True/False Questions

1. The order of the identity element in any group is 1.

True. \( n = 1 \) is the least positive integer such that \( e^n = e \).

2. Every cyclic group is abelian.

True. Let \( G \) be a cyclic group. All elements of \( G \) are of the form \( a^n \), where \( n \in \mathbb{Z} \). Let \( x, y \in G: x = a^p, y = a^q \). Then,

\[
xy = a^p a^q = a^{p+q} = a^q a^p = yx.
\]

Thus, \( xy = yx \) for all \( x, y \in G \). (\( p + q = q + p \) because \( \mathbb{Z} \) is an abelian additive group.)

3. Every abelian group is abelian.

False. Let us take \( U_{12} = \{ [1], [5], [7], [11] \} \subset \mathbb{Z}_{12} \). \( U_{12} \) is abelian group but this group is not cyclic since the order of elements of \( U_{12} \) can not be 4. In fact, \( o([1]) = 1, o([5]) = 2, o([7]) = 2, \) and \( o([11]) = 2 \).

4. If a subgroup \( H \) of a group \( G \) is cyclic, then \( G \) must be cyclic.

False. \( G = (\mathbb{Q},+) \) is a group and \( H = (\mathbb{Z},+) \) is a subgroup of \( G = (\mathbb{Q},+) \). \( H = \mathbb{Z} = \langle 1 \rangle \) is cyclic whereas \( \mathbb{Q} \) is not cyclic.

5. Whether a group \( G \) is cyclic or not, each element \( a \) of \( G \) generates a cyclic subgroup.

True. Look at Remark.

6. Every subgroups of a cyclic group is cyclic.

True. Look at Theorem 3.20.

7. If there exists an \( m \in \mathbb{Z}^+ \) such that \( a^m = e \), where \( a \) is an element of a group \( G \), then \( o(a) = m \).

False. \( m \) must be the least positive integer such that \( a^m = e \).
8. Any group of order 3 must be cyclic

True. Suppose that $G$ is a group of order 3. One of the elements is $e$. So, $G = \{e, a, b\}$. We want to show that $a^2 = b$ and $a^3 = e$. But these are not that obvious to prove. The thing that we can prove is that

$$ab = e.$$  

Proof: It can not be anything else. If $ab = a$ then $b = e$, a contradiction. If $ab = b$ then $a = e$, a contradiction. Next,  

$$a^2 = b$$

because it can not be anything else. If $a^2 = a$ then $a^2 = ab$ would give $a = b$, a contradiction. If $a^2 = a$ then $a = e$, a contradiction. Finally,  

$$a^3 = aa^2 = ab = e$$

and we are done.

9. Any group of order 4 must be cyclic.

False. Let us take $U_{12} = \{[1], [5], [7], [11]\} \subseteq \mathbb{Z}_{12}$. Then, the order of this group is 4. But this group is not cyclic since the order of elements of $U_{12}$ can not be 4. In fact, $o([1]) = 1$, $o([5]) = 2$, $o([7]) = 2$, and $o([11]) = 2$.

10. Let $a$ be an element of a group $G$. Then $\langle a \rangle = \langle a^{-1} \rangle$.

True. We will show that $\langle a \rangle \subseteq \langle a^{-1} \rangle$ and $\langle a^{-1} \rangle \subseteq \langle a \rangle$. For this, let $x \in \langle a \rangle$. So $x = a^k$ for some integer $k$. Moreover, $x = a^k = (a^{-1})^{-k}$ implies that $x \in \langle a^{-1} \rangle$. The first part is complete. Now, we will show that the second part is true. For this, let $x \in \langle a^{-1} \rangle$. So $x = (a^{-1})^k$ for some integer $k$.

Exercises

1. $\langle e \rangle = \{e\}$, $\langle \rho \rangle = \{e, \rho, \rho^2\}$, $\langle \sigma \rangle = \{e, \sigma\}$, $\langle \gamma \rangle = \{e, \gamma\}$, $\langle \delta \rangle = \{e, \delta\}$

2. $\langle 1 \rangle = \{1\}$, $\langle -1 \rangle = \{1, -1\}$, $\langle i \rangle = \{1, i, -1, -i\}$, $\langle -i \rangle = \{1, -i, -1, i\}$

   $\langle j \rangle = \{1, j, -1, -j\}$, $\langle -j \rangle = \{1, -j, -1, j\}$, $\langle k \rangle = \{1, k, -1, -k\}$, $\langle -k \rangle = \{1, -k, -1, k\}$.

3. The element $e$ has order 1. Each of the elements $\sigma$, $\gamma$, and $\delta$ has order 2. Each of the elements $\rho$ and $\rho^2$ has order 3.

4. $o(1) = 1$, $o(-1) = 2$, $o(i) = o(-i) = o(j) = o(-j) = o(k) = o(-k) = 4$.

5. $o(I_3) = 1$, $o(P_1) = o(P_2) = o(P_4) = 2$, $o(P_3) = o(P_5) = 3$
Exercises 3.4

6. a) $n = 2$ is the least positive integer such that $A^2 = I$. Therefore, $o(A) = 2$.
   b) $n = 4$ is the least positive integer such that $A^4 = I$. Therefore, $o(A) = 4$.

7. Since $o(G) = 8$, $a^8 = e$.
   a) $x = 4$ is the least positive integer such that $(a^2)^x = e$. Therefore, $o(a^2) = 4$.
   b) $x = 8$ is the least positive integer such that $(a^3)^x = e$. Therefore, $o(a^3) = 8$.
   c) $x = 2$ is the least positive integer such that $(a^4)^x = e$. Therefore, $o(a^4) = 2$.
   d) $x = 8$ is the least positive integer such that $(a^5)^x = e$. Therefore, $o(a^5) = 8$.
   e) $x = 4$ is the least positive integer such that $(a^6)^x = e$. Therefore, $o(a^6) = 4$.
   f) $x = 8$ is the least positive integer such that $(a^7)^x = e$. Therefore, $o(a^7) = 8$.
   g) $x = 1$ is the least positive integer such that $(a^8)^x = e$. Therefore, $o(a^8) = 1$.

8. Since $o(G) = 9$, $a^9 = e$.
   a) $x = 9$ is the least positive integer such that $(a^2)^x = e$. Therefore, $o(a^2) = 9$.
   b) $x = 6$ is the least positive integer such that $(a^3)^x = e$. Therefore, $o(a^3) = 6$.
   c) $x = 9$ is the least positive integer such that $(a^4)^x = e$. Therefore, $o(a^4) = 9$.
   d) $x = 9$ is the least positive integer such that $(a^5)^x = e$. Therefore, $o(a^5) = 9$.
   e) $x = 3$ is the least positive integer such that $(a^6)^x = e$. Therefore, $o(a^6) = 3$.
   f) $x = 9$ is the least positive integer such that $(a^7)^x = e$. Therefore, $o(a^7) = 9$.
   g) $x = 9$ is the least positive integer such that $(a^8)^x = e$. Therefore, $o(a^8) = 9$.
   h) $x = 1$ is the least positive integer such that $(a^9)^x = e$. Therefore, $o(a^9) = 1$.

9. a) $[1],[3],[5],[7]$  b) $[1],[5],[7],[11]$  c) $[1],[3],[7],[9]$  d) $[1],[2],[4],[7],[8],[11],[13],[14]$  e) $[1],[3],[5],[7],[9],[11],[13],[15]$  f) $[1],[5],[7],[11],[13],[17]$

10. a) The divisors of 12 are $d = 1,2,3,4,6,12$, so the distinct subgroups of $\mathbb{Z}_{12}$ are those subgroups $\langle d[a] \rangle$ where $[a]$ is a generator of $\mathbb{Z}_{12}$. Since $\mathbb{Z}_{12} = \langle [1] \rangle$, the generator $[a]$ can be taken $[1]$. Then,

\[
\begin{align*}
\langle [1] \rangle & = \mathbb{Z}_{12} ; o(\mathbb{Z}_{12}) = 12 , \\
\langle [2] \rangle & = \langle [2] \rangle = \{ [0], [2], [4], [6], [8], [10] \} ; o(\langle [2] \rangle) = 6 .
\end{align*}
\]
Exercises 3.4

Cyclic Groups

\[ \langle 3, [1] \rangle = \langle [3] \rangle = \{[0],[3],[6],[9]\} ; o([3]) = 4, \]
\[ \langle 4, [1] \rangle = \langle [4] \rangle = \{[0],[4],[8]\} ; o([4]) = 3, \]
\[ \langle 6, [1] \rangle = \langle [6] \rangle = \{[0],[6]\} ; o([6]) = 2, \]
\[ \langle 12, [1] \rangle = \langle [0] \rangle = \{[0]\} ; o([0]) = 1. \]

b) The divisors of 8 are \( d = 1,2,4,8 \), so the distinct subgroups of \( \mathbb{Z}_8 \) are those subgroups \( \langle d[a] \rangle \) where \([a]\) is a generator of \( \mathbb{Z}_8 \). Since \( \mathbb{Z}_8 = \langle [1] \rangle \), the generator \([a]\) can be taken \([1]\). Then,
\[ \langle 1, [1] \rangle = \mathbb{Z}_8 ; o(\mathbb{Z}_8) = 8, \]
\[ \langle 2, [1] \rangle = \langle [2] \rangle = \{[0],[2],[4],[6]\} ; o([2]) = 4, \]
\[ \langle 4, [1] \rangle = \langle [4] \rangle = \{[0],[4]\} ; o([4]) = 2, \]
\[ \langle 8, [1] \rangle = \langle [0] \rangle = \{[0]\} ; o([0]) = 1. \]

c) The divisors of 10 are \( d = 1,2,5,10 \), so the distinct subgroups of \( \mathbb{Z}_{10} \) are those subgroups \( \langle d[a] \rangle \) where \([a]\) is a generator of \( \mathbb{Z}_{10} \). Since \( \mathbb{Z}_{10} = \langle [1] \rangle \), the generator \([a]\) can be taken \([1]\). Then,
\[ \langle 1, [1] \rangle = \mathbb{Z}_{10} ; o(\mathbb{Z}_{10}) = 10, \]
\[ \langle 2, [1] \rangle = \langle [2] \rangle = \{[0],[2],[4],[6],[8]\} ; o([2]) = 5, \]
\[ \langle 5, [1] \rangle = \langle [5] \rangle = \{[0],[5]\} ; o([5]) = 2, \]
\[ \langle 10, [1] \rangle = \langle [0] \rangle = \{[0]\} ; o([0]) = 1. \]

d) The divisors of 15 are \( d = 1,3,5,15 \), so the distinct subgroups of \( \mathbb{Z}_{15} \) are those subgroups \( \langle d[a] \rangle \) where \([a]\) is a generator of \( \mathbb{Z}_{15} \). Since \( \mathbb{Z}_{15} = \langle [1] \rangle \), the generator \([a]\) can be taken \([1]\). Then,
\[ \langle 1, [1] \rangle = \mathbb{Z}_{15} ; o(\mathbb{Z}_{15}) = 15, \]
\[ \langle 3, [1] \rangle = \langle [3] \rangle = \{[0],[3],[6],[9],[12]\} ; o([3]) = 5, \]
\[ \langle 5, [1] \rangle = \langle [5] \rangle = \{[0],[5],[10]\} ; o([5]) = 3, \]
\[ \langle 15, [1] \rangle = \langle [0] \rangle = \{[0]\} ; o([0]) = 1. \]

e) The divisors of 16 are \( d = 1,2,4,8,16 \), so the distinct subgroups of \( \mathbb{Z}_{16} \) are those subgroups \( \langle d[a] \rangle \) where \([a]\) is a generator of \( \mathbb{Z}_{16} \). Since \( \mathbb{Z}_{16} = \langle [1] \rangle \), the generator \([a]\) can be taken \([1]\). Then,
Theorem 3.24, the generators of this group is in the form $11^{-12}$.

Exercises 3.4 Cyclic Groups

1. $\{1, [1]\} = Z_{18}; o(Z_{18}) = 16$,
2. $\{2, [1]\} = \langle [2]\rangle = \{[0],[2],[4],[6],[8],[10],[12],[14],[16]\}; o(\langle [2]\rangle) = 8$,
3. $\{4,[1]\} = \langle [4]\rangle = \{[0],[4],[8],[12]\}; o(\langle [4]\rangle) = 4$,
4. $\{8,[1]\} = \langle [8]\rangle = \{[0],[8]\}; o(\langle [8]\rangle) = 2$,
5. $\{16,[1]\} = \langle [0]\rangle = \{[0]\}; o(\langle [0]\rangle) = 1$,
6. $\{1, [1]\} = Z_{18}; o(Z_{18}) = 18$,
7. $\{2, [1]\} = \langle [2]\rangle = \{[0],[2],[4],[6],[8],[10],[12],[14],[16]\}; o(\langle [2]\rangle) = 9$,
8. $\{3,[1]\} = \langle [3]\rangle = \{[0],[3],[6],[9],[12],[15]\}; o(\langle [3]\rangle) = 6$,
9. $\{6,[1]\} = \langle [6]\rangle = \{[0],[6],[12]\}; o(\langle [6]\rangle) = 3$,
10. $\{9,[1]\} = \langle [9]\rangle = \{[0],[9]\}; o(\langle [9]\rangle) = 2$,
11. $\{18,[1]\} = \langle [0]\rangle = \{[0]\}; o(\langle [0]\rangle) = 1$.

f) The divisors of 18 are $d = 1,2,3,6,9,18$, so the distinct subgroups of $Z_{18}$ are those subgroups $\langle a^d \rangle$ where $[a]$ is a generator of $Z_{18}$. Since $Z_{18} = \langle [1]\rangle$, the generator $[a]$ can be taken $[1]$. Then,

$\{1,[1]\} = Z_{18}; o(Z_{18}) = 18$,
$\{2,[1]\} = \langle [2]\rangle = \{[0],[2],[4],[6],[8],[10],[12],[14],[16]\}; o(\langle [2]\rangle) = 9$,
$\{3,[1]\} = \langle [3]\rangle = \{[0],[3],[6],[9],[12],[15]\}; o(\langle [3]\rangle) = 6$,
$\{6,[1]\} = \langle [6]\rangle = \{[0],[6],[12]\}; o(\langle [6]\rangle) = 3$,
$\{9,[1]\} = \langle [9]\rangle = \{[0],[9]\}; o(\langle [9]\rangle) = 2$,
$\{18,[1]\} = \langle [0]\rangle = \{[0]\}; o(\langle [0]\rangle) = 1$.

11-12 a) Since $Z_7 = \langle [0]\rangle = \{[1],[2],[3],[4],[5],[6]\}$, the order of this group is 6. By Theorem 3.24, the generators of this group is in the form $a^m$ iff $(m,6) = 1$. So the values of $m$ are 1 and 5. Therefore, $Z_7 = \langle [0]\rangle = \langle a^1 \rangle = \langle a^5 \rangle$. Let us find the element $a$ of this group. Take the element $[3]$. All of the powers of $[3]$ are


Therefore, $Z_7 = \langle [0]\rangle = \langle [3]^1 \rangle = \langle [3]^5 \rangle = \langle [5]\rangle$.

b) Since $Z_5 = \langle [0]\rangle = \{[1],[2],[3],[4]\}$, the order of this group is 4. By Theorem 3.24, the generators of this group is in the form $a^m$ iff $(m,4) = 1$. So the values of $m$ are 1 and 3.
Therefore, \( \mathbb{Z}_5 - \{0\} = \langle a^1 \rangle = \langle a^3 \rangle \). Let us find the element \( a \) of this group. Take the element \([2]\). All of the powers of \([2]\) are

\[
\begin{align*}
[2]^1 &= [2], \\
[2]^2 &= [4], \\
[2]^3 &= [3], \\
\end{align*}
\]

Therefore, \( \mathbb{Z}_5 - \{0\} = \langle [2] \rangle = \langle [3] \rangle \).

c) Since \( \mathbb{Z}_{11} - \{0\} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} \), the order of this group is 10. By Theorem 3.24, the generators of this group is in the form \( a^m \) iff \((m,10) = 1\). So the values of \( m \) are 1, 3, 7 and 9. Therefore, \( \mathbb{Z}_{11} - \{0\} = \langle a^1 \rangle = \langle a^3 \rangle = \langle a^7 \rangle = \langle a^9 \rangle \). Let us find the element \( a \) of this group. Take the element \([2]\). All of the powers of \([2]\) are

\[
\begin{align*}
[2]^1 &= [2], \\
[2]^2 &= [4], \\
[2]^3 &= [8], \\
[2]^4 &= [5], \\
[2]^5 &= [10], \\
[2]^6 &= [9], \\
[2]^7 &= [7], \\
[2]^8 &= [3], \\
[2]^9 &= [6], \\
\end{align*}
\]

Therefore, \( \mathbb{Z}_{11} - \{0\} = \langle [2] \rangle = \langle [3] \rangle = \langle [7] \rangle = \langle [6] \rangle \).

d) Since \( \mathbb{Z}_{13} - \{0\} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\} \), the order of this group is 12. By Theorem 3.24, the generators of this group is in the form \( a^m \) iff \((m,12) = 1\). So the values of \( m \) are 1, 5, 7 and 11. Therefore, \( \mathbb{Z}_{13} - \{0\} = \langle a^1 \rangle = \langle a^5 \rangle = \langle a^7 \rangle = \langle a^{11} \rangle \). Let us find the element \( a \) of this group. Take the element \([7]\). All of the powers of \([7]\) are
Therefore, $\mathbb{Z}_{13} - \{0\} = \langle [7]^1 \rangle = \langle [7]^5 \rangle = \langle [7]^7 \rangle = \langle [7]^9 \rangle = \langle [7]^{11} \rangle = \langle [7]^{13} \rangle = \langle [7]^{15} \rangle$.

e) Since $\mathbb{Z}_{17} - \{0\} = \{[1],[2],[3],[4],[5],[6],[7],[8],[9],[10],[11],[12],[13],[14],[15],[16]\}$, the order of this group is 16. By Theorem 3.24, the generators of this group is in the form $a^m$ iff $(m,16)=1$. So the values of $m$ are 1, 3, 5, 7, 9, 11, 13, and 15. Therefore, $\mathbb{Z}_{17} - \{0\} = \langle a^1 \rangle = \langle a^3 \rangle = \langle a^5 \rangle = \langle a^7 \rangle = \langle a^9 \rangle = \langle a^{11} \rangle = \langle a^{13} \rangle = \langle a^{15} \rangle$. Let us find the element $a$ of this group. Take the element [3]. All of the powers of [3] are
Therefore,

\[ \mathbb{Z}_{19} - \{0\} = \{[1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18] \} , \]

the order of this group is 18. By Theorem 3.24, the generators of this group is in the form \( a^m \) if \( (m, 18) = 1 \). So the values of \( m \) are 1, 5, 7, 11, 13, and 17. Therefore, \( \mathbb{Z}_{19} - \{0\} = \langle a^1 \rangle = \langle a^5 \rangle = \langle a^7 \rangle = \langle a^{11} \rangle = \langle a^{13} \rangle = \langle a^{17} \rangle \). Let us find the element \( a \) of this group. Take the element \([3]\). All of the powers of \([3]\) are

\[
\begin{align*}
[3]^1 &= [3], \\
[3]^2 &= [9], \\
[3]^3 &= [10], \\
[3]^4 &= [13], \\
[3]^5 &= [5], \\
[3]^6 &= [15], \\
[3]^7 &= [11], \\
[3]^8 &= [16], \\
[3]^9 &= [14], \\
[3]^{10} &= [8], \\
[3]^{11} &= [7], \\
[3]^{12} &= [4], \\
[3]^{13} &= [12], \\
[3]^{14} &= [2], \\
[3]^{15} &= [6], \\
\end{align*}
\]
Therefore,


13. a) By Corollary 3.23 and Exercise 11, $\mathbb{Z}_7 - \{0\}$ is a finite cyclic group of order 6 with $[3] \in \mathbb{Z}_7 - \{0\}$ as a generator. The distinct subgroups of $\mathbb{Z}_7 - \{0\}$ are those subgroups $\langle [3]^d \rangle$ where $d$ is a positive divisor of 6. Therefore, the distinct subgroups are as follows:

$$\langle [3]^1 \rangle = \mathbb{Z}_7 - \{0\},$$
$$\langle [3]^2 \rangle = \{[2],[4],[1]\},$$
$$\langle [3]^3 \rangle = \{[6],[1]\},$$
$$\langle [3]^6 \rangle = \{[1]\}.$$
b) By Corollary 3.23 and Exercise 11, \( \mathbb{Z}_5 - \{[0]\} \) is a finite cyclic group of order 4 with \([2] \in \mathbb{Z}_5 - \{[0]\}\) as a generator. The distinct subgroups of \( \mathbb{Z}_5 - \{[0]\} \) are those subgroups \( \langle [2]^d \rangle \) where \( d \) is a positive divisor of 4. Therefore, the distinct subgroups are as follows:

\[
\langle [2]^1 \rangle = \mathbb{Z}_5 - \{[0]\}, \\
\langle [2]^2 \rangle = \{[4],[1]\}, \\
\langle [2]^4 \rangle = \{[1]\}.
\]

c) By Corollary 3.23 and Exercise 11, \( \mathbb{Z}_{11} - \{[0]\} \) is a finite cyclic group of order 10 with \([2] \in \mathbb{Z}_{11} - \{[0]\}\) as a generator. The distinct subgroups of \( \mathbb{Z}_{11} - \{[0]\} \) are those subgroups \( \langle [2]^d \rangle \) where \( d \) is a positive divisor of 10. Therefore, the distinct subgroups are as follows:

\[
\langle [2]^1 \rangle = \mathbb{Z}_{11} - \{[0]\}, \\
\langle [2]^5 \rangle = \{[4],[5],[9],[3],[1]\}, \\
\langle [2]^10 \rangle = \{[1]\}.
\]

d) By Corollary 3.23 and Exercise 11, \( \mathbb{Z}_{13} - \{[0]\} \) is a finite cyclic group of order 12 with \([7] \in \mathbb{Z}_{13} - \{[0]\}\) as a generator. The distinct subgroups of \( \mathbb{Z}_{13} - \{[0]\} \) are those subgroups \( \langle [7]^d \rangle \) where \( d \) is a positive divisor of 12. Therefore, the distinct subgroups are as follows:

\[
\langle [7]^1 \rangle = \mathbb{Z}_{13} - \{[0]\}, \\
\langle [7]^2 \rangle = \{[10],[9],[12],[3],[4],[1]\}, \\
\langle [7]^3 \rangle = \{[5],[12],[8],[1]\}, \\
\langle [7]^4 \rangle = \{[9],[3],[1]\}, \\
\langle [7]^6 \rangle = \{[12],[1]\}, \\
\langle [7]^12 \rangle = \{[1]\}.
\]
14. Prove that the set $\mathbb{Z}_{17} - \{0\}$ is a finite cyclic group of order 16 with $[3] \in \mathbb{Z}_{17} - \{0\}$ as a generator. The distinct subgroups of $\mathbb{Z}_{17} - \{0\}$ are those subgroups $\langle[3]^d\rangle$ where $d$ is a positive divisor of 16. Therefore, the distinct subgroups are as follows:

$$\langle[3]^1\rangle = \mathbb{Z}_{17} - \{0\},$$
$$\langle[3]^2\rangle = \{[9],[13],[15],[16],[8],[4],[2],[1]\},$$
$$\langle[3]^4\rangle = \{[13],[16],[4],[1]\},$$
$$\langle[3]^8\rangle = \{[16],[1]\},$$
$$\langle[3]^{16}\rangle = \{[1]\}.$$ 

f) By Corollary 3.23 and Exercise 11, $\mathbb{Z}_{19} - \{0\}$ is a finite cyclic group of order 18 with $[2] \in \mathbb{Z}_{19} - \{0\}$ as a generator. The distinct subgroups of $\mathbb{Z}_{19} - \{0\}$ are those subgroups $\langle[2]^d\rangle$ where $d$ is a positive divisor of 18. Therefore, the distinct subgroups are as follows:

$$\langle[2]^1\rangle = \mathbb{Z}_{19} - \{0\},$$
$$\langle[2]^2\rangle = \{[4],[16],[7],[9],[17],[11],[6],[5],[1]\},$$
$$\langle[2]^3\rangle = \{[8],[7],[18],[11],[12],[1]\},$$
$$\langle[2]^6\rangle = \{[7],[11],[1]\},$$
$$\langle[2]^9\rangle = \{[18],[1]\},$$
$$\langle[2]^{18}\rangle = \{[1]\}.$$ 

14. \textit{Proof.} First let’s prove that $H$ is a subgroup of the invertible 2 by 2 real matrices.

Claim: $\left[\begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array}\right]^n = \left[\begin{array}{cc} 1 & n \\ 0 & 1 \end{array}\right]$ for all positive integers $n$.

Clearly the statement holds when $n = 1$. Assume $\left[\begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array}\right]^k = \left[\begin{array}{cc} 1 & k \\ 0 & 1 \end{array}\right]$. Then we have the following.

$$\left[\begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array}\right]^{k+1} = \left[\begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array}\right]^k \left[\begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array}\right]$$
$$= \left[\begin{array}{cc} 1 & k \\ 0 & 1 \end{array}\right] \left[\begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array}\right]$$
$$= \left[\begin{array}{cc} 1 & k+1 \\ 0 & 1 \end{array}\right]$$
Thus by induction \( \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \) for all positive integers \( n \).

By definition \( \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \).

Suppose \( n > 0 \), then we have the following.

\[
\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{-n} = \left( \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n \right)^{-1} = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & -n \\ 0 & 1 \end{bmatrix}
\]

Thus for all integers \( n \), \( \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \).

Now we will prove \( H \) is cyclic. Let \( \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^k \in \langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \rangle \), then \( \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^k = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix} \in H \).

Thus \( \langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \rangle \subseteq H \).

Now we will show \( H \subseteq \langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \rangle \). Let \( A \in H \). Then \( A = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \) for some \( n \in \mathbb{Z} \). By above claim, \( \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n \in \langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \rangle \).

Thus \( H = \langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \rangle \).

15. a) i) Let us prove that

\[
\begin{bmatrix} \cos n\theta & -\sin n\theta \\ \sin n\theta & \cos n\theta \end{bmatrix} = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}^n.
\]

Clearly the statement holds when \( n = 1 \). Assume

\[
\begin{bmatrix} \cos k\theta & -\sin k\theta \\ \sin k\theta & \cos k\theta \end{bmatrix} = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}^k.
\]

Then we have the following.
Exercises 3.4

Cyclic Groups

\[
\begin{bmatrix}
\cos \theta & -\sin \theta \\
\sin \theta & \cos \theta
\end{bmatrix}
\]
\[
\begin{bmatrix}
\cos \theta & -\sin \theta \\
\sin \theta & \cos \theta
\end{bmatrix}
\]
\[
\begin{bmatrix}
\cos k\theta & -\sin k\theta \\
\sin k\theta & \cos k\theta
\end{bmatrix}
\]
\[
\begin{bmatrix}
\cos(k+1)\theta & -\sin(k+1)\theta \\
\sin(k+1)\theta & \cos(k+1)\theta
\end{bmatrix}
\]

Thus by induction
\[
\begin{bmatrix}
\cos n\theta & -\sin n\theta \\
\sin n\theta & \cos n\theta
\end{bmatrix} = \begin{bmatrix}
\cos \theta & -\sin \theta \\
\sin \theta & \cos \theta
\end{bmatrix}^n
\]

for all integers \( n \).

ii) First let us prove that \( H \) is a subgroup of the invertible 2 by 2 real matrices. \( H \) is nonempty since

\[
\begin{bmatrix}
\cos \theta & -\sin \theta \\
\sin \theta & \cos \theta
\end{bmatrix} = \begin{bmatrix} 1 & 0 \\
0 & 1 \end{bmatrix} \in H \text{ for } n = 0.
\]

Take two arbitrary element of \( H \) such that

\[
A = \begin{bmatrix}
\cos n_1\theta & -\sin n_1\theta \\
\sin n_1\theta & \cos n_1\theta
\end{bmatrix}, B = \begin{bmatrix}
\cos n_2\theta & -\sin n_2\theta \\
\sin n_2\theta & \cos n_2\theta
\end{bmatrix} \in H \text{ for all integers } n_1 \text{ and } n_2.
\]

We will show that \( AB \in H \). For this,

\[
AB = \begin{bmatrix}
\cos n_1\theta & -\sin n_1\theta \\
\sin n_1\theta & \cos n_1\theta
\end{bmatrix} \begin{bmatrix}
\cos n_2\theta & -\sin n_2\theta \\
\sin n_2\theta & \cos n_2\theta
\end{bmatrix} = \begin{bmatrix}
\cos \theta & -\sin \theta \\
\sin \theta & \cos \theta
\end{bmatrix}^{n_1} \begin{bmatrix}
\cos \theta & -\sin \theta \\
\sin \theta & \cos \theta
\end{bmatrix}^{n_2} \begin{bmatrix}
\cos(n_1+n_2)\theta & -\sin(n_1+n_2)\theta \\
\sin(n_1+n_2)\theta & \cos(n_1+n_2)\theta
\end{bmatrix} \in H.
\]

So \( H \) is closed under the matrix multiplication. Now we will show that \( A^{-1} \in H \). For this,

\[
A = \begin{bmatrix}
\cos n_1\theta & -\sin n_1\theta \\
\sin n_1\theta & \cos n_1\theta
\end{bmatrix} \Rightarrow A^{-1} = \frac{1}{\det A} \begin{bmatrix}
\cos n_1\theta & -\sin n_1\theta \\
\sin n_1\theta & \cos n_1\theta
\end{bmatrix} = \begin{bmatrix}
\cos n_1\theta & -\sin n_1\theta \\
\sin n_1\theta & \cos n_1\theta
\end{bmatrix} \in H.
\]

Therefore \( H \) is a subgroup of the set of all invertible 2 by 2 real matrices. Now we will prove \( H \) is cyclic. By using the trigonometric identity
In the last equality, Theorem 2.25 guarantees the existence of a solution $s$. Therefore, we have $H = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}$, as required.

b) $H = \begin{bmatrix} \cos 90n & -\sin 90n \\ \sin 90n & \cos 90n \end{bmatrix} \cdot n \in \mathbb{Z} = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right\}$.

c) $H = \begin{bmatrix} \cos 120n & -\sin 120n \\ \sin 120n & \cos 120n \end{bmatrix} \cdot n \in \mathbb{Z} = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ -\frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix} \right\}$.

16. To show that multiplication mod $n$ is a binary operation on $U_n$, I must show that the product of units is a unit. Suppose $a, b \in U_n$. Then $a$ has a multiplicative inverse $a^{-1}$ and $b$ has a multiplicative inverse $b^{-1}$. Now

\[ (b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}e = b^{-1}b = e, \]
\[ (ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a(e)a^{-1} = aa^{-1}e. \]

Hence, $b^{-1}a^{-1}$ is the multiplicative inverse of $ab$, and $ab$ is a unit. Therefore, multiplication mod $n$ is a binary operation on $U_n$.

I will take it for granted that multiplication mod $n$ is associative.

The identity element for multiplication mod $n$ is 1, and 1 is a unit in $\mathbb{Z}_n$.

Finally, every element of $U_n$ has a multiplicative inverse, by definition.

Therefore, $U_n$ is a group under multiplication mod $n$.

17. $\iff$: Let $[a] \in \mathbb{Z}_n$. Assume that $a$ and $n$ are relatively prime. Then $(a,n) = 1$. By Theorem 2.12, $1 = ax + ny$ for some integer $x, y$. Using this fact, we have the following.

\[ 1 = ax + ny \rightarrow 1 \equiv ax \pmod{n} \rightarrow [1] = [ax] \text{ in } \mathbb{Z}_n \rightarrow [1] = [a][x] \text{ in } \mathbb{Z}_n. \]

In the last equality, Theorem 2.25 guarantees the existence of a solution $s$ to the congruence $as \equiv 1 \pmod{n}$. This shows that $[a]$ in $\mathbb{Z}_n$ has the multiplicative inverses. By the definition of $U_n$, $[a] \in U_n$. 

14
\[ \Rightarrow \text{Let } [a] \in U_n. \text{ Suppose first that } [a] \text{ has a multiplicative inverse } [b] \text{ in } \mathbb{Z}_n. \text{ Then} \]
\[ [a][b] = [1]. \]

This means that
\[ [ab] = [1] \text{ and } ab \equiv 1 \pmod{n}. \]

Therefore,
\[ ab - 1 = nq \]

for some integer \( q \), and
\[ a(b) + n(-q) = 1. \]

18. a. \( U_{20} = \{ [1], [3], [7], [9], [11], [13], [17], [19] \} \)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>[17]</td>
<td>[17]</td>
<td>[11]</td>
<td>[19]</td>
<td>[13]</td>
<td>[7]</td>
<td>[1]</td>
<td>[9]</td>
<td>[3]</td>
</tr>
</tbody>
</table>

b. \( U_8 = \{ [a] \in \mathbb{Z}_8 : ([a],[n]) = 1 \} = \{ [1],[3],[5],[7] \} \). The Cayley table for \( U_8 \) is as follows:

<table>
<thead>
<tr>
<th>.</th>
<th>[1]</th>
<th>[3]</th>
<th>[5]</th>
<th>[7]</th>
</tr>
</thead>
<tbody>
<tr>
<td>[1]</td>
<td>[1]</td>
<td>[3]</td>
<td>[5]</td>
<td>[7]</td>
</tr>
<tr>
<td>[3]</td>
<td>[3]</td>
<td>[1]</td>
<td>[7]</td>
<td>[5]</td>
</tr>
<tr>
<td>[5]</td>
<td>[5]</td>
<td>[7]</td>
<td>[1]</td>
<td>[3]</td>
</tr>
<tr>
<td>[7]</td>
<td>[7]</td>
<td>[5]</td>
<td>[3]</td>
<td>[1]</td>
</tr>
</tbody>
</table>

c. \( U_{24} = \{ [a] \in \mathbb{Z}_{24} : ([a],[n]) = 1 \} = \{ [1],[5],[7],[11],[13],[17],[19],[23] \} \).
## Exercises 3.4

### Cyclic Groups

<table>
<thead>
<tr>
<th></th>
<th>[1]</th>
<th>[5]</th>
<th>[7]</th>
<th>[11]</th>
<th>[13]</th>
<th>[17]</th>
<th>[19]</th>
<th>[23]</th>
</tr>
</thead>
<tbody>
<tr>
<td>[1]</td>
<td>[1]</td>
<td>[5]</td>
<td>[7]</td>
<td>[11]</td>
<td>[13]</td>
<td>[17]</td>
<td>[19]</td>
<td>[23]</td>
</tr>
<tr>
<td>[17]</td>
<td>[17]</td>
<td>[13]</td>
<td>[23]</td>
<td>[19]</td>
<td>[5]</td>
<td>[1]</td>
<td>[11]</td>
<td>[7]</td>
</tr>
<tr>
<td>[19]</td>
<td>[19]</td>
<td>[23]</td>
<td>[13]</td>
<td>[17]</td>
<td>[7]</td>
<td>[11]</td>
<td>[1]</td>
<td>[5]</td>
</tr>
<tr>
<td>[23]</td>
<td>[23]</td>
<td>[19]</td>
<td>[17]</td>
<td>[13]</td>
<td>[11]</td>
<td>[7]</td>
<td>[5]</td>
<td>[1]</td>
</tr>
</tbody>
</table>

**d.** \( U_{30} = \{ [a] \in \mathbb{Z}_{30} : ([a],[n]) = 1 \} = \{ [1],[7],[11],[13],[17],[19],[23],[29] \} \).  

<table>
<thead>
<tr>
<th></th>
<th>[1]</th>
<th>[7]</th>
<th>[11]</th>
<th>[13]</th>
<th>[17]</th>
<th>[19]</th>
<th>[23]</th>
<th>[29]</th>
</tr>
</thead>
<tbody>
<tr>
<td>[1]</td>
<td>[1]</td>
<td>[7]</td>
<td>[11]</td>
<td>[13]</td>
<td>[17]</td>
<td>[19]</td>
<td>[23]</td>
<td>[29]</td>
</tr>
<tr>
<td>[7]</td>
<td>[7]</td>
<td>[19]</td>
<td>[17]</td>
<td>[1]</td>
<td>[29]</td>
<td>[13]</td>
<td>[11]</td>
<td>[23]</td>
</tr>
<tr>
<td>[11]</td>
<td>[11]</td>
<td>[17]</td>
<td>[1]</td>
<td>[23]</td>
<td>[7]</td>
<td>[29]</td>
<td>[13]</td>
<td>[19]</td>
</tr>
<tr>
<td>[13]</td>
<td>[13]</td>
<td>[1]</td>
<td>[23]</td>
<td>[19]</td>
<td>[11]</td>
<td>[7]</td>
<td>[29]</td>
<td>[17]</td>
</tr>
<tr>
<td>[17]</td>
<td>[17]</td>
<td>[29]</td>
<td>[7]</td>
<td>[11]</td>
<td>[19]</td>
<td>[23]</td>
<td>[1]</td>
<td>[13]</td>
</tr>
<tr>
<td>[19]</td>
<td>[19]</td>
<td>[13]</td>
<td>[29]</td>
<td>[7]</td>
<td>[23]</td>
<td>[1]</td>
<td>[17]</td>
<td>[11]</td>
</tr>
<tr>
<td>[23]</td>
<td>[23]</td>
<td>[11]</td>
<td>[13]</td>
<td>[29]</td>
<td>[1]</td>
<td>[17]</td>
<td>[19]</td>
<td>[7]</td>
</tr>
<tr>
<td>[29]</td>
<td>[29]</td>
<td>[23]</td>
<td>[19]</td>
<td>[17]</td>
<td>[13]</td>
<td>[11]</td>
<td>[7]</td>
<td>[1]</td>
</tr>
</tbody>
</table>

### 19. a) **If** \( U_{20} \) **is cyclic, then there exists at least one element** \( [a] \in U_{20} \) **whose order must be 8. But**
\[
[1]^4 = [1];
[3]^4 = [1];
[7]^4 = [1];
[9]^2 = [1];
[11]^2 = [1];
[13]^4 = [1];
[17]^4 = [1];
[19]^2 = [1].
\]

### b) **If** \( U_8 \) **is cyclic, then there exists at least one element** \( [a] \in U_8 \) **whose order must be 4. But**
\[
[1]^2 = [1];
[3]^2 = [1];
[5]^2 = [1];
\]
c) If \( U_{24} \) is cyclic, then there exists at least one element \([a]\in U_{20}\) whose order must be 8. But
\[
\]
d) If \( U_{30} \) is cyclic, then there exists at least one element \([a]\in U_{20}\) whose order must be 8. But
\[
\]
\[
\langle [5]^1 \rangle = U_9,
\langle [5]^2 \rangle = \{ [7], [4], [1] \},
\langle [5]^3 \rangle = \{ [8], [1] \},
\langle [5]^4 \rangle = \{ [1] \},
\langle [5]^5 \rangle = \langle [5]^1 \rangle = \{ [7], [4], [1] \},
\]
21. a) \( \phi(8) = 4; a, a^3, a^5, a^7 \)
b) \( \phi(14) = \phi(2)\phi(7) = 1.6 = 6; a, a^3, a^5, a^9, a^{11}, a^{13} \)
c) \( \phi(18) = \phi(2)\phi(3^2) = 1.6 = 6; a, a^5, a^7, a^{11}, a^{13}, a^{17} \)
d) \( \phi(24) = \phi(3)\phi(8) = 2.4 = 8; a, a^5, a^7, a^{11}, a^{13}, a^{17}, a^{19}, a^{23} \)
e) \( \phi(7) = 6; a, a^2, a^3, a^4, a^5, a^6 \)
f) \( \phi(13) = 12; a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9, a^{10}, a^{11}, a^{12} \).

22. a) Let \( G = \langle a \rangle \) be a cyclic group of order 8. The divisors of 8 are 1, 2, 4, and 8, so the distinct subgroups of \( G \) are
\[
\langle a \rangle = G,
\langle a^2 \rangle = \{ a^2, a^4, a^6, a^8 = e \},
\langle a^3 \rangle = \{ a^3, a^5 = e \},
\langle a^4 \rangle = \{ e \}.
\]
b) Let $G = \langle a \rangle$ be a cyclic group of order 14. The divisors of 14 are 1, 2, 7, and 14, so the distinct subgroups of $G$ are

$$\langle a \rangle = G,$$
$$\langle a^2 \rangle = \left\{ a^2, a^4, a^6, a^8, a^{10}, a^{12}, a^{14}, a^{16} = e \right\},$$
$$\langle a^7 \rangle = \left\{ a^7, a^{14} = e \right\},$$
$$\langle a^{14} = e \rangle = \left\{ e \right\}.$$

c) Let $G = \langle a \rangle$ be a cyclic group of order 18. The divisors of 18 are 1, 2, 3, 6, 9, and 18, so the distinct subgroups of $G$ are

$$\langle a \rangle = G,$$
$$\langle a^2 \rangle = \left\{ a^2, a^4, a^6, a^8, a^{10}, a^{12}, a^{14}, a^{16}, a^{18} = e \right\},$$
$$\langle a^3 \rangle = \left\{ a^3, a^6, a^9, a^{12}, a^{15}, a^{18} = e \right\},$$
$$\langle a^6 \rangle = \left\{ a^6, a^{12}, a^{18} = e \right\},$$
$$\langle a^9 \rangle = \left\{ a^9, a^{18} = e \right\},$$
$$\langle a^{18} = e \rangle = \left\{ e \right\}.$$

d) Let $G = \langle a \rangle$ be a cyclic group of order 24. The divisors of 24 are 1, 2, 3, 4, 6, 8, 12, and 24, so the distinct subgroups of $G$ are

$$\langle a \rangle = G,$$
$$\langle a^2 \rangle = \left\{ a^2, a^4, a^6, a^8, a^{10}, a^{12}, a^{14}, a^{16}, a^{18}, a^{20}, a^{22}, a^{24} = e \right\},$$
$$\langle a^3 \rangle = \left\{ a^3, a^6, a^9, a^{12}, a^{15}, a^{18}, a^{21}, a^{24} = e \right\},$$
$$\langle a^4 \rangle = \left\{ a^4, a^8, a^{12}, a^{16}, a^{20}, a^{24} = e \right\},$$
$$\langle a^6 \rangle = \left\{ a^6, a^{12}, a^{18}, a^{24} = e \right\},$$
$$\langle a^8 \rangle = \left\{ a^8, a^{16}, a^{24} = e \right\},$$
$$\langle a^{12} \rangle = \left\{ a^{12}, a^{24} = e \right\},$$
$$\langle a^{24} = e \rangle = \left\{ e \right\}.$$

e) Let $G = \langle a \rangle$ be a cyclic group of order 7. The divisors of 7 are 1 and 7 so the distinct subgroups of $G$ are

$$\langle a \rangle = G,$$
$$\langle a^7 \rangle = \left\{ a^7 = e \right\}.$$

Exercises 3.4 Cyclic Groups
f) Let $G = \langle a \rangle$ be a cyclic group of order 13. The divisors of 13 are 1 and 13 so the distinct subgroups of $G$ are

$$\langle a \rangle = G,$$

$$\langle a^{13} \rangle = \{ a^{13} = e \}.$$

23. Since $o(a) = 24$, $a^{24} = e$.

a) 2 is the least positive integer such that $(a^{12})^2 = a^{24} = e$, so $o(a^{12}) = 2$.

b) $a^8, a^{16}$

c) $a^6, a^{18}$

d) none

24. Since $o(a) = 35$, $a^{35} = e$.

a) none

b) $a^7, a^{14}, a^{21}, a^{28}$

c) $a^5, a^{10}, a^{15}, a^{20}, a^{25}, a^{30}$

d) none

25. If $H \subset \mathbb{Z}$ is a subgroup, then either $H = \{ 0 \}$ is trivial or there exists a unique integer $n \geq 1$ such that $H = n\mathbb{Z} = \{ nk : k \in \mathbb{Z} \}$.

26. All generators of an infinite cyclic group are $a$ and $a^{-1}$, so $G = \langle a \rangle = \langle a^{-1} \rangle$. For example, the additive group $\mathbb{Z}$ is cyclic and $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.

27. First note that $a = b^n$ for some $n \in \mathbb{Z}$ since $a \in \langle b \rangle$. Now let $x \in \langle a \rangle$. This means that $x = a^m$ for some $m \in \mathbb{Z}$. Thus $x = a^m = (b^n)^m = b^{nm} \in \langle b \rangle$. Since this is true for all $x \in \langle a \rangle$ we have $\langle a \rangle \subseteq \langle b \rangle$.

28. a)

$$\left( a^k \right)^{-1} = a^{-k} = \left( a^{-1} \right)^k$$

$a^k = e$

$$\Rightarrow \left( a^{-1} \right)^k = e^{-1} = e$$

$$\Rightarrow o(a^{-1}) \leq o(a) \quad (1)$$

Similarly,
Let $b$. Then
\[ (a^{-1})^k = e \]
\[ \Rightarrow \left( (a^{-1})^k \right)^k = e \]
\[ \Rightarrow a^k = e^{-1} = e \]
\[ \Rightarrow o(a) \leq o(a^{-1}) \] (2)

By (1) and (2), $o(a) = o(a^{-1})$.

b)

Proof of b. Let $e$ be the identity element of $G$. First observe that for any $x, y \in G$ and for any integer $m$ with $m \geq 1$, $(xy^{-1})^m = xy^m x^{-1}$. To prove this proceed by induction on $n$. For $n = 1$ we clearly have $(xyx^{-1})^1 = xy^1 x^{-1}$. So assume that $(xyx^{-1})^k = xy^k x^{-1}$ for some integer $k \geq 1$. Then
\[ (xyx^{-1})^{k+1} = (xyx^{-1})^k (xyx^{-1}) \]
\[ = (xyx^{-1})^{k+1} (xyx^{-1}) \]
\[ = xy^k e y x^{-1} \]
\[ = xy^k y x^{-1} \]
\[ = xy^{k+1} x^{-1}. \]
This completes the induction.

Now let $n = o(a)$. This means that $a^n = e$ and $n$ is the least such positive integer. Then we have $(bab^{-1})^n = ba^n b^{-1} = beb^{-1} = bb^{-1} = e$. Thus $o(bab^{-1}) = n$.

Next assume that $(bab^{-1})^m = e$ for some integer $m$ with $0 < m < n$. Then $e = (bab^{-1})^m = ba^m b^{-1}$. Now
\[ \Rightarrow ba^m b^{-1} = e \]
\[ \Rightarrow a^m b^{-1} = b^{-1} \text{ multiplying by } b^{-1} \text{ on the left} \]
\[ \Rightarrow a^m = e \text{ multiplying by } b \text{ on the right} \]
However, this contradicts that $n$ is the least integer such that $a^n = e$. Therefore $o(bab^{-1}) = n = o(a)$. □

c)

Proof of c. First observe that for any $x, y \in G$, $(xy)^m = x(xy)^{m-1} y$ for all integers $m \geq 1$. To prove this proceed by induction on $n$. For $m = 1$ we have $(xy)^1 = xy = xey = x(xy)^0 y$. So assume that $(xy)^k = x(xy)^{k-1} y$ for some integer $k \geq 1$. Then
\[ (xy)^{k+1} = (xy)^k (xy) \]
\[ = x(xy)^{k-1} y (xy) \]
\[ = x(xy)^{k-1} (xy) y \]
\[ = x(yx)^k y \]
This completes the induction.

Now let $n = o(ab)$. This means that $(ab)^n = e$ and $n$ is the least such positive integer. So
\[ (ab)^n = e \]
\[ \Rightarrow (ba)^{n-1} b = e \text{ by the above observation} \]
\[ \Rightarrow (ba)^{n-1} b = a^{-1} \text{ multiplying by } a^{-1} \text{ on the left} \]
\[ \Rightarrow (ba)^{n-1} ba = e \text{ multiplying by } a \text{ on the right} \]
\[ \Rightarrow (ba)^n = e. \]

Thus $o(ba) \leq n$.

Next assume that $(ba)^m = e$ for some integer $m$ with $0 < m < n$. Then
\[ (ba)^m = e \]
\[ \Rightarrow (ab)^{m-1} a = e \text{ by the above observation} \]
\[ \Rightarrow (ab)^{m-1} a = b^{-1} \text{ multiplying by } b^{-1} \text{ on the left} \]
\[ \Rightarrow (ab)^{m-1} ab = e \text{ multiplying by } b \text{ on the right} \]
\[ \Rightarrow (ab)^m = e. \]

However, this contradicts that $n$ is the least integer such that $(ab)^n = e$. Therefore $o(ba) = n = o(ab)$. □