]

\[ \phi(w^3) = \phi(w)^3, \] as \( \phi \) is a homomorphism.

But \( \phi(w^3) = \phi(1) = 1 \).

\[ \therefore \phi(w) \text{ is a root number with } (\phi(w))^3 = 1 \]

\[ \therefore \phi(w) = 1, \] a contradiction as \( \phi(w) = \phi(1) \) so \( \phi \) is not injective.

(In general, if \( \phi \) is an isomorphism, then for any \( g \) in the domain \( g \) and \( \phi(g) \) will have the same order).

It would also be valid to use the fact that \(-1\) has square roots in \( C - \mathbb{Z}03 \) but not in \( \mathbb{R} - \mathbb{Z}03 \), but only if you used the multiplicative structure of the group to define \(-1\) (it is the square root of \( 1 \) which is not \( 1 \) itself).

An isomorphism of multiplicative groups would not necessarily preserve any of the additive structure that \( \mathbb{R} \) and \( C \) happen to have, so you can’t define \(-1\).
as an additive inverse.

Another possibility would be that $\mathbb{R} - \mathbb{S}^0$ contains elements with no square root, while $\mathbb{C} - \mathbb{S}^0$ does not, without needing to worry about specifying those elements.

1.6.7) The group $D_8$ has 1 element of order 1, 5 elements of order 2 ($s,sr, sr^2, sr^3, r^2$), and 2 elements of order 4 ($r, r^3$).

The group $Q_8$ has 1 element of order 1, 1 element of order 2 ($-1$) and 6 elements of order 4 ($i, -i, j, -j, k, -k$).

Any isomorphism must preserve the orders of elements, which is impossible here (as isomorphisms are bijections).

Extra problem 1) When $n$ is even, then $\sigma$ has cycle decomposition as follows:

$$\sigma = (1 \ n)(2 \ (n-1))(3 \ (n-2)) \cdots (\frac{n}{2} \ (\frac{n}{2} + 1))$$

When $n$ is odd, we have:

$$\sigma = (1 \ n)(2 \ (n-1))(3 \ (n-2)) \cdots (\frac{n-1}{2} \ (\frac{n+3}{2}))$$

(In this case, $\sigma$ fixes $\frac{n+1}{2}$)
Extra 2) Firstly, the case when $n$ is even:

This question is much easier if you draw a diagram to help you see what's happening!

$$r = (1 \ 2 \ 3 \ \ldots \ \ n)$$

$$s = (1)(2 \ n)(3 \ (n-1)) \ldots (\frac{n}{2}+2)(\frac{n}{2}+1)$$

(The fixed points 1 and $\frac{n}{2}+1$ are shown for clarity)

$rs$ is obtained by applying first $s$ and then $r$. Earlier we showed that $rs$ has order 2 so it will be a reflection comprised of cycles of length 2 (and perhaps some of length 1).

$$rs = (1 \ 2)(3 \ n)(4 \ (n-1)) \ldots (\frac{n}{2}+1)(\frac{n}{2}+2)$$

(By multiplying the permutating $r$ and $s$)

Note that $rs$ has no fixed points!

It is a different type of reflection to $r$. It passes through the midpoint of an edge, rather than through a vertex.

$$r^2 = (1 \ 3 \ 5 \ \ldots \ (n-1))(2 \ 4 \ 6 \ \ldots \ n)$$

$r^2$ is obtained just by applying $r$ twice.
Now, when $n$ is odd:

$r = (1 \ 2 \ 3 \ \cdots \ n)$

$s = (1)(2 \ n)(3 \ (n-1)) \cdots \left(\frac{n+1}{2} \ \frac{n+3}{2}\right)$

Again, multiply $r$ and $s$ to get $rs$

$rs = (1 \ 2)(3 \ n)(4 \ (n-1)) \cdots \left(\frac{n+1}{2} \ \frac{n+5}{2}\right)\left(\frac{n+3}{2}\right)$

Note that in this case, both $s$ and $rs$ have a single fixed point! This illustrates a fundamental difference between the groups $D_{2n}$ and $D_m$ when $n$ is odd and $m$ even. In $D_{2n}$, $n$ odd, there is only one "type" of reflection - it fixes a single vertex (and an edge). In $D_{2m}$, $m$ even, there are reflections which fix 2 vertices and no edges and some which fix 2 edges and no vertices. (And also a rotation by $\pi$, which as an element of order 2 is a sort of honorary reflection.)

Note that any reflection passes through a vertex and an edge.

Here, reflections either pass through 2 vertices or 2 edges.
Finally, \( r^2 = (1, 3, 5 - n, 2, 4 \ldots n-1) \).

Another difference between the even and odd cases - the order of \( r^2 \) is either \( \frac{n}{2} \) or \( n \).

Referring to question 1.3.11, this should not be surprising.

Extra 3a) We need to show that \( \text{Supp}(\sigma \tau) \subseteq \text{Supp}(\sigma) \cup \text{Supp}(\tau) \).

\( \implies \) An element of \( \{1, 3 \ldots n\} \) which is not fixed by \( \sigma \tau \) must not be fixed by either \( \sigma \) or \( \tau \).

\( \implies \) Elements of \( \{1, 3 \ldots n\} \) which are fixed by both \( \sigma \) and \( \tau \) are fixed by \( \sigma \tau \).

(This is the contrapositive of the previous statement)

This is clearly true - if \( \sigma \) and \( \tau \) both fix \( x \), then \( \sigma \tau(x) = \sigma(\tau(x)) = \sigma(x) = x \).

Hence \( \text{Supp}(\sigma \tau) \subseteq \text{Supp}(\sigma) \cup \text{Supp}(\tau) \).

3b) Let's try and construct \( \sigma \) and \( \tau \) so that \( \sigma \tau \) fixes something which \( \sigma \) doesn't.

The simplest thing to do here is to have \( \tau(1) = 2 \) and \( \sigma(2) = 1 \), so that \( \sigma \tau(1) = 1 \). Now, we just need \( \tau(1) \neq 1 \).

Let's try \( \sigma(1) = 3 \) and \( \tau(3) = 3 \).
The two such permutations are:

\[ \sigma = (1 \ 3 \ 2) \]
\[ \tau = (1 \ 2) \]

Then \( \sigma \tau = (2 \ 3) \) and \( \tau \sigma = (1 \ 3) \).

So \( \mathrm{Supp}(\sigma \tau) = \{2, 3\} \neq \{1, 3\} = \mathrm{Supp}(\tau \sigma) \).

Notice that \( \sigma \tau \) and \( \tau \sigma \) have the same cycle type. Will this always be the case?