Midterm 3 Practice Worksheet 1: Solutions

Combinatorics

Fall 2026

These are the solutions to Practice Worksheet 1. The write-ups model the amount of explanation expected on the exam. Permutations are composed from right to left: gh means "first h, then g."

True or false

(A) True. $\mathbb{Z}_7 = \langle 1 \rangle$. *(Every group with a prime number of elements is cyclic.)*
(B) False. $(1\ 2)(2\ 3) = (1\ 2\ 3)$, *but* $(2\ 3)(1\ 2) = (1\ 3\ 2)$, *so* S_3 *is not commutative, and a cyclic group is commutative. Also, the elements of* S_3 *have orders* 1, 2, 3, *never* 6.
(C) True. $3 + 3 = 6 \equiv 0$, *so* $\{0, 3\}$ *is closed under addition modulo* 6.
(D) True. *The cycles* $(1\ 2)$ *and* $(3\ 4)$ *are disjoint, and disjoint cycles commute.*
(E) False. *By Lagrange's theorem the number of elements of a subgroup divides* 15, *and* 6 *does not.*
(F) False. $g^k = e$ *exactly when* 6 *divides* k. *In fact* $g^9 = g^6 g^3 = g^3 \neq e$.
(G) True. *The cycles are disjoint, so the order is* $\operatorname{lcm}(2, 4) = 4$.

Groups and subgroups

(A) *The multiples of* 2 *modulo* 8 *are* $2, 4, 6, 8 \equiv 0$, *so* $\langle 2 \rangle = \{0, 2, 4, 6\}$. *The multiples of* 4 *are* $4, 8 \equiv 0$, *so* $\langle 4 \rangle = \{0, 4\}$. *The multiples of* 6 *are* 6, $12 \equiv 4$, $18 \equiv 2$, $24 \equiv 0$, *so* $\langle 6 \rangle = \{0, 2, 4, 6\}$.
$\mathbb{Z}_8 = \langle 1 \rangle$ *is cyclic. An element* a *is a generator exactly when its multiples reach all* 8 *elements before returning to* 0, *that is, when* a *has order* 8. *This happens exactly when* a *and* 8 *have no common divisor greater than* 1: *the generators are* $1, 3, 5, 7$. *(For example, the multiples of* 3 *are* $3, 6, 1, 4, 7, 2, 5, 0$.)
(B) *A finite subset is a subgroup exactly when it is closed under addition.*

- $\{0, 3, 6\} \subseteq \mathbb{Z}_9$: *subgroup;* $3 + 3 = 6$, $3 + 6 = 9 \equiv 0$, $6 + 6 = 12 \equiv 3$.
- $\{0, 4\} \subseteq \mathbb{Z}_8$: *subgroup;* $4 + 4 = 8 \equiv 0$.
- $\{0, 1, 7\} \subseteq \mathbb{Z}_8$: *not a subgroup;* $1 + 1 = 2$ *is not in the set.*
- $\{0, 4, 8\} \subseteq \mathbb{Z}_{12}$: *subgroup;* $4 + 4 = 8$, $4 + 8 = 12 \equiv 0$, $8 + 8 = 16 \equiv 4$.
- $\{0, 5, 10\} \subseteq \mathbb{Z}_{12}$: *not a subgroup;* $5 + 10 = 15 \equiv 3$ *is not in the set. (Also,* 3

divides 12, so size alone does not rule it out; closure does.)

(C) Apply the right factor first. For $(1\ 3)(2\ 3)$: $1 \mapsto 1 \mapsto 3$, $3 \mapsto 2 \mapsto 2$, $2 \mapsto 3 \mapsto 1$, so $(1\ 3)(2\ 3) = (1\ 3\ 2)$. For $(2\ 3)(1\ 3)$: $1 \mapsto 3 \mapsto 2$, $2 \mapsto 2 \mapsto 3$, $3 \mapsto 1 \mapsto 1$, so $(2\ 3)(1\ 3) = (1\ 2\ 3)$. The two products are different, so S_3 is not commutative. The elements of S_3 are e (order 1), the transpositions $(1\ 2)$, $(1\ 3)$, $(2\ 3)$ (order 2), and the 3-cycles $(1\ 2\ 3)$, $(1\ 3\ 2)$ (order 3). No element has order $6 = |S_3|$, so S_3 is not cyclic. (The failure of commutativity gives a second reason: a cyclic group is commutative.)
(D) By Lagrange's theorem the number of elements of a subgroup divides 18. So 6 and 9 are possible, and 4 and 12 are not. The order of an element is the number of elements of the subgroup it generates, so it also divides 18: no element has order 4. An element of order 9 is possible; for example, 2 has order 9 in $\mathbb{Z}_{18}$.
(E) $g^k = e$ exactly when 6 divides k. So $g^{12} = e$, $g^{30} = e$, and $g^{-6} = (g^6)^{-1} = e$, but $g^{15} = g^{12}g^3 = g^3 \neq e$. Since $40 = 6 \cdot 6 + 4$, $g^{40} = (g^6)^6 g^4 = g^4$. Since $g \cdot g^5 = g^6 = e$, $g^{-1} = g^5$.
(F) For disjoint cycles, take the least common multiple of the lengths: $(1\ 2\ 3\ 4)(5\ 6)$ has order $\mathrm{lcm}(4, 2) = 4$; $(1\ 2)(3\ 4\ 5)$ has order $\mathrm{lcm}(2, 3) = 6$; $(1\ 2\ 3)(4\ 5\ 6)$ has order $\mathrm{lcm}(3, 3) = 3$.
The cycles of $(1\ 2\ 3)(3\ 4)$ overlap, so compute the product first: $1 \mapsto 1 \mapsto 2$, $2 \mapsto 2 \mapsto 3$, $3 \mapsto 4 \mapsto 4$, $4 \mapsto 3 \mapsto 1$. So $(1\ 2\ 3)(3\ 4) = (1\ 2\ 3\ 4)$, which has order 4, not $\mathrm{lcm}(3, 2) = 6$.

Working with a permutation

(A) Follow each element under g, starting with the smallest element not yet used: $1 \mapsto 6 \mapsto 3 \mapsto 7 \mapsto 5 \mapsto 1$, then $2 \mapsto 4 \mapsto 2$, then $8 \mapsto 8$. So

$$g = (1\ 6\ 3\ 7\ 5)(2\ 4)(8) = (1\ 6\ 3\ 7\ 5)(2\ 4).$$

The cycle type is $5, 2, 1$ and $\mathrm{cyc}(g) = 3$: the fixed point 8 counts as a cycle.
(B) The order is $\mathrm{lcm}(5, 2, 1) = 10$. The inverse reads each cycle backwards:

$$g^{-1} = (5\ 7\ 3\ 6\ 1)(4\ 2) = (1\ 5\ 7\ 3\ 6)(2\ 4).$$

Check: $g(g^{-1}(1)) = g(5) = 1$.
(C) $(gh)(x) = g(h(x))$, where $h = (1\ 2\ 4)$ sends $1 \mapsto 2$, $2 \mapsto 4$, $4 \mapsto 1$ and fixes the rest:

$1 \mapsto 2 \mapsto 4$, $2 \mapsto 4 \mapsto 2$, $3 \mapsto 3 \mapsto 7$, $4 \mapsto 1 \mapsto 6$, $5 \mapsto 5 \mapsto 1$, $6 \mapsto 6 \mapsto 3$, $7 \mapsto 7 \mapsto 5$, $8 \mapsto$

Following the cycles: $1 \mapsto 4 \mapsto 6 \mapsto 3 \mapsto 7 \mapsto 5 \mapsto 1$, and 2 and 8 are fixed. So

$$gh = (1\ 4\ 6\ 3\ 7\ 5),$$

with cycle type $6, 1, 1$.
(D) Now apply g first: $(hg)(x) = h(g(x))$. $1 \mapsto 6 \mapsto 6$, $6 \mapsto 3 \mapsto 3$, $3 \mapsto 7 \mapsto 7$, $7 \mapsto 5 \mapsto 5$, $5 \mapsto 1 \mapsto 2$, $2 \mapsto 4 \mapsto 1$, and $4 \mapsto 2 \mapsto 4$, $8 \mapsto 8$. So $hg = (1\ 6\ 3\ 7\ 5\ 2)$. It has the same cycle type as gh, but it is a different permutation: gh sends $1 \mapsto 4$, and hg sends $1 \mapsto 6$.
(E) The written cycles move $1, 7, 2, 5, 9, 4$; the fixed points in S_9 are $3, 6, 8$. So $q = (1\ 7)(2\ 5\ 9\ 4)(3)(6)(8)$, with cycle type $4, 2, 1, 1, 1$, $\mathrm{cyc}(q) = 5$, and order $\mathrm{lcm}(2, 4) = 4$.

Another permutation

(A) Follow the elements: $1 \mapsto 3 \mapsto 6 \mapsto 4 \mapsto 1$, $2 \mapsto 8 \mapsto 2$, $5 \mapsto 7 \mapsto 5$. So

$$g = (1\ 3\ 6\ 4)(2\ 8)(5\ 7),$$

with cycle type $4, 2, 2$ and $\mathrm{cyc}(g) = 3$ (there are no fixed points).
(B) The order is $\mathrm{lcm}(4, 2, 2) = 4$. Reading each cycle backwards,

$$g^{-1} = (4\ 6\ 3\ 1)(8\ 2)(7\ 5) = (1\ 4\ 6\ 3)(2\ 8)(5\ 7).$$

(C) $(gh)(x) = g(h(x))$, where $h = (2\ 3\ 5)$ sends $2 \mapsto 3$, $3 \mapsto 5$, $5 \mapsto 2$:

$1 \mapsto 1 \mapsto 3$, $\quad 2 \mapsto 3 \mapsto 6$, $\quad 3 \mapsto 5 \mapsto 7$, $\quad 4 \mapsto 4 \mapsto 1$, $\quad 5 \mapsto 2 \mapsto 8$, $\quad 6 \mapsto 6 \mapsto 4$, $\quad 7 \mapsto 7 \mapsto 5$, $\quad 8 \mapsto$

Following the cycle from 1: $1 \mapsto 3 \mapsto 7 \mapsto 5 \mapsto 8 \mapsto 2 \mapsto 6 \mapsto 4 \mapsto 1$. So

$$gh = (1\ 3\ 7\ 5\ 8\ 2\ 6\ 4),$$

a single 8-cycle.

Cyclic subgroups of $\mathbb{Z}_n$

(A) The multiples of 8 modulo 12 are 8, $16 \equiv 4$, $24 \equiv 0$, so $\langle 8 \rangle = \{0, 4, 8\}$ and 8 has order 3. The multiples of 9 are 9, $18 \equiv 6$, $27 \equiv 3$, $36 \equiv 0$, so $\langle 9 \rangle = \{0, 3, 6, 9\}$ and 9 has order 4. Both orders divide 12, as Lagrange's theorem requires.

(B) The multiples of 5 modulo 12 are

$$5,\ 10,\ 3,\ 8,\ 1,\ 6,\ 11,\ 4,\ 9,\ 2,\ 7,\ 0,$$

all 12 elements, so 5 has order 12 and is a generator. The multiples of 10 are $10, 8, 6, 4, 2, 0$, only 6 elements, so 10 is not a generator. In general a generates $\mathbb{Z}_{12}$ exactly when a and 12 have no common divisor greater than 1; the generators are $1, 5, 7, 11$.

(C) The multiples of 6 modulo 9 are 6, $12 \equiv 3$, $18 \equiv 0$, so $\langle 6 \rangle = \{0, 3, 6\}$; 6 has order 3 and is not a generator. The generators of $\mathbb{Z}_9$ are the elements with no common divisor with 9 other than 1, that is, those not divisible by 3: $1, 2, 4, 5, 7, 8$.

(D) The multiples of 10 modulo 15 are 10, $20 \equiv 5$, $30 \equiv 0$, so $\langle 10 \rangle = \{0, 5, 10\}$ and 10 has order 3. The multiples of 4 modulo 15 are

$$4,\ 8,\ 12,\ 1,\ 5,\ 9,\ 13,\ 2,\ 6,\ 10,\ 14,\ 3,\ 7,\ 11,\ 0,$$

all 15 elements, so 4 has order 15 and is a generator. (Equivalently, 4 and 15 have no common divisor greater than 1.)

Symmetries of the regular pentagon

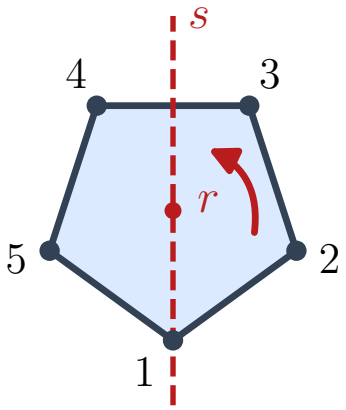


Figure 1: The labeled pentagon, the rotation r, and the mirror line of s.

Figure description: A regular pentagon with corner 1 at the bottom and the other corners counterclockwise: 2 at the lower right, 3 at the upper right, 4 at the upper left, and 5 at the lower left. A dashed vertical mirror line labeled s passes through corner 1 and the center, and a counterclockwise arrow labeled r turns about the center.

(A) The rotation is $r = (1\ 2\ 3\ 4\ 5)$, and r^2 moves each corner two steps: $r^2 = (1\ 3\ 5\ 2\ 4)$. The reflection s fixes corner 1 and exchanges the corners on

the two sides of the axis: $s(i) = 2 - i$, so $s = (2\ 5)(3\ 4)$.
Right to left, $(rs)(i) = r(2 - i) = 3 - i$: $1 \mapsto 2$, $2 \mapsto 1$, $3 \mapsto 5$, $4 \mapsto 4$, $5 \mapsto 3$. So $rs = (1\ 2)(3\ 5)$, the reflection across the axis through corner 4. Similarly $(r^2 s)(i) = 4 - i$: $r^2 s = (1\ 3)(4\ 5)$, the reflection across the axis through corner 2.
(B) $(sr)(i) = s(i + 1) = 1 - i$: $1 \mapsto 5$, $2 \mapsto 4$, $3 \mapsto 3$, $4 \mapsto 2$, $5 \mapsto 1$, so $sr = (1\ 5)(2\ 4)$. Also $(r^{-1}s)(i) = (2 - i) - 1 = 1 - i$, the same permutation. So $sr = r^{-1}s$. Since $rs = (1\ 2)(3\ 5)$ sends $1 \mapsto 2$ while sr sends $1 \mapsto 5$, we have $rs \neq sr$.
(C) The identity has order 1 and $\mathrm{cyc} = 5$. The four rotations r, r^2, r^3, r^4 are 5-cycles: order 5 and $\mathrm{cyc} = 1$. The five reflections $r^j s$ each fix one corner and exchange the other four in two pairs: order 2 and $\mathrm{cyc} = 3$. No element has order $10 = |D_5|$, so D_5 is not cyclic; part (B) gives a second reason, since a cyclic group is commutative.