CHAPTER 1 HW

Sam Chyau
Math 540A

Sec 1.1 #5, 8, 11, 12, 25, 28

5.) Prove: $\langle \mathbb{Z}_n, \cdot \rangle$ is NOT a Group if $n > 1$.

Pf: Assume $n>1$. Let $\bar{a} \in \mathbb{Z}_n$

$\Rightarrow \bar{0} \neq \bar{1}$ in $\mathbb{Z}_n$

$\Rightarrow \bar{0} \cdot \bar{a} = \bar{0} \neq \bar{1}$

$\Rightarrow \bar{0}$ has no multiplicative inverse in $\mathbb{Z}_n$

$\therefore \langle \mathbb{Z}_n, \cdot \rangle$ is NOT a group. ▨

8.) Let $G = \{ z \in \mathbb{C} : z^n = 1 \text{ f.s. } n \in \mathbb{Z}^+ \}$ NOTE: $G \subseteq \mathbb{C}^*$

a.) Prove: $\langle G, \cdot \rangle$ is a Group.

Pf: a.) Let $x, y \in G$

$\Rightarrow x^n = 1 \wedge y^n = 1$

$\Rightarrow (xy)^n = x^n y^n = (1)(1) = 1$, since $\langle \mathbb{C}^*, \cdot \rangle$ is Abelian.

$\Rightarrow xy \in G$

b.) G is Associative, since $\langle \mathbb{C}^*, \cdot \rangle$ is Associative.

c.) $1^n = 1$, so $1 \in G$

d.) Let $x \in G$

$\Rightarrow x^n = 1$

$\Rightarrow (x^{-1})^n = \left(\frac{1}{x}\right)^n = \frac{1}{x^n} = \frac{1}{1} = 1$, so $x^{-1} \in G$

$\therefore \langle G, \cdot \rangle$ is a Group ▨

b.) Prove: $\langle G, + \rangle$ is NOT a Group.

Pf: $0^n = 0 \neq 1$

$\Rightarrow 0 \notin G$

$\therefore \langle G, + \rangle$ is NOT a group, since it has no additive identity. ▨

11.) Find the order of each element of $\mathbb{Z}_{12}$. RECALL: $|\bar{a}| = \frac{n}{\gcd(a,n)}$

$\lvert\bar{0}\rvert = 1$	$\lvert\bar{3}\rvert = 4$	$\lvert\bar{6}\rvert = 2$	$\lvert\bar{9}\rvert = 4$
$\lvert\bar{1}\rvert = 12$	$\lvert\bar{4}\rvert = 3$	$\lvert\bar{7}\rvert = 12$	$\lvert\overline{10}\rvert = 6$
$\lvert\bar{2}\rvert = 6$	$\lvert\bar{5}\rvert = 12$	$\lvert\bar{8}\rvert = 3$	$\lvert\overline{11}\rvert = 12$

12.) Find the order of the following elements of $\mathbb{Z}_{12}^{\times}$.

$|\bar{1}| = 1$

$|\overline{-1}| = 2$, since $(\overline{-1})^2 = \bar{1}$

$|\bar{5}| = 2$, since $(\bar{5})^2 = \overline{25} = \bar{1}$

$|\bar{7}| = 2$, since $(\bar{7})^2 = \overline{49} = \bar{1}$

$|\overline{-7}| = |\bar{5}| = 2$

$|\overline{13}| = |\bar{1}| = 1$

25) <u>Prove</u>: If $x^2 = 1_G \ \forall \ x \in G$, then G is Abelian.

<u>Pf</u>: Assume $x^2 = 1_G \ \forall \ x \in G$. Let $x, y \in G$

$\Rightarrow x^2 = 1_G \wedge y^2 = 1_G \wedge yx \in G$

$\Rightarrow (yx)^2 = 1_G$

$\Rightarrow xy = xy(yx)^2 = (xy)(yx)(yx) = xy^2xyx = x^2yx = yx$

$\therefore$ G is Abelian ▨

28) <u>Prove</u>: If $\langle A, * \rangle, \langle B, \diamond \rangle$ are groups, then $A \times B$ is a group.

<u>Pf</u>: Let $\langle A, * \rangle, \langle B, \diamond \rangle$ be Groups

a.) Let $(a_1, b_1), (a_2, b_2) \in A \times B$

$\Rightarrow (a_1, b_1)(a_2, b_2) = (a_1 * a_2, b_1 \diamond b_2) \in A \times B$

b.) Let $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in A \times B$

$\Rightarrow [(a_1, b_1)(a_2, b_2)](a_3, b_3) = (a_1 * a_2, b_1 \diamond b_2)(a_3, b_3)$

$= ((a_1 * a_2) * a_3, (b_1 \diamond b_2) \diamond b_3) = (a_1 * (a_2 * a_3), b_1 \diamond (b_2 \diamond b_3))$

$= (a_1, b_1)(a_2 * a_3, b_2 \diamond b_3) = (a_1, b_1)[(a_2, b_2)(a_3, b_3)]$

c.) $(1_A, 1_B) \in A \times B$, since $1_A \in A \wedge 1_B \in B$

d.) Let $(a, b) \in A \times B$

$\Rightarrow (a, b)^{-1} = (a^{-1}, b^{-1}) \in A \times B$

$\therefore A \times B$ is a Group ▨

Sam Chyau
Math 540A

Sec 1.2 # 1bc, 4, + A, B, C

1.) Compute the order of each element in D_8 & D_{10}.

D_8:

$\|1\| = 1$	$\|s\| = 2$
$\|r\| = 4$	$\|sr\| = 2$
$\|r^2\| = 2$	$\|sr^2\| = 2$
$\|r^3\| = 4$	$\|sr^3\| = 2$

D_{10}:

$\|1\| = 1$	$\|s\| = 2$
$\|r\| = 5$	$\|sr\| = 2$
$\|r^2\| = 5$	$\|sr^2\| = 2$
$\|r^3\| = 5$	$\|sr^3\| = 2$
$\|r^4\| = 5$	$\|sr^4\| = 2$

4.) Prove: If $n=2k$ $(n\geq 4)$, then r^k is the only non-identity element which commutes w/ ALL elements of D_{2n}.

Pf: Let $n=2k$ $(n\geq 4)$.

a.) By definition, $1\sigma 1^{-1} = \sigma \ \forall \sigma \in D_{2n}$
$\Rightarrow 1$ commutes w/ all elements of D_{2n}

b.) Let $1 \leq i \leq n-1$, where $i \neq k$
$\Rightarrow r^{2i} \neq 1$, since $2i \neq n$
$\Rightarrow (r^i)(s)(r^i)^{-1} = r^i s r^{-i} = r^{2i}s \neq s$
$\Rightarrow r^i$ doesn't commute w/ s if $i \neq k$

c.) Let $0 \leq i \leq n-1$
$\Rightarrow (sr^i)(r)(sr^i)^{-1} = sr^{i+1}sr^i = s^2r^{-i-1+i} = r^{-1} \neq r$, since $n \geq 4$
$\Rightarrow sr^i$ doesn't commute w/ r

d.) Let $0 \leq i \leq n-1$
1.) $(r^k)(r^i)(r^k)^{-1} = r^k r^i r^{-k} = r^{k+i-k} = r^i$
2.) $(r^k)(sr^i)(r^k)^{-1} = r^k s r^i r^{-k} = sr^{-k}r^{i-k} = s\,r^{i-2k} = sr^{i-n} = sr^i$
$\therefore r^k$ commutes w/ every element of D_{2n}

$\therefore$ By exhaustion, r^k is the ONLY non-identity element that commutes w/ every element of D_{2n}. ▨

A.) Compute the group tables of D_6 & D_8:

D_6	1	r	r^2	s	sr	sr^2
1	1	r	r^2	s	sr	sr^2
r	r	r^2	1	sr^2	s	sr
r^2	r^2	1	r	sr	sr^2	s
s	s	sr	sr^2	1	r	r^2
sr	sr	sr^2	s	r^2	1	r
sr^2	sr^2	s	sr	r	r^2	1

D_8	1	r	r^2	r^3	s	sr	sr^2	sr^3
1	1	r	r^2	r^3	s	sr	sr^2	sr^3
r	r	r^2	r^3	1	sr^3	s	sr	sr^2
r^2	r^2	r^3	1	r	sr^2	sr^3	s	sr
r^3	r^3	1	r	r^2	sr	sr^2	sr^3	s
s	s	sr	sr^2	sr^3	1	r	r^2	r^3
sr	sr	sr^2	sr^3	s	r^3	1	r	r^2
sr^2	sr^2	sr^3	s	sr	r^2	r^3	1	r
sr^3	sr^3	s	sr	sr^2	r	r^2	r^3	1

B.) Find the inverse of...

r^2 in D_6: r

r in D_8: r^3

r^2 in D_8: r^2

sr in D_8: sr

r in D_{2n}: r^{n-1}

sr^i in D_{2n}: sr^i

C.) In D_8, simplify the following:

$sr^2sr^3 = sr^2sr^2r = r$

$rsr^{-2} = sr^{-1}r^{-2} = sr^{-3} = sr$

Sam Chyau
Math 540A

Sec 1.3 #1, 2, 4a

1.) Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 4 & 1 \end{pmatrix}$. Find cycle forms for...

$\sigma = (1,3,5)(2,4)$
$\tau = (1,5)(2,3)$
$\sigma^2 = (1,5,3)$
$\sigma\tau = (1,3,5)(2,4)(1,5)(2,3) = (2,5,3,4)$
$\tau\sigma = (1,5)(2,3)(1,3,5)(2,4) = (2,4,3,1)$
$\tau^2\sigma = \tau(\tau\sigma) = (1,5)(2,3)(2,4,3,1) = (2,4)(1,3,5)$

2.) Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 13 & 2 & 15 & 14 & 10 & 6 & 12 & 3 & 4 & 1 & 7 & 9 & 5 & 11 & 8 \end{pmatrix}$
and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 14 & 9 & 10 & 2 & 12 & 6 & 5 & 11 & 15 & 3 & 8 & 7 & 4 & 1 & 13 \end{pmatrix}$
Find cycle forms for...

$\sigma = (1,13,5,10)(3,15,8)(4,14,11,7,12,9)$
$\tau = (1,14)(2,9,15,13,4)(3,10)(5,12,7)(8,11)$
$\sigma^2 = (4,11,12)(14,7,9)(3,8,15)(1,5)(13,10)$
$\sigma\tau = (1,11,3)(2,4)(5,9,8,7,10,15)(13,14)$
$\tau\sigma = (1,4)(2,9)(3,13,12,15,11,5)(8,10,14)$
$\tau^2\sigma = \tau(\tau\sigma) = (1,2,15,8,3,4,14,11,12,13,7,5,10)$

4.) a.) Compute the order of each element of S_3

$\lvert 1 \rvert = 1$	$\lvert (1,2) \rvert = 2$
$\lvert (1,2,3) \rvert = 3$	$\lvert (1,3) \rvert = 2$
$\lvert (1,3,2) \rvert = 3$	$\lvert (2,3) \rvert = 2$

Sam Chyau
Math 540A

Sec. 1.6 # 1, 2, 3, 4, 5, 6, 13, 15

1.) Let $\phi: G \to H$ be a Homomorphism. Prove: $\phi(x^n) = \phi(x)^n \ \forall n \in \mathbb{Z}$.

Pf: Let $\phi: G \to H$ be a Homomorphism. Let $x \in G \wedge n \in \mathbb{Z}$

CASE 1: $n \geq 0$. Induct on n.

BASIC: $n = 0$

$\phi(1_G) = \phi(1_G 1_G) = \phi(1_G)\phi(1_G)$

$\Rightarrow \phi(1_G) = 1_H$

$\Rightarrow \phi(x^n) = \phi(x^0) = \phi(1_G) = 1_H = \phi(x)^0 = \phi(x)^n$

INDUCTIVE: Assume $\phi(x^n) = \phi(x)^n$ f.s. $n \geq 0$

$\Rightarrow \phi(x^{n+1}) = \phi(x^n x) = \phi(x^n)\phi(x) = \phi(x)^n \phi(x) = \phi(x)^{n+1}$

CASE 2: $n = -1$

$1_H = \phi(1_G) = \phi(x x^{-1}) = \phi(x)\phi(x^{-1})$

$\Rightarrow \phi(x^{-1}) = \phi(x)^{-1}$

$\Rightarrow \phi(x^n) = \phi(x^{-1}) = \phi(x)^{-1} = \phi(x)^n$

CASE 3: $n \leq -2$. Let $m = -n$ (so $m > 0$)

$\Rightarrow \phi(x^n) = \phi(x^{-m}) = \phi((x^{-1})^m) = \phi(x^{-1})^m = [\phi(x)^{-1}]^m = \phi(x)^{-m} = \phi(x)^n$

$\therefore \phi(x^n) = \phi(x)^n \ \forall n \in \mathbb{Z}$ ▨

2.) Let $\phi: G \to H$ be an Isomorphism.

a.) Prove: $|x| = |\phi(x)| \ \forall x \in G$

Pf: Let $\phi: G \to H$ be an Isomorphism. Let $x \in G$. Suppose $|x| = m \wedge |\phi(x)| = n$

$\Rightarrow x^m = 1_G \wedge \phi(x)^n = 1_H$

Assume for Contradiction that $m \neq n$.

CASE 1: $m < n$

$\Rightarrow x^m = 1_G$ but $\phi(x)^m \neq 1_H$

$\Rightarrow 1_H = \phi(1_G) = \phi(x^m) = \phi(x)^m \neq 1_H$

CASE 2: $n < m$

$\Rightarrow \phi(x)^n = 1_H$ but $x^n \neq 1_G$

Since ϕ is bijective, 1_H has the unique preimage 1_G.

$\Rightarrow 1_G = \phi^{-1}(1_H) = \phi^{-1}(\phi(x)^n) = \phi^{-1}(\phi(x^n)) = x^n \neq 1_G$

Since both cases are Contradictory, we have $|x| = m = n = |\phi(x)|$ ▨

NOTE: This is not true for all Homomorphisms!

Ex.) $\phi: \mathbb{Z} \to \mathbb{Z}_2$ defined by $\phi(a) = \overline{a} \ \forall a \in \mathbb{Z}$ is a Homomorphism.

$|1| = \infty$ in $\mathbb{Z}$, but $|\overline{1}| = 2$ in $\mathbb{Z}_2$

b.) <u>Prove</u>: G & H have the same number of order-n elements $\forall\, n \in \mathbb{N}$.

<u>Pf</u>: Let $n \in \mathbb{N}$. Let $A = \{x \in G : |x| = n\}$ & $B = \{y \in H : |y| = n\}$.

<u>CLAIM</u>: $\phi(A) = B$

($\subseteq$): Let $a \in A$
$\Rightarrow |\phi(a)| = |a| = n$
$\Rightarrow \phi(a) \in B$
$\Rightarrow \phi(A) \subseteq B$

($\supseteq$): Let $y \in B$
$\Rightarrow \exists\, x \in G$ s.t. $\phi(x) = y$ (ϕ is Onto)
$\Rightarrow |x| = |\phi(x)| = |y| = n$
$\Rightarrow x \in A$
$\Rightarrow y = \phi(x) \in \phi(A)$
$\Rightarrow B \subseteq \phi(A)$

Since ϕ is 1-1, we know by the Claim that $|A| = |\phi(A)| = |B|$ ▨

<u>NOTE</u>: This is not true for all Homomorphisms!
Ex.) $\phi : \mathbb{Z}_3 \to D_6$ defined by $\phi(a) = r^a$ is a Homomorphism.
$|s| = 2$ in D_6, but $\nexists\, \bar{a} \in \mathbb{Z}_3$ s.t. $|\bar{a}| = 2$.

3.) Let $\phi : G \to H$ be an Isomorphism. <u>Prove</u>: G is Abelian <u>iff</u> H is Abelian.

<u>Pf</u>: Let $\phi : G \to H$ be an Isomorphism.

<u>LEMMA</u>: $\phi^{-1} : H \to G$ is an Isomorphism.

<u>Pf</u>: We know $\phi^{-1} : H \to G$ is 1-1 & Onto, since $\phi : G \to H$ is a bijection.
Let $a, b \in H$
$\Rightarrow \exists!\, x, y \in G$ s.t. $\phi(x) = a \wedge \phi(y) = b$
$\Rightarrow \phi^{-1}(ab) = \phi^{-1}(\phi(x)\phi(y)) = \phi^{-1}(\phi(xy)) = xy = \phi^{-1}(a)\phi^{-1}(b)$
$\therefore \phi^{-1} : H \to G$ is an Isomorphism

($\Rightarrow$): Assume G is Abelian. Let $x, y \in G$
$\Rightarrow \phi(x)\phi(y) = \phi(xy) = \phi(yx) = \phi(y)\phi(x)$
$\Rightarrow H = \phi(G)$ is Abelian, since ϕ is Onto.

($\Leftarrow$): Assume H is Abelian. Let $h, k \in H$
$\Rightarrow \phi^{-1}(h)\phi^{-1}(k) = \phi^{-1}(hk) = \phi^{-1}(kh) = \phi^{-1}(k)\phi^{-1}(h)$ (by the Lemma)
$\Rightarrow G = \phi^{-1}(H)$ is Abelian, since ϕ^{-1} is Onto.

$\therefore$ G is Abelian <u>iff</u> H is Abelian ▨

4.) <u>Prove</u>: $\mathbb{R}^* \cong \mathbb{C}^*$

<u>Pf</u>: Compare the solutions of $x^4 = 1$ in $\mathbb{R}^*$ & $\mathbb{C}^*$

<u>$\mathbb{R}^*$</u>: $x^4 = 1$ has 2 solutions, ± 1

$\text{Order}(1) = 1 \qquad \text{Order}(-1) = 2$

<u>$\mathbb{C}^*$</u>: $x^4 = 1$ has 4 solutions, $\pm 1, \pm i$

$\text{Order}(1) = 1 \qquad \text{Order}(-1) = 2$

$\text{Order}(i) = 4 \qquad \text{Order}(-i) = 4$

Since $\mathbb{R}^*$ has no order-4 elements, we know $\mathbb{R}^* \ncong \mathbb{C}^*$ $\blacksquare$

5.) <u>Prove</u>: $\mathbb{R} \ncong \mathbb{Q}$

<u>Pf</u>: $\mathbb{R}$ is Uncountably Infinite & $\mathbb{Q}$ is Countably Infinite.

$\Rightarrow \nexists$ a bijection between $\mathbb{R}$ & $\mathbb{Q}$.

$\therefore \mathbb{R} \ncong \mathbb{Q}$ $\blacksquare$

6.) <u>Prove</u>: $\mathbb{Z} \ncong \mathbb{Q}$

<u>Pf</u>: We prove a Lemma for Isomorphic Groups.

<u>LEMMA</u>: If $\phi: G \to H$ is an Isomorphism, then G is Cyclic <u>iff</u> H is Cyclic.

<u>Pf</u>: Let $\phi: G \to H$ be an Isomorphism.

<u>($\Rightarrow$)</u>: Assume G is Cyclic.

$\Rightarrow \exists\, a \in G$ s.t. $G = \langle a \rangle = \{a^k : k \in \mathbb{Z}\}$

$\Rightarrow \phi(G) = \phi(\langle a \rangle) = \{\phi(a^k) : k \in \mathbb{Z}\} = \{\phi(a)^k : k \in \mathbb{Z}\} = \langle \phi(a) \rangle$

$\therefore H = \phi(G) = \langle \phi(a) \rangle$ is Cyclic, since ϕ is Onto.

<u>($\Leftarrow$)</u>: Assume H is Cyclic.

$\Rightarrow \exists\, b \in H$ s.t. $H = \langle b \rangle = \{b^k : k \in \mathbb{Z}\}$

$\Rightarrow \phi^{-1}(H) = \phi^{-1}(\langle b \rangle) = \{\phi^{-1}(b^k) : k \in \mathbb{Z}\} = \{\phi^{-1}(b)^k : k \in \mathbb{Z}\} = \langle \phi^{-1}(b) \rangle$

$\therefore G = \phi^{-1}(H) = \langle \phi^{-1}(b) \rangle$ is Cyclic, since ϕ^{-1} is Onto.

<u>CLAIM</u>: $\mathbb{Q}$ is <u>NOT</u> Cyclic.

<u>Pf</u>: Suppose $\mathbb{Q}$ is Cyclic.

$\Rightarrow \exists\, r \in \mathbb{Q}$ s.t. $\mathbb{Q} = \langle r \rangle = \{\ldots, -2r, -r, 0, r, 2r, \ldots\}$

$\Rightarrow r/2 \in \mathbb{Q}$, since r is rational

But $r/2 \notin \langle r \rangle$, so $\mathbb{Q} \neq \langle r \rangle$, a Contradiction.

$\therefore \mathbb{Q}$ is <u>NOT</u> Cyclic.

By the Lemma & Claim, we know $\mathbb{Z} \ncong \mathbb{Q}$, since $\mathbb{Z} = \langle 1 \rangle$ is Cyclic. $\blacksquare$

13.) Let $\phi: G \to H$ be a Homomorphism. Prove: $\phi(G) \leq H$

Pf: Let $\phi: G \to H$ be a Homomorphism.

i.) $1_H = \phi(1_G) \in \phi(G)$

ii.) Let $a, b \in \phi(G)$

$\Rightarrow \exists x, y \in G$ s.t. $\phi(x) = a \wedge \phi(y) = b$

$\Rightarrow ab^{-1} = \phi(x)\phi(y)^{-1} = \phi(x)\phi(y^{-1}) = \phi(xy^{-1}) \in \phi(G)$, since $xy^{-1} \in G$.

$\therefore \phi(G) \leq H$ ▨

PROVE: If ϕ is an Injective Homomorphism, then $G \cong \phi(G)$.

Pf: Assume ϕ is an Injective Homomorphism. Let $h \in \phi(G)$

$\Rightarrow \exists g \in G$ s.t. $\phi(g) = h$

$\Rightarrow \phi: G \to \phi(G)$ is Onto

$\Rightarrow \phi: G \to \phi(G)$ is an Isomorphism.

$\therefore G \cong \phi(G)$ ▨

15.) Prove: $\pi: \mathbb{R}^2 \to \mathbb{R}$ defined by $\pi((x,y)) = x \ \forall (x,y) \in \mathbb{R}^2$ is a Homomorphism.
Find $Ker(\pi)$.

Pf: Define $\pi: \mathbb{R}^2 \to \mathbb{R}$ by $\pi((x,y)) = x \ \forall (x,y) \in \mathbb{R}^2$. Let $(a,b), (c,d) \in \mathbb{R}^2$

$\Rightarrow \pi((a,b) + (c,d)) = \pi((a+c, b+d)) = a+c = \phi((a,b)) + \phi((c,d))$

$\therefore \pi$ is a Homomorphism. ▨

$Ker(\pi) = \{(x,y) \in \mathbb{R}^2 : \pi((x,y)) = 0\} = \{(x,y) \in \mathbb{R}^2 : x = 0\} = \{(0,y) : y \in \mathbb{R}\}$

Sam Chyau
Math 540A

Sec 1.7 # 14, 15, 16, 17, 18

For # 14 - 17, let the group G act on itself.

14.) <u>Prove:</u> If G is <u>NOT</u> Abelian, then $g \circ a = ag$ is <u>NOT</u> a Group Action.

<u>Pf:</u> Assume G is <u>NOT</u> Abelian. Let $g \circ a = ag \ \forall\, a, g \in G$

$\Rightarrow \exists\, g_1, g_2 \in G$ s.t. $g_1 g_2 \neq g_2 g_1$. Let $a \in G$

$\Rightarrow a(g_1 g_2) \neq a(g_2 g_1)$

$\Rightarrow g_1 \circ (g_2 \circ a) = g_1 \circ (a g_2) = a(g_2 g_1) \neq a(g_1 g_2) = (g_1 g_2) \circ a$

$\therefore$ $g \circ a = ag$ is <u>NOT</u> a Group Action. ▨

15.) <u>Prove:</u> $g \circ a = ag^{-1}$ is a Group Action.

<u>Pf:</u> Let $g \circ a = ag^{-1} \ \forall\, a, g \in G$

i.) Let $a \in G$

$\Rightarrow 1_G \circ a = a 1_G^{-1} = a$

ii.) Let $g_1, g_2, a \in G$.

$\Rightarrow g_1 \circ (g_2 \circ a) = g_1 \circ (a g_2^{-1}) = (a g_2^{-1}) g_1^{-1} = a(g_1 g_2)^{-1} = (g_1 g_2) \circ a$

$\therefore$ $g \circ a = ag^{-1}$ is a Group Action. ▨

16.) <u>Prove:</u> $g \circ a = gag^{-1}$ is a Group Action (Left Conjugation).

<u>Pf:</u> Let $g \circ a = gag^{-1} \ \forall\, a, g \in G$

i.) Let $a \in G$

$\Rightarrow 1_G \circ a = 1_G a 1_G^{-1} = a$

ii.) Let $g_1, g_2, a \in G$

$\Rightarrow g_1 \circ (g_2 \circ a) = g_1 \circ (g_2 a g_2^{-1}) = g_1 (g_2 a g_2^{-1}) g_1^{-1} = (g_1 g_2) a (g_1 g_2)^{-1} = (g_1 g_2) \circ a$

$\therefore$ $g \circ a = gag^{-1}$ is a Group Action ▨

17.) Let $g \circ x = gxg^{-1}$ $\forall g,x \in G$ (Left Conjugation)

a.) For a fixed $g \in G$, prove Left Conjugation is an isomorphism from G to G.

Pf: Define $\phi_g : G \to G$ by $\phi_g(x) = g \circ x = gxg^{-1}$ $\forall x \in G$

i.) Assume $\phi_g(x) = \phi_g(y)$
$\Rightarrow gxg^{-1} = gyg^{-1}$
$\Rightarrow x = y$

ii.) Let $x \in G$
$\Rightarrow g^{-1}xg \in G$
$\Rightarrow \phi_g(g^{-1}xg) = g(g^{-1}xg)g^{-1} = x \in G$

iii.) Let $x, y \in G$
$\Rightarrow \phi_g(xy) = g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}) = \phi_g(x)\phi_g(y)$

$\therefore$ $\phi_g : G \to G$ is an isomorphism ▨

b.) Prove: $|x| = |gxg^{-1}|$ $\forall x \in G$

Pf: Let $x \in G$. ϕ_g is an isomorphism, so $|x| = |\phi_g(x)| = |gxg^{-1}|$ ▨

c.) Prove: $|A| = |gAg^{-1}|$ $\forall A \subseteq G$

Pf: Let $A \subseteq G$. Then $a \in A$ iff $\phi_g(a) \in \phi_g(A) = \{gag^{-1} : a \in A\} = gAg^{-1}$
$\therefore$ $|A| = |\phi_g(A)| = |gAg^{-1}|$, since ϕ_g is bijective. ▨

18.) Let a group H act on a set A. Define a relation $\sim$ by $a \sim b$ iff $a = h \circ b$ f.s. $h \in H$.
Prove: $\sim$ is an Equivalence Relation on A.

Pf: Define $\sim$ by $a \sim b$ iff $a = h \circ b$ f.s. $h \in H$

i.) REFLEXIVITY: Let $a \in A$
$\Rightarrow 1_H \circ a = a$, so $a \sim a$

ii.) SYMMETRY: Assume $a \sim b$
$\Rightarrow a = h \circ b$ f.s. $h \in H$
$\Rightarrow h^{-1} \circ a = h^{-1} \circ (h \circ b) = (h^{-1}h) \circ b = 1_H \circ b = b$
$\Rightarrow b \sim a$

iii.) TRANSITIVITY: Assume $a \sim b \wedge b \sim c$
$\Rightarrow a = h_1 \circ b \wedge b = h_2 \circ c$ f.s. $h_1, h_2 \in H$
$\Rightarrow a = h_1 \circ (h_2 \circ c) = (h_1 h_2) \circ c$
$\Rightarrow a \sim c$

$\therefore$ $\sim$ is an Equivalence Relation on A ▨