Also, do the assigned HW problems. This is just in addition to HW.

ALWAYS JUSTIFY YOUR ANSWER!

Computations

1. Describe all group homomorphisms $\mathbb{Z}_{45} \to \mathbb{Z}_{10}$.
   Answer:

   - A homomorphism from a cyclic group is determined by the value on a generator.
   - $\mathbb{Z}_{45}$ is cyclic group. A generator of $\mathbb{Z}_{45}$ is 1. (There are other generators.)
   - To define homomorphism from $\mathbb{Z}_{45}$ it is enough to define on 1.
   - Order of $f(x)$ divides order of x, i.e. $|f(x)|$ divides $|x|$.
   - $|1| = 45$ in $\mathbb{Z}_{45}$. Therefore $|f(1)|$ must divide 45.
   - $f(1) \in \mathbb{Z}_{10}$. Therefore $|f(1)|$ must divide $|\mathbb{Z}_{10}| = 10$.
   - $|f(1)|$ divides 45 and 10. Therefore $|f(1)| = 1$ *or* 5.
   - Case 1: $|f(1)| = 1$ implies $f(1) = 0$ since $0 = e \in \mathbb{Z}_{10}$ is the only element of order 1. Then $f(x) = 0(mod 10)$ for all $x \in \mathbb{Z}_{45}$. Call this function f_1.

     $$f_1 : \mathbb{Z}_{45} \to \mathbb{Z}_{10} \text{ defined as } f_1(x) := 0(mod 10), \forall x \in \mathbb{Z}_{45}$$

     Case 2: $|f(1)| = 5$ implies $f(1) = 2, 4, 6, 8$.
     Reason: $10/5 = 2$, so $|2| = 5$.
     Numbers relatively prime to 5 are $\{1, 2, 3, 4\}$.
     Therefore elements of order 5 in $\mathbb{Z}_{10}$ are $\{2 \cdot 1, 2 \cdot 2, 2 \cdot 3, 2 \cdot 4\} = \{2, 4, 6, 8\}$. This defines the following functions:

     $$f_2 : \mathbb{Z}_{45} \to \mathbb{Z}_{10} \text{ defined as } f_2(x) := 2x(mod 10), \forall x \in \mathbb{Z}_{45}$$

     $$f_3 : \mathbb{Z}_{45} \to \mathbb{Z}_{10} \text{ defined as } f_3(x) := 4x(mod 10), \forall x \in \mathbb{Z}_{45}$$

     $$f_4 : \mathbb{Z}_{45} \to \mathbb{Z}_{10} \text{ defined as } f_4(x) := 6x(mod 10), \forall x \in \mathbb{Z}_{45}$$

     $$f_5 : \mathbb{Z}_{45} \to \mathbb{Z}_{10} \text{ defined as } f_5(x) := 8x(mod 10), \forall x \in \mathbb{Z}_{45}$$

     $\{f_1, f_2, f_3, f_4, f_5\}$ are all 5 different group homomorphisms $\mathbb{Z}_{45} \to \mathbb{Z}_{10}$.

2. Describe all group homomorphisms $\mathbb{Z}_{45} \to \mathbb{Z}_7$.
   Answer:

   - A homomorphism from a cyclic group is determined by the value on a generator.
   - $\mathbb{Z}_{45}$ is cyclic group. A generator of $\mathbb{Z}_{45}$ is 1. (There are other generators.)
   - To define homomorphism from $\mathbb{Z}_{45}$ it is enough to define on 1.
   - Order of $f(x)$ divides order of x, i.e. $|f(x)|$ divides $|x|$.
   - $|1| = 45$ in $\mathbb{Z}_{45}$. Therefore $|f(1)|$ must divide 45.
   - $f(1) \in \mathbb{Z}_7$. Therefore $|f(1)|$ must divide $|\mathbb{Z}_7| = 7$.
   - $|f(1)|$ divides 45 and 7. Therefore $|f(1)| = 1$.
   - $|f(1)| = 1$ implies $f(1) = 0$ since $0 = e \in \mathbb{Z}_7$ is the only element of order 1.
     Then $f(x) = 0(mod 7)$ for all $x \in \mathbb{Z}_{45}$. Call this function f_1.

   $$f_1 : \mathbb{Z}_{45} \to \mathbb{Z}_7 \text{ defined as } f_1(x) := 0(mod 7), \forall x \in \mathbb{Z}_{45}$$

   $\{f_1\}$ is the only group homomorphism $\mathbb{Z}_{45} \to \mathbb{Z}_7$.

3. Describe all group homomorphisms $\mathbb{Z}_2 \to \mathbb{Z}_4$.
   Answer:

   - A homomorphism from a cyclic group is determined by the value on a generator.
   - $\mathbb{Z}_2$ is cyclic group. A generator of $\mathbb{Z}_2$ is 1.
   - To define homomorphism from $\mathbb{Z}_2$ it is enough to define on 1.
   - Order of $f(x)$ divides order of x, i.e. $|f(x)|$ divides $|x|$.
   - $|1| = 2$ in $\mathbb{Z}_2$. Therefore $|f(1)|$ must divide 2. Therefore $|f(1)|$ is 1 or 2.
   - $f(1) \in \mathbb{Z}_4$.
   - Case 1: $|f(1)| = 1$ implies $f(1) = 0$ since $0 = e \in \mathbb{Z}_4$ is the only element of order 1.
     Then $f(x) = 0(mod 4)$ for all $x \in \mathbb{Z}_2$. Call this function f_1.

     $$f_1 : \mathbb{Z}_2 \to \mathbb{Z}_4 \text{ defined as } f_1(x) := 0 \ (mod \ 4), \forall x \in \mathbb{Z}_2$$

     Case 2: $|f(1)| = 2$ implies $f(1) = 2$ since $2 \in \mathbb{Z}_4$ is the only element of order 2.

     $$f_2 : \mathbb{Z}_2 \to \mathbb{Z}_4 \text{ defined as } f_2(x) := 2x \ (mod \ 4), \forall x \in \mathbb{Z}_2$$

     $\{f_1, f_2\}$ are the 2 different group homomorphisms $\mathbb{Z}_2 \to \mathbb{Z}_4$.

4. Describe all group homomorphisms $\mathbb{Z}_2 \to S_3$. Answer:

   - A homomorphism from a cyclic group is determined by the value on a generator.
   - $\mathbb{Z}_2$ is cyclic group. A generator of $\mathbb{Z}_2$ is 1.
   - To define homomorphism from $\mathbb{Z}_2$ it is enough to define on 1.
   - Order of $f(x)$ divides order of x, i.e. $|f(x)|$ divides $|x|$.
   - $|1| = 2$ in $\mathbb{Z}_2$. Therefore $|f(1)|$ must divide 2. Therefore $|f(1)|$ is 1 or 2.
   - $f(1) \in S_3$.
   - Case 1: $|f(1)| = 1$ implies $f(1) = (1)$ since $(1) = e \in S_3$ is the only element of order 1. Then $f(x) = (1) \in S_3$ for all $x \in \mathbb{Z}_2$. Call this function f_1.

   $$f_1 : \mathbb{Z}_2 \to S_3 \text{ defined as } f_1(x) := (1) \in S_3, \forall x \in \mathbb{Z}_2$$

   Case 2: $|f(1)| = 2$ implies $f(1) = (12)$ or $f(1) = (13)$ or $f(1) = (23)$ since these are the only elements of order 2 in S_3. This defines the following functions:

   $$f_2 : \mathbb{Z}_2 \to S_3 \text{ defined as } f_2(1) := (12),\ f_2(0) = (1)$$

   $$f_3 : \mathbb{Z}_2 \to S_3 \text{ defined as } f_3(1) := (13),\ f_3(0) = (1)$$

   $$f_4 : \mathbb{Z}_2 \to S_3 \text{ defined as } f_4(1) := (23),\ f_4(0) = (1)$$

   $\{f_1, f_2, f_3, f_4\}$ are all different group homomorphisms $\mathbb{Z}_2 \to S_3$.

5. Let $f : \mathbb{Z}_{18} \to \mathbb{Z}_{27}$ be given by $f(1) = 3$ and therefore $f(i) = 3i(mod 27)$.
   Answer:

   (a) Find $f(0) = 0(mod\ 27)$

   (b) Find $f(3) = 9(mod\ 27)$

   (c) Find $f(9) = 0(mod\ 27)$

   (d) Find $f(10) = 3(mod\ 27)$

   (e) Find $Im(f)$ Answer: $Im(f) = \{0, 3, 6, 9, 12, 15, 18, 21, 24\} = \langle 3 \rangle = 3\mathbb{Z}_{27}$ subgroup of $\mathbb{Z}_{27}$.

   (f) Find $Ker(f) = \{0, 9\} = \langle 9 \rangle = 9\mathbb{Z}_{18}$ subgroup of $\mathbb{Z}_{18}$.

   (g) Is f onto? Justify your answer.
   Answer: No, since $Im(f) \subset \mathbb{Z}_{18}$ but $Im(f) \neq \mathbb{Z}_{18}$. For example $1 \notin Im(f)$.

   (h) Is f one-to-one? Justify your answer.
   Answer: No, since $f(0) = 0 = f(9)$ but $0 \neq 9 \in \mathbb{Z}_{18}$.

6. Let $f : \mathbb{Z}_{45} \to \mathbb{Z}_{100}$ be given by $f(1) = 20$ and therefore $f(i) = 20i(mod100)$.
   Answer:

   (a) Find $f(0)$. Answer: $\boxed{0\ (mod\ 100)}$

   (b) Find $f(5)$. Answer: $\boxed{0\ (mod\ 100)}$

   (c) Find $f(30)$. Answer: $\boxed{0\ (mod\ 100)}$

   (d) Find $f(38)$. Answer: $\boxed{60\ (mod\ 100)}$

   (e) Find $Im(f)$.
   Answer: $Im(f) = \{0, 20, 40, 60, 80\} = \langle 20 \rangle = 20\mathbb{Z}_{100}$ subgroup of $\mathbb{Z}_{100}$.

   (f) Find $Ker(f)$=
   Answer: $Ker(f) = \{0, 5, 10, 15, 20, 25, 30, 35, 40\} = \langle 5 \rangle = 5\mathbb{Z}_{45}$ subgroup of $\mathbb{Z}_{45}$.

   (g) Is f onto? Justify your answer.
   Answer: No, since $Im(f) \subset \mathbb{Z}_{100}$ but $Im(f) \neq \mathbb{Z}_{100}$. For example $1 \notin Im(f)$.

   (h) Is f one-to-one? Justify your answer.
   Answer: No, since $f(0) = 0 = f(5)$ but $0 \neq 5 \in \mathbb{Z}_{45}$.

7. Let $f : \mathbb{Z}_6 \to S_4$ be given by $f(1) = (124)$.

   (a) Find $f(0)$. Answer: $f(0) = e_{S_4} = (1)$. Therefore $\boxed{f(0) = (1)}$

   (b) Find $f(2)$. Answer: $f(2) = f(1)f(1) = (124)(124) = (142)$. Therefore $\boxed{f(2) = (142)}$

   (c) Find $f(3)$. Answer: $f(3) = f(1)f(2) = (124)(142) = (1)$. Therefore $\boxed{f(3) = (1)}$

   (d) Find $f(4)$. Answer: $f(4) = f(1)f(3) = (124)(1) = (124)$. Therefore $\boxed{f(4) = (124)}$

   (e) Find $f(5)$. Answer: $f(5) = f(1)f(4) = (124)(124) = (142)$. Therefore $\boxed{f(5) = (142)}$

   (f) Find $Im(f)$
   Answer: $Im(f) = \{(1), (124), (142)\} = \langle (124) \rangle$ subgroup of S_4.

   (g) Find $Ker(f)$
   Answer: $Ker(f) = \{0, 3\} = \langle 3 \rangle = 3\mathbb{Z}_6$ subgroup of $\mathbb{Z}_6$.

   (h) Is f onto? Justify your answer.
   Answer: No, since $Im(f) \subset S_4$ but $Im(f) \neq S_4$. For example $(12) \notin Im(f)$.

   (i) Is f one-to-one? Justify your answer.
   Answer: No, since $f(2) = (142) = f(5)$ but $2 \neq 5 \in \mathbb{Z}_6$.

8. Let $G = \mathbb{Z}_{12}$.

   (a) Find the subgroup $H = \langle 3 \rangle$.
   Answer: $H = \langle 3 \rangle = \{0, 3, 6, 9\}$

   (b) Find all left cosets of H in G.
   Answer: $H = \langle 3 \rangle = \{0, 3, 6, 9\}$
   $1 + H = 1 + \langle 3 \rangle = \{1, 4, 7, 10\}$
   $2 + H = 2 + \langle 3 \rangle = \{2, 5, 8, 11\}$

   (c) Find all right cosets of H in G.
   Answer: $H = \langle 3 \rangle = \{0, 3, 6, 9\}$
   $H + 1 = \langle 3 \rangle + 1 = \{1, 4, 7, 10\}$
   $H + 2 = \langle 3 \rangle + 2 = \{2, 5, 8, 11\}$

   (d) Is H normal subgroup of G?
   Answer: Yes, since $a + H = H + a$ for all $a \in G$.

   (e) Find G/H.
   Answer: $G/H = \{\langle 3 \rangle, 1 + \langle 3 \rangle, 2 + \langle 3 \rangle\}$
   Cayley Table:

   (f) Find $[G : H]$.
   Answer: $[G : H] = \#$ of left cosets $= 3$.
   Another way: $[G : H] = |G|/|H| = |\mathbb{Z}_{12}|/|\langle 3 \rangle| = 12/4 = 3$. Therefore $[G : H] = 3$.

9. Let $G = S_4$.

   (a) Find the subgroup $H = \langle (1342) \rangle$.
   Answer: $H = \langle (1342) \rangle = \{(1342), (14)(32), (2431), (1)\}$

   (b) Find all left cosets of H in G.
   Answer: $H = \langle (1342) \rangle = \{(1342), (14)(32), (2431), (1)\}$
   $(12)H = (12)\langle (1342) \rangle = \{(12)(1342), (12)(14)(32), (12)(2431), (12)(1)\} = \{(134), (1423), (243), (12)\}$
   $(13)H = (13)\langle (1342) \rangle = \{(13)(1342), (13)(14)(32), (13)(2431), (13)(1)\} = \{(234), (1432), (124), (13)\}$
   $(14)H = (14)\langle (1342) \rangle = \{(14)(1342), (14)(14)(32), (14)(2431), (14)(1)\} = ...$
   $(24)H = (24)\langle (1342) \rangle = \{(24)(1342), (24)(14)(32), (24)(2431), (24)(1)\} = ...$
   $(34)H = (34)\langle (1342) \rangle = \{(34)(1342), (34)(14)(32), (34)(2431), (34)(1)\} = ...$

   (c) Find all right cosets of H in G.
   Answer: $H = \langle (1342) \rangle = \{(1342), (14)(32), (2431), (1)\}$
   $H(12) = \langle (1342) \rangle (12) = \{(1342)(12), (14)(32)(12), (2431)(12), (1)(12)\} = \{(234), (1324), (143), (12)\}$
   $H(13) = ...$
   $H(14) = ...$
   $H(24) = ...$
   $H(34) = ...$

(d) Is H normal subgroup of G?
<u>Answer:</u> NO, since
$(12)H = \{(134), (1423), (243), (12)\} \neq \{(234), (1324), (143), (12)\} = H(12)$

(e) Find $[G : H]$.
<u>Answer:</u> $[G : H] = \#$ of left cosets of H. Therefore $[G : H] = 6$
Another way: $[G : H] = |G|/|H| = |S_4|/|\langle(1342)\rangle| = 24/4 = 6$.

10. Let $G = S_4$.

(a) Find the subgroup A_4 of even permutations.
<u>Answer:</u>
$G = S_4 = \{(1234), (1243), (1324), (1342), (1423), (1432),$
$(123), (132), (124), (142), (134), (143), (234), (243),$
$(12)(34), (13)(24), (14)(23), (12), (13), (14), (23), (24), (34), (1)\}$,
A_4 is the subgroup of all even permutations:
$\boxed{A_4 = \{(123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23), (1)\}}$

(b) Find all left cosets of A_4 in G.
<u>Answer:</u>
$A_4 = \{(123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23), (1)\}$
$(12)A_4 = \{(12)(123), (12)(132), (12)(124), (12)(142), (12)(134), (12)(143), (12)(234), (12)(243),$
$(12)(12)(34), (12)(13)(24), (12)(14)(23), (12)(1)\} =$
$\{(23), (13), (24), (14), (1342), (1432), (1234), (1243), (34), (1324), (1423), (12)\}$
$(12)A_4$ are all odd permutations.
Left cosets: $\{A_4, (12)A_4\}$, i.e.
$\boxed{A_4 = \{(123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23), (1)\}}$
$\boxed{(12)A_4 = \{(23), (13), (24), (14), (1342), (1432), (1234), (1243), (34), (1324), (1423), (12)\}}$

(c) Find all right cosets of A_4 in G.
<u>Answer:</u>
Right cosets: $\{A_4, A_4(12)\}$: A_4 are all even permutations, $A_4(12)$ are all odd permutations. $\boxed{A_4 = \{(123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23), (1)\}}$
$\boxed{A_4(12) = \{(23), (13), (24), (14), (1342), (1432), (1234), (1243), (34), (1324), (1423), (12)\}}$

(d) Is A_4 normal subgroup of G?
<u>Answer:</u> Check if $\alpha A_4 = A_4\alpha$ for all $\alpha \in S_4$.
Case 1: α is even permutation.
So $\alpha \in A_4$. Therefore $\alpha A_4 = A_4$ (true in general $hH = H$ for $\forall h \in H$, see problem #22).
Similarly $A_4\alpha = A_4$. Therefore $\alpha A_4 = A_4\alpha$ for all $\alpha in A_4$, i.e. α even permutation.
Case 2: α is odd permutation.
Then $\alpha A_4 = \{$odd permutations$\}$ since (odd permut.)(even permut.)=(odd permut.).
Also $A_4\alpha = \{$odd permutations$\}$ since (even permut.)(odd permut.)=(odd permut.).
Therefore $\alpha A_4 = A_4\alpha$ for all odd permutations α.

Case 1 and Case 2 $\implies \alpha A_4 = A_4\alpha$ for all $\alpha \in S_4$.
Therefore A_4 is normal subgroup in S_4.
Remark: Another argument: Since $|A_4| = 12 = 24/2 = |S_4|/2$ it follows from a Theorem from class that A_4 is normal subgroup in S_4.

(e) Find G/H.
Answer: Elements of G/H are $\{A_4, (12)A_4\}$ and Cayley table is:

S_4/A_4	A_4	$(12)A_4$
A_4	A_4	$(12)A_4$
$(12)A_4$	$(12)A_4$	A_4

(f) Find $[G:H]$. Answer: $\boxed{[G:H] = |G|/|H| = 24/12 = 2}$

11. Consider the group $\mathbb{Z}_{15}^{\times}$.

(a) Find the subgroup $H = \langle 2\rangle$
Answer: $\mathbb{Z}_{15}^{\times} = \{x \in \mathbb{Z} \mid 1 \le x \le 14,\ gcd(x,15) = 1\} = \{1,2,4,7,8,11,13,14\}$
$H = \langle 2\rangle = \{2,4,8,1\}$

(b) Find all left cosets of H in G.
Answer:
$H = \langle 2\rangle = \{2,4,8,1\}$
$7H = 7\langle 2\rangle = \{7\cdot 2, 7\cdot 4, 7\cdot 8, 7\cdot 1\} = \{14,13,11,7\}$
$\boxed{(\text{left cosets of } \langle 2\rangle \text{ in } \mathbb{Z}_{15}^{\times}) = \{\langle 2\rangle, 7\langle 2\rangle\} = \{\{2,4,8,1\},\{14,13,11,7\}\}}$

(c) Find all right cosets of H in G.
Answer:
$H = \langle 2\rangle = \{2,4,8,1\}$
$H = \langle 2\rangle 7 = \{2\cdot 7, 4\cdot 7, 8\cdot 7, 1\cdot 7\} = \{14,13,11,7\}$
$\boxed{(\text{right cosets of } \langle 2\rangle \text{ in } \mathbb{Z}_{15}^{\times}) = \{\langle 2\rangle, \langle 2\rangle 7\} = \{\{2,4,8,1\},\{14,13,11,7\}\}}$
Remark: You could also point out that the group $\mathbb{Z}_{15}^{\times}$ is abelian, so left cosets are the same as right cosets.

(d) Is H normal subgroup of G?
Answer: Yes, since left cosets are the same as right cosets.
Another answer: Yes. Since $\mathbb{Z}_{15}^{\times}$ is abelian all subgroups are normal in $\mathbb{Z}_{15}^{\times}$.

(e) Find G/H.
Answer: Elements of G/H are $\{\langle 2\rangle, 7\langle 2\rangle\}$ and Cayley table is:

$\mathbb{Z}_{15}^{\times}/\langle 2\rangle$	$\langle 2\rangle$	$7\langle 2\rangle$
$\langle 2\rangle$	$\langle 2\rangle$	$7\langle 2\rangle$
$7\langle 2\rangle$	$7\langle 2\rangle$	$\langle 2\rangle$

(f) Find $[G:H]$. Answer: $\boxed{[G:H] = |G|/|H| = 8/4 = 2}$

Theoretic Questions

12. Write the definition of *Normal Subgroup.*
13. Write the definition of *Left coset.*
14. Write the definition of *Subgroup.*
15. Write the definition of *Quotient group.*
16. Write the definition of *Kernel of a homomorphism.*

Proofs

17. Let $f : G \to G'$ be a group homomorphism. Prove that $f(e_G) = e_{G'}$.

Proof. (a) $e_G = e_G \cdot e_G$ since e_G is the identity in G.

(b) $f(e_G) = f(e_G \cdot e_G) = f(e_G) \cdot f(e_G)$ since f is a group homomorphism. So

(c) $f(e_G) = f(e_G) \cdot f(e_G)$ Now multiply both sides by the inverse $(f(e_G))^{-1}$, on the right.

(d) $f(e_G) \cdot (f(e_G))^{-1} = f(e_G) \cdot f(e_G) \cdot (f(e_G))^{-1}$

(e) $f(e_G) \cdot (f(e_G))^{-1} = e_{G'}$ by the property of inverse in G'.

(f) $f(e_G) \cdot f(e_G) \cdot (f(e_G))^{-1} = f(e_G) \cdot e_{G'} = f(e_G)$ Therefore:

(g) $e_{G'} \overset{\text{(e)}}{=} f(e_G) \cdot (f(e_G))^{-1} \overset{\text{(d)}}{=} f(e_G) \cdot f(e_G) \cdot (f(e_G))^{-1} \overset{\text{(f)}}{=} f(e_G)$. Therefore:

(h) $e_{G'} = f(e_G)$.

(Notice how many times you use transitive and symmetric property of "=" and associative property of the operation in groups!) □

18. Let $f : G \to G'$ be a group homomorphism. Let $g \in G$. Prove that $|f(g)|$ divides $|g|$.

Proof.
- Let $|g| = n$ and $|f(g)| = m$.
- Since $|g| = n$ it follows that $g^n = e_G$. Apply f to both sides.
- $f(g^n) = f(e_G) = e_{G'}$ from the fact that $f(e_G) = e_{G'}$ (proved in the previous problem).
- $f(g^n) = (f(g))^n$ from the property of group homomorphisms.
- $(f(g))^n = e_{G'}$ from the last two equality.
- Then $m|n$ - proved in class (If $a^m = e$ then $|a|$ divides m.) Therefore:
- $|f(g)|$ divides $|g|$.

□

19. Let $f : G \to G'$ be a homomorphism. Prove that $Im(f)$, the image of f is a subgroup of G'.

Proof.
- By definition $Im(f) := \{a \in G' \mid \exists x \in G, s.t.\ f(x) = a\}$.
- (0) $Im(f) \subseteq G'$ since every $a \in Im(f)$ by definition $a \in G'$, i.e. $Im(f)$ is a subset of G'.
- (00) $Im(f) \neq \emptyset$ since $f(e_G) = e_{G'}$ and therefore $e_{G'} \in Im(f)$, i.e. $Im(f)$ is nonempty.
- (1) Let $a, b \in Im(f)$. WTS $ab \in Im(f)$, i.e. $Im(f)$ is closed under operation in G'.
  $(a \in Im(f)) \implies (\exists x \in G$ such that $f(x) = a)$
  $(b \in Im(f)) \implies (\exists y \in G$ such that $f(y) = b)$
  $(x, y, \in G) \implies (xy \in G)$ since G is a group and therefore closed under operation.
  $f(xy) = f(x)f(y)$ since f is a group homomorphism. So: $f(xy) = f(x)f(y) = ab$.
  Therefore $ab \in Im(f)$, i.e. $Im(f)$ is closed under operation in G'.

- (2) Let $a \in Im(f)$. WTS $a^{-1} \in Im(f)$, i.e. $Im(f)$ is closed under inverses in G'.
  $(a \in Im(f)) \implies (\exists x \in G \text{ such that } f(x) = a)$
  $(x \in G) \implies (x^{-1} \in G)$ since G is a group and therefore closed under inverses.
  $f(x^{-1}) = (f(x))^{-1}$ since f is a group homomorphism. So: $f(x^{-1}) = (f(x))^{-1} = a^{-1}$.
  Therefore $a^{-1} \in Im(f)$, i.e. $Im(f)$ is closed under inverses in G'.
- Therefore, from (0), (00), (1), (2) it follows that $Im(f)$ is a nonempty subset of G' which is closed under operations and inverses in G'. Therefore $Im(f)$ is a subgroup of G'.

$\square$

20. Let $f : G \to G'$ be a homomorphism. Prove that $Ker(f)$, the kernel of f is a subgroup of G.
21. Let $f : G \to G'$ be a homomorphism. Prove that $Ker(f)$ is normal subgroup of G.
22. Let H be a subgroup of group G. Prove that $(aH = H) \iff (a \in H)$.

Proof. $(aH = H) \implies (a \in H)$

- Suppose $(aH = H)$. WTS $(a \in H)$
- $a = ae$ where e is the identity in G.
- Since H is a subgroup, $e \in H$. Therefore $a = ae \in aH$.
- Since $aH = H$, this implies $a \in H$.

$(aH = H) \Longleftarrow (a \in H)$

- Suppose $(a \in H)$. WTS $(aH = H)$
- Let $x \in aH$. Then $\exists h \in H$ so that $x = ah$.
- Since H is a subgroup, it is closed under operation.
- Since both $a, h \in H$, it follows that $ah \in H$. $\therefore x = ah \in H$ $\therefore (aH \subseteq H)$
- Let $x \in H$. Then $x = ex = (aa^{-1})x = a(a^{-1})x) \in aH$ since H is closed under inverses and operations (since H is a subgroup). $\therefore (H \subseteq aH)$ $\therefore (H = aH)$

$\square$

23. Let H be a subgroup of group G. Let $a \in G$ and let $aHa^{-1} = \{aha^{-1} \mid h \in H\}$. Prove that aHa^{-1} is a subgroup of G.

Proof.
- (0) aHa^{-1} is a subset of G.
  Reason: $(x \in aHa^{-1}) \implies (x = aha^{-1})$ for some $h \in H \subseteq G$.
  Therefore $aha^{-1} \in G$ since G is closed under inverses and operations (G is a group).
  $\implies x \in G$ So $aHa^{-1} \subseteq G$.
- $aHa^{-1} \neq \emptyset$. Reason: $e = aea^{-1} \in aHa^{-1}$.

- (1) aHa^{-1} is closed under operation in G.
  Reason: Let $x, y \in aHa^{-1}$. WTS $xy \in aHa^{-1}$.
  – $(x \in aHa^{-1}) \implies (x = aha^{-1}$ for some $h \in H)$
  – $(y \in aHa^{-1}) \implies (y = aka^{-1}$ for some $k \in H)$
  – $xy = (aha^{-1})(aka^{-1}) = ah(a^{-1}a)ka^{-1} = aheka^{-1} = ahka^{-1} \in aHa^{-1}$ since $h, k \in H$
  – and H is closed under operation in G (since H is a subgroup of G)
  – $xy \in aHa^{-1}$
- (2) aHa^{-1} is closed under inverses in G.
  Reason: Let $x \in aHa^{-1}$. WTS $x^{-1} \in aHa^{-1}$.
  – $(x \in aHa^{-1}) \implies (x = aha^{-1}$ for some $h \in H)$
  – $x^{-1} = (aha^{-1})^{-1} = (a^{-1})^{-1}h^{-1}a^{-1}$ by the property of inverse of a product.
  –$(a^{-1})^{-1}h^{-1}a^{-1} = ah^{-1}a^{-1} \in aHa^{-1}$ since $h \in H$ and H is closed under inverses in G (since H is a subgroup of G).
  – $x^{-1} \in aHa^{-1}$.
- Therefore, from (0), (00), (1), (2) it follows that aHa^{-1} is a nonempty subset of G which is closed under operations and inverses in G. Therefore aHa^{-1} is a subgroup of G.

□

24. Prove that the center of a group is normal subgroup, i.e. $Z(G)$ is normal subgroup in G.

Proof. $Z(G) := \{g \in G \mid xg = gx \text{ for } \forall x \in G\}$
Claim 1: $Z(G)$ is a subgroup of G.
Claim 2: $Z(G)$ is normal subgroup of G.
Proof of Claim 1:

- (0) $Z(G)$ is a subset of G by definition.
- (00) $Z(G)$ is nonempty. Reason: $(xe = x = ex$ for $\forall x \in G) \implies$ the identity $e \in Z(G)$.
- (1) $Z(G)$ is closed under operation in G. Reason:
  – Let $a, b \in Z(G)$. Then $xa = ax$ for $\forall x \in G$ (*) and $xb = bx$ for $\forall x \in G$ (**).
  – $x(ab) \overset{\text{assoc}}{=} (xa)b \overset{(*)}{=} (ax)b \overset{\text{assoc}}{=} a(xb) \overset{(**)}{=} a(bx) \overset{\text{assoc}}{=} (ab)x$ for $\forall x \in G$. Therefore:
  – $ab \in Z(G)$.
- (2) $Z(G)$ is closed under inverses in G. Reason:
  – Let $a \in Z(G)$. Then $xa = ax$ for $\forall x \in G$ (*).
  – Multiply this equation by a^{-1} on the left.
  – $a^{-1}xa = a^{-1}ax$
  – $a^{-1}xa = x$
  – Multiply this equation by a^{-1} on the right.
  – $a^{-1}xaa^{-1} = xa^{-1}$. Therefore: $a^{-1}x = xa^{-1}$. Therefore:
  – $a^{-1} \in Z(G)$.
- It follows from (0), (00), (1), (2) that $Z(G)$ is a subgroup of G.
  Proof of Claim 2:

- WTS $gZ(G)g^{-1} \subseteq Z(G)$ for $\forall g \in G$ i.e.
- WTS $gzg^{-1} \in Z(G)$ for $\forall z \in Z(G)$ and $\forall g \in G$.
- $gzg^{-1} \overset{\text{Z(G)}}{=} zgg^{-1} \overset{\text{inverse}}{=} z \in Z(G)$.
- Therefore $gZ(G)g^{-1} \subseteq Z(G)$ and hence $Z(G)$ is a normal subgroup.

$\square$

True -False - Sometimes

25. True -False - Sometimes

T $\boxed{F}$ S - $\mathbb{Z}_n^\times$ is a subgroup of $\mathbb{Z}_n$.

$\boxed{T}$ F S - Let $G = (\mathbb{Z}_n, +_n)$, let H be a subgroup of G. Then H is normal subgroup.

T F $\boxed{S}$ - Let $G = S_7$, let H be a subgroup of G. Then H is normal subgroup.

T F $\boxed{S}$ - Let H be a subgroup of G. Let $a \in G$. Then $aH = Ha$.

$\boxed{T}$ F S - $(2\mathbb{Z}, +)$ is a normal subgroup of $(\mathbb{Z}, +)$.

$\boxed{T}$ F S - $\langle 6 \rangle$ is a normal subgroup of $(\mathbb{Z}_9, +_9)$

T F $\boxed{S}$ - Let H be a proper subgroup of S_3. Then H is normal subgroup.

T $\boxed{F}$ S - All proper subgroups of S_4 are normal.

T $\boxed{F}$ S - Let G be a group of order $|G| = 5$. Let $H < G$. Then $|H| = 4$.

T F $\boxed{S}$ - Let G be a group of order $|G| = 5$. Let $H < G$. Then $|H| = 1$.

T F $\boxed{S}$ - Let G be a group of order $|G| = 15$. Let $H < G$. Then $[G : H] = 5$.

T $\boxed{F}$ S - Let G be a cyclic group of order $|G| = 15$. Let $H < G$. Then $|H| = 10$.

T F $\boxed{S}$ - Let G be a group. Let $g \in G$. Then $\langle g \rangle$ is normal subgroup.

Examples

26. Give an example of a group and a subgroup which is not normal. Prove your statement.
<u>Answer:</u>

- $G = S_4$, $H = \langle (1423) \rangle$, proofs are missing.
- $G = S_4$, $H = \{(12)(34), (1)\}$, proofs are missing.
- $G = S_4$, $H = \{(123), (132), (12), (13), (23), (1)\}$, proofs are missing.
- $G = Gl_2(\mathbb{Q})$, $H = \{D \in Gl_2(\mathbb{Q}) \mid D \text{ is diagonal}\}$, proofs are missing.

27. Give an example of a group and a subgroup which is normal. Prove your statement.
<u>Answer:</u>

- $G = S_4$, $H = A_4$, proofs are missing.
- $G = S_4$, $H = \{(12)(34), (13)(24), (14)(23), (1)\}$, proofs are missing.
- $G = \mathbb{Z}_{50}$, $H = \langle 8 \rangle$, proofs are missing.
- $G = \mathbb{Z}_8$, $H = \langle 4 \rangle$, proofs are missing.
- $G = \mathbb{Z}_8^\times$, $H = \langle 3 \rangle$, proofs are missing.

28. Give an example of a non cyclic group and a subgroup which is normal. Prove your statement.
Answer:

- $G = S_4$, $H = A_4$, proofs are missing.
- $G = S_4$, $H = \{(12)(34), (13)(24), (14)(23), (1)\}$, proofs are missing.
- $G = \mathbb{Q}$, $H = \mathbb{Z}$, proofs are missing.

29. Give an example of a group homomorphism which is onto. Prove your statement.
Answer:

- $f : \mathbb{Z} \to \mathbb{Z}_9$, $f(x) = x(mod\ 9)$, proofs are missing.
- $f : \mathbb{Z}_{27} \to \mathbb{Z}_9$, $f(x) = x(mod\ 9)$, proofs are missing.
- $f : \mathbb{Z}_{27} \to \mathbb{Z}_9$, $f(x) = 4x(mod\ 9)$, proofs are missing.

30. Give an example of a group homomorphism which is not onto. Prove your statement.
Answer:

- $f : \mathbb{Z} \to \mathbb{Z}_9$, $f(x) = 3x(mod\ 9)$, proofs are missing.
- $f : \mathbb{Z}_{27} \to \mathbb{Z}_9$, $f(x) = 3x(mod\ 9)$, proofs are missing.
- $f : \mathbb{Z}_{27} \to \mathbb{Z}_9$, $f(x) = 6x(mod\ 9)$, proofs are missing.
- $f : S_3 \to S_4$ where $f(\alpha) = \alpha$. (It is actually $\alpha(4)$), proofs are missing.

31. Give an example of a group homomorphism which is one-to-one. Prove your statement.
Answer:

- $f : \mathbb{Z} \to \mathbb{Z}$, $f(x) = 3x$, proofs are missing.
- $f : \mathbb{Z}_{27} \to \mathbb{Z}_{54}$, $f(x) = 2x(mod\ 54)$, proofs are missing.
- $f : \mathbb{Z}_{27} \to \mathbb{Z}_{54}$, $f(x) = 4x(mod\ 54)$, proofs are missing.
- $f : \mathbb{Z}_{27} \to \mathbb{Z}_{54}$, $f(x) = 50x(mod\ 54)$, proofs are missing.
- $f : S_3 \to S_4$ where $f(\alpha) = \alpha$. (It is actually $\alpha(4)$), proofs are missing.

32. Give an example of a group homomorphism $f : G \to G'$ such that $Ker(f) = \{e_G\}$. Prove your statement.
Answer:

- $f : \mathbb{Z} \to \mathbb{Z}$, $f(x) = 3x$, proofs are missing.
- $f : \mathbb{Z}_{27} \to \mathbb{Z}_{54}$, $f(x) = 2x(mod\ 54)$, proofs are missing.
- $f : \mathbb{Z}_{27} \to \mathbb{Z}_{54}$, $f(x) = 4x(mod\ 54)$, proofs are missing.
- $f : \mathbb{Z}_{27} \to \mathbb{Z}_{54}$, $f(x) = 50x(mod\ 54)$, proofs are missing.

33. Give an example of a group homomorphism $f : G \to G'$ such that $Ker(f) \neq \{e_G\}$. Prove your statement.
Answer:

- $f : \mathbb{Z} \to \mathbb{Z}_5$, $f(x) = 3x$, proofs are missing.
- $f : \mathbb{Z}_{27} \to \mathbb{Z}_{54}$, $f(x) = 6x(mod\ 54)$, proofs are missing.
- $f : \mathbb{Z}_{27} \to \mathbb{Z}_{54}$, $f(x) = 30x(mod\ 54)$, proofs are missing.
- $f : \mathbb{Z}_{27} \to \mathbb{Z}_{54}$, $f(x) = 24x(mod\ 54)$, proofs are missing.

34. Give an example of a group G and a subgroup H such that $[G : H] = 3$.
Answer:

- $G = S_3$, $H = (12)$, proofs are missing.
- $G = \mathbb{Z}_{51}$, $H = \langle 17 \rangle$, proofs are missing.
- $G = \mathbb{Z}_9^\times$, $H = \langle 8 \rangle$, proofs are missing.
- $G = \mathbb{Z}_8 \times \mathbb{Z}_3$, $H = \{(a, 0) \mid a \in \mathbb{Z}_8, 0 \in \mathbb{Z}_3\}$, proofs are missing.

35. Give an example of a group G and a subgroup H such that $[G : H] = 2$.
Answer:

- $G = S_3$, $H = (123)$, proofs are missing.
- $G = \mathbb{Z}_{50}$, $H = \langle 2 \rangle$, proofs are missing.
- $G = \mathbb{Z}_9^\times$, $H = \langle 4 \rangle$, proofs are missing.
- $G = \mathbb{Z}_8 \times \mathbb{Z}_2$, $H = \{(a, 0) \mid a \in \mathbb{Z}_8, 0 \in \mathbb{Z}_2\}$, proofs are missing.