1-3 Consider $G = D_{2n}$ and let r be a generator for the rotations. Show r^n is in the center $Z(G)$ and let $H = \{e, r^n\}$. G/H is a group of order n. Find a known group of order n which is isomorphic to G/H.

Solution We need to prove that r^n commutes with all the elements D_{2n}. Recall that in D_{2n}, we have $fr = r^{2n-1}f$.

It's clear that r^n commutes with r^m for any power m, so it suffices to check commutativity with the flip f, i.e., $r^n f = fr^n \iff f = r^{-n}fr^n = r^n fr^n$.

$$r^n fr^n = r^n r^{2n-1} fr^{n-1} = r^n (r^{2n-1})^n f = r^n r^{-n} f = f,$$

so r^n is in the center. It is also clearly normal by definition, so G/H is a group.

Notice that

$$\begin{aligned}(rH)^n &= r^n H = H\\ (fH)^2 &= f^2 H = H\\ fH \cdot rH &= r^{2n-1} fH = r^n r^{n-1} fH = r^n H \cdot r^{n-1} fH = r^{n-1} fH,\end{aligned}$$

so we can write

$$G/H = \langle rH, fH \mid (rH)^n = (fH)^2 = 1,\ fH \cdot rH = r^{n-1}H \cdot fH\rangle \simeq D_n.$$

11.9.8ii Let H be a subgroup of G. We defined the *core* of H in G to be $\mathrm{Cor}_G(H) \coloneqq \bigcap xHx^{-1}$, and the *normalizer* of H in G to be $N_G(H) \coloneqq \{x \in G \mid xHx^{-1} = H\}$, respectively.

Show $N_G(H)$ is the unique largest subgroup of G containing H as a normal subgroup.

Solution First, we need to check that $N_G(H)$ is a group. It's easy to see that e is the identity, and that if $x \in N_G(H)$,

$$xHx^{-1} = H \implies H = x^{-1}Hx,$$

so $x^{-1} \in N_G(H)$. Lastly, if $x, y \in N_G(H)$, then

$$H = x^{-1}Hx = yHy^{-1} \implies xyHy^{-1}x^{-1} = H,$$

so $xy \in N_G(H)$. Thus, $N_G(H)$ is a subgroup of G.

It's clear that $H \triangleleft N_G(H)$, so we only need to show that it's the largest subgroup.

Let N be a subgroup of G which contains H as a normal subgroup. If $x \in N$, then

$$xHx^{-1} = H \implies x \in H \implies N \subseteq H,$$

so it is the largest one.

By the same argument above, if N, N' are the largest subgroups containing H as a normal subgroup, $N \subseteq N' \subseteq N$, so $N = N' = N_G(H)$, which completes the proof.

11.9.11 Let G be a cyclic group. Determine $\mathrm{Aut}(G)$ and $\mathrm{Inn}(G)$ up to isomorphism as groups that we know. Prove your result. *Hint*: Where do generators go?

Solution By definition, there exists $x \in G$ with order n such that $\langle x \rangle = G$.

We claim that $\mathrm{Aut}(G) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.

Let $\sigma \in \mathrm{Aut}(G)$. We must have that $\operatorname{ord}\sigma(x) = |G|$. Otherwise, there exists some $N < |G|$ such that $\sigma(x)^N = e \implies x^N \in \ker\sigma$. But this contradicts the injectivity of σ, so $\sigma(x)$ generates G.

Moreover, if $\sigma(x) = x^m$, then $d = \gcd(n, m) = 1$. Otherwise, there exists n', m' such that $n = dn'$ and $m = dm'$ with $n' < n$ so that

$$\sigma(x)^{n'} = x^{mn'} = x^{dn'm'} = x^{nm'} = e,$$

which is a contradiction, since $\sigma(x)$ generates G.

Thus, we can identify the elements of $\mathrm{Aut}(G)$ with the numbers coprime with and smaller than n, e.g., if $\sigma(x) = x^a$, then we identify $\sigma \sim a$.

Lastly, if $\sigma(x) = x^a$ and $\sigma'(x) = x^b$, $\sigma \circ \sigma'(x) = \sigma' \circ \sigma(x) = \sigma(x)^{ab}$, which is the same as multiplication in $(\mathbb{Z}/n\mathbb{Z})^\times$. Thus, $\mathrm{Aut}(G) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.

Our next claim is that $\mathrm{Inn}(G) \simeq \{e\}$, the trivial group. If we pick $x^n \in G$, then

$$\theta_{x^a}(x^b) = x^a x^b x^{-a} = x^a \implies \theta_{x^a} = \mathrm{id},$$

for any a. So, any inner automorphism is the identify function, which shows $\mathrm{Inn}(G) \simeq \{e\}$.

11.9.12 Let G and H be finite cyclic groups of order m and n, respectively.

Show the following:

a. If m and n are relatively prime, then $\mathrm{Aut}(G \times H) \simeq \mathrm{Aut}(G) \times \mathrm{Aut}(H)$ and is abelian.

b. If m and n are not relatively prime, then $\mathrm{Aut}(G \times H)$ is never abelian.

Solution Notice that $G \simeq \mathbb{Z}/m\mathbb{Z}$ and $H \simeq \mathbb{Z}/n\mathbb{Z}$ since they are cyclic, so we will work with those groups specifically.

a. Let $\gcd(m, n) = 1$.

By the Chinese remainder theorem, $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/mn\mathbb{Z}$, so by the previous problem,

$$\mathrm{Aut}(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) \simeq \mathrm{Aut}(\mathbb{Z}/mn\mathbb{Z}) \simeq (\mathbb{Z}/mn\mathbb{Z})^\times \simeq (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times.$$

Indeed, the last isomorphism comes from the fact that since m and n are coprime, given an element $N \in (\mathbb{Z}/mn\mathbb{Z})^\times$, we can take the natural map $[a]_{mn} \mapsto ([a]_m, [a]_n)$.

b. Let $d = \gcd(m, n) \neq 1$, so that there exist $m', n' \in \mathbb{Z}$ such that $m = dm'$ and $n = dn'$.

Let $\sigma \in \mathrm{Aut}(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})$. We can represent σ as a 2×2 matrix.

Indeed, since σ is a homomorphism, we know that

$$\sigma(ax, by) = \sigma(ax, 0) + \sigma(0, by) = a\sigma(x, 0) + b\sigma(0, y),$$

so it's linear. However, we must be careful, since coefficients will come from the $\mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Z}/nZ$.

Consider the following pair of matrices:

$$\begin{pmatrix} 1 & m' \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ n' & 1 \end{pmatrix} = \begin{pmatrix} 1 + m'n' & m' \\ n' & 1 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 0 \\ n' & 1 \end{pmatrix} \begin{pmatrix} 1 & m' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & m' \\ n' & 1 + m'n' \end{pmatrix}.$$

We now need to check if the entries are truly different.

Notice that the first row is from $\mathbb{Z}/m\mathbb{Z}$ and the second row is from $\mathbb{Z}/n\mathbb{Z}$, so if the matrices were equivalent, we need to have both

$$m'n' \equiv 0 \mod m \iff m \mid m'n' \quad \text{and} \quad m'n' \equiv 0 \mod n \iff n \mid m'n'.$$

However, if this were the case, $mn \mid m'n' \implies d^2mn \mid mn$, which is a contradiction since $d > 1$.

Thus, the two products are different, so our matrices don't commute. Thus, $\mathrm{Aut}(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})$ is never abelian.

11.9.19** A *commutator* in G is an element of the form $xyx^{-1}y^{-1}$ where $x, y \in G$. Let G' be the subgroup of G generated by all commutators, i.e., every element in G' is the product of commutators. We call G' the *commutator* or *derived subgroup* of G. It is also denoted $[G, -G]$.

Show

a. $G' \lhd G$.

b. $G' \lhd \lhd G$.

Solution a. Let $x \in G$. Then

$$xG'x^{-1} = xeG'x^{-1}e^{-1} = G,$$

so G' is normal.

b. Let $\sigma \in \mathrm{Aut}(G)$ and consider its restriction $\sigma|_{G'}$.
Let $xyx^{-1}y^{-1}\ inG'$. Then

$$\sigma(xyx^{-1}y^{-1}) = \sigma(x)\sigma(y)(\sigma(x))^{-1}(\sigma(y))^{-1} \in G',$$

by definition. Thus, $\sigma|_{G'}$ maps G' to G'. $|G'| = |G'|$ and σ is injective, so by the pigeonhole principle, $\sigma|_{G'}$ is a bijection, which means $\sigma|_{G'} \in \mathrm{Aut}(G')$. Hence, by definition, $G' \lhd \lhd G$.

11.9.20 Let $K \subseteq H \subseteq G$ be subgroups of G. Show all of the following:

a. If $K \lhd \lhd H$ and $H \lhd G$ then $K \lhd G$.

b. $Z(G) \lhd \lhd G$.

c. $G' \lhd \lhd G$.

d. Inductively define $G^{(n)}$ as follows: $G^{(1)} = G'$. Having defined $G^{(n)}$ define $G^{(n+1)} := (G^{(n)})'$. Then $G^{(n+1)} \lhd \lhd G$.

Solution a. Since $H \lhd G$, we have that $xHx^{-1} = H$ for all $x \in G$, so $\theta_x(h) := xhx^{-1}$ is an automorphism of H for any $x \in G$.
Thus, since $K \lhd \lhd H$, we get that $\theta_x|_K$ is an automorphism of K, we get

$$K = \theta_x|_K(K) = xKx^{-1}$$

for all $x \in G$, so $K \lhd G$.

b. Let $\sigma \in \mathrm{Aut}(G)$. Then for $x \in Z(G)$ and $g \in G$. Since σ is bijective, there exists $g_0 \in G$ such that $\sigma(g_0) = g$, so

$$xg_0 = g_0x \implies \sigma(x)g = g\sigma(x) \implies \sigma(x) \in Z(G).$$

Thus, $\sigma|_{Z(G)} \in \mathrm{Aut}(Z(G))$, so by definition, $Z(G) \lhd \lhd G$.

c. See problem 11.9.19(b) right before this problem.

d. We'll prove this by induction on n. We have already shown the base step, so we only need to show the inductive step.
Suppose $G^{(1)}, \ldots, G^{(n)} \lhd\lhd G$. We wish to show that $G^{(n+1)} \lhd\lhd G$.
Let $\sigma \in \mathrm{Aut}(G)$.
Pick $xyx^{-1}y^{-1} \in G^{(n+1)}$, for $x, y \in G^{(n)}$. Then

$$\sigma(xyx^{-1}y^{-1}) = \sigma(x)\sigma(y)(\sigma(x))^{-1}(\sigma(y))^{-1}.$$

$\sigma(x)$ and $\sigma(y)$ are in $G^{(n)}$, since $G^{(n)} \lhd\lhd G$ and σ is an automorphism of G, so $\sigma(xyx^{-1}y^{-1}) \in G^{(n+1)}$.
Thus, $\sigma|_{G^{(n+1)}} \in \mathrm{Aut}(G^{(n+1)})$.

12.11.7** Let H be a subgroup of G. Define the *centralizer* of H in G to be

$$Z_G(H) := \{x \in G \mid xh = hx \text{ for all } h \in H\}.$$

Show that it is a normal subgroup of $N_G(H)$ and the map given by $x \mapsto (\theta_x \mid g \mapsto xgx^{-1})$ induces $\tilde{\theta}\colon N_G(H)/Z_G(H) \to \mathrm{Aut}(H)$, a monomorphism defined by $xZ_G(H) \to \theta_x|_H$.

Solution Notice that $Z_G(H) \subseteq N_G(H)$.
Let $x \in N_G(H)$ and $y \in Z_G(H)$. We wish to show that $xyx^{-1} \in Z_G(H)$.
Let $g \in G$. By definition, there exists $g' \in G$ such that $g' = x^{-1}gx$, so we get

$$xyx^{-1}gxyx^{-1} = xyg'yx^{-1} = xg'x^{-1} = g,$$

so $xyx^{-1} \in Z_G(H) \implies xZ_G(H)x^{-1} \subseteq Z_G(H)$.
We now wish to show that $y \in xZ_G(H)x^{-1}$, which is equivalent to showing that $x^{-1}yx \in Z_G(H)$. This is the same as the previous argument, so we're done.

We now wish to show that $xZ_G(H) \overset{\tilde{\theta}}{\mapsto} \theta_x|_H$ is a well-defined, injective homomorphism.
Let $x, x' \in N_G(H)$ so that $xZ_G(H) = x'Z_G(H)$. Then by definition, for every $h \in H$, there exists $h' \in H$ such that $h' = xhx^{-1}$. Moreover, since the cosets are the same, for every $y \in Z_G(H)$, there exists $y' \in Z_G(H)$ such that $xy = x'y' \implies x' = xyy'^{-1}$. Then

$$\theta_{x'}|_H(h) = x'hx'^{-1} = xyy'^{-1}hy'y^{-1}x^{-1} = xyhy^{-1}x^{-1} = xhx^{-1} = \theta_x|_H(h),$$

so the map is well-defined.
Let $\theta_x|_H = \theta_{x'}|_H$. Then for all $h \in H$,

$$xhx^{-1} = x'hx'^{-1} \implies h = (x^{-1}x')h(x^{-1}x')^{-1} \implies x^{-1}x' \in Z_G(H) \implies x' \in xZ_G(H).$$

Thus, $x'Z_G(H) \subseteq xZ_G(H)$. We can perform the same argument to see that $xZ_G(H) \subseteq x'Z_G(H)$, so $xZ_G(H) = x'Z_G(H)$, which means the map is injective.
Lastly, we need to show that the map is a homomorphism.
Let $xZ_G(H), x'Z_G(H) \in N_G(H)/Z_G(H)$. Then

$$\tilde{\theta}(xZ_G(H) \cdot x'Z_G(H)) = \tilde{\theta}(xx'Z_G(H)) = \theta_{xx'}|_H.$$

But

$$\theta_{xx'}|_H(h) = x(x'hx'^{-1})x = \theta_x|_H(h) \circ \theta_{x'}|_H(h),$$

so the map is homomorphic.
Thus, $\tilde{\theta}$ is a monomorphism.