1. **a)** Give an example of a non-abelian group of infinite order and one of finite order. (Say which is which.)

b) Find the order of each element in $U(5)$, the group of units mod 5.

c) What is 3^{-1} in $U(5)$?

d) **Definition:** An element x in a finite group G is said to **generate** G if $|x| = |G|$. Which elements, if any, generate $U(5)$?

e) Let a, b, and c be elements in a group G. What is the inverse of $a^{-1}b^3c$?

2. **a)** Determine whether the operation $m * n = m - n$ is *associative* on $\mathbf{Z}$.

b) Find $\gcd(532, 400)$.

c) Write $\gcd(532, 400)$ as a linear combination of 532 and 399.

3. Give two different reasons why the set $G = \{a, b, c, d\}$ is *not* in the Cayley table below is **not** a group under $*$. Extra Credit: Give a third reason.

$*$	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	c	d	b
d	a	d	b	f

4. **a)** Let $A = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$. Prove by induction that $A^n = \begin{pmatrix} 1 & 0 \\ -n & 1 \end{pmatrix}$ for all positive integers n.

b) What is the order of the matrix $A = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$ in $GL(\mathbf{R}, 2)$. Briefly **justify** your answer.

5. Assume the set G in the table below is a group of order 6.

$\cdot$	e	v	w	x	y	z
e	e	v	w	x	y	z
v	v	w	e	z	x	y
w	w	e	v	y	z	x
x	x	y	z	e	v	w
y	y	z	x	w	e	v
z	z	x	y	v	w	e

a) Is G abelian? Briefly **explain**.

b) What elements are in $C(G)$, the center of G? Briefly **explain**.

c) What is $|w|$?

6. Let G be a group and let both H and K be subgroups of G. Let $J = H \cap K$. Carefully prove that J is also a subgroup of G.

7. Let G be a group and H a subgroup of G. For $a, b \in G$, define $a \sim b$ to mean $a^{-1}b \in H$. Is $\sim$ is an equivalence relation on G? Carefully note any properties of H that you use.

8. Recall that $GL(\mathbf{R}, n)$ is the multiplicative group of $n \times n$ matrices with non-zero determinant. Let $H = \{A \in GL(\mathbf{R}, n) \mid \det A > 0\}$. Carefully determine whether H a subgroup of $GL(\mathbf{R}, n)$.

9. **a)** Suppose that $a^6 = a^{10}$ in a group. What is the **maximum** possible order of a? Explain.

b) Find the order of $-\frac{1}{2} - \frac{i\sqrt{3}}{2}$ in $\mathbf{C}^*$.

c) Suppose that G is a group and that a and x are elements of G such that $ax = xa$. Prove that $a^{-1}x = xa^{-1}$. (In other words, if a commutes with x, it also commutes with x^{-1}.)

1. **a)** Give an example of a non-abelian group of infinite order and one of finite order.

$GL(\mathbf{R}, n)$ and $SL(\mathbf{R}, N)$ is are infinite non-abelian groups; D_n or Q_8 are finite non-abelian groups.

b) Find the order of each element in $U(5)$, the group of units mod 5.

$|1| = 1$, $|2| = 4$, $|3| = 4$, and $|4| = 2$.

c) What is 3^{-1} in $U(5)$?

$3^{-1} = 2$ because $3 \odot 2 = 1$.

d) **Definition:** An element x in a finite group G is said to **generate** G if $|x| = |G|$. Which elements, if any, generate $U(5)$?

Both 2 and 3 generate $U(5)$ since $|2| = |3| = |U(5)| = 4$.

e) Let a, b, and c be elements in a group G. What is the inverse of $a^{-1}b^3c$?

$(a^{-1}b^3c)^{-1} = c^{-1}b^{-3}a$, i.e., the product of the inverses in inverse order.

2. **a)** Determine whether the operation $m * n = m - n$ is *associative* on $\mathbf{Z}$.

Let $a, b, c \in \mathbf{Z}$.

$$(a * b) * c = (a - b) - c = a - (b + c),$$

while

$$a * (b * c) = a * (b - c) = a - (b - c) = a + c - b.$$

These expressions are not equal in general, so $*$ is not associative.

b) Find $\gcd(532, 400)$.

$$\begin{aligned} 532 &= 1 \cdot 400 + 132 \\ 400 &= 3 \cdot 132 + 4 \\ 132 &= 33 \cdot 4 + 0 \end{aligned}$$

So $\gcd(532, 400) = 4$.

c) Write $\gcd(532, 400)$ as a linear combination of 532 and 400.

$$4 = 400 - 3 \cdot 132 = 400 - 3(532 - 400) = -3 \cdot 532 + 4 \cdot 400.$$

3. Give two different reasons why the set $G = \{a, b, c, d\}$ is *not* in the Cayley table below is **not** a group under $*$. Extra Credit: Give a third reason.

Here are several reasons: (1) even though b is the identity, a has no inverse; (2) it is not closed since $d * d = f$; (3) it is not associative since $(c * c) * d = d * d = f$ while $c * (c * d) = c * b = c$, (4) some elements appear more than once in a row (column); (5) some elements don't appear at all in a row or column. (6) it is not a Latin square.

4. **a)** Let $A = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$ in $GL(\mathbf{R}, 2)$. Prove by induction that $A^n = \begin{pmatrix} 1 & 0 \\ -n & 1 \end{pmatrix}$.

Case $n = 1$: Clearly $A^1 = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$.

Induction hypothesis: $A^n = \begin{pmatrix} 1 & 0 \\ -n & 1 \end{pmatrix}$. Show $A^{n+1} = \begin{pmatrix} 1 & 0 \\ -(n+1) & 1 \end{pmatrix}$. But

$$A^{n+1} = AA^n = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ -n & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -n-1) & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -(n+1) & 1 \end{pmatrix}.$$

b) What is the order of the matrix $A = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$ in $GL(\mathbf{R}, 2)$. Carefully explain your answer.

From the problem above, $A^n \neq I$ for any $n \in \mathbf{N}$. So $|A| = \infty$.

5. Assume the set G in the table below is a group of order 6.

$\cdot$	e	v	w	x	y	z
e	e	v	w	x	y	z
v	v	w	e	z	x	y
w	w	e	v	y	z	x
x	x	y	z	e	v	w
y	y	z	x	w	e	v
z	z	x	y	v	w	e

a) Is the group abelian?

No, for example, $wx = y$ but $xw = z$.

b) What is $C(G)$?

Remember that $a \in C(G) \iff ax = xa \ \forall x \in G$. From the table, $C(G) = \{e\}$.

c) What is $|w|$?

$w^2 = v$, while $w^3 = ww^2 = wv = e$. So $|w| = 3$.

6. Let G be a group and let both H and K be subgroups of G. Let $J = H \cap K$. Carefully prove that J is also a subgroup of G.

Let's use the one step method. J is not empty since $e \in H$ and $e \in K$ because they are subgroups of G. So at least e is in J. So let $a, b \in J$. We must show that $ab^{-1} \in J$. But $a, b \in J$ implies that $a, b \in H$. Since H is a subgroup, $b^{-1} \in H$. Since H is a subgroup, it is closed, so $ab^{-1} \in H$. By the exact same reasoning, $ab^{-1} \in K$. Therefore, $ab^{-1} \in H \cap K = J$ and by the one step method, K is a subgroup.

7. Let G be a group and H a subgroup of G. For $a, b \in G$, define $a \sim b$ to mean $a^{-1}b \in H$. Is $\sim$ is an equivalence relation on G? Carefully note any properties of H that you use.

Reflexive: Notice $a^{-1}a = e \in H$ since H is a (sub)group.

Symmetric: Given $a \sim b$, show $b \sim a$. But $a \sim b$ implies $a^{-1}b \in H$. But H is a subgroup so it contains inverses of all its elements. In particular, $(a^{-1}b)^{-1} = b^{-1}a \in H$. But this means $b \sim a$.

Transitive: Given $a \sim b$ and $b \sim c$. Show $a \sim c$. Since $a \sim b$ and $b \sim c$, we have $a^{-1}b$ and $b^{-1}c$ both in H. But H is closed (since it is a subgroup), so $a^{-1}b \cdot b^{-1}c = a^{-1}c \in H$. So $a \sim c$.

Notice how the basic group properties are used to show this is an equivalence relation. This happens to be an equivalence relation that we will explore in greater detail latter in the term.

8. Recall that $GL(\mathbf{R}, n)$ is the multiplicative group of $n \times n$ matrices with non-zero determinant. Let $H = \{A \in GL(\mathbf{R}, n) \mid \det A > 0\}$. Carefully determine whether H a subgroup of $GL(\mathbf{R}, n)$.

Let's use the two step method this time. Closure: Let $A, B \in H$. We must show that $AB \in H$. But $\det A > 0$ and $\det B > 0$, so by basic determinant properties

$$\det AB = \det A \det B > 0.$$

But this means that $AB \in H$.

Now for Inverses: Let $A \in H$. Show $A^{-1} \in H$. But $\det A > 0$, so A^{-1} exists. But then by basic determinant properties,

$$\det(A^{-1}) = [\det A]^{-1} > 0$$

because the reciprocal of a positive number is positive. So $A^{-1} \in H$. Therefore $H \leq GL(\mathbf{R}, n)$.

9. **a)** Suppose that $a^6 = a^{10}$ in a group. What is the **maximum** possible order of a? Explain.

If we use cancellation (or multiply by a^{-6}, we have

$$a^6 = a^{10} \Rightarrow e = a^4.$$

Since the order of a is the **minimum** positive integer so that $a^n = e$, then $|a| \leq 4$. The order could be smaller than 4, but not greater.

b) Find the order of $-\frac{1}{2} - \frac{i\sqrt{3}}{2}$ in $\mathbf{C}^*$.

Check that: $a^2 = -\frac{1}{2} + \frac{i\sqrt{3}}{2}$ and then $a^3 = 1$, so $|a| = 3$.

c) Suppose that G is a group and that a and x are elements of G such that $ax = xa$. Prove that $a^{-1}x = xa^{-1}$. (In other words, if a commutes with x, it also commutes with x^{-1}.)

Notice that

$$ax = xa \Rightarrow a^{-1}ax = a^{-1}xa \Rightarrow x = a^{-1}xa \Rightarrow xa^{-1} = a^{-1}xaa^{-1} \Rightarrow xa^{-1} = a^{-1}x.$$