Math 220A HW 1

Zih-Yu Hsieh

October 13, 2025

1 D

Problem 1

Lang Chapter 1 #11:
Let G be a group, and A a normal abelian subgroup, show that G/A operates on A by conjugation, and in this manner get a homomorphism of G/A into $\text{Aut}(A)$.

Solution: For all $\overline{g} \in G/A$ (with representative $g \in G$) and $a \in A$, define a map $\mu : G/A \times A \to A$ by $\mu(\overline{g}, a) = gag^{-1}$.

First, one needs to show the map is well-defined: Suppose g, g' both are representatives of $\overline{g} \in G/A$, then there exists $h \in A$, such that $g' = gh$ (since they're representing the same left coset), then consider the conjugation of g, g' on any $a \in A$, based on the assumption that A is abelian, we get:

$$gag^{-1} = g(hh^{-1}a)g^{-1} = g(hah^{-1})g^{-1} = (gh)a(gh)^{-1} = g'a(g')^{-1} \tag{1.1}$$

Hence, g, g' both act on a in the same manner, hence there's no ambiguity defining $\mu(\overline{g}, a) = gag^{-1}$ (since every element in the same left coset acts on a the same).

Then, to show it's indeed an action, it follows from the below equality, for all $\overline{g}, \overline{h} \in G/A$, and $a \in A$:

$$\mu\Big(\overline{g}, \mu\big(\overline{h}, a\big)\Big) = \mu(hah^{-1}) = g(hah^{-1})g^{-1} = (gh)a(gh)^{-1} = \mu(gh, a) \tag{1.2}$$

So, μ is indeed a well-defined left action, hence generating a group homomorphism $\pi : G/A \to \text{Aut}(A)$, by $\pi(\overline{g})(\_) = \mu(\overline{g}, \_)$.

2 D

Problem 2

Lang Chapter 1 #12:
Let G be a group and let H, N be subgropus with N normal. Let γ_x be conjugation by an element $x \in G$.

(a) Show that $x \mapsto \gamma_x$ induces a homomorphism $f : H \to \text{Aut}(N)$.

(b) If $H \cap N = \{e\}$, show that the map $H \times N \to HN$ given by $(x, y) \mapsto xy$ is a bijection, and that this map is an isomorphism if and only if f is trivial, i.e. $f(x) = \mathrm{id}_N$ for all $x \in H$.

We define G to be the **semidirect product** of H and N if $G = HN$ and $H \cap N = \{e\}$.

(c) Conversely, let N, H be groups, and let $\psi : H \to \mathrm{Aut}(N)$ be a given homomorphism. Construct a semidirect product as follows: Let G be the set of pairs (x, h) with $x \in N$ and $h \in H$. Define the composition law:

$$(x_1, h_1)(x_2, h_2) = (x_1\psi(h_1)x_2, h_1h_2) \tag{2.1}$$

Show that this is a group law, and yields a semidirect product of N and H, identifying N with the set of elements $(x, 1)$ and H with the set of elements $(1, h)$.

Solution:

(a) For all $x, y \in H$, if consider γ_{xy}, it satisfies the following:

$$\forall n \in N, \quad \gamma_{xy}(n) = (xy)n(xy)^{-1} = xyny^{-1}x^{-1} = x\gamma_{y(n)}x^{-1} = \gamma_x\big(\gamma_y(n)\big) \tag{2.2}$$

Hence, the equality demonstrates that $\gamma_{xy} = \gamma_x \circ \gamma_y$, showing that $f : H \to \mathrm{Aut}(N)$ by $f(xy) = \gamma_{xy} = \gamma_x \circ \gamma_y$, which is a group homomorphism.

(b) Given $H \cap N = \{e\}$, first regardless of this condition, it's clear that $H \times N \to HN$ by $(x, y) \mapsto xy$ is surjective (since by definition HN collects all xy, where $x \in H$ and $y \in N$).

To prove that it's injective, suppose $(x, y), (x', y') \in H \times N$ satisfies $xy = x'y'$, then it satisfies $(x')^{-1}xy = y'$, or $(x')^{-1}x = y'y^{-1}$. Notice this expression is both in H and N (since $x, x' \in H$ and $y, y' \in N$), hence $(x')^{-1}x = y'y^{-1} = e$, showing $x = x'$ and $y = y'$, hence the map is injective. This shows that set wise, $H \cap N = \{e\}$ implies $H \times N$ and HN are set isomorphic.

Now, to prove the equivalence statement for the two groups above being group isomorphic, consider the following:

$\Longrightarrow$: Suppose $H \times N \to HN$ by $(x, y) \mapsto xy$ is an isomorphism, in particular it's a group homomorphism, then for all $(x, y), (x', y') \in H \times N$, it satisfies the following:

$$(x, y) \mapsto xy, \quad (x', y') \mapsto x'y' \tag{2.3}$$

$$(x, y) \cdot (x', y') = (xx', yy') \mapsto (xx')(yy') = (xy)(x'y') \tag{2.4}$$

Hence, then equality shows $x'y = yx'$ (by canceling x and y' on the sides). Since $(x, y), (x', y') \in H \times N$ are arbitrary (which $x' \in H$, $y \in N$ are arbitrary also), then $\gamma_{x'}(y) = x'y(x')^{-1} = y$, showing that $\gamma_{x'} = \mathrm{id}_N$. So, all $x' \in H$ satisfies $\gamma_{x'} = \mathrm{id}_N$.

$\Longleftarrow$: Suppose all $x \in H$ satisfies $\gamma_x = \mathrm{id}_N \in \mathrm{Aut}(N)$, we'll show the map $H \times N \to HN$ by $(x, y) \mapsto xy$ is a group homomorphism (since it's a bijection with assumption $H \cap N = \{e\}$, being a group homomorphism implies it's an isomorphism). Since for all $x \in H$ and $n \in N$ satisfies $xnx^{-1} = \gamma_{x(n)} = n$, hence $xn = nx$ (or all eleements in H and N commutes). Hence, given any $(x, y), (x', y') \in H \times N$, they satisfy:

$$(x, y) \cdot (x', y') = (xx', yy') \mapsto (xx')(yy') = (xy)(x'y') \tag{2.5}$$

$$(x, y) \mapsto xy, \quad (x', y') \mapsto x'y' \tag{2.6}$$

Hence, $(x, y) \cdot (x', y')$ gets mapped to the product of the image of (x, y) and (x', y'), hence the map $H \times N \to HN$ is indeed a group homomorphism, which is an isomorphism (given that it's a bijection).

(c) To show the given law satisfies group property, we'll first show it's associative: Given any $(x_1, h_1), (x_2, h_2), (x_3, h_3) \in G$, they satisfy:

$$((x_1, h_1)(x_2, h_2))(x_3, h_3) = (x_1\psi(h_1)x_2, h_1h_2)(x_3, h_3) = (x_1(\psi(h_1)x_2)(\psi(h_1h_2)x_3), h_1h_2h_3) \tag{2.7}$$

$$(x_1, h_1)((x_2, h_2)(x_3, h_3)) = (x_1, h_1)(x_2\psi(h_2)x_3, h_2h_3) = (x_1\psi(h_1)(x_2\psi(h_2)x_3), h_1h_2h_3) \tag{2.8}$$

Notice that the second equation's first entry can be rewrite as follow:

$$x_1\psi(h_1)(x_2\psi(h_2)x_3) = \psi(h_1)(x_2) \cdot \psi(h_1)(\psi(h_2)x_3) = \psi(h_1)(x_2) \cdot \psi(h_1h_2)(x_3) \tag{2.9}$$

Where the second equality is formed by the fact that ψ is a group homomorphism. Hence, one can conclude that $((x_1, h_1)(x_2, h_2))(x_3, h_3) = (x_1, h_1)((x_2, h_2)(x_3, h_3))$, which the given law is associative.

Then, we'll explicitly show that $(e, e) \in G$ serves as an identity: Given any $(x, h) \in G$, the following is satisfied:

$$(e_N, e_H)(x, h) = (e_N\psi(e_H)(x), e_Hh) = \left(e_N \operatorname{id}_{N(x)}, h\right) = (e_Nx, h) = (x, h) \tag{2.10}$$

$$(x, h)(e_N, e_H) = (x\psi(h)(e_N), he_H) = (xe_N, h) = (x, h) \tag{2.11}$$

Which, (e, e) is indeed an identity under this law.

Now, to compute the inverse, given any $(x, h) \in G$, consider the element $(\psi(h^{-1})(x^{-1}), h^{-1})$, which satisfies the following:

$$(x, h)(\psi(h^{-1})(x^{-1}), h^{-1}) = x(\psi(h)\psi(h^{-1})(x^{-1}), hh^{-1}) \tag{2.12}$$

$$= (x \cdot \psi(e_H)(x^{-1}), e) = \left(x \operatorname{id}_{N(x^{-1})}, e\right) = (xx^{-1}, e) = (e, e) \tag{2.13}$$

$$(\psi(h^{-1})(x^{-1}), h^{-1})(x, h). = (\psi(h^{-1})(x^{-1}) \cdot \psi(h^{-1})(x), h^{-1}h) \tag{2.14}$$

$$= (\psi(h^{-1})(x^{-1}x), e_H) = (\psi(h^{-1})(e_N), e_H) = (e_N, e_H) \tag{2.15}$$

Hence, this shows the existence of inverse for every element. So, under this rule, G forms a group.

3 D

Problem 3

Lang Chapter 1 #20:

Let P be a p-group. Let A be a normal subgroup of order p. Prove that A is contained in the center of P.

Solution: First, since $|A| = p$ where p is a prime, then A is automatically cyclic, or there exists $a \in A$ (which $|a| = p$), with $A = \langle a \rangle$.

Also, since $A \trianglelefteq G$, then for all $g \in G$ and $a^k \in \langle a \rangle = A$, $ga^kg^{-1} \in A$. Hence, one can consider the conjugation action $G \curvearrowright A$.

To prove that A belongs to the center of G, it suffices to show that every nontrivial element $a^k \in A$ has the same stabilizer, or for all integer $0 < k < p$, we have $G_{a^k} = G_a$ under conjugation action.

Suppose the contrary that A is not contained in the center of G, while every of its nontrivial element has the same stabilizer. Then, there exists $a \in A$ and $g \in G$, such that $ag \neq ga$, or $gag^{-1} \neq a$. Notice that $gag^{-1} \neq e$, since if $gag^{-1} = e$, then $a = e$, which $gag^{-1} = a$; so, since gag^{-1} is nontrivial in A, there exists integer $0 < k < p$, such that $gag^{-1} = a^k$, where $k \neq 1$ because $gag^{-1} \neq a$ by assumption. However, recall that under a left group action, if $g \cdot a = b$, then the stabilizer $G_b = gG_ag^{-1}$. So, we get that $G_{a^k} = gG_ag^{-1}$, while $G_{a^k} = G_a$ by assumption, hence $g \in gG_ag^{-1} = G_a$. Yet, this implies that $gag^{-1} = a$, which contradicts the assumption that $gag^{-1} \neq a$. Hence, we derived that A must be contained in the center of G (if assuming all nontrivial element of A has the same stabilizer, under G's conjugation action).

Then, to prove the main lemma, for all integer $0 < k < p$ (where $a^k \in A$ is nontrivial), we'll show that $G_a = G_{a^k}$:

$\subseteq$: Given any $g \in G_a$, since $gag^{-1} = a$, then $a^k = \left(gag^{-1}\right)^k = ga^kg^{-1}$ by internal cancellation, showing that $g \in G_{a^k}$, or $G_a \subseteq G_{a^k}$.

$\supseteq$: Given any $h \in G_{a^k}$, notice that since $a^k \in A = \langle a \rangle$ is not trivial, then $|a^k| = p$ (since $|A| = p$, if $|a^k| \neq 1$ due to the fact that $a^k \neq e$, then $|a^k| = p$ is enforced). Hence, a^k also generates A (since $|\langle a^k \rangle| = p = |A|$), so there exists $r \in \mathbb{Z}$, such that $\left(a^k\right)^r = a$. Then, $a = \left(a^k\right)^r = \left(ha^kh^{-1}\right)^r = h\left(a^k\right)^r h^{-1} = hah^{-1}$, again by internal cancellation. Hence, $h \in G_a$, or $G_{a^k} \subseteq G_a$.

The two inclusion concludes that $G_a = G_{a^k}$, hence all nontrivial elements in A has the same stabilizer. Together with the claim beforehand, A must be contained in the center.

4 D

Problem 4

Lang Chapter 1 #31:

Determine all groups of order ≤ 10 up to isomorphism. In particular, show that a non-abelian group of order 6 is isomorphic to S_3.

Solution: For $n = 1$, the only group of such order is $\{e\}$ (since by definition a group must need an identity, so it's the only element).

For case $n = 2, 3, 5, 7$ (prime numbers ≤ 10), we'll show that all group must be isomorphic to $\mathbb{Z}/n\mathbb{Z}$: Given a group G with $|G| = n$, since $n \neq 1$ on our list, then G is nontrivial, hence there exists $g \in G$ where $g \neq e$. Then, since $|g|$ divides $|G| = n$, while n (in our list) is prime, then with $g \neq e$ (implying $|g| \neq 1$), we must have $|g| = n$, hence the cyclic subgroup $\langle g \rangle \leq G$ satisfies $|\angle, lg\rangle| = |g| = n = |G|$, showing that $\langle g \rangle = G$. Then, since g has order n, then $G = \langle g \rangle \cong \mathbb{Z}/n\mathbb{Z}$.

For case $n = 4, 9$ (where $4 = 2^2$ and $9 = 3^2$, both prime square), since $n = p^2$ for some prime p, we'll show that all such group must be ablian: Suppose the contrary that there exists non-abelian group G with prime square power, let G acts on itself via conjugation action, then by class equation, $|G| = |Z(G)| + |\sum_{j \in J} \left[G : G_{x_i}\right]|$, where J runs through all distinct representatives of group elements with nontrivial conjugation classes.

Since each of the nontrivial conjugation class must be proper (due to the fact that $\{e\}$ itself forms a conjugation class), then $\left[G : G_{x_i}\right] \neq 1, p^2$ (since they're asumed to not be central, which has nontrivial conjugation class; while the conjugation class is proper, therefore its stabilizer can't be the whole group). In case for $\left[G : G_{x_i}\right]$ to divide $|G| = p^2$, it enforces $\left[G : G_{x_i}\right] = p$. So, in the class equation, since $|G| = p^2$ is divisible by p, similarly $|\sum_{j \in J} \left[G : G_{x_i}\right]$ is also divisible by p (since each term is), then so is $|Z(G)|$, showing that $|Z(G)| \neq 1$, or $Z(G) \neq \{e\}$. Then, by the assumption that it's non-abelian, $Z(G) \neq G$, hence $|Z(G)| \neq p^2$ either, showing that $|Z(G)| = p$ (the only order that still divides p^2), or it's cyclic. Which, there exists $g \in Z(G)$ (with $|g| = p$), such that $\langle g \rangle = Z(G)$.

Finally, recall that $Z(G) \trianglelefteq G$, hence $G/Z(G)$ has a natural quotient group structure, and $|G/Z(G)| = [G : Z(G)] = |G| Z(G)| = \frac{p^2}{p} = p$,hence $G/Z(G)$ is also cyclic, there exists $h \in G$, such that $\overline{h} \in G/Z(G)$ satisfies $\langle \overline{h} \rangle = G/Z(G)$. Which, every $k \in G$, since $\overline{k} = \overline{h}^i$ for some $i \in \mathbb{Z}$, then $k = h^i \cdot g^j$ for some $j \in \mathbb{Z}$ (since $k \in hZ(G) = h\langle g \rangle$). So, for every $k, k' \in G$, the followign is true:

$$kk' = (h^i g^j)\left(h^{i'} g^{j'}\right) = \left(h^i h^{i'}\right)\left(g^j g^{j'}\right) = \left(h^{i'} h^i\right)\left(g^{j'} g^j\right) = \left(h^{i'} g^{j'}\right)(h^i g^j) = k'k \tag{4.1}$$

Where the above equation uses the fact that g is in the center, and h commutes with itself. Yet, this shows that $kk' = k'k$ for arbitrary $k, k' \in G$, which G is abelian, contradicting our initial assumption. Hence, the assumption is wfalse, G with prime square power must be abelian.

Back to the classification, for $n = 4$ by Classification Theorem of Finite Abelian Group, $|G| = 4$ implies it's abelian, hence $G \cong \mathbb{Z}/4\mathbb{Z}$ or $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Similarly, for $|G| = 9$, since it's also abelian, $G \cong \mathbb{Z}/9\mathbb{Z}$ or $G \cong \mathbb{Z}/3\mathbb{Z} \times Z/3\mathbb{Z}$.

For $n = 8$, there are two cases: If G is abelian, then again by fundamental theorem of finite abelian group, $G \cong \mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Else, if it's non-abelian, then there doesn't have any element with order 8 (or else G is cyclic), and must have an element with order 4 (or else all nontrivial element with order 2 is abelian, since $(ab)^2 = e \implies abab = e = e^2 = a^2 b^2$, so $ba = ab$).

Now, let $\sigma \in G$ be an element of order 4, the cyclic subgroup $H = \langle\sigma\rangle$ is an order 4 subgroup of G (where $|G| = 8$), hence with index 2, which is normal (since any $\tau \notin H$ satisfies $\tau H \sqcup H = H\tau \sqcup H$, or $\tau H = H\tau$). Then, if $\tau \notin H$, notice that $\overline{\tau} \in G/H$ must have order 2 (since G/H has order 2), then $\tau^2 \in H$.

Notice that $\tau^2 \neq \sigma, \sigma^3$. If not, with σ, σ^3 both are order 4, w getheyerate $H = \langle\sigma\rangle$. Since $G = H \sqcup \tau H$, every element in G is of the form $\tau^i\sigma^j$ (or $\tau^i(\sigma^3)^{j'}$), which can be generated by τ (by swapping σ or σ^3 with τ^2). So, we are left with two cases:

- If $\tau^2 = e$, then $G = D_8$ the dihedral group of regular 4-gon: Given $(\tau\sigma) \in \tau H$, then $(\tau\sigma)^2 \in (\tau H)^2 = H$. However, $(\tau\sigma)^2 \neq \sigma$ (or else $\tau\sigma\tau = e$, showing $\sigma = e$, a contradiction), $(\tau\sigma)^2 \neq \sigma^2$ (or else $\tau\sigma\tau = \sigma$, showing $\tau\sigma = \sigma\tau$, then the generator of H and the generator of G/H commutes, showing G is abelian, again a contradiction), and $(\tau\sigma)^2 \neq \sigma^3$ (since then $(\tau\sigma)^2$ has order 4, and $(\tau\sigma)$ has order 8, which would have order 8 and generates everything, again a contradiction). So, it enforces $(\tau\sigma)^2 = e$, showing $\tau\sigma\tau = \sigma^{-1}$, the dihedral group relation.
- Else if $\tau^2 = \sigma^2$, then notice that $\tau^3 = \tau\sigma^2 \in \tau H$ is nontrivial, while $\tau^4 = \sigma^4 = e$, so $|\tau| = 4$. We'll relable $1 := e$, $i := \sigma$, $-1 := i^2 = \sigma^2$ and $j := \tau$ for this case.

  Then, notice that now $G = H \sqcup jH$ (with $H = \langle i\rangle$) is as follow:

  $$G = \{1, i, -1, i^3 = (-1)\cdot i\} \sqcup \{j, ji, j(-1), j(-1)i\} \tag{4.2}$$

  Now, notice that $(-1)^2 = \left(i^2\right)^2 = i^4 = 1$, and the fact that $(-1) = i^2 = j^2$ shows that $(-1)i = i^3 = i(-1)$, and $(-1)j = j^3 = j(-1)$, showing that (-1) commutes with the generators of G, hence (-1) is central with order 2. Also, if consider the fact that G is non-abelian, the i, j cannot commute (since i, j generates the whole G, if they commute everything commutes). So, with $ij \in Hj = jH$ (by the fact that $j \notin H$), the $ij = j, ji, j(-1)$, or $j(-1)i$. However, $ij \neq j^{-1} = j^3$ (or else $i = j^2 = i^2$ is a contradiction), $ij \neq ji$ by the statement that i, j cannot commute, and $ij \neq j$ simply because $i \neq e$. So, it enforces $ij = j(-1)i = (-1)ji$. Which also shows that $(ij)^2 = (ij)(-1)(ji) = (-1)(ij^2i) = (-1)i(-1)i = i^6 = i^2 = -1$. Hence, we get the following relation:

  $$i^2 = j^2 = (ij)^2 = -1, \quad j(ij) = j(-1)ji = j^4 i = i \tag{4.3}$$

  $$(ij)i = (-1)(ji)i = (-1)j(-1) = (-1)^2 j = j, \quad (-1)^2 = 1 \tag{4.4}$$

  Hence, relable $k := (ij)$, we get:

  $$i^2 = j^2 = k^2 = -1, \quad (-1)^2 = 1, \quad ij = k, jk = i, ki = j \tag{4.5}$$

  $$ij = (-1)ji, \quad kj = (ij)j = i(-1) = (-1)i = (-1)jk \tag{4.6}$$

  $$ik = i(ij) = (-1)j = (-1)ki \tag{4.7}$$

  Hence, it's a quaternion group relation.

So, for non-abelian group of order 8, it's either dihedral group D_8, or the quaternion group (formed by multiplication of $1, i, j, k$).

Finally, for $n = 6, 10$, since $6 = 2 \cdot 3$ and $10 = 2 \cdot 5$, both are the case of $n = 2p$ for some prime p.

If the given group G of order $2p$ is abelian, then $G \cong \mathbb{Z}/(2p)\mathbb{Z}$ or $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ by Fundamental Theorem of Finite Abelian group.

Else, if the group is non-abelian, we claim that it's in fact dihedral group D_{2p}: If G is non-abelian, it cannot have any order $2p$ elements, hence all elements are either order $1, 2$, or p. But, we've proven that all nontrivial element has order 2 implies it's abelian, so there must have nontrivial element $\sigma \in G$ with order p.

Now, since $H = \langle \sigma \rangle$ is order p, with $|G| = 2p$, H is an index 2 subgroup, which is normal. Hence, G/H is a group of order 2, so for all $\tau \notin H$, we have $\overline{\tau} \in G/H$ with order 2, hence $\tau^2 \in H$. But notice that if $\tau^2 \neq e$ (i.e. $\tau^2 = \sigma^k$ for some integer $0 < k < p$), then since σ^k has order p (since k, p are coprime), then σ^k generates H also. Hence, because $G = H \sqcup \tau H$, hence every element is in the form $\tau^i (\sigma^k)^j = \tau^i \cdot \tau^{2j}$, showing τ generates the whole group, yet this is a contradiction (since then G is abelian). So, it enforces $\tau^2 = e$.

Finally, given $(\tau\sigma) \in \tau H$, since $(\tau H)^2 = H$, then $(\tau\sigma)^2 = \sigma^k$ for some integer $0 \leq k < p$. However, if $(\tau\sigma)^2 \neq e$ (or $(\tau\sigma)^2 = \sigma^k$ for some integer $0 < k < p$, where σ^k generates H), since $\tau\sigma \notin H$, then $G = H \sqcup (\tau\sigma)H$. So, every element is in the form $(\tau\sigma)^k (\sigma^k)^j = (\tau\sigma)^{k+2j}$, showing again that $\tau\sigma$ generates G, which is a contradiction. So, $(\tau\sigma)^2 = e$, showing that $\tau\sigma\tau = \sigma^{-1} = \sigma^{p-1}$, hence τ, σ satisfies the dihedral group relation, or G is group isomorphic to a dihedral group.

So, if G has order $2p$, and not abelian, then $G \cong D_{2p}$.

In particular, since $p = 3$ has $D_6 = S_3$, then any non-abelian group of order 6 must be S_3.

5 D

Problem 5

Lang Chapter 1 #34:

(a) Let n be an even positive integer. Show that there exists a group of order $2n$, generated by two elements σ, τ such that $\sigma^n = e = \tau^2$, and $\sigma\tau = \tau\sigma^{n-1}$. This group is called the **dihedral group**.

(b) Let n be an odd positive integer. Let D_{4n} be the group generated by the matrices

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix} \tag{5.1}$$

where ζ is a primitive n-th root of unity. Show that D_{4n} has order $4n$, and give the commutation relations between the above generators.

Solution:

(a) Here, consider a regular n-gon, then its rotation by radian $\frac{2\pi}{n}$ counterclockwise (denote as σ) has order n, and a reflection along one of the symmetric axis passing through the 1^{st} vertex (labeled as τ) has order 2, so $\sigma^n = \tau^2 = e$.

Then, since every of the symmetry on regular n-gon must send consecutive vertices to consecutive vertices, $\sigma\tau$ send vertices 1 and 2 to 1 and n (τ as reflection), then send vertex 1 and n to vertices 2 and 1 (so it swaps the two vertices).

For $\tau\sigma^{n-1}$, they first send vertices 1 and 2 to vertices n and 1 (by σ^{n-1}), then send vertices n and 1 to 2 and 1 (by τ). Hence, $\sigma\tau$ and $\tau\sigma^{n-1}$ provides the same permutation on the vertices (since knowing the relation between 2 of the vertices immediately determines the other vertices, due to the property of isometry on n-gon). Hence, $\sigma\tau = \tau\sigma^{n-1}$ (since they provides the same permutation on the vertices).

(b) Given that $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2 = -\mathrm{id}$, then $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ has order 4; also, since ζ is a primitive n-th root of unity, then $\zeta^n = \zeta^{-n} = 1$ (while any integer $0 < k < n$ doesn't satisfy this relation). Hence, $\begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}$ has order n since its power k has the form $\begin{pmatrix} \zeta^k & 0 \\ 0 & \zeta^{-k} \end{pmatrix}$). So, if D_{4n} is finite, then 4 and n (order of the two generators) must divide $|D_{4n}|$, hence $\mathrm{lcm}(4, n) = 4n$ divides $|D_{4n}|$ (since n is odd).

The reason why D_{4n} is finite, is because if consider the multiplication of the two generators, we get:

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix} = \begin{pmatrix} 0 & -\zeta^{-1} \\ \zeta & 0 \end{pmatrix} = \begin{pmatrix} \zeta^{-1} & 0 \\ 0 & \zeta \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}^{-1}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \tag{5.2}$$

if consider the subgroup H generated by $\left(\begin{smallmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{smallmatrix}\right)$, the above relation shows that it's normal (since both generators has the conjugation of elements in H staying in H). Also, since it provides that the two generators can swap position, with the cost that the one with primitive n-th root is inverted), then every group element $\sigma \in D_{4n}$ in fact can be written as $\left(\begin{smallmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{smallmatrix}\right)^k \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)^l$ for some $k, l \in \mathbb{Z}$. Since there are at most n distinct elements for $\left(\begin{smallmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{smallmatrix}\right)^k$ and there are at most 4 distinct elements for $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)^l$, then there are at most $4n$ distinct elements in D_{4n}.

Hence, this enforces that $|D_{4n}| = 4n$ (since $4n$ divides the order, and the order is at most $4n$).

6 D

Problem 6

Lang Chapter 1 #50:

(a) Show that fiber products exist in the category of abelian groups. In fact, if X, Y are abelian groups with homomorphisms $f : X \to Z$ and $g : Y \to Z$ show that $X \times_Z Y$ is the set of all pairs (x, y) with $x \in X$ and $y \in Y$ such that $f(x) = g(y)$. The maps p_1, p_2 are the projections on the first and second factor respectively.

(b) Show that the pull-back of a surjective homomorphism is surjective.

Solution:

(a) First, recall that product in Grp and Ab (category of groups and abelian groups respectively) is the direct product with the associated group structure. Which, given $f : X \to Z$ and $g : Y \to Z$ two abelian group homomorphisms, let $X \times Y$ denotes the product, and $\pi_X : X \times Y \to X$ and $\pi_Y : X \times Y \to Y$ denote the two projections respectively. Then, $f \circ \pi_X, g \circ \pi_Y : X \times Y \to Z$ are two group homomorphisms.

Since Z is an abelian group, the inversion map $\iota : Z \xrightarrow{\sim} Z$ is in fact a group homomorphism (since for all $a, b \in Z$, $\iota(ab) = (ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} = \iota(a)\iota(b)$), consider the map $h : X \times Y \to Z$, defined as follow:

$$h(x, y) = (\iota \circ f \circ \pi_X(x, y)) \cdot (g \circ \pi_Y(x, y)) = (f(x))^{-1}g(y) \tag{6.1}$$

since $\iota \circ f \circ \pi_X$ and $g \circ \pi_Y$ are both group homomorphisms with codomain Z, while Z is abelian, then the above h is also a group homomorphism. Then, it's valid to consider $\ker(h) \leq X \times Y$.

Now, define $p_1 : \ker(h) \to X$ as restriction of $\pi_X : X \times Y \to X$, similarly $p_2 : \ker(h) \to Y$ as restriction of $\pi_Y : X \times Y \to Y$. We claim that $\ker(h)$ together with p_1, p_2 forms a fiber product of f and g.

First, to show it „equalizes“ f and g, for all $(x, y) \in \ker(h)$, since $h(x, y) = (f(x))^{-1}g(y) = e$ in Z, then $g(y) = f(x)$. Hence:

$$\forall (x,y) \in \ker(h), \quad f \circ p_1(x,y) = f(x) = g(y) = g \circ p_2(x,y) \tag{6.2}$$

This shows that $f \circ p_1 = g \circ p_2$.

Now, to prove it's universal with fiber product property. Given any abelian group G, together with $q_1 : G \to X$ and $q_2 : G \to Y$ that satisfies $f \circ q_1 = g \circ q_2$, by the universal property of product $X \times Y$, there exists a unique group homomorphism $(q_1, q_2) : G \to X \times Y$ such that $q_1 = \pi_X \circ (q_1, q_2)$ and $q_2 = \pi_Y \circ (q_1, q_2)$. However, notice that (q_1, q_2) satisfies $(q_1, q_2)(a) = (q_1(a), q_2(a)) \in X \times Y$ satisfies $f(q_1(a)) = g(q_2(a))$ by definition, hence:

$$h(q_1(a), q_2(a)) = (f(q_1(a)))^{-1} g(q_2(a)) = e \in Z \tag{6.3}$$

Hence, $(q_1(a), q_2(a)) = (q_1, q_2)(a) \in \ker(h)$, showing that $\mathrm{im}\ (q_1, q_2) \subseteq \ker(h) \subseteq X \times Y$, hence it restricts to a group homomorphism $(q_1, q_2) : G \to \ker(h)$ that satisfies $p_1 \circ (q_1, q_2) = \pi_X \circ (q_1, q_2) = q_1$, and $p_2 \circ (q_1, q_2) = \pi_Y \circ (q_1, q_2) = q_2$, this shows the existence of a group homomorphism $G \to \ker(h)$.

Finally, to show this map is indeed unique, suppose $l : G \to \ker(h)$ is another group homomorphism such that $p_1 \circ l = q_1$ and $p_2 \circ l = q_2$. Then, for all $a \in G$, $p_1 \circ l(a) = \pi_X(l(a)) = q_1(a)$ and $p_2 \circ l(a) = \pi_Y(l(a)) = q_2(a)$, hence $l(a) = (q_1(a), q_2(a)) = (q_1, q_2)(a) \in \ker(h) \leq X \times Y$, showing $l = (q_1, q_2)$. Hence, such map $G \to \ker(h)$ is unique.

This shows that $\ker(h)$ together with $p_1 : \ker(h) \to X$ and $p_2 : \ker(h) \to Y$ is indeed a fiber product of $f : X \to Z$ and $g : Y \to Z$, showing fiber product exists in Ab.

Now, recall that $(x, y) \in \ker(h)$ iff $h(x, y) = (f(x))^{-1} g(y) = e$, which is equivalent to $f(x) = g(y)$. Hence, $\ker(h)$ is also characterized by all $(x, y) \in X \times Y$, such that $f(x) = g(y)$.

(b) For definiteness, given $f : X \to Z$ and $g : Y \to Z$ two abelian group homomorphisms, and say g is surjective. Then, let the fiber product $X \times_Z Y \leq X \times Y$ collect all the element $(x, y) \in X \times Y$ satisfying $f(x) = g(y)$ (together with $p_1 : X \times_Z Y \to X$ and $p_2 : X \times_Z Y \to Y$ be the two projections).

To show that p_1 (the pull-back of g) is also surjective, consider the following: For all $x \in X$, since $f(x) \in Z$ and g is surjective, there exists $y \in Y$, such that $g(y) = f(x)$. Hence, the pair $(x, y) \in X \times_Z Y$, and $p_1(x, y) = x$, this shows that $x \in \mathrm{im}(p_1)$, or $X = \mathrm{im}(p_1)$. Hence, p_1 (the pull-back of g) is also surjective.

7 ND

Problem 7

Lang Chapter 1 #51:

(a) Show that fiber products exist in the category of sets.

(b) In any category $\mathcal{C}$, consider the category $\mathcal{C}_Z$ of objects over Z. Let $h : T \to Z$ be a fixed object in this category. Let F be the functor such that

$$F(X) = \mathrm{Mor}_Z(T, X) \tag{7.1}$$

where X is an object over Z, and Mor_Z denotes morphisms over Z. Show taht F transforms fiber products over Z into products in the category of sets.

Solution:

(a) Given any $f : X \to Z$ and $g : Y \to Z$ as set functions, let $X \times Y$ denote the product of the two sets, $\pi_1 : X \times Y \to X$ and $\pi_2 : X \times Y \to Y$ denote the two projections, while $H \subseteq X \times Y$ collects all $(x, y) \in X \times Y$, such that $f(x) = g(y)$. We claim that H together with the restriction of π_1, π_2 onto H forms a fiber product of f, g in the category of sets.

First, for all $(x, y) \in H$, we have $f \circ \pi_1(x, y) = f(x) = g(y) = g \circ \pi_2(x, y)$, hence $f \circ \pi_1 = g \circ \pi_2 : H \to Z$, showing that it satisfies the basic properties a fiber product needs.

Then, to show its universality, suppose set A together with $q_1 : A \to X$ and $q_2 : A \to Y$ satisfies $f \circ q_1 = g \circ q_2$. Since it maps from A to both X and Y, by the universality of direct product in sets, there exists a unique map $(q_1, q_2) : A \to X \times Y$, such that $\pi_1 \circ (q_1, q_2) = q_1$, and $\pi_2 \circ (q_1, q_2) = q_2$ (without restricting the domain of π_1, π_2). Now, notice that for all $a \in A$, since $f \circ q_1(a) = g \circ q_2(a)$, then $(q_1, q_2)(a) = (q_1(a), q_2(a)) \in H$ by definition, hence $(q_1, q_2) : A \to H$ is a well-defined function after restriction.

Also, notice that $(q_1, q_2) : A \to H$ must necessarily be unique: Suppose some other $h : A \to H$ satisfies $\pi_1 \circ h = q_1$ and $\pi_2 \circ h = q_2$, then $\pi_1(h(a)) = q_1(a)$ and $\pi_2(h(a)) = q_2(a)$, showing that $h(a) = (q_1(a), q_2(a)) = (q_1, q_2)(a)$, hence $h = (q_1, q_2)$.

So, this proves that given set A with $q_1 : A \to X$ and $q_2 : A \to Y$ satisfying $f \circ q_1 = g \circ q_2$, then this pair (A, q_1, q_2) necessarily factors through the pair (H, π_1, π_2) (where π_i are restricted to H), hence (H, π_1, π_2) does serve as a fiber product of f, g, inside the category of sets.

(b) IDK