1. For \( n = 16, 17, 18, 19 \) or 20, express \( \mathbb{Z}_n^\times \) as a product of cyclic groups.
(A product can have one or more factors.)

**Solution.** For \( n = 16 \), \( G = \mathbb{Z}_n^\times = \{[1], [3], [5], [7], [9], [11], [13], [15]\}. The order of any element other than [1] can only be 2, 4 or 8. Since \([3]^2 = [9] \neq [1]\) and \([3]^4 = [81] = [1]\), the order of [3] is 4. It follows that the order of \([9] = [3]^2\) is 2, and the order of \([11] = [3]^3\) is 4. Furthermore, the order of \([5] = [-11]\) is 4, the order of \([7] = [-9]\) is 2, the order of \([13] = [-3]\) is 4 and the order of \([15] = [-1]\) is 2. In particular, we see that \( G \) is not cyclic. Let \( H = \langle [3]\rangle = \{[1], [3], [9], [11]\} \). If we set \( K = \langle [15]\rangle = \langle [-1]\rangle \), then it is clear that \( H \cap K = \{[1]\} \) and \( HK = G \). So \( G \cong H \times K \cong \mathbb{Z}_4 \times \mathbb{Z}_2 \) by Proposition 2.127. (There are other good choices for \( H \) and \( K \), but this one is perhaps the most obvious.)

For \( n = 17 \), \( G = \mathbb{Z}_n^\times = \{[1], [2], [3], \ldots, [16]\}. The order of any element other than [1] can only be 2, 4, 8 or 16. Since \([2]^2 = [4] \neq [1], [2]^4 = [16] \neq [1]\) and \([2]^8 = [16^2] = [-1]^2 = [1]\), the order of [2] is 8. It follows that the powers of [2], i.e., \([4], [8], [16], [15], [13], [9]\), have orders 4, 8, 2, 8, 4, 8 respectively. The negatives of these do not give us any new information, and we proceed with finding the order of [3]. Since \([3]^2 = [9] \neq [1], [3]^4 = [9^2] = [13] = [-4] \neq [1]\) and \([3]^8 = [-4^2] = [16] \neq [1]\), the order of [3] is 16, and hence \( G = \langle [3]\rangle \cong \mathbb{Z}_{16} \). (It was also possible to conclude this from Theorem 3.55, but I did not expect you to use that since we have not covered it yet.)

For \( n = 18 \), the elements of \( G = \mathbb{Z}_n^\times \) are \([1], [5], [7], [11], [13]\) and [17]. The order of any element other than [1] can only be 2, 3 or 6. Since \([5]^2 = [25] = [7] \neq [1]\) and \([5]^3 = [35] = [-1] \neq [1]\), the order of [5] is 6, and \( G \cong \mathbb{Z}_6 \).

For \( n = 19 \), \( G = \mathbb{Z}_n^\times = \{[1], [2], [3], \ldots, [18]\}. The order of any element other than [1] can only be 2, 3, 6, 9 or 18. Since \([2]^2 = [4] \neq [1], [2]^3 = [8] \neq [1]\), \([2]^6 = [64] = [7] \neq [1]\) and \([2]^9 = [56] = [-1] \neq [1]\), the order of [2] is 18.
and $G = <[2]> \cong \mathbb{Z}_{18}$. (It was also possible to conclude this from Theorem 3.55, but I did not expect you to use that since we have not covered it yet.)

For $n = 20$, $G = \mathbb{Z}_{n}^{x} = \{[1], [3], [7], [9], [11], [13], [17], [19]\}$. The order of any element other than $[1]$ can only be 2, 4 or 8. Since $[3]^{2} = [9] \neq [1]$ and $[3]^{4} = [9]^{2} = [1]$, the order of $[3]$ is 4. It follows that the order of $[9] = [3]^{2}$ is 2, and the order of $[7] = [3]^{3}$ is 4. Furthermore, the order of $[11] = [\bar{9}]$ is 2, the order of $[13] = [\bar{7}]$ is 4, the order of $[17] = [\bar{3}]$ is 4 and the order of $[19] = [\bar{1}]$ is 2. In particular, we see that $G$ is not cyclic. Let $H = <[3]> = \{[1], [3], [9], [7]\}$. Since $[3]^{2} = [9] \neq [1]$ and $[3]^{4} = [9]^{2} = [1]$, the order of $[3]$ is 4. It follows that the order of $[9] = [3]^{2}$ is 2, and the order of $[7] = [3]^{3}$ is 4. Furthermore, the order of $[11] = [\bar{9}]$ is 2, the order of $[13] = [\bar{7}]$ is 4, the order of $[17] = [\bar{3}]$ is 4 and the order of $[19] = [\bar{1}]$ is 2. In particular, we see that $G$ is not cyclic. Let $H = <[3]> = \{[1], [3], [9], [7]\}$. If we set $K = <[19]> = <[\bar{1}]>$, then it is clear that $H \cap K = \{[1]\}$ and $HK = G$. So $G \cong H \times K \cong \mathbb{Z}_{4} \times \mathbb{Z}_{2}$ by Proposition 2.127. (There are other good choices for $H$ and $K$, but this one is perhaps the most obvious.)

2. Let $G$ be a group of order 10. Assume that $G$ is generated by two elements of order 2. Prove that $G \cong D_{10}$. Is $G$ abelian? What is the number of non-isomorphic abelian groups of order 10?

Solution. Let us first show that $G$ can not be abelian. Suppose that $G$ is generated by $x$ and $y$, each of order 2, and such that $xy = yx$. Then multiplying $x$, $y$ and their inverses, we can only get 1, $x$, $y$ or $xy$. (Indeed, taking products or inverses of these 4 elements always brings us back to the same 4 elements.) Hence $|G| = 4$, a contradiction.

To show that $G \cong D_{10}$, we first recall that $D_{10}$ is defined as the group generated by $a$ of order 5 and $b$ of order 2, such that $bab = a^{-1}$. This definition includes the fact that the given information is sufficient to write out all elements and their multiplication table, so that the described group is unique up to isomorphism.

We set $a = xy$ and $b = y$. The subgroup of $G$ generated by $a$ and $b$ contains $y$ and $x = ab$, so it is all of $G$. Moreover, $bab = yxyy = yx = y^{-1}x^{-1} = (xy)^{-1} = a^{-1}$. So we will be done if we show that the order of $a$ is 5.

The order of $a$ can only be 1, 2, 5 or 10. If the order were 10, $G$ would be cyclic, but that cannot be because we proved $G$ is not abelian. If $|a| = 1$, then $a = xy = 1$, so $x = y$, but then $G$ would consist only of 1 and $x$, a contradiction. If $|a| = 2$, then $a^{2} = xyxy = 1$, so $x(xyxy)y = x(1)y$, i.e., $yx = xy$. This implies $G$ is abelian, a contradiction. So the only possibility is $|a| = 5$ and this completes the proof that $G \cong D_{10}$.

If $H$ is an abelian group of order 10, then by Cauchy’s theorem it contains an element $c$ of order 5 and an element $d$ of order 2. Since $c$ and $d$ commute
is abelian), and \(gcd(5, 2) = 1\), \(cd\) has order 10 by Proposition 2.129. So \(H \cong \mathbb{Z}_{10}\), and there is only one abelian group of order 10 up to isomorphism.

3. If \(n\) is odd, find the number of conjugacy classes of \(n\)-cycles in \(A_n\). What happens if \(n\) is even?

**Solution.** Since an \(n\)-cycle is odd for even \(n\), there are no \(n\)-cycles in \(A_n\) for even \(n\), and the number of classes is 0. So assume \(n\) is odd; then all the \(n\)-cycles are in \(A_n\). We make use of Exercise 2.122; since \([S_n : A_n] = 2\), that exercise tells us how to relate \(A_n\)-conjugacy classes to \(S_n\)-conjugacy classes, which we understand well. In particular, we know that all \(n\)-cycles are conjugate in \(S_n\). The number of \(n\)-cycles is \(n! / n = (n-1)!\) (there are \(n!\) ways to write an \(n\)-cycle, but for each cycle the \(n\) cyclic permutations give the same cycle.) So if \(C_{S_n}(\sigma)\) denotes the centralizer of \(\sigma = (1, 2, 3, \ldots, n)\) in \(S_n\), we conclude

\[ [S_n : C_{S_n}(\sigma)] = |\sigma^{S_n}| = (n-1)! \]

and consequently \(|C_{S_n}(\sigma)| = \frac{n!}{(n-1)!} = n\). On the other hand, \(\sigma\) has \(n\) distinct powers that certainly commute with it, so we conclude that \(C_{S_n}(\sigma) = \{1, \sigma, \sigma^2, \ldots, \sigma^{n-1}\}\). But all powers of \(\sigma\) are in \(A_n\), so \(C_{A_n}(\sigma) = C_{S_n}(\sigma)\). In this situation, Exercise 2.122 tells us that

\[ |\sigma^{A_n}| = \frac{1}{2} |\sigma^{S_n}| = \frac{(n-1)!}{2}. \]

In particular, \(\sigma^{A_n}\) does not contain all \(n\)-cycles, but only half of them. Picking any \(n\)-cycle \(\tau\) not contained in \(\sigma^{A_n}\), we can repeat the above argument with \(\tau\) in place of \(\sigma\), and conclude that \(\tau^{A_n}\) contains the other half of \(n\)-cycles. Hence the number of conjugacy classes of \(n\)-cycles in \(A_n\) is 2.

4. For each natural number \(n\), determine the commutator subgroup \(A'_n\) of \(A_n\).

**Solution.** We use Exercise 2.113, which says that for any group \(G\), \(G'\) is a normal subgroup of \(G\). We also need the obvious fact that \(G' = \{1\}\) is equivalent to all the commutators being equal to 1, i.e., to \(G\) being abelian.

If \(n \geq 5\), we know that \(A_n\) is simple and non-abelian. It follows that \(A'_n = A_n\); namely, \(A'_n\) is normal, so it has to be \(\{1\}\) or \(A_n\), but cannot be \(\{1\}\) since \(A_n\) is not abelian.

Since \(A_1 = \{1\}\) and \(A_2 = \{1\}\), we see that \(A'_1 = \{1\}\) and \(A'_2 = \{1\}\). Moreover, \(|A_3| = 3! / 2 = 3\), so \(A_3 \cong \mathbb{Z}_3\) is abelian, and hence \(A_3 = \{1\}\).
It remains to settle the case \( n = 4 \). The elements of \( A_4 \) are the eight 3-cycles, and the elements of the normal subgroup

\[ H = \{(1), (12)(34), (13)(24), (14)(23)\}. \]

(\( H \) is normal because it contains all elements with cycle structure \((ab)(cd)\); see Example 2.96.)

If \( \sigma \) is a 3-cycle and \( \tau \in H \), then the commutator \( \sigma \tau \sigma^{-1} \tau^{-1} \) is in \( H \), because \( \sigma \tau \sigma^{-1} \in H \) by normality of \( H \). Moreover, all elements in \( H \) can be obtained as such commutators, because for any \( a, b, c, d \) such that \( \{a, b, c, d\} = \{1, 2, 3, 4\} \), one readily checks that

\[(ab)(cd) = (acb)(ac)(bd) \cdot (acb)^{-1}(ac)(bd)^{-1}.\]

It remains to describe the commutators of 3-cycles. We claim that they are all in \( H \); if we prove this, then we can conclude that \( A'_4 = H \). One possibility is to calculate all these commutators, but there are many of them. Most of you calculated some of them, and then claimed that others are analogous; that’s sort of OK, but let me try to be more precise.

Let \( \sigma \) and \( \tau \) be 3-cycles. If they both fix the same element, we can assume by relabeling that they fix 4. Then each of \( \sigma, \tau \) is either \((123)\) or \((132) = (123)^2\). So they commute, and the commutator is \((1)\).

The other possibility is that \( \sigma \) fixes one element, and \( \tau \) fixes a different element. By relabeling, we can assume that \( \sigma \) fixes 4 and \( \tau \) fixes 1. Moreover, we can relabel further to make \( \sigma = (123) \), and then there are two cases for \( \tau \): \( \tau = (234) \) or \( \tau = (243) \).

Now we calculate

\[(123)(234)(123)^{-1}(234)^{-1} = (123)(234)(132)(243) = (14)(23) \quad \text{and} \quad \]


and we are done.

5. True or false, with reasons:

(a) There is a subring of \( \mathbb{Z} \) isomorphic to \( \mathbb{Z}_6 \);

False. Let \( R \) be any subring of \( \mathbb{Z} \). Then \( R \) contains 1, but 1 generates the additive group \( \mathbb{Z} \), so the additive subgroup \( R \) must be all of \( \mathbb{Z} \). Clearly, there can be no bijection between \( \mathbb{Z} \) and \( \mathbb{Z}_6 \), and hence also no isomorphism.

(b) There is a subring of \( \mathbb{Z}_{12} \) isomorphic to \( \mathbb{Z}_6 \);

False. Let \( R \) be any subring of \( \mathbb{Z}_{12} \). Then \( R \) contains 1, but 1 generates the additive group \( \mathbb{Z}_{12} \), so the additive subgroup \( R \) must be all of \( \mathbb{Z}_{12} \).
Clearly, there can be no bijection between $\mathbb{Z}_{12}$ and $\mathbb{Z}_6$, and hence also no isomorphism.

(c) If $S$ is a subring of a commutative ring $R$, then the group $S^\times$ of invertible elements in $S$ is a subgroup of $R^\times$;

True. If $s \in S^\times$, then there is $t \in S \subseteq R$ such that $st = 1$, and this shows that $s \in R^\times$. So $S^\times \subseteq R^\times$. To check that it is a subgroup, we note that $S^\times$ is closed under multiplication in $S$, hence also in $R$ since $S$ is a subring, and hence also in $R^\times$. Finally, if $s \in S^\times$, then $s^{-1} \in S^\times$ must also be the inverse of $s$ in $R$, by uniqueness of inverse.

(d) If $S$ is a subring of a commutative ring $R$, then $S^\times = S \cap R^\times$.

False. For example, let $S = \mathbb{Z}$ and $R = \mathbb{Q}$. Then $S^\times = \{1, -1\}$, $R^\times = \mathbb{Q} \setminus \{0\}$, and $S \cap R^\times = \mathbb{Z} \setminus \{0\}$. So $S \cap R^\times$ can be much larger than $S^\times$. The point is that $s \in S$ may have an inverse in $R$ which is not contained in $S$. 