Instructions. Answer each of the questions on your own paper and be sure to show your work so that partial credit can be adequately assessed. Put your name on each page of your paper.

Some useful notation: $\mathbb{Z}$ is the group of integers under addition; $\mathbb{Z}_n$ is the group of congruence classes modulo n under addition of congruence classes; $\mathbb{Z}_n^*$ is the group of invertible congruence classes modulo n under multiplication of congruence classes; S_n is the group of permutations of the set $\{1, \ldots, n\}$ under composition of permutations.

1. **[15 Points]** Let $\sigma = (2, 4, 9, 7)(6, 4, 2, 5, 9)(1, 6)(3, 8, 6) \in S_9$.

   (a) Write σ as a product of disjoint cycles.

   ▶ **Solution.** $\sigma = (1, 9, 6, 3, 8)(2, 5, 7)$ ◀

   (b) What is the order of σ.

   ▶ **Solution.** $\operatorname{lcm}\{5, 3\} = 15$ ◀

   (c) Write σ^{-1} as a product of disjoint cycles.

   ▶ **Solution.** $\sigma^{-1} = (1, 8, 3, 6, 9)(2, 7, 5)$ ◀

2. **[18 Points]**

   (a) If G is a group and H is a subset of G, list the conditions that H must satisfy to guarantee that H is a subgroup.

   ▶ **Solution.** This is Proposition 3.2.2: H is a subgroup of G if and only if the following conditions hold:

   i. $ab \in H$ for all $a, b \in H$;
   ii. $e \in H$;
   iii. $a^{-1} \in H$ for all $a \in H$.

   ◀

   (b) Decide in each of the following cases whether the given subset is a subgroup of the group S_4. Justify your answer.

   i. $H_1 = \{(1), (1, 3, 4), (1, 4, 3)\}$

   ▶ **Solution.** Let $e = (1)$, $a = (1, 3, 4)$, and $b = (1, 4, 3)$, and look at the multiplication table for these elements:

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

   Since all the elements of this table are in H_1, it follows that H_1 is closed under the multiplication on S_4. Moreover, the identity of S_4, namely (1), is in H_1, and $a^{-1} = b$, $b^{-1} = a$ so H_1 is closed under inverses. Hence, H_1 is a subgroup of S_4. ◀

ii. $H_2 = \{(1),\ (1,\ 2,\ 3,\ 4),\ (1,\ 4,\ 3,\ 2)\}$

▶ **Solution.** $(1,\ 2,\ 3,\ 4)(1,\ 2,\ 3,\ 4) = (1,\ 3)(2,\ 4)$ so H_2 is not closed under multiplication, and hence is not a subgroup of S_4. ◀

3. **[18 Points]** Let G be a group and let $a \in G$.

   (a) Complete the definition of what it means for a to have finite order $o(a) = n$: *If n is a positive integer, then the element $a \in G$ has order n provided*

n is the smallest positive integer such that $a^n = e$.

   (b) Let $a \in G$ be an element of order 20 and let $b = a^5$. What is the order of b? Prove that your answer is correct directly from the definition of order given in part (a).

   ▶ **Solution.** First note that $b^4 = (a^5)^4 = a^{20} = e$ because $o(a) = 20$. But $b = a^5 \neq e$, $b^2 = (a^5)^2 = a^{10} \neq e$, and $b^3 = (a^2)^5 = a^{15} \neq e$ since $a^k \neq e$ for $1 \leq k < 20$ because 20 is the smallest n for which $a^n = e$. Thus, 4 is the smallest n such that $b^n = e$, and hence $o(b) = 4$. ◀

4. **[18 Points]** $\mathbb{Z}_7^* = \{1,\ 2,\ 3,\ 4,\ 5,\ 6\}$ is the group of invertible congruence classes modulo 7 under multiplication.

   (a) Compute the cyclic subgroup $\langle 2 \rangle$ of $\mathbb{Z}_7^*$ generated by 2.

   ▶ **Solution.** $\langle 2 \rangle = \{2,\ 4 = 2^2,\ 1 = 2^3\}$ ◀

   (b) Compute the cyclic subgroup $\langle 3 \rangle$ of $\mathbb{Z}_7^*$ generated by 3.

   ▶ **Solution.** $\langle 3 \rangle = \{3,\ 3^2 = 2,\ 3^3 = 6,\ 3^4 = 4,\ 3^5 = 5,\ 3^6 = 1\}$ ◀

   (c) Show that $\mathbb{Z}_7^*$ is a cyclic group and give a generator of $\mathbb{Z}_7^*$.

   ▶ **Solution.** By part (b), $\mathbb{Z}_6^* = \langle 3 \rangle$ so $\mathbb{Z}_6^*$ is cyclic with generator 3. ◀

5. **[16 Points]**

   (a) State Lagrange's theorem.

   ▶ **Solution.** If G is a finite group and H is a subgroup, then $|H|\,|\,|G|$. ◀

   (b) Suppose that a finite group G has a subgroup of order 4 and and another of order 10 and assume that $|G| < 50$. What can you conclude about $|G|$? Justify your answer.

   ▶ **Solution.** If H is a subgroup of G of order 4 and K is a subgroup of G of order 10, then Lagrange's theorem implies that $4\,|\,|G|$ and $10\,|\,|G|$ so that $|G|$ is a common multiple of 4 and 10. Hence $|G|$ is a multiple of the least common multiple of 4 and 10, namely 20. Since $|G| < 50$, the only possibilities for $|G|$ are 20 and 40. ◀

6. **[15 Points]** Assume $H = \{u, v, w, x, y, z\}$ is a group with respect to multiplication and $\varphi : \mathbb{Z}_6 \to H$ is a group isomorphism with

$$\varphi([0]_6) = u, \quad \varphi([1]_6) = v, \quad \varphi([2]_6) = w,$$
$$\varphi([3]_6) = x, \quad \varphi([4]_6) = y, \quad \varphi([5]_6) = z.$$

Replace each of the following products by the appropriate element of H, i.e., either u, v, w, x, y, or z.

(a) Identity of H (b) xw (c) w^{-1} (d) w^5 (e) $zy^{-1}x$

► **Solution.** Note that the group operation on $\mathbb{Z}_6$ is addition of congruence classes modulo 6. Thus, the homomorphism property of φ is given by

$$\varphi([a]_6 + [b]_6) = \varphi([a]_6)\varphi([b]_6).$$

Then:

(a) The identity of $\mathbb{Z}_6$ is $[0]_6$ so the identity of H is $\varphi([0]_6) = u$.
(b) $xw = \varphi([3]_6)\varphi([2]_6) = \varphi([3]_6 + [2]_6) = \varphi([5]_6) = z$.
(c) $w^{-1} = (\varphi([2]_6))^{-1} = \varphi(-[2]_6) = \varphi([4]_6) = y$.
(d) $w^5 = (\varphi([2]_6))^5 = \varphi(5[2]_6) = \varphi([10]_6) = \varphi([4]_6) = y$.
(e) $zy^{-1}x = \varphi([5]_6)(\varphi([4]_6)^{-1}\varphi([3]_6) = \varphi([5]_6 - [4]_6 + [3]_6) = \varphi([4]_6) = y$.

◄

[Extra Credit Problem, 8 Points] Let p and q be distinct primes. Suppose that H is a proper subgroup of $\mathbb{Z}$ (i.e., $H \neq \mathbb{Z}$). Recall that the group operation is addition. Assume that H contains exactly three elements of the following set

$$\{p,\ p+q,\ pq,\ p^q,\ q^p\}\,.$$

Determine which of the following are the three elements in H.

(a) pq, p^q, q^p
(b) $p+q$, pq, p^q
(c) p, $p+q$, pq
(d) p, p^q, q^p
(e) p, pq, p^q

► **Solution.** If H contains two relatively prime integers a and b, then it also contains all integers of the form $na + mb$. But the set of all of these integers is $\mathbb{Z}$ since a and b are relatively prime. But $H \neq \mathbb{Z}$ so H cannot contain two relatively prime integers. Since p and q are distinct primes, the only set of 3 elements of the given set that does not contain two relatively prime integers is the set p, pq, p^q, all of which are multiples of the prime p. Thus, the correct answer is (e). ◄