Math 343 October 5, 2026	Midterm Exam 1	Time: 90 minutes
Detailed Solutions		

[5pts] **Q1**: Determine whether each statement is true or false and justify your answer. (**Choose 4 only**)

1. If a, b and c are elements of a group G such that $ab = ca$, then $b = c$.

Solution: FALSE. *Counterexample in* D_4. $HR_{90} = R_{270}H$. Take $a = H$, $b = R_{90}$ and $c = R_{270}$. Then $ab = HR_{90} = R_{270}H = ca$, but $b = R_{90} \neq R_{270} = c$.

Remark. Multiplying $ab = ca$ on the right by a^{-1} shows that $ab = ca$ is the same as $c = aba^{-1}$. So $b = c$ holds exactly when $ab = ba$. The statement is true in every abelian group; it fails here because H and R_{90} do not commute ($HR_{90} = D$ but $R_{90}H = D'$).

2. If x is an element of a group G such that $C(x) = \{e\}$, then $x = e$.

Solution: TRUE. By definition, $C(x) = \{g \in G : gx = xg\}$. Since $xx = xx$, the element x commutes with itself, so $x \in C(x)$. If $C(x) = \{e\}$, then $x \in \{e\}$, that is, $x = e$.

Remark. The hypothesis is very strong. $C(x)$ always contains e and x (indeed all of $\langle x \rangle$). Once $x = e$ we get $C(x) = C(e) = G$, so $C(x) = \{e\}$ can happen only when $G = \{e\}$ is the trivial group. The implication is nevertheless true.

3. If a is the only element of order 2 in a group G, then $a \in Z(G)$.

Solution: TRUE. Let $g \in G$ be arbitrary.

$$
\begin{aligned}
(gag^{-1})^2 &= (gag^{-1})(gag^{-1}) && \\
&= ga(g^{-1}g)ag^{-1} && \textit{associativity} \\
&= ga^2g^{-1} && g^{-1}g = e \\
&= geg^{-1} = e && a^2 = e \textit{ because } |a| = 2
\end{aligned}
$$

Since a is the only element of order 2, either $gag^{-1} = e$, then multiplying on the left by g^{-1} and on the right by g gives $a = g^{-1}eg = e$, which is impossible because $|a| = 2$. Hence $gag^{-1} = a$. Multiplying on the right by g gives $ga = ag$. So $a \in Z(G)$.

Remark. The same computation gives $(gag^{-1})^n = ga^ng^{-1}$ for every $n \geq 1$, so $|gag^{-1}| = |a|$ for all $a, g \in G$.

4. If a is an element of a group G with $|a^2| = 3$, then $|a| = 6$.

Solution: FALSE. Counterexample: $G = U(7) = \{1,2,3,4,5,6\}$ and $a = 2$. Modulo 7, $2^2 = 4$ and $2^3 = 8 \equiv 1$, so $|a| = 3$. Also $a^2 = 4$ satisfies $4^2 = 16 \equiv 2$ and $4^3 = 64 \equiv 1$, so $|a^2| = 3$. Thus $|a^2| = 3$ while $|a| = 3 \neq 6$.

Remark. Any element of order 3 is a counterexample, because then $a^2 = a^{-1}$ also has order 3; e.g. $a = R_{120}$ in D_3 or $a = 1$ in $\mathbb{Z}_3$.

5. If every proper subgroup of a group G is cyclic, then G is cyclic.

Solution: FALSE. Counterexample: $G = U(8) = \{1,3,5,7\}$.

$U(8)$ *is not cyclic.* Modulo 8, $3^2 = 9 \equiv 1$, $5^2 = 25 \equiv 1$ and $7^2 = 49 \equiv 1$. So $\langle 1\rangle = \{1\}$, $\langle 3\rangle = \{1,3\}$, $\langle 5\rangle = \{1,5\}$ and $\langle 7\rangle = \{1,7\}$; no element generates the four-element group $U(8)$.

Every proper subgroup of $U(8)$ *is cyclic.* The product of any two different elements of $\{3,5,7\}$ is the third one:

$$3 \cdot 5 = 15 \equiv 7, \quad 3 \cdot 7 = 21 \equiv 5, \quad 5 \cdot 7 = 35 \equiv 3 \pmod 8.$$

So a subgroup that contains two of 3, 5, 7 contains the third as well, and it contains the identity 1; it is all of $U(8)$. A proper subgroup K therefore contains 1 and at most one element of $\{3,5,7\}$, so $K = \{1\} = \langle 1\rangle$ or $K = \{1, x\} = \langle x\rangle$ with $x \in \{3,5,7\}$. Each of these is cyclic.

Remark. The subgroup $\{R_0, R_{180}, H, V\}$ of D_4 is another counterexample, for the same reason: each of R_{180}, H, V has order 2 and the product of any two of them is the third.

6. If G is a group such that $(xy)^2 = x^2y^2$ for all $x, y \in G$, then G must be abelian.

Solution: TRUE. Let $x, y \in G$. Writing out both sides of $(xy)^2 = x^2y^2$ and cancelling:

$$\begin{aligned} & xyxy = xxyy && \textit{the hypothesis, written out} \\ \Longrightarrow \quad & yxy = xyy && \textit{cancel } x \textit{ on the left (Theorem 2.2)} \\ \Longrightarrow \quad & yx = xy && \textit{cancel } y \textit{ on the right (Theorem 2.2)} \end{aligned}$$

Since x and y were arbitrary, G is abelian.

Remark. The converse also holds: in an abelian group, $(xy)^2 = xyxy = xxyy = x^2y^2$.

[5pts] **Q2**

(a) Show that the set $A = \{2,4,6,8\}$ under multiplication modulo 10 forms an abelian group.

Solution. We check closure, associativity, identity, inverses and commutativity. The operation table of multiplication modulo 10 on A is:

mod 10	**2**	**4**	**6**	**8**
2	4	8	2	6
4	8	6	4	2
6	**2**	**4**	**6**	**8**
8	6	2	8	4

Closure. Every entry of the table lies in A.

Associativity. Multiplication modulo n is associative, in fact multiplication of the integers is associative. So, $(xy)z = x(yz)$ as integers, hence modulo any positive integer n.

Identity. The row of 6 repeats the column headings, so $6x \equiv x \pmod{10}$ for every $x \in A$.

Inverses. Every row contains the identity 6: $2 \cdot 8 = 16 \equiv 6$, $4 \cdot 4 = 16 \equiv 6$ and $6 \cdot 6 = 36 \equiv 6$. Hence

$$2^{-1} = 8,\ 4^{-1} = 4,\ 6^{-1} = 6,\ 8^{-1} = 2.$$

Commutativity. $xy \equiv yx \pmod{10}$ because multiplication of integers is commutative; the table is symmetric about its main diagonal.

Therefore A is an abelian group under multiplication modulo 10.

> ***Remark.*** A is even cyclic: modulo 10, $2^1 = 2$, $2^2 = 4$, $2^3 = 8$ and $2^4 = 16 \equiv 6$, so $A = \langle 2 \rangle$. Compare Exercise 16 of Chapter 2, where $\{5,15,25,35\}$ is a group under multiplication modulo 40 with identity 25.

(b) Let G be a group and let H and K be subgroups of G.

i) State the One-Step Subgroup Test.

Solution. (Theorem 3.1) Let G be a group and H a nonempty subset of G. If $ab^{-1} \in H$ whenever $a, b \in H$, then H is a subgroup of G. (In additive notation: if $a - b \in H$ whenever $a, b \in H$, then $H \leq G$.)

ii) Show that $H \cap K \leq G$.

Solution. We apply the One-Step Subgroup Test to $H \cap K$.

Nonempty. H and K are subgroups, so both contain the identity e of G. Hence $e \in H \cap K$.

The test. Let $a, b \in H \cap K$. Then $a, b \in H$, and since H is a subgroup, $ab^{-1} \in H$. In the same way, $a, b \in K$ gives $ab^{-1} \in K$. Hence $ab^{-1} \in H \cap K$.

By the One-Step Subgroup Test, $H \cap K \leq G$.

iii) Suppose that G is abelian. Show that $HK = \{hk : h \in H,\ k \in K\}$ is a subgroup of G. Give an example of a group G and subgroups H and K of G such that HK is not a subgroup of G.

Solution. *HK is a subgroup when G is abelian.* We use the One-Step Subgroup Test again. First, $e = ee \in HK$, so HK is nonempty. Let $x, y \in HK$, say $x = h_1k_1$ and $y = h_2k_2$ with $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Then

$$\begin{aligned} xy^{-1} &= h_1k_1(h_2k_2)^{-1} \\ &= h_1k_1k_2^{-1}h_2^{-1} && \textit{Socks–Shoes Property (Theorem 2.4)} \\ &= h_1h_2^{-1}k_1k_2^{-1} && \textit{G is abelian, so h_2^{-1} commutes with $k_1k_2^{-1}$} \end{aligned}$$

Since H is a subgroup, $h_1h_2^{-1} \in H$; since K is a subgroup, $k_1k_2^{-1} \in K$. So $xy^{-1} = (h_1h_2^{-1})(k_1k_2^{-1}) \in HK$, and $HK \leq G$ by the One-Step Subgroup Test.

An example where HK is not a subgroup. Let $G = D_4$, $H = \{R_0, V\}$ and $K = \{R_0, D\}$. By Table 1.1, $V^2 = R_0$ and $D^2 = R_0$, so each of these sets is closed under the operation; being finite and nonempty, each is a subgroup by the Finite Subgroup Test (Theorem 3.3). Using Table 1.1 again,

$$HK = \{R_0R_0,\ R_0D,\ VR_0,\ VD\} = \{R_0,\ D,\ V,\ R_{270}\}.$$

This set is not closed: $R_{270}R_{270} = R_{180} \notin HK$ (also $DV = R_{90} \notin HK$). So HK is not a subgroup of D_4.

[5pts] **Q3**: Determine if the following groups are cyclic and if so find all their generators:

(1) $\mathbb{Q}$, the group of rational numbers under addition.

Solution: not cyclic.

Suppose $\mathbb{Q} = \langle r \rangle$ for some $r \in \mathbb{Q}$. In additive notation, $\langle r \rangle = \{nr : n \in \mathbb{Z}\}$. Since $\mathbb{Q} \neq \{0\}$, $r \neq 0$. The rational number $r/2$ belongs to $\mathbb{Q}$, so $r/2 = nr$ for some integer n. Dividing by $r \neq 0$ gives $n = 1/2$, which is not an integer. This contradiction shows that $\mathbb{Q}$ is not cyclic.

(2) $U(14)$

Solution: cyclic, with generators 3 and 5.

$U(14) = \{1,3,5,9,11,13\}$, the positive integers less than 14 that are relatively prime to 14, so $|U(14)| = 6$. The powers of 3 modulo 14 are:

k	**1**	**2**	**3**	**4**	**5**	**6**
3^k **mod 14**	3	9	13	11	5	1

So $|3| = 6 = |U(14)|$ and $U(14) = \langle 3 \rangle$ is cyclic. By Theorem 4.2, Corollary 3, the generators are the powers 3^k with $\gcd(6, k) = 1$, that is, $k = 1$ and $k = 5$. They are $3^1 = 3$ and $3^5 \equiv 5 \pmod{14}$.

As a check, here are the orders of all elements of $U(14)$; exactly two of them, 3 and 5, have order 6.

x	**1**	**3**	**5**	**9**	**11**	**13**
$\|x\|$	1	**6**	**6**	3	3	2

(3) $U(15)$

Solution: not cyclic.

$U(15) = \{1,2,4,7,8,11,13,14\}$, so $|U(15)| = 8$. Squaring each element modulo 15:

x	**1**	**2**	**4**	**7**	**8**	**11**	**13**	**14**
x^2 **mod 15**	1	4	1	4	4	1	4	1
$\|x\|$	1	4	2	4	4	2	4	2

So 4, 11 and 14 all have order 2 ($4^2 = 16 \equiv 1$, $11^2 = 121 \equiv 1$, $14^2 = 196 \equiv 1$). A cyclic group of order 8 has exactly $\varphi(2) = 1$ element of order 2 (Theorem 4.4), so $U(15)$ is not cyclic.

Direct check. Every square is 1 or 4, and $4^2 \equiv 1$, so $x^4 \equiv 1 \pmod{15}$ for every $x \in U(15)$. No element has order 8, so no element generates $U(15)$.

(4) The subgroup of all rotations in D_8.

Solution: cyclic, with generators R_{45}, R_{135}, R_{225}, R_{315}.

D_8 has order 16. Its rotations are $R_0, R_{45}, R_{90}, \dots, R_{315}$, the rotations through multiples of 360°/8 = 45°. Since $(R_{45})^k$ is the rotation through $45k$ degrees, $(R_{45})^k = R_{45k}$ for $k = 0,1, \dots ,7$, and the rotation subgroup is

$$\{R_0, R_{45}, R_{90}, \dots, R_{315}\} = \langle R_{45} \rangle,$$

a cyclic group of order 8. By Theorem 4.2, Corollary 3, its generators are $(R_{45})^k$ with $\gcd(8, k) = 1$, that is, $k = 1,3,5,7$:

$$R_{45}, R_{135}, R_{225}, R_{315}.$$

[5pts] **Q4**: Let $G = \langle a \rangle$ be a cyclic group of order 42. Find:

Throughout, $|a| = 42 = 2 \cdot 3 \cdot 7$. For every positive integer k, Theorem 4.2 gives

$$\langle a^k \rangle = \langle a^{\gcd(42,k)} \rangle \quad \text{and} \quad |a^k| = \frac{42}{\gcd(42,k)}.$$

(1) $|a^{35}|$ and all generators of $\langle a^{35} \rangle$.

Solution. Since $\gcd(42,35) = 7$,

$$|a^{35}| = \frac{42}{\gcd(42,35)} = \frac{42}{7} = 6$$

$$\langle a^{35} \rangle = \langle a^7 \rangle = \{e, a^7, a^{14}, a^{21}, a^{28}, a^{35}\}.$$

This is a cyclic group of order 6 generated by a^7, so by Theorem 4.2, Corollary 3, its generators are $(a^7)^j$ with $\gcd(6, j) = 1$, that is, $j = 1$ and $j = 5$: $(a^7)^1 = a^7$ and $(a^7)^5 = a^{35}$.

Answer: $|a^{35}| = 6$, and the generators of $\langle a^{35} \rangle$ are a^7 and a^{35}.

(2) All elements of order 14 in G.

Solution. By Theorem 4.3, G has exactly one subgroup of order 14, namely $\langle a^{42/14} \rangle = \langle a^3 \rangle$. An element b of order 14 generates a subgroup of order 14, because $|b| = |\langle b \rangle|$ (Theorem 4.1, Corollary 1), so $\langle b \rangle = \langle a^3 \rangle$ by uniqueness. Hence the elements of order 14 are exactly the generators of $\langle a^3 \rangle$. Since $|a^3| = 14$, Corollary 3 of Theorem 4.2 says these generators are $(a^3)^j$ with $\gcd(14, j) = 1$ and $1 \le j \le 13$, that is, $j = 1,3,5,9,11,13$.

Answer: the elements of order 14 are a^3, a^9, a^{15}, a^{27}, a^{33}, a^{39}.

(3) A generator for $\langle a^{10} \rangle \cap \langle a^{15} \rangle$.

Solution. First simplify both subgroups with Theorem 4.2:

$$\langle a^{10} \rangle = \langle a^{\gcd(42,10)} \rangle = \langle a^2 \rangle \quad \text{and} \quad \langle a^{15} \rangle = \langle a^{\gcd(42,15)} \rangle = \langle a^3 \rangle.$$

By Theorem 4.1, $\langle a^2\rangle = \{e, a^2, a^4, \ldots, a^{40}\}$ consists of the a^m $(0 \le m \le 41)$ with m even, and $\langle a^3\rangle = \{e, a^3, a^6, \ldots, a^{39}\}$ consists of those with $3 \mid m$. An element a^m $(0 \le m \le 41)$ lies in both exactly when $2 \mid m$ and $3 \mid m$, that is, when $6 \mid m$. Hence

$$\langle a^{10}\rangle \cap \langle a^{15}\rangle = \{e, a^6, a^{12}, a^{18}, a^{24}, a^{30}, a^{36}\} = \langle a^6\rangle.$$

Answer: a^6 is a generator (it has order $42/6 = 7$). Each of a^{12}, a^{18}, a^{24}, a^{30}, a^{36} also generates this subgroup, by Corollary 3 of Theorem 4.2.

(4) All subgroups of G.

Solution. By the Fundamental Theorem of Cyclic Groups (Theorem 4.3), every subgroup of G is cyclic, its order divides 42, and for each positive divisor k of 42 there is exactly one subgroup of order k, namely $\langle a^{42/k}\rangle$. The positive divisors of 42 are 1, 2, 3, 6, 7, 14, 21 and 42, so G has exactly eight subgroups. The table lists them, and Figure 1 shows how they fit together.

Order	Subgroup	Elements
1	$\langle a^{42}\rangle = \{e\}$	e
2	$\langle a^{21}\rangle$	e, a^{21}
3	$\langle a^{14}\rangle$	e, a^{14}, a^{28}
6	$\langle a^7\rangle$	e, a^7, a^{14}, a^{21}, a^{28}, a^{35}
7	$\langle a^6\rangle$	e, a^6, a^{12}, a^{18}, a^{24}, a^{30}, a^{36}
14	$\langle a^3\rangle$	e, a^3, a^6, a^9, ..., a^{39}
21	$\langle a^2\rangle$	e, a^2, a^4, a^6, ..., a^{40}
42	$\langle a\rangle = G$	all 42 elements of G

If j divides i (both divisors of 42), then $a^i = (a^j)^{i/j}$, so $\langle a^i\rangle \subseteq \langle a^j\rangle$. Following the lines of Figure 1 upward gives all such containments.

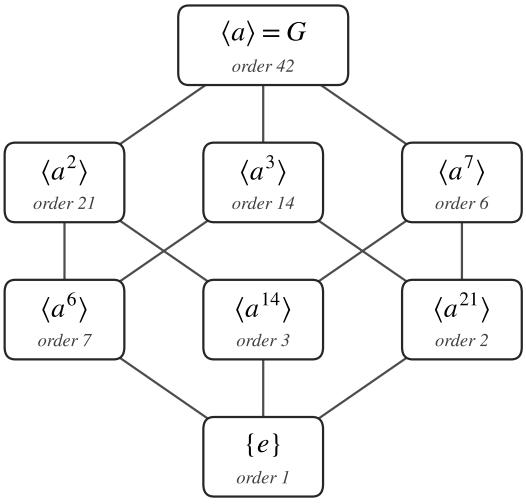


Figure 1. Subgroup lattice of G. A line joins two subgroups when the lower one is contained in the upper one and no subgroup lies strictly between them.