Exercise 9.9. *Let $H \leq G$, the index of H is 2. Show that H is normal.*

Proof. Since $[G : H] = 2$, $G = H \cup gH = H \cup Hg$ where $g \notin H$. Also $H \cap gH = H \cap Hg = \varnothing$. Removing H from G we get $gH = Hg$.

Informally, gH and Hg are the another half part of G. □

Exercise 9.11. *Prove that a quotient group of a cyclic group is cyclic.*

Proof. For any cyclic group G and normal subgroup H, let $G = \langle g \rangle$ and $H = \langle g^n \rangle$ for some minimum $n \in \mathbb{N}$. We claim $G/H \approx Z_n$ or $G/H \approx G$ if $n = 0$ which is trivial.

We claim:

$$\boxed{\langle gH \rangle = G/H}$$

Every element in $\langle gH \rangle$ is a coset of H, thus $\langle gH \rangle \subseteq G/H$.

Any element in G/H has form hH where $h \in G$, therefore $h = g^s$ for some s. Then $hH = g^s H \in \langle gH \rangle$.

We claim $|gH| = n$. $(gH)^n = g^n H$ where $g^n \in H$, so $g^n H = H$. Suppose $0 < m < n, g^m H = H$. Then $g^m \in H$ and $g^{\gcd(m,n)} \in H$ where $\gcd(m,n) \leq m$ and $\gcd(m,n)$ divides n. But this contradict our assumption that n is minimum such that $\langle g^n \rangle = H$, because $\langle g^{\gcd(m,n)} \rangle = H$.

Thus, $\langle gH \rangle$ is cylic and order n, which is isomorphic to Z_n □

Exercise 9.12. *Prove that a quotient group of an Abelian group is abelian.*

Proof. For any Abelian group G and normal subgroup H. For all aH and bH in G/H where $a\ b \in G$. $(aH)(bH) = abH = baH = (bH)(aH)$. □

Exercise 9.21. *For any Abelian group G of order $p_0 p_1 \cdots p_{n-1}$ where p_i are distinct primes. Shows that G is cyclic.*

Proof. Since $|G| = p_0 p_1 \cdots p_{n-1}$, there are elements of each prime orders, say, $|g_0| = p_0, |g_1| = p_1 \cdots$. We claim $G = \langle g_0 \rangle \times \langle g_1 \rangle \times \cdots \times \langle g_{n-1} \rangle$.

They are all normal because G is Abelian, so the first property satisfied. Let $H = (\langle g_0 \rangle \langle g_1 \rangle \cdots \langle g_{i-1} \rangle) \cap \langle g_i \rangle$ for some i. H must be the subgroup of both $\langle g_0 \rangle \langle g_1 \rangle \cdots \langle g_{i-1} \rangle$ and $\langle g_i \rangle$, therefore, $|H|$ divides $p_0 p_1 \cdots p_{i-1}$ and p_i. But all p's are distinct prime, so $|H|$ must be 1, thus $H = \{e\}$. Then, since the product of two Abelian subgroups is also a subgroup, and the property we just proved, it is easy to show $G = \langle g_0 \rangle \langle g_1 \rangle \cdots \langle g_{n-1} \rangle$ by $\forall H\ K \leq G, |HK| = \dfrac{|H||K|}{|H \cap K|}$

So G is the internal direct product of $\langle g_0\rangle \times \langle g_1\rangle \times \cdots \times \langle g_{n-1}\rangle$, which is isomorphic to $G' = \langle g_0\rangle \oplus \langle g_1\rangle \oplus \cdots \oplus \langle g_{n-1}\rangle$. And the order of $\langle g_i\rangle$ are relative primes, so G' is cyclic, so is G. $\square$

Exercise 9.41. *Let H be proper subgroup of Q, the group of rational numbers under addition. Show that H is infinite index.*

Proof. Since Q Abelian, we need to show Q/H is infinite. Suppose $|Q/H|$ is some finite n, let $aH \in Q/H$ and $aH \neq H$, then $(aH)^n = (na)H = H$. But we found that $(\frac{a}{n})H \in Q/H$ since it is a coset of H, but $((\frac{a}{n})H)^n = aH$ which is not identity, contradict the fact that $\forall aH \in G/H, (aH)^n = H$

Another solution: $\forall x \in Q$, we have $xH \in Q/H$, if $|Q/H| = n$, then $(xH)^n = nxH = H \to nx \in H$. Consider $f(x) = nx : Q \to Q$, it is surjection, thus $Q \subseteq H$.

In fact, these solutions are the same, proving f is surjection is exactly finding $f(x/n) = x$, which we done in the first proof. $\square$

Exercise 9.47. *Show that D_{13} is isomorphic to $\text{Inn}(D_{13})$. Moreover, show that any group G where $Z(G) = \{e\}$, is isomorphic to $\text{Inn}(G)$*

Proof. By Theorem 9.4, $G/Z(G) \approx \text{Inn}(G)$. Since $Z(G) = \{e\}$, $G/Z(G) = G/\{e\} \approx G$, thus $G \approx \text{Inn}(G)$. $\square$

Exercise 9.57. *Show that the intersection of two normal subgroups of G is also a normal subgroup of G.*

Proof. Let $H \triangleleft G$ and $K \triangleleft G$, we need to show $(H \cap K) \triangleleft G$, or equivalently, $\forall g \in G, g(H \cap K)g^{-1} \subseteq (H \cap K)$.

For any $h \in H \cap K$, since H is normal, there is a h' such that $ghg^{-1} = h'gg^{-1}$. Similarly, there is a h'' such that $ghg^{-1} = h''gg^{-1}$. By cancellation, $h' \in H = h'' \in K$, thus $h' = h'' \in H \cap K$, $ghg^{-1} = h'gg^{-1} = h' \in H \cap K$.

Moreover, we can proof that for n normal subgroups of G, the intersection of those subgroups is also a normal subgroup of G.

We induction on n:

- Base: The intersection of 1 normal subgroup is itself, and it is a normal subgroup of G.

- Induction: We have the following induction hypothesis:

$$\boxed{\text{The intersection of } n-1 \text{ normal subgroups is a normal subgroup of } G}$$

And we need to show:

$$\boxed{\text{The intersection of } n \text{ normal subgroups is a normal subgroup of } G}$$

Let H be the intersection of $n-1$ normal subgroups, and we know it is normal in G. Let K be the nth normal subgroup, we already prove that $H \cap K$ is also a normal subgroup of G.

□

Exercise 9.59. *Let $N \lhd G$ and N is cyclic. Show that any subgroup of N is normal in G.*

Proof. Suppose $M = \langle n^k \rangle$ is a subgroup of N, then M is cyclic. For any $g \in G$, $n^{ks} \in M$, $gn^{ks}g^{-1} = (gn^s g^{-1})^k$. By N is normal, $gn^s g^{-1} = n^t$ for some $n^t \in N$. Then $(gn^s g^{-1})^k = (n^t)^k = n^{tk} = (n^k)^t \in M$ □

Exercise 9.61. *Let $H \lhd G$ and G a finite group. Let $x \in G$ and $|x|$ is coprime to $|G/H|$. Show that $x \in H$.*

Proof. Let $xH \in G/H$, since G finite, so is G/H. So we suppose the order of $|xH|$ is n. If n doesn't divide $|x|$, then $|x| = nq + r$. We have $(xH)^{|x|} = (xH)^{nq+r} = (xH)^r = H$ where $r < n$, which contradict $|xH| = n$. So n has to divide $|x|$, but n also divides $|G/H|$ and we know $|x|$ is coprime to $|G/H|$. Thus n has to be 1, which implies $xH = H \to x \in H$. □

Exercise 9.62. *Let G be a group of order pm where p is prime, $p > m$. If H is a subgroup of G of order p, prove that H is normal.*

Proof. We first show H is the only subgroup of G of order p. Let K be another subgroup of G of order p. Since $H \neq K$, we have $H \cap K = \{e\}$. Then $|HK| = \dfrac{|H||K|}{|H \cap K|} = p^2$ where $HK \subseteq G$. But $p^2 > pm$ since $p > m$.

For any $x \in G$, ϕ_x sends H to a subgroup of order p in G, but we already prove that H is the only subgroup of G, thus, for any $h \in H$, $\phi_x(h) = xhx^{-1} \in H$. □

Exercise 9.63. *If a group of order 24 has more than one subgroups of order 3. Show that none of them is normal.*

Proof. Suppose $H \triangleleft G$, K is a distinct subgroup of G, and $|H| = |K| = 3$. By the example of Theorem 9.1, HK is a subgroup of G. But now $|HK| = \dfrac{|H||K|}{|H \cap K|}$, since $H \neq K$ and $|H| = |K| = 3$, $|H \cap K| = 1$ and $|HK| = 3 * 3 = 9$. Now, $|HK|$ must divides $|G| = 24$ which doesn't. □

Exercise 9.66. *Suppose G has a subgroup of order n. Prove that the intersection of all subgroups of order n of G is normal in G.*

Proof. We need to show: Let $\phi : G \to G$ an isomorphism, H be the intersection of all subgroups of G of order n, shows that $\phi(H) = \{ \phi(h) \mid h \in H \}$ is the intersection of all subgroups of $\overline{G}$ of order n .

Let $H = H_0 \cap H_1 \cap \cdots \cap H_m$, then $\phi(H) = \phi(H_0 \cap H_1 \cap \cdots \cap H_m) =$ (since ϕ is injective) $\phi(H_0) \cap \phi(H_1) \cap \cdots \cap \phi(H_m)$. Let K be a subgroup of $\overline{G}$ of order n. Since ϕ is an isomorphism, there is a H_i such that $\phi(H_i) = K$. Thus, $\phi(H)$ is the intersection of all subgroups of $\overline{G}$ of order n.

Now, taking automorphism $\phi_g(h) = ghg^{-1}$, we can prove $\phi_g(H) = H$, then $\forall g \in G, ghg^{-1} \in \phi_g(H) = H$ which implies normal. □

Exercise 9.67. *If G is non-Abelian, show that $Aut(G)$ is not cyclic.*

Proof. We consider the converse of our goal:

$$\boxed{\text{If } Aut(G) \text{ is cyclic, show that } G \text{ is Abelian.}}$$

For any $a\ b \in G$, consider the automorphisms $T_{ab}(g) = abg$. $T_{ab}(g) = (ab)g = a(bg) = T_a(T_b(g))$. Since $Aut(G)$ is cyclic and T_a , T_b are automorphisms, we can write T_a and T_b in ϕ^i and ϕ^j for some i and j where $Aut(G) = \langle \phi \rangle$. Then $T_{ab}(g) = T_a(T_b(g)) = \phi^i(\phi^j(g)) = \phi^{i+j}(g) = \phi^{j+i}(g) = \phi^j(\phi^i(g)) = T_b(T_a(g)) = T_{ba}(g)$. We take $g = e$, $T_{ab}(e) = T_{ba}(e) \to ab = ba$. □

Exercise 9.68. *Let $|G| = p^n m$ where p is prime and p is coprime to m. Suppose H is a normal subgroup of G of order p^n, if K is a subgroup of G of order p^k, show that $K \subseteq H$.*

Proof. Since H is normal, $|G/H| = \dfrac{|G|}{|H|} = m$. For any $a \in K$, $(aH)^{p^k} = a^{p^k} H = eH = H$, we know $|aH|$ divides p^k. Also, since $aH \in G/H$, $|aH|$ divides $|G/H| = m$. Thus $|aH|$ divides p^k and m. By p is coprime to m and p is prime, we know p^k is also coprime to m, so $|aH| = 1 \to a \in H$. □

Exercise 9.71. *If $|G| = 30$ and $|Z(G)| = 3$, which group is $G/Z(G)$ isomorphic to? What about $|Z(G)| = 5$? What about $|G| = 2pq$ where p and q are distinct odd primes?*

Proof. First, we know the group of order $2p$ where p is prime is isomorphic to Z_{2p} or D_p.

For $|G/Z(G)| = 30/3 = 10$. Suppose $G/Z(G)$ is cyclic, by Theorem 9.3, G is Abelian, but then $|G = Z(G)| = 30$. So $G/Z(G)$ can not be cyclic, thus $G/Z(G)$ is isomorphic to D_3 Similarly, $G/Z(G)$ is isomorphic to D_5 if $|Z(G)| = 5$.

Moreover, suppose $|G| = 2pq$ and $|Z(G)| = p$. If $G/Z(G)$ is cyclic, then $|Z(G)| = 2pq$ which is not cool. So $G/Z(G)$ is isomorphic to D_q. □

Exercise 9.72. *If $H \triangleleft G$ and $|H| = 2$, prove that $H \subseteq Z(G)$.*

Proof. Since $|H| = 2$, we suppose the only non-identity element in H is h. For any $g \in G$, $gh \in gH$, since H is normal, we know there is an h' such that $gh = h'g$. Suppose $h' = e$, then $gh = g$ give us $h = e$ which contradicts our assumption. So h' has to be h, then $gh = hg$, $h \in Z(G)$. □

Exercise 9.74. *Let $H \triangleleft G$ and the index of $H = 2$. Show that H contains all the elements of odd order.*

Proof. Suppose $g \in G$ is odd order. Then by $(gH)^|g| = H$ we know $|gH|$ divides $|g|$ where $|gH|$ might be 1 or 2. Since $|g|$ is odd, so the only choice is $|gH| = 1 \to gH = H \to g \in H$. □

Exercise 9.77. *Show that A_5 has no normal subgroup of order* 12.

Proof. Suppose $H \triangleleft A_5$ and $|H| = 12$. Then $|A_5/H| = 5$. □

Exercise 9.81. *Let $g \in G$ and $H \triangleleft G$, if $|g| iscoprimeto |H|$, show that $|gH| = |g|$.*

Proof. Suppose $|gH| = n$, then $g^n \in H$. Let $|g^n| = m$ which divides $|H|$, then $(g^n)^m = e$ and $|g|$ divides nm. Since $|g|$ is coprime to $|H|$ and m divides H, $|g|$ is coprime to $|m|$, so $|g|$ divides n.

Another solution: Since $g^n \in \langle g \rangle$, $|g^n|$ divides $|g|$. Also, by $g^n \in H$, $|g^n|$ divides $|H|$. Then by $|g|$ is coprime to $|H|$, $|g^n| = 1 \to g^n = e$, Then $|g|$ divides $|n|$. □

Exercise 9.84. *For any $n \geq 3$, prove that D_{2n} can be expressed as an internal direct product of D_n and a subgroup of order 2 iff n is odd.*

Proof. Suppose $D_{2n} = D_n \times H$ for some normal subgroup H of order 2. Since $|H| = 2$, $H \subseteq Z(D_{2n})$, we know $Z(D_{2n}) = \{R_0, R_{180}\}$, thus $H = Z(D_{2n})$. If n is even, $R_{180} \in D_n$, and $R_{180} \in H$ since $H = Z(D_{2n})$. $D_n \cap H \neq \{e\}$ which contradicts the requirement of internal direct product.

If n is odd, we claim $D_{2n} = D_n \times \{R_0, R_{180}\}$. It is easy to show $\{R_0, R_{180}\}$ is normal, so we focus on D_n. Let $a \in D_{2n}$ and $b \in D_n$, we need to show $aba^{-1} \in D_n$.

- a and b are rotations, $aba^{-1} = aa^{-1}b = b \in D_n$.

- a is reflection and b is rotation, then ab is reflection, $(ab)a^{-1} = (b^{-1}a^{-1})a^{-1} = b^{-1} \in D_n$.

- a is rotation and b is reflection, then ab is reflection, $(ab)a^{-1} = b^{-1}a^{-1}a^{-1}$, we need to show $a^{-2} \in D_n$. Let Z_{2n} the rotations of D_{2n} and Z_n the rotations of D_n, since Z_{2n} is Abelian (or the index of Z_n is 2), $Z_n \triangleleft Z_{2n}$, $|Z_{2n}/Z_n| = \dfrac{2n}{n} = 2$ Then $(a^{-1}Z_n)^2 = a^{-2}Z_n = Z_n$ which implies $a^{-2} \in Z_n$.

  Thus, by $b^{-1} \in D_n$ and $a^{-1}a^{-1} \in D_n$, $b^{-1}a^{-1}a^{-1} \in D_n$.

- a and b are reflections, let $H \in D_n$ and H is reflection. Then we can write a and b in RH and $R'H$ for some R and R' which are rotations. Then

$$
\begin{aligned}
aba^{-1} &= RHR'H(RH)^{-1} \\
&= RHR'HHR^{-1} && (a \text{ is reflection}) \\
&= RHR'R^{-1} \\
&= R(HR')R^{-1}
\end{aligned}
$$

  where $H \in D_n$ and $R' \in D_n$, this is the last case we just proved.

Then $\forall a \in D_{2n}, aD_na^{-1} \subseteq D_n \to D_n \triangleleft D_{2n}$.

And, I just realized that the index of D_n is 2, then $D_n \triangleleft D_{2n}$. LOL.

Since n is odd, $R_{180} \notin D_n$, $D_n \cap \{R_0, R_{180}\} = \{R_0\}$.

$|D_n\{R_0, R_{180}\}| = \dfrac{|D_n||\{R_0, R_{180}\}|}{|D_n \cap \{R_0, R_{180}\}|} = (2n) \times 2 = |D_{2n}|$, thus $D_n\{R_0, R_{180}\} = D_{2n}$. □

Exercise 9.85. *Suppose G is an Abelian group and $H_0, H_1, \cdots, H_{k-1}$ are subgroups of G such that for any $g \in G$ is uniquely expressible in the form $h_0 h_1 \cdots h_{k-1}$ where $h_i \in H_i$. Prove that $G = H_0 \times H_1 \times \cdots \times H_{k-1}$.*

Proof. It is trivial that H_i are normal and the product of them is exactly G. We need to show $\forall i, (H_0 H_1 \cdots H_i) \cap H_{i+1} = \{e\}$. Suppose $g \in (H_0 H_1 \cdots H_i) \cap H_{i+1}$ and $g \neq e$. Then g can be expressed in form $h_0 h_1 \cdots h_i$ and h_{i+1} which contradict the assumption. □

Exercise 9.86 (Normalizer)**.** *Let G be a group and H be a subgroup of G. Define $N(H) = \{x \in G \mid xHx^{-1} = H\}$. Prove that $N(H)$ is a subgroup of G.*

Proof. By two-steps:

- $e \in N(H)$ since $H = H$.
- For any $a\ b \in N(H)$, $abHab^{-1} = abHb^{-1}a^{-1} = aHa^{-1} = H$.
- For any $a \in N(H)$, $H = a^{-1}aHa^{-1}a = a^{-1}Ha$.

□

Exercise 9.89. *Let G be a group of order pm where p is prime and p is coprime to m. Suppose G has a normal subgroup of p, show that it is the only subgroup of order p.*

Proof. Let $H \triangleleft G$ and $|H| = p$, if $K \leq G$, $|K| = p$ and $H \neq K$. Then HK is a subgroup of G since H is normal. It is easy to show $H \cap K = \{e\}$ since they are order p. Thus $|HK| = |H||K| = p^2$, and since HK is a subgroup of G, $|HK|$ divides G, that is, p^2 divides pm, which implies p divides m, but p is coprime to m. □

Exercise 9.90. *For any group G, show that* $\mathrm{Inn}(G) \triangleleft \mathrm{Aut}(G)$.

Proof. Let $\phi \in \mathrm{Aut}(G)$ and $\phi_g \in \mathrm{Inn}(G)$ for some $g \in G$.

$$\begin{aligned}
&(\phi\phi_g\phi^{-1})(x) \\
=&\phi(\phi_g(\phi^{-1}(x))) \\
=&\phi(g\phi^{-1}(x)g^{-1}) \\
=&\phi(g)\phi(\phi^{-1}(x))\phi(g^{-1}) \\
=&\phi(g)x\phi(g)^{-1} \\
=&\phi_{\phi(g)} \in \mathrm{Inn}(G)
\end{aligned}$$

□

Exercise 9.91. *Let G be an Abelian group of order 2^n where n is positive integer. If G has exactly one element of order 2, show that G is cyclic.*

Proof. Induction on n. If $n = 1$, $|G| = 2$, it is obviously that G is cyclic. So we focus on induction step.

Let $g \in G$ be the element of order 2, $H = \langle g \rangle$. Since G is Abelian, G/H is also Abelian. So there is an element aH of order 2 in G/H. We will prove that it is the unique element of order 2.

Suppose $bH \in G/H$ and $|bH| = 2$. Since $(aH)^2 = H$, we know $a^2 \in H$. If $a^2 = e$, then $|a| = 1$ or 2, both cases indicate that $a \in H \to |aH| = 1$, so $a^2 = g$. Similarly, $b^2 = g$. Then $a = ga^{-1}$ and $b = gb^{-1}$. By $a^{-1}b = ag^{-1}gb^{-1} = ab^{-1}$, we know $(a^{-1}b)^2 = a^{-1}bab^{-1} = a^{-1}abb^{-1} = e$, that is, $|a^{-1}b| = 1$ or $2 \to a^{-1}b \in H \to aH = bH$.

Since G is Abelian, so is G/H, and $|G/H| = 2^{n-1}$ where $n-1$ is positive since $n > 1$. And we proved G/H has exactly one element of order 2, by induction hypothesis, G/H is cyclic.

Consider $aH \in G/H$ that $|aH| = 2^{n-1}$. Then $a^{2^{n-1}} \in H$. If $a^{2^{n-1}} = e$, $(a^{2^{n-2}})^2 = a^{2^{n-2}\times 2} = a^{2^{n-1}} = e$. This implies $|a^{2^{n-2}}| = 1$ or 2, both cases indicate that $(aH)^{2^{n-2}} = H$ which contradicts $|aH| = 2^{n-1}$. Thus $a^{2^{n-1}} = g$ and $a^{2^n} = a^{2^{n-1}\times 2} = (a^{2^{n-1}})^2 = g^2 = e$. Since $|aH| = 2^{n-1}$ implies $|a| \geq 2^{n-1}$ and we proved that $|a| \neq 2^{n-1}$, $|a| = 2^n$, G is cyclic.

We can generalize the induction step and show that G is cyclic if G has exactly $\phi(p) = p - 1$ element of order p where p is prime. □

Exercise 9.92. *Let G be finite Abelian group of order mn, where m is coprime to n. Define $G^d = \{x \in G \mid x^d = e\}$, show that $G = G^m \times G^n$.*

Proof. We first show G^m and G^n are subgroups. By two-steps:

- $e \in G^m$
- $\forall x\ y \in G^m$, $(xy)^m = x^m y^m = e$
- $\forall x \in G^m$, $(x^{-1})^m = x^{-m} = (x^m)^{-1} = e$

Same for G^n.

Then we show G^m and G^n are normal. For any $g \in G$, $x \in G^m$. $(gxg^{-1})^m = gx^m g^{-1} = geg^{-1} = e \to gxg^{-1} \in G^m$, same for G^n.

Then we show $G^m \cap G^n = \{e\}$. Let $g \in G$ and $g^m = g^n = e$, then $|g|$ divides m and n, since m is coprime to n, $|g| = 1 \to g = e$.

Finally we show that $G = G^m G^n$. For any $g \in G$, $|g| = d$. d must divides mn. Let $s = \gcd(m, d)$ and $t = \gcd(n, d)$. In other words, we separate d into two parts: the factors of m and the factors of n. Then $g^d = g^{st} = g^s g^t$ where $(g^s)^n = e$ since t divides n, and $(g^t)^m = e$ since s divides m. Then $g^s g^t = e \rightarrow g \in G^m G^n$. Thus $G \subseteq G^m G^n$. $\square$