Sam Chyau
Math 540A

CHAPTER 2 HW

Sec 2.1 #1, 2, 3, 10, 11, 12, 14

1.) Prove: $H = \{z \in \mathbb{C} : |z| = 1\} \leq \mathbb{C}^*$

Pf: i.) $|1| = 1$, so $1 \in H$
ii.) Let $x, y \in H$
$\Rightarrow |x| = 1 \wedge |y| = 1$
$\Rightarrow |xy^{-1}| = \left|\frac{x}{y}\right| = \frac{|x|}{|y|} = \frac{1}{1} = 1$
$\Rightarrow xy^{-1} \in H$
$\therefore H \leq \mathbb{C}^*$ ▨

2.) Prove: $H = \{\sigma \in S_n : \sigma \text{ is a 2-cycle}\} \not\leq S_n$ if $n \geq 3$

Pf: $1 \notin H$, so H has no identity element.
$\therefore H \not\leq S_n$ ▨

3.) Prove: $H = \{1, r^2, sr, sr^3\} \leq D_8$

Pf: Observe the operation table of H.

H	1	r^2	sr	sr^3
1	1	r^2	sr	sr^3
r^2	r^2	1	sr^3	sr
sr	sr	sr^3	1	r^2
sr^3	sr^3	sr	r^2	1

i.) $H \neq \emptyset$
ii.) H is closed under $\circ$
iii.) $1^{-1} = 1 \in H$ $\quad (r^2)^{-1} = r^2 \in H$
$(sr)^{-1} = sr \in H$ $\quad (sr^3)^{-1} = sr^3 \in H$
$\therefore H \leq D_8$ ▨

10.) Prove: If $H \leq G$ & $K \leq G$, then $H \cap K \leq G$

Pf: Assume $H \leq G \wedge K \leq G$
i.) $1_G \in H \wedge 1_G \in K$
$\Rightarrow 1_G \in H \cap K$
ii.) Let $a, b \in H \cap K$
$\Rightarrow a, b \in H \wedge a, b \in K$
$\Rightarrow ab^{-1} \in H \wedge ab^{-1} \in K$
$\Rightarrow ab^{-1} \in H \cap K$
$\therefore H \cap K \leq G$ ▨

11.) Let A, B be Groups. Prove $H \leq A \times B$.

a.) $H = \{(a, 1_B) : a \in A\}$:

Pf: i.) $(1_A, 1_B) \in H$, since $1_A \in A$

ii.) Let $(x, 1_B), (y, 1_B) \in H$

$\Rightarrow (x, 1_B)(y, 1_B)^{-1} = (x, 1_B)(y^{-1}, 1_B) = (xy^{-1}, 1_B) \in H$, since $xy^{-1} \in A$

$\therefore H \leq A \times B$ ▨

b.) $H = \{(1_A, b) : b \in B\}$:

Pf: i.) $(1_A, 1_B) \in H$, since $1_B \in B$

ii.) Let $(1_A, h), (1_A, k) \in H$

$\Rightarrow (1_A, h)(1_A, k)^{-1} = (1_A, h)(1_A, k^{-1}) = (1_A, hk^{-1}) \in H$, since $hk^{-1} \in B$

$\therefore H \leq A \times B$ ▨

c.) $H = \{(a, a) : a \in A\}$, where $A = B$:

Pf: i.) $(1_A, 1_A) \in H$, since $1_A \in A$

ii.) Let $(x, x), (y, y) \in H$

$\Rightarrow (x, x)(y, y)^{-1} = (x, x)(y^{-1}, y^{-1}) = (xy^{-1}, xy^{-1}) \in H$, since $xy^{-1} \in A$

$\therefore H \leq A \times A = A \times B$ ▨

12.) Prove $H = \{a \in A : a^n = 1_A\} \leq A$, where A is Abelian.

Pf: Let A be Abelian.

i.) $1_A^n = 1_A$, so $1_A \in H$

ii.) Let $a, b \in H$

$\Rightarrow a^n = 1_A \wedge b^n = 1_A$

$\Rightarrow (ab^{-1})^n = a^n (b^{-1})^n = a^n (b^n)^{-1} = 1_A 1_A^{-1} = 1_A$

$\Rightarrow ab^{-1} \in H$

$\therefore H \leq A$ ▨

14.) Prove $H = \{x \in D_{2n} : x^2 = 1\} \not\leq D_{2n}$ $(n \geq 3)$

Pf: $(sr)^2 = 1 \wedge s^2 = 1$

$\Rightarrow sr, s \in H$

But $s(sr) = s^2 r = r \notin H$, since $|r| = n \geq 3$

$\therefore H \not\leq D_{2n}$ ▨

Sam Chyau
Math 540A

Sec 2.2 #2, 5, 6, 7, 11

2.) Prove $C_G(Z(G)) = G$ & $N_G(Z(G)) = G$

a.) $\underline{C_G(Z(G)) = G}$:

Pf: By definition, $C_G(Z(G)) \subseteq G$

Let $g \in G$. Let $z \in Z(G)$

$\Rightarrow gzg^{-1} = z$

$\Rightarrow g \in C_G(Z(G))$

$\Rightarrow G \subseteq C_G(Z(G))$

$\Rightarrow G = C_G(Z(G))$ ▨

b.) $\underline{N_G(Z(G)) = G}$:

Pf: By definition, $N_G(Z(G)) \subseteq G$

Let $g \in G$

$\Rightarrow gZ(G)g^{-1} = \{gzg^{-1} : z \in Z(G)\} = \{zgg^{-1} : z \in Z(G)\} = \{z : z \in Z(G)\} = Z(G)$

$\Rightarrow g \in N_G(Z(G))$

$\Rightarrow G \subseteq N_G(Z(G))$

$\Rightarrow G = N_G(Z(G))$ ▨

5.) Show $C_G(A) = A$ & $N_G(A) = G$, where $A \leq G$

a.) $A = \{1, (1,2,3), (1,3,2)\}$, $G = S_3$

NOTE: $\langle (1,2,3) \rangle = \{1, (1,2,3), (1,3,2)\} = A$, so A is cyclic & therefore Abelian.

$\therefore A \subseteq C_G(A) \subseteq N_G(A)$

i.) $(1,2)(1,2,3)(1,2)^{-1} = (2,1,3)$, so $(1,2) \notin C_G(A)$

$(1,3)(1,2,3)(1,3)^{-1} = (3,2,1)$, so $(1,3) \notin C_G(A)$

$(2,3)(1,2,3)(2,3)^{-1} = (1,3,2)$, so $(2,3) \notin C_G(A)$

$\therefore C_G(A) = A$ ▨

ii.) $(1,2)A(1,2)^{-1} = \{1, (2,1,3), (2,3,1)\} = A$, so $(1,2) \in N_G(A)$

$(1,3)A(1,3)^{-1} = \{1, (3,2,1), (3,1,2)\} = A$, so $(1,3) \in N_G(A)$

$(2,3)A(2,3)^{-1} = \{1, (1,3,2), (1,2,3)\} = A$, so $(2,3) \in N_G(A)$

$\therefore N_G(A) = G$ ▨

6.) Let $H \leq G$

a.) Prove: $H \leq N_G(H)$

Pf: Let $a \in H$

CLAIM: $aHa^{-1} = H$

Pf ($\subseteq$): $aHa^{-1} = \{aha^{-1} : h \in H\} \subseteq H$, since H is closed under the Operation & Inversion.

Pf ($\supseteq$): Let $h \in H$

$\Rightarrow a^{-1}ha \in H$, since H is closed under the Operation & Inversion

$\Rightarrow h = 1_G h 1_G = (aa^{-1})h(aa^{-1}) = a(a^{-1}ha)a^{-1} \in aHa^{-1}$

$\Rightarrow H \subseteq aHa^{-1}$

$\therefore aHa^{-1} = H$

By this Claim, we know $a \in N_G(H)$

$\Rightarrow H \subseteq N_G(H)$

$\Rightarrow H \leq N_G(H)$, since H is a Group ▨

NOTE: This is not true if $H \not\leq G$.

COUNTEREXAMPLE: $H = \{1, r^2, s\} \subseteq D_6$

$\Rightarrow r^2 H r^{-2} = \{1, r^2, sr^2\} \neq H$

$\Rightarrow r^2 \notin N_G(H)$

But $r^2 \in H$, so $H \not\leq N_{D_6}(H)$

b.) Prove: $H \leq C_G(H)$ iff H is Abelian

Pf ($\Rightarrow$): Assume $H \leq C_G(H)$. Let $a \in H$

$\Rightarrow a \in C_G(H)$

$\Rightarrow aha^{-1} = h \ \forall \ h \in H$

$\Rightarrow H$ is Abelian

Pf ($\Leftarrow$): Assume H is Abelian. Let $a \in H$

$\Rightarrow aha^{-1} = h \ \forall \ h \in H$

$\Rightarrow a \in C_G(H)$

$\Rightarrow H \subseteq C_G(H)$

$\Rightarrow H \leq C_G(H)$, since H is a Group

$\therefore H \leq C_G(H)$ iff H is Abelian. ▨

7.) Let $n \in \mathbb{Z}$ w/ $n \geq 3$

a.) Prove: $Z(D_{2n}) = \{1\}$ if n is Odd.

Pf: Let n be Odd

1.) $1\sigma 1^{-1} = \sigma \ \forall \sigma \in D_{2n}$, so $1 \in Z(D_{2n})$

2.) Let $1 \leq i \leq n-1$

$\Rightarrow r^{2i} \neq 1$, since $2i \neq n$

$\Rightarrow (r^i)(s)(r^i)^{-1} = r^{2i}s \neq s$, so $r^i \notin Z(D_{2n})$

3.) Let $0 \leq i \leq n-1$

$\Rightarrow (sr^i)(r)(sr^i)^{-1} = sr^{i+1}sr^i = s^2r^{-i-1}r^i = r^{-i-1+i} = r^{-1} \neq r$, since $n \geq 3$

$\Rightarrow sr^i \notin Z(D_{2n})$

$\therefore Z(D_{2n}) = \{1\}$ if n is Odd. ▨

b.) Prove: $Z(D_{2n}) = \{1, r^k\}$ if $n = 2k$ $(k \geq 2)$

Pf: Let $n = 2k$

1.) $1\sigma 1^{-1} = \sigma \ \forall \sigma \in D_{2n}$, so $1 \in Z(D_{2n})$

2.) Let $1 \leq i \leq n-1$, where $i \neq k$

$\Rightarrow r^{2i} \neq 1$, since $2i \neq n$

$\Rightarrow (r^i)(s)(r^i)^{-1} = r^{2i}s \neq s$, so $r^i \notin Z(D_{2n})$

3.) Let $0 \leq i \leq n-1$

$\Rightarrow (sr^i)(r)(sr^i)^{-1} = sr^{i+1}sr^i = s^2r^{-i-1}r^i = r^{-i-1+i} = r^{-1} \neq r$, since $n \geq 4$

$\Rightarrow sr^i \notin Z(D_{2n})$

4.) Let $0 \leq i \leq n-1$

a.) $(r^k)(r^i)(r^k)^{-1} = r^{k+i-k} = r^i$

b.) $(r^k)(sr^i)(r^k)^{-1} = sr^{-k}r^{i-k} = sr^{i-2k} = sr^{i-n} = sr^i$

$\therefore r^k \in Z(D_{2n})$

$\therefore Z(D_{2n}) = \{1, r^k\}$ if $n = 2k$ ▨

11.) Prove: $Z(G) \leq N_G(A)$ for any $A \subseteq G$

Pf: Let $x \in Z(G)$

$\Rightarrow xax^{-1} = a \ \forall a \in A \subseteq G$

$\Rightarrow xAx^{-1} = \{xax^{-1} : a \in A\} = \{a : a \in A\} = A$

$\Rightarrow x \in N_G(A)$

$\Rightarrow Z(G) \subseteq N_G(A)$

$\Rightarrow Z(G) \leq N_G(A)$, since $Z(G)$ is a Group ▨

Sam Chyau
Math 540A

Sec. 2.3 #11, 12, 13, 26, +A

11.) Find all cyclic subgroups of D_8. Find a Non-cyclic proper subgroup.

CYCLIC:
$\langle 1 \rangle = \{1\}$
$\langle r \rangle = \{1, r, r^2, r^3\} = \langle r^3 \rangle$
$\langle r^2 \rangle = \{1, r^2\}$
$\langle s \rangle = \{1, s\}$
$\langle sr \rangle = \{1, sr\}$
$\langle sr^2 \rangle = \{1, sr^2\}$
$\langle sr^3 \rangle = \{1, sr^3\}$

NON-CYCLIC:
$\{1, r^2, s, sr^2\}$
$\{1, r^2, sr, sr^3\}$

12.) Prove the following groups are NOT cyclic.

a.) $\mathbb{Z}_2 \times \mathbb{Z}_2$:

Pf: $|(\bar{0}, \bar{0})| = 1$, $|(\bar{0}, \bar{1})| = 2$, $|(\bar{1}, \bar{0})| = 2$, $|(\bar{1}, \bar{1})| = 2$
Since no element has order 4, $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic. ▨

b.) $\mathbb{Z}_2 \times \mathbb{Z}$:

Pf: Suppose $\mathbb{Z}_2 \times \mathbb{Z}$ is cyclic
$\Rightarrow \mathbb{Z}_2 \times \mathbb{Z} \cong \mathbb{Z}$, since $\mathbb{Z}_2 \times \mathbb{Z}$ is infinite
$\Rightarrow$ Every element of $\mathbb{Z}_2 \times \mathbb{Z}$ has order 1 or infinity
But $|(\bar{1}, \bar{0})| = 2$, so $\mathbb{Z}_2 \times \mathbb{Z}$ cannot be cyclic. ▨

c.) $\mathbb{Z} \times \mathbb{Z}$:

Pf: Suppose $\langle (a,b) \rangle = \mathbb{Z} \times \mathbb{Z}$
$\Rightarrow \langle a \rangle = \mathbb{Z} \wedge \langle b \rangle = \mathbb{Z}$ (so $a = \pm 1$ & $b = \pm 1$)
$\begin{cases} \langle (1,1) \rangle = \{\ldots, (-2,-2), (-1,-1), (0,0), (1,1), (2,2), \ldots\} = \langle (-1,-1) \rangle \\ \langle (1,-1) \rangle = \{\ldots, (-2,2), (-1,1), (0,0), (1,-1), (2,-2), \ldots\} = \langle (-1,1) \rangle \end{cases}$
But $(0,1) \notin \langle (1,1) \rangle \cup \langle (1,-1) \rangle$, so $\mathbb{Z} \times \mathbb{Z}$ is not cyclic ▨

13.) Prove the following pairs are NOT isomorphic.

a.) $\mathbb{Z} \times \mathbb{Z}_2 \not\cong \mathbb{Z}$:

Pf: $\mathbb{Z} \times \mathbb{Z}_2$ is not cyclic, but $\mathbb{Z} = \langle 1 \rangle$
$\Rightarrow \mathbb{Z} \times \mathbb{Z}_2 \ncong \mathbb{Z}$ ▨

b.) $\mathbb{Q} \times \mathbb{Z}_2 \not\cong \mathbb{Q}$:

Pf: $|(0, \bar{1})| = 2$ in $\mathbb{Q} \times \mathbb{Z}_2$, but $\mathbb{Q}$ has no order-2 element
$\Rightarrow \mathbb{Q} \times \mathbb{Z}_2 \ncong \mathbb{Q}$ ▨

26.) Let Z_n be a cyclic Group of order n, and $\forall a \in \mathbb{Z}$, define

$$\sigma_a : Z_n \to Z_n \text{ by } \sigma_a(x) = x^a \quad \forall x \in Z_n$$

a.) Prove σ_a is an Automorphism of Z_n iff $\gcd(a,n) = 1$

Pf: Let $Z_n = \langle z \rangle = \{1, z, z^2, \ldots, z^{n-1}\}$

Then $\sigma_a(Z_n) = \{\sigma_a(1), \sigma_a(z), \sigma_a(z^2), \ldots, \sigma_a(z^{n-1})\}$

$= \{1^a, z^a, (z^2)^a, \ldots, (z^{n-1})^a\}$

$= \{1, z^a, (z^a)^2, \ldots, (z^a)^{n-1}\} = \langle z^a \rangle$

($\Rightarrow$): $\gcd(a,n) \neq 1$

$\Rightarrow |\sigma_a(Z_n)| = |\langle z^a \rangle| = |z^a| = \frac{n}{\gcd(a,n)} < \frac{n}{1} = n = |Z_n|$

$\Rightarrow \sigma_a$ is NOT 1-1

$\Rightarrow \sigma_a$ is NOT an Automorphism of Z_n

($\Leftarrow$): $\gcd(a,n) = 1$

$\Rightarrow |\sigma_a(Z_n)| = |\langle z^a \rangle| = |z^a| = \frac{n}{\gcd(a,n)} = \frac{n}{1} = n = |Z_n|$

$\Rightarrow \sigma_a$ is 1-1 and Onto

Now let $z^h, z^k \in Z_n$

$\Rightarrow \sigma_a(z^h z^k) = \sigma_a(z^{h+k}) = (z^{h+k})^a = z^{(h+k)a} = z^{ha+ka} = z^{ha} z^{ka}$

$= (z^h)^a (z^k)^a = \sigma_a(z^h)\sigma_a(z^k)$

$\Rightarrow \sigma_a$ is an Automorphism of Z_n.

$\therefore \sigma_a$ is an Automorphism of Z_n iff $\gcd(a,n) = 1$ ▨

b.) Prove $\sigma_a = \sigma_b$ iff $a \equiv b \pmod n$

Pf ($\Rightarrow$): Assume $\sigma_a = \sigma_b$

$\Rightarrow \sigma_a(z) = \sigma_b(z)$

$\Rightarrow z^a = z^b$

$\Rightarrow z^{a-b} = z^a z^{-b} = z^b z^{-b} = 1$

$\Rightarrow n \mid a-b$

$\Rightarrow a - b = kn$ f.s. $k \in \mathbb{Z}$

$\Rightarrow a \equiv b \pmod n$

Pf ($\Leftarrow$): Assume $a \equiv b \pmod n$

$\Rightarrow a - b = nk$ f.s. $k \in \mathbb{Z}$

$\Rightarrow a = nk + b$

Let $z^r \in Z_n$

$\Rightarrow \sigma_a(z^r) = (z^r)^a = (z^r)^{nk+b}$

$= z^{r(nk+b)} = z^{nrk} z^{rb}$

$= (z^n)^{rk}(z^r)^b = 1^{rk}(z^r)^b = (z^r)^b = \sigma_b(z^r)$

$\Rightarrow \sigma_a = \sigma_b$

$\therefore \sigma_a = \sigma_b$ iff $a \equiv b \pmod n$ ▨

c.) Prove EVERY Automorphism of Z_n is equal to σ_a f.s. $a \in \mathbb{Z}$.

Pf: Let $f: Z_n \to Z_n$ be an Automorphism of Z_n. Let $z^r \in Z_n$
$\Rightarrow f(z) = z^a$ f.s. $a \in \mathbb{Z}$, $\because$ each member of Z_n is a power of z.
$\Rightarrow f(z^r) = f(z)^r = (z^a)^r = (z^r)^a = \sigma_a(z^r)$

$\therefore$ Every Automorphism of Z_n is equal to σ_a f.s. $a \in \mathbb{Z}$ ▨

d.) Prove $\sigma_a \circ \sigma_b = \sigma_{ab}$. Deduce that the map $\bar{a} \mapsto \sigma_a$ is an isomorphism of $\mathbb{Z}_n^\times$ onto $Aut(Z_n)$.

Pf: Let $z^r \in Z_n$
$\Rightarrow (\sigma_a \circ \sigma_b)(z^r) = \sigma_a(\sigma_b(z^r)) = \sigma_a(z^{rb}) = z^{rba} = (z^r)^{ab} = \sigma_{ab}(z^r)$
$\Rightarrow \sigma_a \circ \sigma_b = \sigma_{ab}$
Now define $\phi: \mathbb{Z}_n^\times \to Aut(Z_n)$ by $\phi(\bar{a}) = \sigma_a \ \forall \ \bar{a} \in \mathbb{Z}_n^\times$

1.) Assume $\bar{a} = \bar{b}$ in $\mathbb{Z}_n^\times$
$\Rightarrow a \equiv b \pmod n$
$\Rightarrow \sigma_a = \sigma_b$ by (b)
$\Rightarrow \phi(\bar{a}) = \phi(\bar{b})$
$\therefore \phi$ is Well-Defined

2.) Assume $\phi(\bar{a}) = \phi(\bar{b})$
$\Rightarrow \sigma_a = \sigma_b$
$\Rightarrow a \equiv b \pmod n$ by (b)
$\Rightarrow \bar{a} = \bar{b}$ in $\mathbb{Z}_n^\times$
$\therefore \phi$ is 1-1

3.) Let $f \in Aut(Z_n)$
$\Rightarrow f = \sigma_a$ f.s. $a \in \mathbb{Z}$ by (c)
$\Rightarrow \gcd(a, n) = 1$ by (a)
$\Rightarrow \bar{a} \in \mathbb{Z}_n^\times$
$\Rightarrow \phi(\bar{a}) = \sigma_a = f \in Aut(Z_n)$
$\therefore \phi$ is Onto

4.) Let $\bar{a}, \bar{b} \in \mathbb{Z}_n^\times$
$\Rightarrow \phi(\bar{a}\bar{b}) = \phi(\overline{ab}) = \sigma_{ab} = \sigma_a \circ \sigma_b = \phi(\bar{a}) \circ \phi(\bar{b})$
$\therefore \phi$ is a Homomorphism

$\therefore \phi$ is an isomorphism from $\mathbb{Z}_n^\times$ onto $Aut(Z_n)$ ▨

A. Find all generators of $\mathbb{Z}_8$:

$\{\bar{a} \in \mathbb{Z}_8 : \langle \bar{a} \rangle = \mathbb{Z}_8\} = \{\bar{a} \in \mathbb{Z}_8 : \gcd(a, 8) = 1\} = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$