MODERN ALGEBRA NOTES

KLINT QINAMI

Preamble. The following is a collection of exercises relating to modern algebra, together with my proofs of those exercises. Use at your own risk.

Proposition 1. *Let S be a set and G be a group. Let $F(S,G)$ be the set of all functions $f : S \mapsto G$. We can define a binary operation, denoted for a pair of functions $f, g \in F(S,G)$ as fg, to be such that $\forall s \in S$, $(fg)(s) = f(s) \cdot g(s)$. $F(S,G)$ forms a group with this operation.*

Proof. To verify $F(S,G)$ forms a group with this operation, we must check the existence of an identity element, the existence of inverses, and associativity.

The identity element for $F(S,G)$ will be the function $i : S \mapsto G$ such that $\forall s \in S, i(s) = e$ where e is the identity element in G. It is simple to check that for all functions $g \in F(S,G)$, $\forall s \in S, (ig)(s) = i(s) \cdot g(s) = e \cdot g(s) = g(s)$ and $(gi)(s) = g(s) \cdot i(s) = g(s) \cdot e = g(s)$.

For a function $f \in F(S,G)$, the inverse function $f^{-1} \in F(S,G)$ is the function such that $\forall s \in S, (ff^{-1})(s) = (f^{-1}f)(s) = f^{-1}(s) \cdot f(s) = f(s) \cdot f^{-1}(s) = e = i(s)$. This function is well defined as $\forall s \in S, f(s) \in G$ has a unique inverse by the definition of group. This uniqueness means that $\forall x, y \in S, x = y \implies f^{-1}(x) = f^{-1}(y)$ and thus the inverse function exists and is well defined.

Finally, we need associativity. We see $\forall f, g, p \in F(S,G), \forall s \in S, (f(gp))(s) = f(s) \cdot (g(s) \cdot p(s))$. By associativity of the group G, we have $f(s) \cdot (g(s) \cdot p(s)) = (f(s) \cdot g(s)) \cdot p(s) = ((fg)p)(s)$ and thus the group operation on $F(S,G)$ is associative.

Since we have associativity, the identity element, and inverses, $F(S,G)$ forms a group with the given binary operation.

Interpreting $S = G = \mathbb{R}$, we have that $F(S,G)$ is the set of all real valued functions with a real argument. We have function addition where $\forall x \in \mathbb{R}, \forall f, g \in F(S,G), (f+g)(x) = f(x) + g(x)$. ∎

Proposition 2. *$\{f \in \Sigma_n \mid f(1) = 1\}$ is a subgroup of Σ_n.*

Proof. Let $S = \{f \in \Sigma_n \mid f(1) = 1\}$. The identity function $\mathrm{id} : \langle n \rangle \mapsto \langle n \rangle$ is in S as $\mathrm{id}(1) = 1$. Additionally, for any function $f \in S$, we must have the inverse function $f^{-1} \in S$ as $f^{-1}(1) = 1$. Associativity of function composition still remains in the subgroup. Checking closure we see that $\forall f, g \in S, (f \circ g)(1) = f(g(1)) = f(1) = 1$ and thus $f \circ g \in B$. Since we have associativity, the identity element, and inverses,S is a subgroup of Σ_n. ∎

Proposition 3. *For a set S and an element $x \in S$, $\{f \in Bij\, S \mid f(x) = x\}$ is a subgroup of $BijS$ which denotes the set of all bijections from S to itself with function composition.*

Proof. Let $B = \{f \in \text{Bij } S \mid f(x) = x\}$. Since the identity bijection $\text{id} : S \mapsto S$ has $\text{id}(x) = x$, $\text{id} \in B$. Additionally, we also have that $\forall f \in B$, f^{-1} is also in B as $f^{-1}(x) = x$. Lastly, associativity of function composition remains. We also have closure as $\forall f, g \in S, (f \circ g)(x) = f(g(x)) = f(x) = x$ and thus $f \circ g \in B$. Since we satisfy all of the group axioms, B must be a subgroup of Bij S. ■

Proposition 4. *The only subgroups of $\mathbb{Z} \times \mathbb{Z}_2$ are of the form $k\mathbb{Z} \times \mathbb{Z}_2$, $k\mathbb{Z} \times \{0\}$, and all tuples of the form$(k\mathbb{Z}, [\mathbb{Z}])$, where k is the least positive integer appearing as a left element.*

Proof. We can prove this by partitioning the subgroups into cases. First, let us note the set of elements appearing as the first coordinate of any subgroup form a subgroup of $\mathbb{Z}$, namely of the form $k\mathbb{Z}$. That is, for the least positive integer k appearing as the left element, we must have all multiples of $(k, 0)$ appearing as well. This follows from the closure under addition, existence of inverse, and existence of the identity.

Next we partition all subgroups into the cases where $(k, 0)$ and $(k, 1)$ are in the subgroup, $(k, 0)$ is in the subgroup only, and $(k, 1)$ is in the subgroup only.

If both $(k, 0)$ and $(k, 1)$ appear, then we must have that the subgroup is $k\mathbb{Z} \times \mathbb{Z}_2$. This is because we can always take $(-k, 0) + (k, 1) = (0, 1)$, and thus having $(0, 1)$ we can always get from $(kz, 0)$ to $(kz, 1)$ by adding $(0, 1)$ and vice-versa.

If only $(k, 0)$ appears, then we must have that our subgroup is of the form $k\mathbb{Z}\times\{0\}$. To see why we cannot have any element $(a, 1)$ appear, we note that if such an element existed, then a must be a multiple of k by definition of k. If a is a multiple of k, then we must also have $(a, 0)$ be in the subgroup as we have all multiples $k\mathbb{Z}$ in the subgroup. This would imply that $(0, 1)$ is also in the subgroup, as we can take $(-a, 0) + (a, 1)$. But then this would mean $(k, 1)$ is in the subgroup, as we could take $(k, 0) + (0, 1)$, which is a contradiction and thus we must not have any element of the form $(a, 1)$.

Lastly, if only $(k, 1)$ appears, then we must have that the group has tuples of the form $(k\mathbb{Z}, [Z])$ where $[\,]$ indicate result modulo 2. This is because we must have all integer multiples of $(k, 1)$ in the subgroup, which we can write as $\mathbb{Z}(k, 1)$, which is a slight abuse of notation but tells us that all tuples of the form $(k\mathbb{Z}, [\mathbb{Z}])$ are in the subgroup. Now we must only show that there are no other kinds of elements in the subgroup. This follows again from the fact that we do not have the element $(0, 1)$ in the subgroup for the same reason as above, and therefore if we have any element $(a, 0)$, we must not have $(a, 1)$, and vice-versa. Since we know that there are no tuples that do not contain a multiple of k as the left element of the tuple, we have shown that all elements of the subgroup must be of the form $(k\mathbb{Z}, [\mathbb{Z}])$.

Since we have exhaustively enumerated all possible subgroups through a partition, we are done. ■

Proposition 5. *If $\#G$ is even and G is a group, then there must exist an element other than the identity which is its own inverse.*

Proof. Let $S = \{g \in G \mid g \neq g^{-1}\}$. Let $T = \{g \in G \mid g = g^{-1}\}$.We must have $\#S + \#T = \#G$ as $S \cap T = \varnothing$ and $S \cup T = G$. We also must have $\#S$ be even

as each element can be paired with its own inverse. Since $\#G$ is even and $\#S$ is even and $\#S + \#T = \#G$, then $\#T$ is even and therefore there must be an element other than the identity that is its own inverse. ■

Proposition 6. *Let G be a group and $g, h \in G$. Let e be the identity element in G. Then $gh = hg \iff h^{-1}gh = g \iff g^{-1}h^{-1}gh = e$.*

Proof. We have

$$\begin{aligned} gh &= hg && \\ h^{-1}gh &= h^{-1}hg && \text{Def. equality} \\ h^{-1}gh &= eg && \text{Def. inverse} \\ h^{-1}gh &= g && \text{Def. identity} \\ g^{-1}h^{-1}gh &= g^{-1}g && \text{Def. equality} \\ g^{-1}h^{-1}gh &= e && \text{Def. inverse} \end{aligned}$$

Since each step is invertible, we have shown the three way iff. ■

Proposition 7. *If G is a group and $\forall g \in G, g^2 = e$, then G is abelian.*

Proof. To show G is abelian, we need to show that $\forall g, h \in G, gh = hg$. All elements in G are their own inverse, we must have

$$\begin{aligned} (gh)(gh) &= e && \\ (gh)(gh)h &= h && \\ (gh)(g)(hh) &= h && \text{Associativity} \\ (gh)g &= h && \text{Def. inverse} \\ (gh)gg &= hg && \\ gh &= hg && \text{Def. inverse} \end{aligned}$$

Since we have commutativity, we know that G is abelian. ■

Proposition 8. *For groups G and H, $G \times H$ is abelian $\iff$ G and H are abelian.*

Proof. If $G \times H$ is abelian, then for $g_1, g_2 \in G, h_1, h_2 \in H$, $(g_1, h_1)(g_2, h_2) = (g_2, h_2)(g_1, h_1)$. This implies $(g_1g_2, h_1h_2) = (g_2g_1, h_2h_1)$ and $g_1g_2 = g_2g_1$ and $h_1h_2 = h_2h_1$. Therefore, G and H are abelian.

If G and H are abelian, then $\forall g_1, g_2 \in G, h_1, h_2 \in H$, $g_1g_2 = g_2g_1$ and $h_1h_2 = h_2h_1$. We thus have $(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2) = (g_2g_1, h_2h_1) = (g_2, h_2)(g_1, h_1)$ and thus $G \times H$ is abelian. ■

Proposition 9. *Let $H < K < G$ with $[G : H]$ finite. Then $[G : H], [K : H]$ are also finite and $[G : H] = [G : K][K : H]$.*

Proof. Consider $f : G/H \mapsto G/K$ such that $f(gH) = gK$ for some $g \in G$. This is well defined as $gH = g'H \implies g' = gh$ for some $h \in H$, and this means $f(g'H) = g'K = ghK = gK$ by $H < K$. Thus $gH = g'H \implies f(gH) = f(g'H)$.

f must also be surjective, as for any $gK \in G/K$ we must have $gH \in G/H$ and thus $f(gH) = gK$.

Now we define a new bijection from the preimages of f to G/K, namely $l_{g^{-1}} : f^{-1}(gK) \mapsto K/H$ such that $l_{g^{-1}}(xH) = g^{-1}xH$. We can see $f(xH) = xK = gK$ and thus $g^{-1}x \in K$. Checking that it's well defined as for $xH, x'H \in f^{-1}(gK)$, $x = x'h'$ and $l_{g^{-1}}(x'H) = g^{-1}x'H = g^{-1}xhH = g^{-1}xH = l_{g^{-1}}(xH)$. Checking injectivity, we have $l_{g^{-1}}(xH) = l_{g^{-1}}(x'H) = g^{-1}xH = g^{-1}x'H$. Multiplying by g inverse on the left, $xH = x'H$. Checking surjectivity, for any xH in the range we have $f(gxH) = g^{-1}gxH = xH$ and thus the map is surjective and therefore is bijective.

We know that we have a bijection from the preimages of f to G/K. Because f is surjective then the preimages are non empty as G/K is nonempty as cosets are never empty. Because the preimages are also disjoint, and their disjoint union is a finite set (that is G/H is finite), we must have finitely many preimages and thus G/K is finite. We also know that K/H has to be finite as we have a bijection $l_{g^{-1}}$ from the preimages of f and G/K.

Lastly we can create a bijection from $u : G/K \mapsto G/K \times K/H$ by arbitrarily ordering the preimages of each gK as we know there are exactly $[K/H]$ of them through our bijection $l_g{-}1$. Since we have this bijection u, we must then have that $[G : H] = [G : K][K : H]$. ■

Proposition 10. *If $H < G$ and $K < G$, with $[G : H] = m$ and $[G : K] = n$, then $lcm(m, n)] \leqslant [G : H \cap K] \leqslant mn$. Also, if $gcd(m, n) = 1$, then $[G : H \cap K] = [G : H][G : K]$.*

Proof. Let us begin by quickly showing that $H \cap K$ is a subgroup of K and a subgroup of H. Since $e \in H \wedge e \in K$, $e \in (H \cap K)$. Additionally, $g \in H \wedge g \in K \implies g^{-1} \in H \wedge g^{-1} \in K \implies g^{-1} \in (H \cap K)$ and thus we have closure under inverses. Closure under the group operation follows as $g, h \in H \wedge g, h \in K \implies gh \in H \wedge gh \in K \implies gh \in (H \cap K)$.

Then by **Proposition 9** we must have that

$$\begin{aligned}[G : H \cap K] &= [H : H \cap K][G : H] \\ &= m[H : H \cap K] \\ &= [H : H \cap K][G : H] \\ &= n[H : H \cap K]\end{aligned}$$

Since $[G : H \cap K]$ is a multiple of m and n, it must be greater than or equal to the least common multiple of m and n.

All that's left to show is that $[G : H \cap K] \leqslant mn$. We can show this by defining a function $f : G/(H \cap K) \mapsto G/H \times G/K$. If we can define f such that it is well defined and injective, then $[G : H \cap K] \leqslant mn$ as $\#(G/H \times G/K) = mn$ and f would be a bijection from the domain to a subset of the range. Let f be such that for a coset $g(H \cap K) \in G/(H \cap K)$, $f(g(H \cap K)) = (gH, gK)$. To see that f is well defined, we show $g(H \cap K) = g'(H \cap K)$ implies $f(g(H \cap K)) = f(g'(H \cap K))$. For

this we will non-chronologically reference the equivalence relation in **Proposition 5**.

If $g(H \cap K) = g'(H \cap K)$, then $g \overset{H\cap K}{\sim} g'$, and $g' = gh_1$ for $h_1 \in H \cap K$. Since $H < G$ and $K < G$, then we must also have that $g \overset{H}{\sim} g'$ and $g \overset{K}{\sim} g'$. This means $gH = g'H$ and $gK = g'K$ and thus $f(g(H \cap K)) = f(g'(H \cap K))$. This shows f is well-defined.

Now we must show injectivity and be done. We have

$$f(g(H \cap K)) = f(g'(H \cap K)) \tag{1}$$

$$(gH, gK) = (g'H, g'K) \tag{2}$$

$$gH = g'H \quad gK = g'K \tag{3}$$

$$gH \cap gK = g'K \cap g'L \tag{4}$$

$$g(H \cap K) = g'(H \cap K) \tag{5}$$

Step 5 is justified as the left cosets are bijections and for bijections g we have $g(S \cap T) = g(S) \cap g(T)$. Since $f(g(H \cap K)) = f(g'(H \cap K)) \implies g(H \cap K) = g'(H \cap K)$, f is injective and $[G : H \cap K] \leqslant mn$.

To deduce that if $\gcd(m, n) = 1$, $[G : H \cap K] = [G : H][G : K]$, we employ the fact that $\operatorname{lcm}(m, n) \times \gcd(m, n) = mn$. Since $\gcd(m, n) = 1$, then $\operatorname{lcm}(m, n) = mn$ and $[G : H \cap K] = mn = [G : H][G : K]$. ■

Proposition 11. *If $H < G$, $K < G$, and $gcd(\#H, \#K) = 1$, then $H \cap K = \{e\}$.*

Proof. Since $H \cap K < H$ and $H \cap K < K$, then by Lagrange's Theorem $\#(H \cap K) \mid \#K$ and $\#(H \cap K) \mid \#H$. We therefore must have that $\#(H \cap K) = 1$ as $\gcd(\#H, \#K) = 1$ and thus $H \cap K = \{e\}$. ■

Proposition 12. *If $\forall g \in G, f \circ l_g = l_g \circ f$, then $f = r_h$ for some $h \in G$.*

Proof. $(f \circ l_g) = f(l_g(x)) = f(gx)$ and $(l_g \circ f)(x) = l_g(f(x)) = gf(x)$ and thus $\forall g \in G, f(gx) = gf(x)$. Thus $f(x) = f(xe) = xf(e)$. Therefore for any $x \in G$, we can express $f(x) = xh = r_h(x)$. ■

Proposition 13. *For $H < G$, $g \sim g' \iff \exists h \in H$ s.t. $g' = gh$ defines an equivalence relation whose equivalence classes are left H-cosets.*

Proof. $\sim$ is reflexive as $g \sim g$, since for $h = e$, we have $g = ge = g$ and $e \in H$ because H is a group. $\sim$ is also symmetric as $g \sim g'$ implies $g' = gh$ and thus $g'h^{-1} = ghh^{-1} = g$ and thus $g' \sim g$ since $h^{-1} \in H$ by group closure under inverses. Transitivity follows as $x \sim y$ implies $y = xh_1$ and $y \sim z$ implies $z = yh_2$ and thus $z = xh_1h_2$ and $x \sim z$ as $h_1h_2 \in H$ because of group closure under the group operation.

To show the equivalence classes are the left cosets of H, we must show $g \sim g' \iff g, g'$ are in the same left coset. If $g \sim g'$, then $g' = gh$ and thus $g' \in gH$. Since we also have that $g \in gH$ and that the left cosets are disjoint, then g, g' are in the same left coset and in no other cosets.

We also have that if g and g' are in the same left coset, then $g \in \gamma H$ and $g' = \gamma H$ for some $\gamma \in G$. Then we must have $g = \gamma h$ and $g' = \gamma h'$. But then $g' = gh^{-1}h'$ and thus $g \sim g'$. ■

Proposition 14. *Let $H < G$ and $f : G \mapsto G$ such that $f(x) = x^{-1}$. Then f gives a bijection from left cosets to right cosets.*

Proof. Let us consider $f : G \mapsto G$ and prove this is a bijection. We must show that f is injective and surjective. f is injective as if $x = y$, then $f(x) = f(y)$ by uniqueness of inverses. f is surjective as again as for any x, we have $f(x^{-1}) = x$. Since f is bijective, we must have that $Pf : PG \mapsto PG$ is bijective, and thus is f is a bijection on the left cosets of G.

Now we must only show that f takes left cosets to right cosets and we are done. For any left coset gH where $g \in G$, any element $gh \in gH$ gets mapped by f as $f(gh) = (gh)^{-1} = h^{-1}g^{-1}$. Therefore we have that the image of $f(gH)$ is Hg^{-1} and thus f is a bijection from left cosets to right cosets. ■

Proposition 15. $\#Z_p^\times = p - 1$.

Proof. For all $a \in Z_p \backslash \{0\}$, $\gcd(a, p) = 1$ since p is prime, and thus all $a \in Z_p \backslash \{0\}$ have a reciprocal. Note that zero has no reciprocal as $(0, p) = p$ and $p \neq 1$. Since there are exactly $p - 1$ nonzero elements in Z_n, we have that $\#Z_p^\times = p - 1$. This also follows from the fact that the Euler Totient function $\phi(p) = p - 1$ for any prime p. ■

Proposition 16. *If p is prime, then $\forall a \in Z, a^p \equiv a \,(mod\, p)$.*

Proof. Let us first consider the case where $a = 0$. We have $0^p = 0$ and thus $0^p \equiv 0 \pmod p$. For $a \neq 0$, we can consider the group $Z_p^\times$. Let n be the order of an arbitrary element $a \in Z_p$. The order of any element must divide the order of the group, and thus $n \mid p - 1$. We then must have that, for some $k \in Z$, $a^{p-1} \equiv a^{nk} \equiv (a^n)^k \equiv 1^k \equiv 1$ and thus $a^p \equiv a$. ■

Proposition 17. *For all $i \in \mathbb{Z}, R^i S = SR^{-i}$.*

Proof. First, we consider $i \geqslant 0$. For $i = 0$, we have $S = S$. Assuming $R^i S = SR^{-i}$, we have $R^i SR^{-1} = SR^{-i}R^{-1}$, by multiplying on the right by R^{-1}. Using $RS = SR^{-1}$, we have $R^i(RS) = SR^{-(i+1)} = R^{i+1}S$. The inductive hypothesis holds and thus we have shown the proposition for non-negative i.

For negative i, we must have $i = -j$ for some $j > 0$. We know $R^j S = SR^{-j}$. This gives $R^{-i}S = SR^i$. Multiplying on the left by S gives $SR^{-i}S = S^2R^i = R^i$. Multiplying on the right by S gives $SR^{-i}S^2 = R^iS = SR^{-i}$ and thus the formula holds for all $i \in \mathbb{Z}$. ■

Proposition 18. *All elements of the form R^iS have order 2.*

Proof. Since $R^iS = SR^{-i}$, we can multiply on the left by R^iS and see $R^iSR^iS = R^iSSR^{-i} = R^i(SS)R^{-i} = R^iR^{-i} = e$ and thus $(R^iS)(R^iS) = e$ and all elements of the form R^iS have order 2. ■

Proposition 19. *$D_{2n} = \langle RS, S\rangle$.*

Proof. We know D_{2n} is generated by R and S. Since $R = RSS$ and $R^{-1} = SRS$, then D_{2n} must also be generated by $\langle RS, S\rangle$. We also have that $S^2 = e$ and $(RS)(RS) = e$, and thus D_{2n} is generated by two elements with order 2. ■

Proposition 20. *For $n = 2k$ where $k > 1$, R^k commutes with all elements of D_{2n} and is the the only element besides the identity to do so.*

Proof. For elements of the form R^i, we have $R^kR^i = R^{i+k} = R^iR^k$. For elements of the form R^iS, we see $R^kR^iS = R^kSR^{-i} = SR^{-k}R^{-i} = SR^{-i}R^{-k} = R^iSR^{-k} = R^iSR^k$, where the last step uses $R^k = R^{-k}$ as $R^{2k} = R^n = e$. This shows R^k commutes with all elements of the group.

To show uniqueness, consider an element R^i commutes with everything. Then we have $R^iS = SR^i = R^{-i}S$ and thus $R^i = R^{-i}$ and $R^{2i} = e$. Then either $i = 0$, giving that $R^i = e$, or $2i = n$, giving that $R^i = R^k$.

Lastly, we consider an element R^iS that commutes with all other elements. We must have $(R^iS)R = R(R^iS) = R^iR^{-1}S = R^{i+1}S$ and thus $R^{i-1} = R^{i+1}$. This means $i + 1 - (i - 1) \equiv 0 \,(\text{mod n})$ or that $2 \equiv 0(\text{mod n})$. This can never happen for $n > 2$, and thus the element of the form R^iS that commutes must not exist. This shows that R^k and the identity are the only elements that commute with all other elements of D_{2n} when n is even. ■

Proposition 21. *For odd n, there is no element that commutes with every element of D_{2n} besides the identity.*

Proof. Suppose such an element exists. If it is of the form R^i, then $R^iS = SR^i = R^{-i}S$ and $R^i = R^{-i}$ and thus $R^{2i} = e$. This gives $2i \equiv 0 \,(\text{mod n})$. Since n is odd, this can never happen unless $i = 0$, which would mean this element is the identity. If this element is of the form R^iS, we reach the same contradiction as $(R^iS)S = S(R^iS) \implies R^i = R^{-i}$ and thus $2i \equiv 0 \,(\text{mod n})$. ■

Proposition 22. *For any group G, $\forall g \in G, \exists!$ homomorphism $\phi : \mathbb{Z} \to G$ such that $\phi(1) = g$.*

Proof. For all $n \in \mathbb{Z}$, let $\phi(n) = g^n$. This is well defined as $n = m \implies g^n = g^m$. This is a homomorphism as $\phi(n + m) = g^{n+m} = g^ng^m = \phi(n)\phi(m)$. We also see $\phi(1) = g^1 = g$. Consider another homomorphism $\psi : \mathbb{Z} \to G$ such that $\psi(1) = g$. We know $\phi(0) = e = \psi(0)$. Assume $\phi(n) = \psi(n)$ for some positive n. Then $\phi(n + 1) = \phi(n)\phi(1) = \psi(n)\psi(1) = \psi(n + 1)$, thus ψ and ϕ agree on all nonegative values of n. For negative values of n, let $m = -n$. Then $\phi(n) = \phi(-m) = \phi(m)^{-1} = \psi(m)^{-1} = \psi(-m) = \psi(n)$ and they are identical for all $n \in \mathbb{Z}$. ■

Proposition 23. *Image of ϕ is a cyclic group.*

Proof. Since for all $n \in \mathbb{Z}, \phi(n) = g^n$, all elements in the image of ϕ are of the form g^n, which form the group $\{g^n \mid n \in \mathbb{Z}\}$, as the image of any homomorphism is a group. ■

Proposition 24. *Any cyclic group is isomorphic to $\mathbb{Z}$ or $\mathbb{Z}_n$ for some natural number n.*

Proof. Let G be a cyclic group with infinite order. Then we can define an isomorphism $\phi : \mathbb{Z} \to G$ with $\phi(n) = g^n$ when g is the generator of G. We have already shown this mapping is well defined and a homomorphism. It is also surjective as by definition of ϕ, for any $g^n \in G, \phi(n) = g^n$. It is also injective, as $g^m = g^n \implies m = n$. This follows as if $m \neq n$, then $g^{m-n} = e$ and this would contradict that G has infinite order.

If G has finite order, then let n be $\|g\|$ and also $\|G\|$. We can write any integer m as $nk + r$, for some integers r, k, where $[r] = [m]$ and $0 \leqslant r < n$. We then construct the isomorphism $\phi : \mathbb{Z}_n \to G$ such that $\phi([m]) = g^r$. If $\phi([a]) = g^l = g^k = \phi([b])$, then $g^{k-l} = e$, which can only happen if $k - l = 0$, as the order of g is n and $0 \leqslant k < n$ and $0 \leqslant l < n$. This means $[a] = [b]$ as they have the same remainder modulo n. Surjectivity also follows as for any g^m, we can write m as $nk + r$, and thus $g^m = g^{nk+r} = g^{nk}g^r = (g^n)^k g^r = e^k g^r = g^r$, and thus $\phi([r]) = g^m$. In both cases ϕ is a bijective homomorphism and thus an isomorphism, making all cyclic groups isomorphic to either $\mathbb{Z}$ or $\mathbb{Z}_n$. ■

Proposition 25. *If $\phi : G \to H$ is an isomorphism, then for all $g \in G$, $\|g\| = \|\phi(g)\|$.*

Proof. We know $\phi(g^0) = \phi(e) = e = \phi(g)^0$. Assume $\phi(g^n) = \phi(g)^n$ for some positive n. Then $\phi(g^{n+1}) = \phi(g^n g) = \phi(g)\phi(g^n) = \phi(g)\phi(g)^n = \phi(g)^{n+1}$. For some negative n, let $m = -n$. Then $\phi(g^n) = \phi(g^{-m}) = \phi(g^m)^{-1} = \phi(g)^{-m} = \phi(g)^n$. Thus $\phi(g^n) = \phi(g)^n$ for all $n \in \mathbb{Z}$. Suppose $\|g\| = n$ and $\|\phi(g)\| = m$ for $m, n \in \mathbb{N}$. Since $\phi(g^n) = \phi(g)^n = e$, $m \leqslant n$. We also have that $\phi(g)^m = \phi(e) = \phi(g^m)$, and by injectivity of $\phi, g^m = e$. Then $n \leqslant m$ and thus $m = n$ and $\|g\| = \|\phi(g)\|$.

Suppose g has infinite order but it's image has order n for finite n. Then $\phi(g)^n = e = \phi(g^n)$ and $g^n = e$, as ϕ is injective, but this contradicts our assumption that g has infinite order, thus it's image must also have infinite order. Alternatively, if $\|\phi(g)\| = \infty$ and $\|g\| = m$ for some m, then $\phi(g^m) = \phi(e) = e = \phi(g)^m$ and thus $\phi(g)$ has finite order, which is a contradiction. Thus they must both have either finite order or infinite order. We've shown that when they have finite order, they must be equal, and when either has infinite order, then they must both have infinite order, and therefore $\|g\| = \|\phi(g)\|$. ■

Proposition 26. $Q_8 \ncong D_8$

Proof. There is only one element in Q_8 with order 2, namely -1. All other elements have either order 1 or 4. On the other hand, D_8 has at least two elements with order 2, namely S and RS. Any isomorphism must map elements of order two to elements of order two, yet since these groups have different numbers of elements with order two, no such isomorphism can exist, and thus they are not isomorphic. ■

Proposition 27. *$\|g\| = n$. Then for any homomorphism ϕ, $\|\phi(g)\|$ divides $\|g\|$.*

Proof. $\phi(g^n) = e = \phi(g)^n$. Thus the order of $\phi(g)$ is at most n. Let $\|\phi(g)\| = m$. Then $n = mk + r$. We have $\phi(g^{mk+r}) = \phi(g^{mk})\phi(g)^r = (\phi(g)^m)^k \phi(g)^r = e^k \phi(g)^r = \phi(g)^r$. Since $0 \leqslant r < m, r = 0$ and thus the order of $\phi(g)$ divides the order of g. ■

Proposition 28. *For two homomorphisms $\phi, \psi : G \to H$, $\{g \in G \mid \phi(g) = \psi(g)\} < G$.*

Proof. Since all homomorphisms map the identity to the identity, we must have $\phi(e) = \psi(e)$ and thus $e \in \{g \in G \mid \phi(g) = \psi(g)\}$. To see we also have closure under inverses, we have $\phi(g) = \psi(g) \implies \phi(g^{-1}) = \phi(g)^{-1} = \psi(g)^{-1} = \psi(g^{-1})$. Finally, closure under the group operation follows as $\phi(g) = \psi(g)$ and $\phi(h) = \psi(h)$ means $\phi(gh) = \phi(g)\phi(h) = \psi(g)\psi(h) = \psi(gh)$. Since we have the identity element and closure under inverses and the group operation, $\{g \in G \mid \phi(g) = \psi(g)\}$ must be a subgroup of G. ■

Proposition 29. *The order of rigid motions of the cube is 48.*

Proof. Here is a non-rigorous argument. Consider a corner of the cube. This corner can be moved to any of the 8 corners of the cube. Considering a neighbor of the corner, we see the neighbor can be mapped to 3 possible positions, namely the 3 neighbors of the image of the corner under the transformation. This is enough to determine the entire transformation, up to a reflection about the plane intersecting the two vertices and the antipodal vertices. This reflection gives 2 new arrangements. We see that in total, we have $8 \times 3 \times 2 = 48$ total symmetries of the cube. ■

Proposition 30. *Let $\phi : G \to H$ be any homomorphism. Then $J < H$ implies $\phi^{-1}(J) < G$ and $J \lhd H$ implies $\phi^{-1}(J) \lhd G$.*

Proof. We check that the $\phi^{-1}(J)$ has the identity element, is closed under the group operation, and is closed under inverses. $\phi(e_G) = e_H \in J$ as $J < G$, and thus $e_G \in \phi^{-1}(J)$. If $g \in \phi^{-1}(J)$, let $\phi(g) = j \in J$. Then $\phi(g^{-1}) = \phi(g)^{-1} = j^{-1} \in J$ and thus $g^{-1} \in \phi^{-1}(J)$. Let $g_1, g_2 \in \phi^{-1}(J)$. Then $\phi(g_1 g_2) = \phi(g_1)\phi(g_2) \in J$ as $\phi(g_1) \in J$ and $\phi(g_2) \in J$, thus we have all three properties of subgroups and $\phi^{-1}(J)$ is a subgroup of G.

If $J \lhd H$, then $hJ = Jh$ for all $h \in H$. Take $\mathfrak{g} \in \phi^{-1}(J)$ and $g \in G$. We have $\phi(\mathfrak{g}g) = \phi(\mathfrak{g})\phi(g)$. Since $\phi(\mathfrak{g}) \in J$, then $\phi(\mathfrak{g})\phi(g) = \phi(g)\phi(\mathfrak{g}) = \phi(g\mathfrak{g})$ since $J \lhd H$ and ϕ is a homomorphism. Since $\phi(\mathfrak{g}g) = \phi(g\mathfrak{g})$, then $\mathfrak{g}g = g\mathfrak{g}$ as ϕ is well defined. This holds for all $g \in G$, and thus $\phi^{-1}(J) \lhd G$. ■

Proposition 31. *A homomorphism $\phi : G \to H$ has $\ker\phi = 1$ if and only if it is injective.*

Proof. Assume ϕ is injective. Since ϕ is a homomorphism, we must have that $\phi(e_G) = e_H$. Let $g \in G$ be such that $\phi(g) = e_H$. Then $\phi(g) = \phi(e_G)$ and thus $g = e_G$ by injectivity of ϕ. This means the kernel of ϕ only contains the identity element.

Assume the kernel of ϕ is trivial. Let $\phi(g_1) = \phi(g_2)$ for $g_1, g_2 \in G$. Then $\phi(g_1)\phi(g_2)^{-1} = e_H = \phi(g_1)\phi(g_2^{-1}) = \phi(g_1 g_2^{-1})$. Since the kernel of ϕ is trivial, we must have that only $\phi(e_G) = e_H$, and thus $g_1 g_2^{-1} = e_G$ and $g_1 = g_2$. Therefore ϕ is injective since $\phi(g_1) = \phi(g_2) \implies g_1 = g_2$. ■

Proposition 32. $[G : H] = 2 \implies H \lhd G$.

Proof. If $g \in H$, then $gH = H = Hg$. If $g \notin H$, then $gH = G - H$ since the left cosets partition G and H is the only other left cosets besides gH. We must also

have that $Hg = G - H$ as the right cosets also partition G. This implies $gH = Hg$ for all G and thus $H \lhd G$. ■

Proposition 33. *$K \lhd H \lhd G$ does not imply $K \lhd G$.*

Proof. As a counterexample, consider D_8 and $\langle S\rangle \lhd \langle R^2, S\rangle \lhd \langle R, S\rangle = D_8$.

The only two elements in $\langle S\rangle$ are S and the identity. The identity commutes with all elements. For elements of the form $R^{2i} \in \langle R^2, S\rangle$, we know $R^{4i} = e$ and thus $R^{2i} = R^{-2i}$, so $R^{2i}S = SR^{-2i} = SR^{2i}$. For elements of the form $R^{2i}S$, we have $R^{2i}SS = R^{2i} = SSR^{2i}$. Thus $\langle S\rangle \lhd \langle R^2, S\rangle$.

Since $\langle R^2, S\rangle$ has index 2, it is normal by the previous proposition. Here is a proof through cases for completeness. To show $\langle R^2, S\rangle \lhd D_8$, consider any element of the form $R^{2i} \in \langle R^2, S\rangle$ and an element of the form $R^k \in D_8$. We have $R^{2i}R^k = R^{2i+k} = R^{k+2i} = R^kR^{2i}$. Consider an element of the form $R^kS \in D_8$. We have $R^{2i}R^kS = R^kR^{2i}S = R^kSR^{-2i} = R^kSR^{2i}$ as $R^{2i} = R^{-2i}$. Now take elements of the form $R^{2i}S \in \langle R^2, S\rangle$. For elements of the form $R^k \in D_8$, we have $R^{2i}R^kS = R^kR^{2i}S = R^kSR^{-2i} = R^kSR^{2i}$. Lastly, any element of the form $R^{2i}S \in \langle R^2, S\rangle$ and an element of the form $R^kS \in D_8$, we see the conjugation is in $\langle R^2, S\rangle$ as $R^kSR^{2i}SSR^{-k} = R^kSR^{2i-k} = SR^{2(i-k)} \in \langle R^2, S\rangle$.

Finally, we check that $\langle S\rangle \not\lhd D_8$. Take $RS \in D_8$, the conjugation gives $RSSSR^{-1} = R^2S \notin \langle S\rangle$. we've concluded the counterexample is valid and thus in general, $K \lhd H \lhd G \implies K \lhd G$. ■

Proposition 34. *The set Aut G forms a group under composition.*

Proof. Since every automorphism $\psi : G \to G$ is an isomorphism, by the Main Theorem on Inverses, there exists an inverse isomorphism $\psi^{-1} : G \to G$. Since the inverse is an isomorphism and maps G to G, it is also an automorphism in Aut G. This implies Aut G is closed under inverses. Associativity follows as composition of functions is associative. The identity automorphism id maps all $g \in G$ back to g. To see this is the identity, consider any automorphism ψ. We have $(\psi \circ id)(g) = \psi(id(g)) = \psi(g) = id(\psi(g)) = (id \circ g)(g)$. Thus the set of all automorphisms of a group G forms a group under composition. ■

Proposition 35. *For any $h \in G, \phi_h(g) = hgh^{-1}$ is an automorphism and $f : G \to$ Aut G such that $f(h) = \phi_h$ is a homomorphism.*

Proof. Confirming ϕ_h is a homomorphism, consider $g_1, g_2 \in G$. We have $\phi(g_1g_2) = hg_1g_2h^{-1} = hg_1h^{-1}hg_2h^{-1} = \phi_h(g_1)\phi_h(g_2)$. Injectivity follows as $\phi_h(g_1) = \phi_h(g_2)$ implies $hg_1h^{-1}hg_2h^{-1}$. Multiplying on the right by h and on the left by h^{-1} gives $g_1 = g_2$. Surjectivity also follows as for any $g \in G$, take $\phi_h(h^{-1}gh) = hh^{-1}gh^{-1}h = g$.

Consider $h_1, h_2 \in G$. We have $f(h_1h_2) = \phi_{h_1h_2}$. We must now show $\phi_{h_1h_2} = \phi_{h_1} \circ \phi_{h_2}$. First we note that $(h_1h_2)^{-1} = h_2^{-1}h_1^{-1}$ (You put on socks first then shoes but take off shoes first then socks). For any $g \in G, \phi_{h_1h_2}(g) = h_1h_2gh_2^{-1}h_1^{-1}$. We also have that $(\phi_{h_1} \circ \phi_{h_2})(g) = \phi_{h_1}(\phi_{h_2}(g)) = \phi_{h_1}(h_2gh_2^{-1}) = h_1h_2gh_2^{-1}h_1^{-1}$. Since $\phi_{h_1h_2} = \phi_{h_1} \circ \phi_{h_2}$, we see that f is a homomorphism. ■

Proposition 36. *$f(G) \lhd Aut\, G$.*

Proof. Since $f(G)$ is the image of a homomorphism, it is necessarily a subgroup. To show normality, we need to show closure under conjugation. Consider an automorphism ψ. We must show for all $g \in G$, $\psi \circ f(g) \circ \psi^{-1}$ is in $f(G)$. For all $h \in G$, we see $(\psi \circ f(g) \circ \psi^{-1})(h) = (\psi \circ \phi_g \circ \psi^{-1})(h) = \psi(\phi_g(\psi^{-1}(h))) = \psi(g\psi^{-1}(h)g^{-1}) = \psi(g)\psi(\psi^{-1}(h))\psi(g^{-1}) = \psi(g)h\psi(g)^{-1} = \phi_{\psi(g)}(h) = f(\psi(g))(h) \in f(G)$. ■

Proposition 37. *$Aut\, \mathbb{Z}_n \cong \mathbb{Z}_n^\times$.*

Proof. Consider a homomorphism $\phi : \mathbb{Z}_n \to \mathbb{Z}_n$. Let $\phi(1) = a$. Then $\phi(n) = \phi(\sum_{i=1}^n 1) = \sum_{i=1}^n a = a\sum_{i=1}^n 1 = an$. Thus any such homomorphism is a multiplication by a. Furthermore, it is only an automorphism if $(a, n) = 1$. This follows because $im(\phi) = \mathbb{Z}_n$, and thus $\langle a \rangle = Z_n$. Thus the order of is a is n and thus a must be coprime with n.

Consider the map $\psi : \text{Aut } \mathbb{Z}_n \to \mathbb{Z}_n^\times$ such that for all $\phi \in \text{Aut } \mathbb{Z}_n, \psi(\phi) = \phi(1)$. Checking it's a homomphism, for any automorphisms of $\mathbb{Z}_n$, ϕ_1, ϕ_2, we have $\psi(\phi_1 \circ \phi_2) = (\phi_1 \circ \phi_2)(1) = \phi_1(\phi_2(1)) = \phi_2(1)\phi_1(1) = \psi(\phi_1)\psi(\phi_2)$ where $\phi_1(\phi_2(1)) = \phi_2(1)\phi_1(1)$ follows from the fact that such automorphisms are multiplications by the image of 1. Injectivity follows as $\psi(\phi_1) = \psi(\phi_2) = \phi_1(1) = \phi_2(1)$. Since the the image of 1 under both automorphisms is the same, then they must be equal as they are entirely determined by where they map 1. We have surjectivity as well since for any $z \in \mathbb{Z}_n^\times$, take ϕ such that $\phi(1) = z$. We see this automorphism exists as $(n, z) = 1$ and therefore $\psi(\phi) = \phi(1) = z$. We can finally conclude that ψ is an isomorphism and thus Aut $\mathbb{Z}_n \cong \mathbb{Z}_n^\times$. ■

Proposition 38. *If $N \lhd G$ has prime index p, and if $H < G$, then either $H < N$ or $G = HN$ and $[H : H \cap N] = p$.*

Proof. Consider the homomorphism $\phi : G \to G/N$ such that $\phi(g) = gN$. Checking it's well defined we have $g_1 = g_2 \implies g_1N = g_2N$. Checking it is a homomorphism, we have $\phi(g_1g_2) = g_1g_2N = g_1g_2NN = g_1Ng_2N = \phi(g_1)\phi(g_2)$. This follows from the fact that $N \lhd G$.

Since the image of any subgroup under a homomorphism is a subgroup, it follows that the order of $\phi(H) \mid [G : N]$. Since $[G : N]$ is prime, the order of $\phi(H)$ is either 1 or p. If $\|\phi(H)\| = 1$, then $\phi(H) = \{N\}$ (the trivial subgroup of G/N). Thus $H < N$ as for all $h \in H, hN = N$.

If $\|\phi(H)\| = p$, then $\phi(H) = G/N$. Since the set of left cosets partition G, their union must equal G, and thus $G = HN$. A more explicit argument is that $\phi(H) = G/N$ implies $\forall g \in G, gN = hN$ for some $h \in H$. Then $g = hn$ for some $n \in N$, and thus $\forall g, g \in G \iff g \in HN$ and thus $G = HN$. The Second Isomorphism Theorem states that $\frac{H}{H \cap N} \cong \frac{HN}{N}$. Since $G = HN$, we have $\frac{H}{H \cap N} \cong \frac{G}{N}$ and thus $[H : H \cap N] = [G : N] = p$. ■

Proposition 39. *Suppose $M \lhd G$ and $N \lhd G$ and $G = MN$. Then $G/(M \cap N) \cong G/M \times G/N$.*

Proof. Consider $\phi : G \to G/M \times G/N$ such that for all $g \in G, \phi(g) = (gM, gN)$. Checking this is a homomorphism, for $g_1, g_2 \in G, \phi(g_1g_2) = (g_1g_2M, g_1g_2N) =$

$(g_1g_2MM, g_1g_2NN) = (g_1Mg_2M, g_1Ng_2M) = \phi(g_1)(\phi(g_2)$, where we've used the fact that $g_1M = Mg_1$ and $g_1N = Ng_1$ (the normality of M and N).

Consider an arbitrary element $(g_1M, g_2N) \in G/M \times G/N$. Consider an element g_3 such that $g_3M = g_1M$ and $g_3N = g_2N$. If this element exists, then ϕ is surjective. The first condition gives that $g_3 = g_1m$ for some $m \in M$ and the second gives that $g_3 = g_2n$ for some $n \in N$. This gives that $g_1m = g_2n$ or that $g_2^{-1}g_1 = m^{-1}n$. Since $g = MN$, for any $g \in G$, we have that $g = mn$ for some $m \in M$ and $n \in N$. Since $g_2^{-1}g_1 \in G$, then it can be expressed as some elements as $m^{-1}n$ for some m and n and thus g_3 exists and therefore ϕ is surjective. In particular, we have that $im(\phi) = G/M \times G/N$.

The kernel of ϕ are all elements $g \in G$ such that $\phi(g) = (M, N)$. Therefore it is necessary and sufficient that $g \in M \cap N$ and so the kernel of ϕ is $M \cap N$. By the First Isomorphism Theorem, we have that $im(\phi) \cong G/\ker\phi$ and so $G/M \times G/N \cong G/(M \cap N)$. ■

Proposition 40. *Suppose $M \lhd G, N \lhd G, G = MN$, and $M \cap N = 1$. Then $G \cong M \times N$.*

Proof. Since $M \cap N = 1$, we have that $G/(M \cap N) = G, M/(M \cap N) = M$, and $N/(M \cap N) = N$. By **Proposition 39**, we have that $G/(M \cap N) \cong G/M \times G/N$ and therefore $G \cong G/M \times G/N$. The Second Isomorphism Theorem gives that $M/(M \cap N) \cong MN/N$ and thus $M \cong G/N$. Additionally, we have that $N/(M \cap N) \cong MN/M$ and thus $N \cong G/M$. Thus $G/N \times G/M \cong M \times N$. Finally, we get that $G \cong M \times N$. ■

Proposition 41. *If $\sigma = (a_1 \cdots a_m) \in \Sigma_n$, then $\forall i \in \langle m \rangle, \sigma^i(a_k) = a_j$ for $j \in \langle m \rangle$ such that $j \equiv k + i \pmod m$ and $|\sigma| = m$.*

Proof. We will show this by induction on i. For $i = 0$, we note $\sigma^0(a_k) = a_k$ and $k \equiv k \pmod m$. Assuming the proposition for $i = l$, consider $\sigma^{l+1}(a_k)$. Let $\sigma^l(a_k) = a_j$. We see $\sigma^{l+1}(a_k) = \sigma(\sigma^l(a_k)) = \sigma(a_j) = a_{j+1 \pmod m}$ and thus the inductive hypothesis holds as $j \equiv k + i \pmod m$ so $j + 1 \equiv k + i + 1 \pmod m$. To see σ has order m, consider $\sigma^m(a_k) = a_j$. Since $j \equiv k + m \pmod m$, we have $j \equiv k$ and thus $\sigma^m(a_k) = a_k$ for all k. This cannot happen for any $i < m$ as $k \not\equiv k + i \pmod m$ for such an i, and thus the order of σ is m. ■

Proposition 42. *The order of $\tau \in \Sigma_n$ is equal to the least common multiple of the lengths of its disjoint cycle decomposition.*

Proof. Let τ have disjoint cycle decomposition $\sigma_1\sigma_2 \ldots \sigma_n$ for some n. Since the cycles commute, we must have that $\tau^i = (\sigma_1\sigma_2 \ldots \sigma_n)^i = \sigma_1^i\sigma_2^i \ldots \sigma_n^i$. τ^i is the identity if and only if each of its cycles are the identity, and each cycle is the identity if and only if the original cycle in the disjoint cycle decomposition of τ has been composed with itself i times such that i is a multiple of the original cycle's length by proposition 1 and the fact that each cycle is disjoint in the disjoint cycle decomposition. Therefore, if τ^i is the identity, i has to be a multiple of the lengths of all the cycles in the disjoint cycle decomposition of τ, and the smallest of such

multiples is necessarily the least common multiple. Thus τ has order equal to the l.c.m. of the lengths of the cycles of its disjoint cycle decomposition. ■

Proposition 43. *Following are all numbers n such that Σ_7 has an element of order n.* $1, 2, 3, 4, 5, 6, 7, 10, 12$.

Proof. By *Proposition*42, the order of each element is the lcm of the lengths of its disjoint cycle decomposition, so we need to come up with all of the possible lcms. We readily see that we must have $n = 1, 2, 3, 4, 5, 6, 7$ just by coming up with permutations with a single cycle of those lengths. We note that the largest possible order of an element in Σ_7 is 12, which we can get from an element with two cycles of order 3 and 4. We cannot have a permutation of order 11 as 11 is a prime number greater than 7. We also cannot have a permutation of order 8 as the lcm of 4 and 2 is 4. Additionally, we cannot have a permutation of order 9 as the lcm of 3 and 3 is just 3. Finally, we can get a permutation of order 10 with two cycles, one of length 5 and another of length 2. ■

Proposition 44. *Here we rewrite* $(123)(145)$*, and* $(123)(125)$*, and* $(23)(12)(23)$ *as products of disjoint cycles.*

Proof. Composing right to left we see $(123)(145) = (14523)$ and that cycle has order 5. We see also that $(123)(125) = (13)(25)$ and that has order 2. Finally, we have that $(23)(12)(23) = (13)$ and that has order 2. ■

Proposition 45. *For $\sigma, \tau \in \Sigma_n$, if*

$$\sigma = (a_1 a_2 \dots a_k)(b_1 b_2 \dots b_l) \dots (z_1 z_2 \dots z_m)$$

then $\tau\sigma\tau^{-1}$ has cycle decomposition

$$(\tau(a_1)\tau(a_2)\dots\tau(a_k))(\tau(b_1)\tau(b_2)\dots\tau(b_l))\dots(\tau(z_1)\tau(z_2)\dots\tau(z_m))$$

.

Proof. To verify the equality, we will consider $\tau(g)$ for all $g \in \langle n \rangle$. For $j \in \langle k-1 \rangle$, we note $\tau(\sigma(\tau^{-1}(\tau(a_i)))) = \tau(\sigma(a_i)) = \tau(a_{i+1})$ and see the equality holds. For $i = k$, note $\tau(\sigma(\tau^{-1}(\tau(a_k)))) = \tau(\sigma(a_k)) = \tau(a_0)$ and the equality holds. The case for elements $b \dots z$ follows similarly. Lastly, consider an element h such that $\sigma(h) = h$. We check that $\tau(\sigma(\tau^{-1}(\tau(h)))) = \tau(\sigma(h)) = \tau(h)$ and thus such elements are sent back to themselves and thus the proposition holds. Since we have shown the proposition for all elements $\tau(a)$ such that $\sigma(a) \neq a$ and all elements $\tau(a)$ such that $\sigma(a) = a$, we have shown it for all elements. ■

Proposition 46. *If $\sigma = (12)$ and $\tau = (12345) \in \Sigma_5$, then $\Sigma_5 = \langle\{\sigma, \tau\}\rangle$.*

Proof. We can make an exhaustive list of all transpositions, showing how they can be created using σ and τ.

$$\begin{aligned}(12) &= \sigma\\ (23) &= \tau \circ \sigma \circ \tau^{-1}\\ (13) &= (23)(12)(23)\\ (34) &= \tau^2 \circ \sigma \circ \tau^{-2}\\ (14) &= (13)(34)(13)\\ (51) &= \tau^{-1} \circ \tau\\ (45) &= \tau^3 \circ \sigma \circ \tau^{-3}\\ (24) &= (12345)(13)\\ (35) &= (12345)(24)\\ (25) &= (12345)(14)\end{aligned}$$

■

Proposition 47. *If G is a finite group with $H \lhd G$, then G has a composition series where on of the terms is H.*

Proof. Since H is normal in G, G/H is a subgroup of G. Also, since H and G/H are finite, they must have their own composition series. Let $1 \lhd H_1 \lhd H_2 \lhd \ldots \lhd H_m = H$ and $1 \lhd J_1 \lhd J_2 \ldots \lhd J_n = G/H$ be the composition series for H and G/H, respectively. Let $\pi : G \to G/H$ be the natural projection. Let $G_i = \pi^{-1}(J_i)$. Note that $G_0 = H$ as $H = \pi^{-1}(1)$. Consider $\pi|_{G_i} : G_i \to J_i$. By the First Isomorphism Theorem, we have that $G_i/H \cong J_i$. Therefore, $J_i/J_{i-1} \cong \frac{G_i/H}{G_{i-1}/H}$. We must have that $G_{i-1} \lhd G_i$, and thus by the Third Isomorphism theorem, $\frac{G_i/H}{G_{i-1}/H} \cong G_i/G_{i-1}$. Since J_i/J_{i-1} is simple, G_i/G_{i-1} must be simple. Finally, we can construct a composition series for G by stitching the H_i and G_j together, giving

$$1 \lhd H_1 \lhd H_2 \lhd \ldots \lhd H_m = H = G_0 \lhd G_1 \lhd G_2 \lhd \ldots \lhd G_n = G$$

Since this composition series has H appearing as a term, the proposition is proven. ■

Proposition 48. *For a group G with composition series $1 \lhd N \lhd G$, there does not necessarily exist a second composition series $1 \lhd H \lhd G$ such that $N \cong G/H$ and $G/N \cong H$.*

Proof. Consider for a counterexample Σ_5 and the composition series $1 \lhd A_5 \lhd \Sigma_5$. Suppose for a contradiction there exists a normal subgroup $N \cong \Sigma_5/A_5$ as Σ_5/A_5. Then N must have order 2, as Σ_5/A_5 has order 2. We therefore must have that $N = \{1, \sigma\}$ where σ is either a transposition or the composition of two disjoint transpositions by Proposition 2. However, by Proposition 5, we can conjugate σ by another permutation τ such that $\tau\sigma\tau^{-1}$ is not in N by letting $\tau = (12345)$, and thus N is not normal. ■

Proposition 49. *Let $G \circlearrowright S$. Then $s \sim t \iff s = g \cdot t$ is an equivalence relation.*

Proof. Reflexivity of $\sim$ follows from the identity Axiom of group actions, namely that $s = e \cdot s$ so $s \sim s$ for all $s \in S$. It is also symmetric. $s \sim t$ implies $s = g \cdot t$. Then, multiplying on the left by g^{-1} gives $g^{-1} \cdot s = g^{-1} \cdot (g \cdot t)$. By the compatibility axiom, we have $g^{-1} \cdot s = (g^{-1}g) \cdot t = e \cdot t = t$ and thus $t \sim s$. For transitivity, consider $s \sim t$ and $t \sim u$. Then $s = g_1 \cdot t$ and $t = g_2 \cdot u$. Substituting gives $s = g_1 \cdot (g_2 \cdot u) = (g_1 g_2) \cdot u$ and thus $s \sim u$. ■

Proposition 50. *$g \cdot h := ghg^{-1}$ defines an action $G \circlearrowright G$.*

Proof. We check the two axioms. For the identity axiom, we have that $e \cdot h = ehe^{-1} = h$ for all $h \in G$. For the compatibility axiom, we have $g_1 \cdot (g_2 \cdot h) = g_1 \cdot (g_1 h g_1^{-1}) = g_2 g_1 h g_1^{-1} g_2^{-1} = (g_2 g_1) \cdot h$. ■

Proposition 51. *$g \cdot h := ghg^{-1}$ defines an action $G \circlearrowright G$.*

Proof. Q_8 has 5 orbits, $O = \{\{1\}, \{-1\}, \{i, -i\}, \{j, -j\}, \{k, -k\}\}$. 1 and -1 are in the center, so they're in their own conjugacy classes. We also see $i = j - ij^{-1} = j - i - j = jij = jk = i$ and similarly for $j, -j$ and $k, -k$. We see we cannot go from $j = gig^{-1}$ by trying out all g, similarly for j, k and i, k.

For D_{10}, we have 4 orbits, $O = \{\{e\}, \{S, RS, R^2S, R^3S, R^4S\}, \{R, R^4\}, \{R^2, R^3\}\}$. Again, e is in the center so it is the only element in its conjugation class. We can get from S to any $R^i S$ as $R^j SS(R^j S)^{-1} = R^j S R^{-j} = R^{2j} S$. Letting $j = 1, 2, 3, 4$ gives $R^2S, R^4S, R^6S = RS, R^8S = R^3S$. Conjugation S by an itself gives back S, and conjugating by a rotation again gives $R^{2i}S$. We can see that $R = SR^4S = R^{-4}$ and $R^2 = SR^3S = R^{-3}$. This gives the result.

For $\mathbb{Z}_5$, every element is in itss own conjugacy class, as the group is abelian, so the center is the entire group. We thus have $O = \{\{[0]\}, \{[1]\}, \{[2]\}, \{[3]\}, \{[4]\}\}$. ■

Proposition 52. *Let $H < G$. Then $g \cdot kH := gkH$ specifies a well defined and transitive action $G \circlearrowright G/H$.*

Proof. It's well defined as $k_1 H = k_2 H$ implies $gk_1 H = gk_2 H$ as we can multiply on the left by g^{-1}. To check the identity axiom, notice that $e \cdot kH = ekH = kH$. Compatibility also follows as $g_1 \cdot (g_2 \cdot kH) = g_1 \cdot (g_2 kH) = g_1 g_2 kH = (g_1 g_2) \cdot kH$.

Consider $k_1 H$ and $k_2 H$. Then $k_1 H = gk_2 H$. Letting $g = k_1 k_2^{-1}$, we have $k_1 H = k_1 k_2^{-1} k_2 H = k_1 H$. Thus the action is transitive as all elements are in the same orbit. ■

Proposition 53. *The stabilizer of $s = kH$ is $G_S = kHk^{-1}$.*

Proof. Let g be a stabilizer of s. Then $g \cdot kH = kH$. This gives that $gk = kh$ for some $h \in H$. Thus $g = khk^{-1}$. Thus $G_s = \{khk^{-1} \mid h \in H\} = kHk^{-1}$. ■

Proposition 54. *Σ_n acts on $P\langle n \rangle$ by $\sigma \cdot S := \sigma(S)$, where $\sigma : \langle n \rangle \to \langle n \rangle$ and $S \subset \langle n \rangle$.*

Proof. Checking the identity axiom, we see $\mathrm{id}_{\langle n \rangle} \cdot S = \mathrm{id}_{\langle n \rangle}(S) = S$. Checking compatibility, we note $\sigma \cdot (\tau \cdot S) = \sigma \cdot (\tau(S)) = \sigma(\tau(S)) = (\sigma \circ \tau)(S)$. ■

Proposition 55. *There are $n+1$ orbits of $\Sigma_n \circlearrowright P\langle n\rangle$.*

Proof. For two subsets of $\langle n\rangle$ to have the same orbit, there must be exist a bijection between them. This means that for any two subsets U, V, $U \sim V \implies |U| = |V|$. Additionally, if $|U| = |V|$, we can always construct a bijection $\sigma : U \to V$, so $|U| = |V| \implies U \sim V$. There can be subsets of size 0 to n, so there must be $n+1$ possibles orbits of $\Sigma_n \circlearrowright P\langle n\rangle$. ■

Proposition 56. *The group of rotations G of a regular tetrahedron is isomorphic to A_4.*

Proof. Consider the action of G on the set of faces of the tetrahedron. Each face can be rotated to any other face, so they must all be in the same orbit. That is, G acts transitively on the 4 faces. Additionally, the stabilizer for any face consists of the identity, rotation counterclockwise through axis going through midpoint of the face, and rotation clockwise through axis going through the midpoint of the face, giving that 3 elements compose the stabilizer.

By the counting formula, we have $\#G = \#O_s \#G_s = 4 \times 3 = 12$. Thus $\#G = \#A_4$ as $\#A_4 = \frac{4!}{2} = 12$. Label the vertices of the tetrahedron with the numbers $1, 2, 3, 4$. The rotations consist of the identity rotation e, rotations about the axis joining the midpoints of two edges about two vertices to be interchanged given by

(12)(34) is a rotation about the axis connecting the midpoint between vertices 1 and 2 and vertices 3 and 4. Similarly, we have (13)(24) and (14)(23).

Additionally, we have rotations by $\frac{2\pi}{3}$ going through a vertex and the center of its opposite face. One such rotation is (123), rotating about the axis going through vertex 4 and the face triangle with vertices 1, 2, and 3. Other such rotations are (234), (132), (243), (314), (412), (341), (421).

Since any action determines a homomorphism, we must have a homomorphism from G to the bijections of the set of vertices of the tetrahedron, or Σ_4. The action is faithful because the only rotation that fixes all the vertices is the identity, and thus the kernel of the homomorphism is trivial. The image of the homomorphism is A_4, as they have the same order and all permuations have an even number of even length cycles in their cycle decomposition. Thus, by the First Isomorphism Theorem, we have that $\operatorname{Im}\phi \cong G/\ker\phi$ or $A_4 \cong G$. ■

Proposition 57. *The group of rotations H of a cube is isomorphic to Σ_4.*

Proof. Consider the action of G on the faces of the cube. Since any face can be rotated into any other face, the orbits must consist of a single orbit with all of the 6 faces of the cube. Additionally, for any face, the stabilizer consists of the identity rotation, as well as three rotations about the axis going through the center of the face. By the counting formula, the order of H must be $6 \times 4 = 24$.

The action of H on the set of opposite vertices defines a homomorphism from H to the set of bijections of the four diagonals, or Σ_4 if we label the diagonals 1, 2, 3, and 4. This action is faithful, as the only way to fix all four diagonals without a reflection is by doing nothing. This gives that ϕ is an isomorphism since it's kernel is trivial and $|G| = 24$. ■

Proposition 58. *$ZG \lhd G$.*

Proof. Consider $\phi : G \to \text{Aut } G$ given by $g \to \psi_g$ where $\psi_g(h) = ghg^{-1}$. ψ_g is an automorphism, ϕ is a homomorphism. Elements in the kernel of ϕ satisfy $ghg^{-1} = h$ thus $gh = hg$ for all h and $g \in ZG$. Therefore, $\ker \phi = ZG \lhd G$. ■

Proposition 59. *If $[G : ZG] = n$, then each conjugacy class in G has at most n elements.*

Proof. Consider $G \circlearrowright G$ by conjugation. Then $ZG < G_g$ where G_g is the stabilizer group of any element $g \in G$. We have $[G : ZG] = [G : G_g][G_g : ZG]$. Since $[G : G_g] = \#O_g$ where O_g is the orbit or conjugacy class of g, and thus $\#O_g$ divides $[G : ZG] = n$. In particular, $\#O_g$ is at most n. ■

Proposition 60. *The number of ways to color the faces of a regular tetrahedron up to rotational equivalence with n colors is $\frac{1}{12}(n^4 + 11n^2)$.*

Proof. Let G be the group of rotations of a regular tetrahedron, F be the set of faces of a regular tetrahedron, and C be the set of n colors. Let $S = F \times C$. Consider $G \circlearrowright S$. We have that $|G| = 12$ (This follows by considering that G acts transitively on the 4 faces, and each there are 3 rotations that fix a face, and the use of the orbit-stabilizer theorem). Thus by Burnside's Lemma, the number of orbits (equal to the number of ways to color the faces up to rotational equivalence) is

$$|S/G| = \frac{1}{12} \sum_{g \in G} |S^g|$$

The identity rotation fixes all n^4 face colorings.

Additionally, the 8 rotations about the axis through a vertex and the center of the opposite face fix the face and color of the opposite vertex. Since they sway all other faces, those faces must have the same color. This gives n^2 possible colorings.

Lastly, consider the rotations about the axis joining two opposite edges. There are 3 such rotations, and since they swap two sets of faces, they must have the same colors, again giving n^2 colorings. Summing these up we get

$$\frac{1}{12}(n^4 + 11n^2)$$

For $n = 3$, we have 15 possible colorings. ■

Proposition 61. *Each $\sigma \in \Sigma_n$ fixes, on average, one subset $S \subset \langle n \rangle$ with exactly m elements.*

Proof. Let $T = \{S \in P\langle n \rangle \mid \#S = m\}$. Consider $\Sigma_n \circlearrowright T$ by $\sigma \cdot S = \sigma(S)$. This action is transitive as any two sets $S, U \in T$ have the same cardinality, and thus there exists $\sigma \in \Sigma_n$ such that $\sigma(S) = U$. Thus by Burnside's Lemma, the average number of subsets of size m fixed by any permutation σ is 1. ■

Proposition 62. *The number of conjugacy classes in the dihedral group D_{2n} is $(n + 3)/2$ for odd n and $(n + 6)/2$ for even n.*

Proof. Consider $D_{2n} \circlearrowright D_{2n}$ by conjugation. By Burnside's Lemma, the number of conjugacy classes is $\frac{1}{2n}\sum_{g\in D_{2n}} |D_{2n}^g|$. It suffices to sum all fixed point sets.

D_{2n}	$n = 2k$	$n = 2k+1$
e	$2n$	$2n$
S	$1_e + 1_S + 1_{R^k} + 1_{R^kS}$	$1_e + 1_S$
R^i	if $i \neq k$, $(1_e + n - 1 + 1)$ else $(2n)$	$1_e + n - 1$
R^iS	if $i \neq k$ $(1_e + 1_{R^iS} + 1_{R^k})$ else $1_e + 1_S + 1_{R^iS} + 1_{R^k}$	$1_e + 1_{R^iS}$

The results of the table follow as the identity fixes all $2n$ elements. The reflection S fixes the identity and itself. For even $n = 2k$, it also fixes R^k as and R^kS. All $n-1$ rotations fix the identity and all other rotations. For even n, R^k also fixes all $2n$ elements and rotations fix R^kS. Elements R^iS also fix the identity and themselves. For even n, they also fix R^k. The element R^kS also fixes S.

Summing these results for even n gives

$$\frac{1}{2n}(2n + 4 + (n-2)(n+1) + 2n + 3(n-2) + 4)$$
$$\frac{1}{2n}(2n + 4 + n^2 - n - 2 + 2n + 3n - 6 + 4)$$
$$\frac{1}{2n}(n^2 + 6n)$$
$$\frac{n+6}{2}$$

Summing the results for odd n gives

$$\frac{1}{2n}(2n + 2 + (n-1)(n) + 2(n-1)$$
$$\frac{n+3}{2}$$

■

Proposition 63. *Any finite group G with two conjugacy classes is isomorphic to $\mathbb{Z}_2$.*

Proof. The identity element is in its own conjugacy class of order 1. Thus, the other conjugacy class O_g must have order $|G| - 1$, as the conjugacy classes partition G. By the orbit-stabilizer theorem, $|G| - 1$ divides $|G|$ and therefore $|G| = 2$. Since G is a cyclic group of order two, it is isomorphic to $\mathbb{Z}_2$. ■

Proposition 64. *Any group G with $|G| = 20$ has exactly 4 elements of order 5.*

Proof. Since $20 = 5 \times 2^2$, the First Sylow Theorem guarantees that G has a Sylow 5-subgroup, P_5. By the Third Sylow Theorem, P_5 must be unique, as the number of Sylow 5-subgroups must divide 2^2 and be congruent to 1 modulo 5. Since the order of any element $g \in P_5$ divides 1 or 5, there must be 4 non-identity elements with order 5. There cannot be any other element $h \notin P_5$ with $|h| = 5$ because if there were, then $\langle h \rangle = P_5$, a contradiction. ■

Proposition 65. *If G is a group such that its only subgroups are 1 and G, then G is cyclic.*

Proof. If G is the trivial group, then $G = \langle e \rangle$. Otherwise, pick any non-identity element $g \in G$. Since $\langle g \rangle$ contains the identity and g, it cannot be trivial. Furthermore, since G has no other subgroups other than itself, $\langle g \rangle = G$. ■

Proposition 66. *If G is a nontrivial, simple p-group, it must have order p.*

Proof. Assume for a contradiction that $|G| = p^n$ for $n > 1$. Since G is a p-group, $ZG \neq 1$. If $ZG \neq G$, then G is not simple. Otherwise, $ZG = G$ and G is abelian. Since G is simple, it must not have any non-trivial, proper subgroups. By **Proposition 65**, G is cyclic. Pick any non-identity element of $g \in G$. If g is not a generator, then $\langle g \rangle \neq G$ and $\langle g \rangle \neq 1$, and thus G is not simple. Otherwise, $|g| = p^n$ and thus $|g^p| = p^{n-1}$. Therefore $\langle g^p \rangle \neq G$ and $\langle g^p \rangle \neq 1$ and so G is not simple. Therefore, it cannot be that G does not have order p. ■

Proposition 67. *If G is a p-group, every composition factor of G is isomorphic to $\mathbb{Z}_p$.*

Proof. Let $1 = N_0 \triangleleft N_1 \triangleleft N_2 \triangleleft \cdots \triangleleft N_n = G$ be a composition series for G. Consider any composition factor N_{i+1}/N_i. This composition factor is necessarily a p-group and simple. It follows by **Proposition 66** that the composition factor has order p and thus $N_{i+1}/N_i \cong \mathbb{Z}_p$. ■

Proposition 68. *A Sylow p-subgroup P of G is unique iff it is normal.*

Proof. Conjugating P by any element gives a subgroup of the same order, which must be P since P is unique and therefore P must be normal. If P is normal, it must be unique since all Sylow p-subgroups are conjugate. ■

Proposition 69. *Any group G with $|G| = 132$ is not simple.*

Proof. Since $132 = 2^2 \times 3 \times 11$, there exists a Sylow 11-subgroup, P_{11}. Furthermore, it must be unique as the number of Sylow 11-subgroups divides 12 and is equal to 1 modulo 11. Since P_{11} is unique, it must be normal by **Proposition 68**, and thus G cannot be simple. ■

Proposition 70. *Any group G with $|G| = 33$ is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_{11}$.*

Proof. Since $33 = 3 \times 11$, there must exist a Sylow 11-subgroup, P_{11}. This subgroup is unique as the number of such elements must divide 3 and be congruent to 1 modulo 11. Similarly, there must also exist a unique Sylow 3-subgroup P_3. Since both of the subgroups are unique, they must be normal. Additionally, $P_3 \cap P_{11} = 1$ as the order of any element in the intersection must divide 3 and 11, and thus must have order 1. We also have that $P_3 < P_3P_{11}$ and $P_{11} < P_3P_{11}$ and thus $|P_3P_{11}|$ is divisible by 3 and 11 and can be at most 33, and thus in fact must be 33. Therefore, $G = P_3P_{11}$ and by the Main Theorem on Direct Products, $G = P_3P_{11} \cong P_3 \times P_{11} \cong \mathbb{Z}_3 \times \mathbb{Z}_{11}$. ■

Proposition 71. *$k^2 \equiv 1 \pmod{p}$ implies $k \equiv 1$ or $k \equiv -1 \pmod{p}$.*

Proof. If $k^2 \equiv 1 \pmod{p}$, then $(k-1)(k+1) \equiv 0 \pmod{p}$. Since p is a prime, p must divide either $(k-1)$ or $(k+1)$. Thus, $k \equiv 1 \pmod{p}$ or $k \equiv -1 \pmod{p}$. Since $p > 2$, these solutions are distinct. ■

Proposition 72. *The only automorphisms $\phi : \mathbb{Z}_p \to \mathbb{Z}_p$ such that $\phi \circ \phi = id$ are $\phi(g) = g^{\pm 1}$.*

Proof. Any such automorphism ϕ is determined by $\phi(g) = kg$ for some $k \in \mathbb{Z}_p^\times$. The condition $(\phi \circ \phi) = \text{id}$ is satisfied if and only if for all $g \in \mathbb{Z}_p$, $(\phi \circ \phi)(g) = \phi(\phi(g)) = \phi(kg) = k^2 g = g$ and thus $k^2 \equiv 1 \pmod{p}$ which only holds for $k \equiv 1$ or $k \equiv -1 \pmod{p}$. ■

Proposition 73. *Any group G with $|G| = 2p$ is isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_2$ or D_{2p}.*

Proof. G has a unique, normal Sylow p-subgroup S_p as the number of such subgroups must divide 2 and be equal to 1 modulo p. Furthermore, G must also have a Sylow 2-subgroup S_2. It must also be the case that $S_p \cap S_2 = 1$ as the order of the intersection must divide both 2 and p. Since $S_p S_2$ is divisible by both 2 and p it must have order $2p$ and thus equal G. If S_2 is normal, then $G = S_p S_2 \cong S_p \times S_2 \cong \mathbb{Z}_p \times \mathbb{Z}_2$. Otherwise, $G = S_2 S_p \cong S_p \rtimes S_2 \cong \mathbb{Z}_p \rtimes \mathbb{Z}_2 \cong D_{2p}$ where the action is conjugation. ■

Proposition 74. *Let N be a normal Sylow p-subgroup of G and H be any subgroup of G. $H \cap N$ must be the unique Sylow p-subgroup of H.*

Proof. Since N is the unique Sylow p-subgroup of G, every p-subgroup of G is contained in N. Consider for a contradiction that $H \cap N$ is not a Sylow p-subgroup of H. Then there exists some other Sylow p-subgroup P with an element not contained in N, as otherwise it would be in the intersection. This cannot be as P must be contained in N. Thus $H \cap N$ must be a Sylow p-subgroup of H. Furthermore, it is unique, as $H \cap N$ is normal by the Second Isomorphism Theorem. ■

Proposition 75. *For $n \geqslant 3$, $Z\Sigma_n$ is trivial.*

Proof. For an arbitrary non-identity element $\sigma \in \Sigma_n$, let $\sigma(i) = j$ for some $i \neq j$. Since $n \geqslant 3$, there exists $\tau \in \Sigma_n$ such that for some $k \neq i$ and $k \neq j, \tau = (kj)$. Since $(\tau \circ \sigma \circ \tau^{-1})(i) = k$, $\tau \circ \sigma \neq \sigma \circ \tau$ and thus $\sigma \notin Z\Sigma_n$. ■

Proposition 76. *For $n \geqslant 3$, Σ_n has no normal subgroup of order 2.*

Proof. Assume for a contradiction that $N = \{e, \sigma\} \lhd \Sigma_n$. We must have that for all $\tau \in \Sigma_n, \tau \circ \sigma \circ \tau^{-1} = \sigma$. This cannot be since by **Proposition 75**, the center of Σ_n is trivial. ■

Proposition 77. *For $n \geqslant 5$, A_n and 1 are the only proper, normal subgroups of Σ_n.*

Proof. Consider for a contradiction a proper, nontrivial, normal subgroup $N \lhd \Sigma_n$. Since A_n is simple, we must have $N \cap A_n = 1$ or $N \cap A_n = A_n$. If $N \cap A_n = 1$, then by the Second Isomorphism Theorem, $\#N \# A_n = \#N A_n$. Since $[\Sigma_n : A_n] = 2$, $\#N = 1$ or $\#N = 2$. If $\#N = 1$, N is trivial. If $\#N = 2$, N cannot be normal by **75**. If $N \cap A_n = A_n$, then $N = A_n$ or $N = \Sigma_n$ since $[\Sigma_n : A_n] = 2$. ■

Proposition 78. *The center of a direct product is the direct product of the centers.*

$$Z(G_1 \times \ldots \times G_n) = ZG_1 \times \ldots \times ZG_n$$

Proof. For $n = 1$, the proposition follows trivially. For $n = 2$, let $(h_1, h_2) \in Z(G_1 \times G_2)$. For all $(g_1, g_2) \in G_1 \times G_2$, we have $(g_1, g_2)(h_1, h_2) = (h_1, h_2)(g_1, g_2)$ and thus $h_1 g_1 = g_1 h_1$ and $h_2 g_2 = g_2 h_2$. Hence, $h_1 \in ZG_1$ and $h_2 \in ZG_2$. Conversely, consider $(k_1, k_2) \in ZG_1 \times ZG_2$. For all $(g_1, g_2) \in G_1 \times G_2$, we have $(k_1, k_2)(g_1, g_2) = (k_1 g_1, k_2 g_2) = (g_1 k_1, g_2 k_2) = (g_1, g_2)(k_1, k_2)$ and thus $(k_1, k_2) \in Z(G_1 \times G_2)$. Assume the proposition holds for $n = k$. Then

$$\begin{aligned} Z(G_1) \times \ldots \times ZG_k \times ZG_{k+1} &= Z(G_1 \times \ldots \times G_k) \times ZG_{k+1} && \text{Inductive hypothesis} \\ &= Z(G_1 \times \ldots \times G_k \times G_{k+1}) && \text{Case where } n = 2 \end{aligned}$$

■

Proposition 79. *$G_1 \times \ldots G_n$ is abelian if and only if each G_i is abelian.*

Proof. A group G is abelian if and only if $ZG = G$. Therefore, $G_1 \times \ldots G_n = Z(G_1 \times \ldots G_n) = ZG_1 \times \ldots \times ZG_n$. Therefore, for all $i, G_i = ZG_i$ and hence G_i is abelian. Since each step is reversible, the converse holds. ■

Proposition 80. *For an abelian group A and $n \in \mathbb{N}$, the set $A(n)$ of elements whose order is finite and divides n is a subgroup.*

Proof. Closure under multiplication follows as if $|a| \mid n$ and $|b| \mid n$ then $a^n b^n = e = (ab)^n$ and $|ab| \mid n$. Closure under inverses follows as for all $a \in A$, $|a| = |a^{-1}|$. The identity has order 1, which divides n. Therefore, this set must be a subgroup. ■

Proposition 81. *If $A \cong B$, then $A(n) \cong B(n)$.*

Proof. Consider an isomorphism $\psi : A \to B$. For all $a \in A(n), |\psi(a)| = a$ and thus $|\psi(a)| \in B(n)$. We must have $\psi(A(n)) < B(n)$. By considering ψ^{-1} in a similar manner, we must have $\psi^{-1}(B(n)) < A(n)$ and therefore $A(n) \cong B(n)$. ■

Proposition 82. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \ncong \mathbb{Z}_4 \times \mathbb{Z}_4$.

Proof. It suffices to show $\mathbb{Z}_2 \times \mathbb{Z}_2 \ncong \mathbb{Z}_4$. We have $(\mathbb{Z}_2 \times \mathbb{Z}_2)(2) = \mathbb{Z}_2 \times \mathbb{Z}_2$ while $\mathbb{Z}_4(2) = \{[0], [2]\}$, hence $(\mathbb{Z}_2 \times \mathbb{Z}_2)(2) \ncong \mathbb{Z}_4(2)$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \ncong \mathbb{Z}_4$. ■

Proposition 83. *Let k be the number of partitions of an integer n. Let p be a prime. The number of isomorphism classes of abelian groups of order p^n is k.*

Proof. Let G be an abelian group with $|G| = p^n$. Then G can be decomposed into a direct product of cyclic groups. Let $G \cong Z_{p^{k_1}} \times Z_{p^{k_2}} \times \ldots \times Z_{p^{k_m}}$. We must have that $|G| = |Z_{p^{k_1}} \times Z_{p^{k_2}} \times \ldots \times Z_{p^{k_m}}| = |Z_{p^{k_1}}| \times |Z_{p^{k_2}}| \times \ldots \times |Z_{p^{k_m}}|$. Thus $p^n = p^{k_1} \times \ldots \times p^{k_m}$ and hence $n = k_1 + \ldots + k_m$. Therefore, the number of isomorphism classes is the number of ways to partition n. ■

Proposition 84. *Abelian groups of order* 400 *have* 10 *isomorphism classes.*

Proof. Let A be an abelian group with $|A| = 400 = 5^2 \times 2^4$. We must have that A is isomorphic to the direct product of its Sylow 5-subgroup and its Sylow 2-subgroup. By **Proposition 83**, the number of isomorphism classes for the Sylow 2-subgroup is the number of ways to partition 4 and the number of isomorphism classes for the Sylow-5 subgroup is the number of ways to partition 2. 4 can be partitioned 5 ways and 2 can be partitioned 2 ways. Hence the number of isomorphism classes for A is $5 \times 2 = 10$. ■

Proposition 85. *Any finite abelian group is cyclic or contains a subgroup isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$ for some prime p.*

Proof. Let G be a finite abelian group with cyclic decomposition $G \cong \mathbb{Z}_{p_1^{k_1}} \times \ldots \times \mathbb{Z}_{p_m^{k_m}}$. If the $\mathbb{Z}_{p_i^{k_i}}$ have pairwise coprime order, then by the Chinese Remainder Theorem, G is cyclic. If G is not cyclic, then we must have that $p_i = p_j = p$ for some $i \neq j$. Hence $Z_p \times Z_p \cong p^{k_i-1}\mathbb{Z}_{p^{k_i}} \times p^{k_j-1}\mathbb{Z}_{p^{k_j}} \cong 1 \times \ldots \times p^{k_i-1}\mathbb{Z}_{p^{k_i}} \times \ldots \times p^{k_j-1}\mathbb{Z}_{p^{k_j}} \times \ldots \times 1 < \mathbb{Z}_{{p_1}^{k_1}} \times \ldots \times \mathbb{Z}_{{p_m}^{k_m}} \cong G$. ■

Proposition 86. *Let Bij $\mathbb{R}^3$ be the group of all bijections $\mathbb{R}^3 \to \mathbb{R}^3$. The subset of Bij $\mathbb{R}^3$ consisting of translations is a subgroup isomorphic to the additive group $\mathbb{R}^3$.*

Proof. Define $\phi : \mathbb{R}^3 \to \text{Bij } \mathbb{R}^3$ such that $\phi(\vec{w})(\vec{v}) = f_{\vec{w}}(\vec{v}) = \vec{v} + \vec{w}$. Note $(f_{\vec{u}} \circ f_{\vec{w}})(\vec{v}) = f_{\vec{u}}(f_{\vec{w}}(\vec{v})) = f_{\vec{u}}(\vec{v} + \vec{w}) = (\vec{v} + \vec{w}) + \vec{u} = \vec{v} + (\vec{w} + \vec{u}) = f_{\vec{u}+\vec{w}}(\vec{v})$. Hence $\phi(\vec{u} + \vec{w}) = f_{\vec{u}+\vec{w}} = f_{\vec{u}} \circ f_{\vec{w}} = \phi(\vec{u}) \circ \phi(\vec{w})$ and therefore ϕ is a homomorphism. If $\phi(\vec{w}) = \text{id}$, then for any $\vec{v}$ we have $\vec{v} + \vec{w} = \vec{v}$, and thus $\vec{w} = \vec{0}$. ϕ then has trivial kernel and is injective. This gives that $\text{im } \phi \cong \mathbb{R}^3$. Since the image of ϕ consists of translations, we are done. ■

Proposition 87. *The subset SO(3) $\subset$ Bij $\mathbb{R}^3$ consisting of rotations is a subgroup.*

Proof. The identity matrix has determinant 1 and is orthogonal. Each transpose acts as a two sided inverse and is orthogonal with unit determinant since

$$1 = \det I = \det A^T A = \det A \det A^T = 1 \times \det A^T = \det A^T$$

Any matrix product is also orthogonal and has unit determinant since

$$(AB)(AB)^{-1} = I$$
$$(AB)^{-1} = B^T A^T = (AB)^T$$
$$\det AB = \det A \det B = 1 \times 1 = 1$$

■

Proposition 88. *Consider SO(3)$\circlearrowright\mathbb{R}^3$ by $A \cdot \vec{w} = A\vec{w}$. The subset Aff $\mathbb{R}^3 \subset$ Bij $\mathbb{R}^3$ of bijections $f(\vec{v}) = \vec{w} + A\vec{v}$ is a subgroup isomorphic to $\mathbb{R}^3 \rtimes$ SO(3).*

Proof. Let $g(\vec{v}) = A\vec{v} + \vec{w}$ and $f(\vec{v}) = B\vec{v} + \vec{u}$. The composition of affine functions is affine since $(f \circ g)(\vec{v}) = f(g(\vec{v})) = f(A\vec{v} + \vec{w}) = B(A\vec{v} + \vec{w}) + \vec{u} = BA\vec{v} + B\vec{w} + \vec{u}$. Closure under inverses follows since $f^{-1}(\vec{v}) = B^{-1}\vec{v} - B^{-1}\vec{u}$ gives $(f \circ f^{-1})(\vec{v}) = f(f^{-1}(\vec{v})) = f(A^{-1}\vec{v} - A^{-1}\vec{u}) = A(A^{-1}\vec{v} - A^{-1}\vec{u}) + \vec{u} = \vec{v}$. Checking the other side, $(f^{-1} \circ f)(\vec{v}) = f^{-1}(f(\vec{v})) = f(A\vec{v} + \vec{u}) = A^{-1}(A\vec{v} + \vec{u}) - A^{-1}\vec{u} = \vec{v}$.

Let $T \subset \operatorname{Bij} \mathbb{R}^3$ consisting of translations. Let $f(\vec{v}) = A\vec{v} + \vec{w}$. Conjugating a translation $g(\vec{v}) = \vec{v}+\vec{u}$ gives $(f \circ g \circ f^{-1})(\vec{v}) = f(g(f^{-1}(\vec{v}))) = f(g(A^{-1}\vec{v} - A^{-1}\vec{w})) = f(A^{-1}\vec{v} - A^{-1}\vec{w} + \vec{u}) = A(A^{-1}\vec{v} - A^{-1}\vec{w} + \vec{u}) + \vec{w} = \vec{v} - \vec{w} + A\vec{u} + \vec{w} = \vec{v} + A\vec{u}$, another translation. Hence, $T \lhd \operatorname{Aff} \mathbb{R}^3$.

Since translations in $\mathbb{R}^3$ cannot be represented by 3×3 matrices, we must have $T \cap \operatorname{SO}(3) = 1$. By the main theorem on semi-direct products, $\operatorname{Aff} \mathbb{R}^3 \cong T \rtimes \operatorname{SO}(3)$.

Let $\operatorname{SO}(3)$ act on translations by conjugation. Let $\operatorname{SO}(3)$ act on $\mathbb{R}^3$ by matrix multiplication. Let $\phi : \operatorname{SO}(3) \to \operatorname{SO}(3)$ be the identity map. Let $\psi : \mathbb{R}^3 \to T$ be given by $\psi(\vec{w})(\vec{v}) = \vec{v} + \vec{w}$. ϕ is trivially an isomorphism and ψ is an isomorphism by **Proposition 87**. Note that $\psi(A \cdot \vec{w})(\vec{v}) = \vec{v} + A\vec{w}$ and $(\phi(A) \cdot \psi(\vec{w}))(\vec{v}) = (A \circ \psi(\vec{w}) \circ A^{-1})(\vec{v}) = A(\psi(\vec{w})(A^{-1}\vec{v})) = A(A^{-1}\vec{v} + \vec{w}) = \vec{v} + A\vec{w}$. Hence $\beta : \mathbb{R}^3 \rtimes \operatorname{SO}(3) \to T \rtimes \operatorname{SO}(3)$ given by $\beta(\vec{w}, A) = (\psi(\vec{w}), \phi(A))$ is an isomorphism. ■

Proposition 89. *Any permutation of the 3 non-identity elements of $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ defines an automorphism, and so $\operatorname{Aut} G \cong \Sigma_3$.*

Proof. Since each automorphism maps the identity to itself, the automorphism group of G must be a subset of the group of permutations of the 3 non-identity elements of G. These permutations are automorphisms since any permutation ϕ is a bijection and the sum of any two non-identity elements yields the third, so $\phi(a + b) = \phi(c) = \phi(a) + \phi(b)$. ■

Proposition 90. $\mathbb{Z}_5^\times \cong \mathbb{Z}_4$.

Proof. By **Proposition 37**, it suffices to show $\operatorname{Aut} \mathbb{Z}_5 \cong \mathbb{Z}_4$. Each such automorphism is entirely determined by the image of the identity. Since it must map generators to generators, the identity can be mapped to $1, 2, 3$ or 4. Thus $|\operatorname{Aut} \mathbb{Z}_5| = 4$. Hence it must be isomorphic to $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$. Since the automorphism with $\phi(1) = 2$ has order 4, and all non-identity elements in $\mathbb{Z}_2 \times \mathbb{Z}_2$ have order 2, we must have $\operatorname{Aut} \mathbb{Z}_5 \cong \mathbb{Z}_4$. ■

Proposition 91. *Let $p < q$ be two primes. Any group G of order pq is isomorphic to a semidirect product $\mathbb{Z}_q \rtimes \mathbb{Z}_p$ for some action of $\mathbb{Z}_p$ on $\mathbb{Z}_q$.*

Proof. G has a unique, normal Sylow q-subgroup Q since $n_q \equiv 1 \pmod{q}$ and $n_q \mid p$. G must also have a Sylow p-subgroup P with $P \cap Q = 1$ and $PQ = G$ since the order of any element in the intersection must divide p and q and the order of PQ must divide pq and must be divisible by p and q and therefore must equal pq. Hence, by the main theorem on semidirect products, $G \cong Q \rtimes P$ where the action is conjugation.

Let $\psi : Q \to \mathbb{Z}_q$ and $\phi : P \to \mathbb{Z}_p$ be two isomorphisms. Let $\mathbb{Z}_p \circlearrowright \mathbb{Z}_q$ by $[i] \cdot [j] := \psi(\phi^{-1}([i]) \cdot \psi^{-1}([j]))$.

Note $[0] \cdot [j] = \psi(\phi^{-1}([0]) \cdot \psi^{-1}([j]) = \psi(\psi^{-1}([j])) = [j]$ and $[i] \cdot ([j] \cdot [k]) = [i] \cdot \psi(\phi^{-1}([j]) \cdot \psi^{-1}([k])) = \psi(\phi^{-1}([i]) \cdot \psi^{-1}(\psi(\phi^{-1}([j]) \cdot \psi^{-1}([k])))) = \psi(\phi^{-1}([i]) \cdot \phi^{-1}([j]) \cdot \psi^{-1}([k])) = \psi(\phi^{-1}([ij]) \cdot \psi^{-1}([k])) = [ij] \cdot [k]$. Hence, the action is well defined.

Additionally, $\psi(p \cdot q) = \phi(p) \cdot \psi(q) = \psi(\phi^{-1}(\phi(p)) \cdot \psi^{-1}(\psi(q))) = \psi(p \cdot q)$ and thus $\beta : Q \rtimes P \to \mathbb{Z}_q \rtimes \mathbb{Z}_p$ given by $\beta(n, k) = (\psi(n), \phi(k))$ is an isomorphism. Finally,

$G \cong Q \rtimes P \cong \mathbb{Z}_q \rtimes \mathbb{Z}_p$ equipped with the previously defined action, $[i] \cdot [j] := \psi(\phi^{-1}([i]) \cdot \psi^{-1}([j]))$. ■

Proposition 92. *Any group G with $|G| = 55$ is isomorphic to $\mathbb{Z}_{11} \times \mathbb{Z}_5$ or $\mathbb{Z}_{11} \rtimes \mathbb{Z}_5$ equipped with the action defined by the homomorphism $f : \mathbb{Z}_5 \mapsto Aut\, \mathbb{Z}_{11}$ sending $1 \mapsto [i \mapsto i^2]$.*

Proof. By **Proposition 91** we see $G \cong \mathbb{Z}_{11} \rtimes \mathbb{Z}_5$ equipped with some action. If the Sylow 5-subgroup is normal, then the action is trivial and G is abelian since the semidirect product reduces to the direct product.

Otherwise, the action must be nontrivial and G cannot be abelian. Consider two different nontrivial actions defined by homomorphisms $f, g : \mathbb{Z}_5 \to \text{Aut } \mathbb{Z}_{11}$. The image of any such homomorphism must have order 5, since it can send 1 to any element of order 5, and since $\text{Aut } \mathbb{Z}_{11} \cong \mathbb{Z}_{10}$, there are 5 possible elements, namely the even elements. Furthermore, $\mathbb{Z}_{10}$ must have a unique Sylow 5-subgroup N. Hence, any nontrivial action must give an isomorphism from $\mathbb{Z}_5 \to N$. Therefore we have an isomorphism $g^{-1} \circ f : \mathbb{Z}_5 \to \mathbb{Z}_5$. Letting $\phi = g^{-1} \circ f$ and $\psi = \text{id}$, note $\psi(f([i])([j])) = f([i])([j])$ and $g(\phi([i]))(\psi([j])) = g(g^{-1} \circ f([i]))([j]) = f([i])([j])$. Hence, all semi-direct products $\mathbb{Z}_{11} \rtimes \mathbb{Z}_5$ with any non-trivial action must be isomorphic.

Therefore, we can specify any non-trivial action to pin down all non-trivial semi-direct products, up to isomorphism. Let f be the homomorphism such that $1 \mapsto [i \mapsto i^2]$. Putting these facts together gives that G is isomorphic to $\mathbb{Z}_{11} \times \mathbb{Z}_5$ or $\mathbb{Z}_{11} \rtimes \mathbb{Z}_5$ equipped with f. ■

Proposition 93. *Groups G of order 20 are isomorphic to one and only one of $\mathbb{Z}_{20}, \mathbb{Z}_{10} \times \mathbb{Z}_2, \mathbb{Z}_5 \rtimes \mathbb{Z}_4$ with either the action sending $1 \mapsto [i \mapsto i]$ or $1 \mapsto [i \mapsto i^2]$, or $\mathbb{Z}_5 \rtimes \mathbb{Z}_2 \times \mathbb{Z}_2$ with the action sending $(1, 0) \mapsto [i \mapsto i^2]$ and $(0, 1) \mapsto [i \mapsto i^2]$.*

Proof. G has a unique, normal Sylow 5-subgroup S_5 since $n_5 \equiv 1 \pmod 5$ and $n_5 \mid 2$ and a Sylow 2-subgroup S_2. Hence, $G \cong S_5 \rtimes S_2$. If S_2 is normal, then the action is trivial and $G \cong S_5 \times S_2$. If $S_2 \cong \mathbb{Z}_4$, then $G \cong \mathbb{Z}_5 \times \mathbb{Z}_4 \cong \mathbb{Z}_{20}$. If $S_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, then $G \cong \mathbb{Z}_5 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \cong \mathbb{Z}_{10} \times \mathbb{Z}_2$. These are the only abelian isomorphism classes.

Otherwise, S_2 is not normal and G is not abelian. If $S_2 \cong \mathbb{Z}_4$, then let $\mathbb{Z}_4 \circlearrowright \mathbb{Z}_5$. There are three non-trivial homomorphisms $g, g', g'' : \mathbb{Z}_4 \mapsto \text{Aut } \mathbb{Z}_5$ where $g(1) = [i \mapsto i]$, $g'(1) = [i \mapsto i^2]$ and $g''(1) = [i \mapsto i^3]$. Note that the semi-direct products given by g and g'' are isomorphic, related by the automorphism of $\mathbb{Z}_4$ sending $1 \mapsto 3$. The semi-direct product given by g' is not isomorphic to either, however, since 2 acts trivially and is thus in the center of the semi-direct product given by g' while it is not in the center of the semi-direct products given by g, g''. Hence, we have two isomorphism classes in this case, given by $\mathbb{Z}_5 \rtimes \mathbb{Z}_4$ equipped either with g or g'.

The final case is if S_2 is not normal and isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. However, all possible nontrivial actions of $\mathbb{Z}_2 \times \mathbb{Z}_2 \circlearrowright \mathbb{Z}_5$ give isomorphic semi-direct products, since by **Proposition 89**, we can swap any non-identity elements arbitrarily to determine an automorphism. Hence, we can choose the action defined by the homomorphism sending $(1, 0) \mapsto [i \mapsto i^2]$ and $(0, 1) \mapsto [i \mapsto i^2]$. ■