Definition 9.1 (Normal Subgroup). *A subgroup H of G is normal if for any $a \in G$, $aH = Ha$.*

Theorem 9.1 (Normal Subgroup Test). *A subgroup H of G is normal in G $\iff$ $xHx^{-1} \subseteq H$ for all x in G.*

Proof. We must show fisrt:

$$\boxed{\text{The subgroup } H \subseteq G \text{ is normal } \implies \forall x \in G, xHx^{-1} \subseteq H}$$

By the definition of normal, we know $\forall a \in G, aH = Ha$, that is, $\forall a \in G, h \in H, \exists h', ah = h'a$. Therefore, for all elements xhx^{-1} in xHx^{-1}, $xhx^{-1} = h'xx^{-1} = h'e = h$ which is in H.

So $xHx^{-1} \subseteq H$.

Secondly, we must show:

$$\boxed{\forall x \in G, xHx^{-1} \subseteq H \implies \text{the subgroup } H \subseteq G \text{ is normal}}$$

By the definition of normal, we need to show $\forall a \in G, aH = Ha$, or equivalently, $aH \subseteq Ha$ and $Ha \subseteq aH$.

By the hypothesis, we know $aHa^{-1} \subseteq H$, that is, $\forall h \in H, aha^{-1} \in H$.

By multiplying a at right side, we get $(aha^{-1})a = ah(a^{-1}a) = ah \in Ha$ where $ah \in aH$. And we finished the left half part of our goal. By taking a^{-1} as the argument of hypothesis, we can finish the right half part in a similar way. □

Example. *Let H be a normal subgroup of G and K be any subgroup of G. Shows that $HK = \{hk \mid h \in H, k \in K\}$ is a subgroup of G.*

Proof. By two-steps test of subgroup:

1. $ee \in HK$, thus HK is not empty.

2. $\forall h_0k_0\ h_1k_1 \in HK$, $h_0k_0h_1k_1 = h_0(k_0h_1)k_1 = h_0(h_1'k_0)k_1 = h_0h_1'k_0k_1 \in HK$, thus HK is closed under multiplication.

3. $\forall hk \in HK$, $(hk)^{-1} = k^{-1}h^{-1} = (h^{-1})'k^{-1} \in HK$.

□

Theorem 9.2 (Quotient Group). *Let G a group and H a normal group of G, the quotient group $G/H = \{aH \mid a \in G\}$ is a group under multiplication $\forall aH\ bH \in G/H \mapsto (aH)(bH)$.*

Proof. Before our proof, we need to show an important property of this multiplication:

$$\boxed{\forall aH\ bH \in G, (aH)(bH) = abH}$$

For all $h_0\ h_1 \in H$, $ah_0bh_1 = a(h_0b)h_1 = a(bh_0')h_1 = abh_0'h_1 \in abH$. Also, for all $h \in H$, $abh = aebh \in (aH)(bH)$.

Group axioms:

- eH is the identity:
  - $\forall aH \in G/H, aHeH = aeH = aH$
  - $\forall aH \in G/H, eHaH = eaH = aH$
- For all $aH \in G/H$, $a^{-1}H$ is the inverse of aH:
  - $aHa^{-1}H = aa^{-1}H = eH$
  - $a^{-1}HaH = a^{-1}aH = eH$
- For all $aH\ bH\ cH \in G/H$, the associativity: $(aHbH)cH = abHcH = (ab)cH = a(bc)H = aHbcH = aH(bHcH)$

□

Theorem 9.3 (G/Z)**.** *Let G a group, $Z(G)$ the center of G, if $G/Z(G)$ is cyclic, G is Abelian.*

Proof. Let $b\ c \in G$ but $b\ c \notin Z(G)$. If no such b or c, then G is Abelian. Since $G/Z(G)$ is cyclic, $G/Z(G) = \langle aZ(G) \rangle$ for some a. b and c must in some coset, say, $b \in a^mZ(G)$ and $c \in a^nZ(G)$.

$$\begin{aligned}
bc &= a^m g a^n g' \\
&= a^m a^n g g' && (g \in Z(G)) \\
&= a^n a^m g g' && \text{(By property of power)} \\
&= a^n a^m g' g && (g \in Z(G)) \\
&= a^n g' a^m g && (g \in Z(G)) \\
&= cb && \text{(By definition)}
\end{aligned}$$

Thus, b and c commute. □

Lemma 9.1. *Suppose G is a finite group, and H is a normal subgroup of G. If $|aH \in G/H| = n$. Then there is an element of order n in G.*

Proof. Since $|aH| = n$, $(aH)^n = a^nH = H$. Suppose $|a| = k$, we have $(aH)^k = a^kH = H$, thus $|aH| = n$ divides k. So we have $|a^{\frac{k}{n}}| = n$. $\square$

Theorem 9.4 ($G/Z(G) \approx Inn(G)$)**.** *For any group G, $G/Z(G)$ is isomorphic to $Inn(G) = \{\phi_g(x) = gxg^{-1} \mid g \in G\}$.*

Proof. We claim the following function is an isomorphism:

$$\boxed{\psi(aZ(G)) = \phi_a}$$

However, we must show that it **is** a function. That is, for all $a\ b \in G$, $aZ(G) = bZ(G) \implies \psi(aZ(G)) = \psi(bZ(G))$. Since $aZ(G) = bZ(G)$, by property of coset, $a \in bZ(G)$. Then $\forall x, \phi_a(x) = axa^{-1} = (bg)x(bg)^{-1} = bgxg^{-1}b^{-1} = bxb^{-1} = \phi_b(x)$. Thus ψ is a function.

- One-to-one: $\forall aZ(G)\ bZ(G) \in G/Z(G), \psi(aZ(G)) = \psi(bZ(G))$.

$$\begin{aligned}
\psi(aZ(G)) &= \psi(bZ(G)) \\
\phi_a &= \phi_b \\
axa^{-1} &= bxb^{-1} \quad \text{(introduce } x\text{)} \\
b^{-1}ax &= xb^{-1}a
\end{aligned}$$

  Thus $b^{-1}a \in Z(G)$, by property of coset, $aZ(G) = bZ(G)$.

- Onto: $\forall \phi_g \in Inn(G)$, $\psi(gZ(G)) = \phi_g$

- Structure-Preserve: $\forall aZ(G)\ bZ(G) \in G/Z(G)$

$$\begin{aligned}
\psi(aZ(G)bZ(G)) &= \psi(abZ(G)) \\
&= \phi_{ab} \\
&= \phi_a \circ \phi b \\
&= \psi(aZ(G)) \circ \psi(bZ(G))
\end{aligned}$$

$\square$

Theorem 9.5 (Cauchy's Theorem)**.** *Let G be finite Abelian group and let p be a prime where p divides $|G|$. Then there is an element of order p in G.*

Proof. Induction on the number of prime factors of $|G|$:

- Base: We must show that $\forall G, G$ is Abelian, $|G| = p$ where p is prime has an element of order p. Since $|G| = p$, G must be cyclic, then the order of the generator of G is p.

- Induction: We have the induction hypothesis: $\forall G$ a Abelian group, $|G| =$ product of n primes, p divides $|G|$, $\exists x \in G, |x| = p$.

  Suppose $g \in G$, if p divides $|g|$, then $|g^{\frac{|g|}{p}}| = p$, we assume that p doesn't divide $|g|$. Let q a prime that divides $|g|$, then $|g^{\frac{|g|}{q}}| = q$. We let $h = g^{\frac{|g|}{q}}$, and $H = \langle h \rangle$. Since G is Abelian, $\langle h \rangle$ is a normal subgroup. Consider G/H, since G is abelian, so is G/H, and $|G/H| = \frac{|G|}{|H|}$ which is the product of $n+1-1 = n$ primes. Also, p divides G but not divides H, so p divides G/H. Then by induction hypothesis, we know $\exists x \in G/H, |x| = p$. By Lemma 9.1, $\exists x \in G, |x| = p$.

$\square$

Definition 9.2 (Internal Direct Product)**.** *Let* $\{H_0, H_1, H_2 \cdots H_{n-1}\}$ *be a finite collection of normal subgroups of* G*. We say* G *is an internal direct product of* $\{H_0, H_1, H_2 \cdots H_{n-1}\}$ *(write* $G = H_0 \times H_1 \times \cdots \times H_{n-1}$*) if:*

- $G = H_0 H_1 \cdots H_{n-1} = \{h_0 h_1 \cdots h_{n-1} \mid h_i \in H_i\}$
- $(H_0 H_1 \cdots H_{i-1}) \cap H_i = \{e\}$ *for all* $0 \leq i < n$

Lemma 9.2 (Unique Representation of Internal Direct Product)**.** *For all* $h = h_0 h_1 \cdots h_{n-1}$ *and* $h' = h'_0 h'_1 \cdots h'_{n-1}$*,* $h = h'$ *implies* $h_i = h'_i$ *for all* $0 \leq i < n$

Proof. Induction on n:

- Base: We must show $h_0 = h'_0$ implies $h_0 = h'_0$ which is trivial.

- Induction: We have the following induction hypothesis:

$$\boxed{h_0 h_1 \cdots h_{i-1} = h'_0 h'_1 \cdots h'_{i-1} \implies h_j = h'_j \quad (\forall 0 \leq j < i)}$$

  and we must show:

$$\boxed{h_0 h_1 \cdots h_i = h'_0 h'_1 \cdots h'_i \implies h_j = h'_j \quad (\forall 0 \leq j \leq i)}$$

Let $h = h_0h_1 \cdots h_{i-1}$ and $h' = h'_0h'_1 \cdots h'_{i-1}$, $hh_i = h'h'_i$ gives $h = h'h'_ih_i^{-1}$, where $h\ h' \in H_0H_1 \cdots H_{i-1}$ and $h_i^{-1}\ h'_i \in H_i$. Then $h'h'_ih_i^{-1} \in H_0H_1 \cdots H_{i-1}$. By the property of group multiplication, $h'_ih_i^{-1} \in H_0H_1 \cdots H_{i-1}$. But by the property of internal direct product, $(H_0H_1 \cdots H_{i-1}) \cap H_i = \{e\}$. So $h'_ih_i^{-1} = e \to h_i = h'_i$, $hh_i = h'h'_i \to h = h'$. By induction hypothesis, $h_j = h'_j \quad (\forall 0 \leq j < i)$.

$\square$

Example. *Let G is the internal direct product of subgroups $H_0, H_1 \cdots H_{n-1}$. Let $h_i \in H_i$, $h_j \in H_j$ where $0 \leq i, j < n$. $h_ih_j = h_jh_i$ if $i \neq j$.*

Proof. By property of normal, $h'_ih_j = h_jh_i = h_ih'_j$, then by Lemma 9.2, $h_i = h'_i$ $h_j = h'_j$. Thus $h_jh_i = h_ih'_j = h_ih_j$ $\square$

Lemma 9.3 (Center of $h \in H$)**.** *Let G be the internal direct product of subgroups $H_0, H_1, \cdots, H_{n-1}$, $\forall\ h \in H_i, \prod_{j=0, i \neq j} H_j$ is a subgroup of $C(h)$.*

Proof. Since for any normal subgroup H of G, and any subgroup K of G, HK is a subgroup of G, then $\prod_{j=0, i \neq j} H_j$ is a subgroup of G. Consider $k \in H_s$ for some s. By property of normal subgroup H_s, $hk = k'h$ for some k'. Also, for normal subgroup H_i, $hk = kh'$ for some h'. Then $hk = k'h = kh'$, by Lemma 9.2, $h = h'$ and $k = k'$. So $hk = k'h = kh$, $k \in C(h)$. Now we consider any element k in $\prod_{j=0, i \neq j} H_j$, it must be the product of elements k_s in the corresponding H_s, h commutes with all the k_s, so does k. Thus, $\forall\ k \in \prod_{j=0, i \neq j} H_j, k \in C(h)$. $\square$

Theorem 9.6 (Internal Direct Product $\approx$ External Direct Product)**.** *If G is the internal direct product of subgroups $H_0, H_1 \cdots H_{n-1}$, then $H_0 \times H_1 \times \cdots \times H_{n-1} \approx H_0 \oplus H_1 \oplus \cdots \oplus H_{n-1}$.*

Proof. We claim the following function:

$$\boxed{\phi(h_0h_1 \cdots h_{n-1}) = (h_0, h_1, \cdots, h_{n-1})}$$

is an isomorphism, and by Lemma 9.2, we know ϕ **is** a function.

- One-to-one: trivial.
- Onto: trivial.

- Structure-Preserve:

$$\begin{aligned}
&\phi(h_0h_1\cdots h_{n-1})\phi(h_0'h_1'\cdots h_{n-1}')\\
=&(h_0,h_1,\cdots h_{n-1})(h_0',h_1',\cdots h_{n-1}')\\
=&(h_0h_0',h_1h_1',\cdots,h_{n-1}h_{n-1}')\\
=&\phi(h_0h_0'h_1h_1'\cdots h_{n-1}h_{n-1}')\\
=&\phi(h_0h_1h_1'\cdots h_{n-1}h_0'h_{n-1}')\\
=&\cdots\\
=&\phi(h_0h_1\cdots h_{n-1}h_0'h_1'\cdots h_{n-1}')
\end{aligned}$$

□

Lemma 9.4 (Normal Subgroup of External Direct Product)**.** *For all $G = H_0 \oplus H_1$, $H_0 \oplus \{e\}$ and $\{e\} \oplus H_1$ are normal subgroups of G.*

Proof. $\forall\,(a,b) \in H_0 \oplus H_1, (h,e) \in H_0 \oplus \{e\}$, $(a,b)(h,e)(a^{-1},b^{-1}) = (aha^{-1}, bb^{-1}) = (aha^{-1}, e) \in H_0 \oplus \{e\}$. Similarly for $\{e\} \oplus H_1$. □

Lemma 9.5 (Isomorphism respect normal)**.** *For any group G $\overline{G}$ and normal subgroup H of G, if $\phi : G \approx \overline{G}$, then $\phi(H)$ is normal.*

Proof. We need to show $\forall\, g \in \overline{G}, g\phi(H)g^{-1} \in \phi(H)$. Since $\phi^{-1}(g)H\phi^{-1}(g^{-1}) \in H$, by applying ϕ, we get $g\phi(H)g^{-1} \in \phi(H)$. □

Lemma 9.6 (Isomorphism is congruent on Quotient)**.** *For all group G $\overline{G}$ and normal subgroup H of G. If $\phi : G \approx \overline{G}$, then $G/H \approx \overline{G}/\phi(H)$.*

Proof. We claim the following function is an isomorphism:

$$\boxed{\psi(gH) = \phi(g)\phi(H)}$$

We need to show the function we claim **is** a function. $\forall\; gH\; g'H \in G/H$, $gH = g'H$, shows that $\psi(gH) = \psi(g'H)$. Since $gH = g'H$, $g^{-1}g' \in H$, then $\phi(g^{-1}g') \in \phi(H) \to \phi(g^{-1})\phi(g') \in \phi(H) \to \phi(g)\phi(H) = \phi(g')\phi(H)$.

- One-to-one: $\psi(gH) = \psi(g'H) \to \phi(g)\phi(H) = \phi(g')\phi(H)$, then

$$\begin{aligned}
&\phi(g^{-1})\phi(g') \in \phi(H)\\
\to\;& \phi^{-1}(\phi(g^{-1})\phi(g'))\\
=\;& \phi^{-1}(\phi(g^{-1}))\phi^{-1}(\phi(g'))\\
=\;& g^{-1}g' \in H
\end{aligned}$$

which implies $gH = g'H$.

- Onto: $\forall\ g\phi(H) \in \overline{G}/\phi(H)$

$$\begin{aligned}
&\psi(\phi^{-1}(g\phi(H))) \\
=&\psi(\phi^{-1}(g)\phi^{-1}(\phi(H))) \\
=&\psi(\phi^{-1}(g)H) \\
=&\phi(\phi^{-1}(g))\phi(H) \\
=&g\phi(H)
\end{aligned}$$

- Structure-Preserve:

$$\begin{aligned}
&\psi(gHg'H) \\
=&\psi(gg'H) \\
=&\phi(gg')\phi(H) \\
=&\phi(g)\phi(g')\phi(H) \\
=&\phi(g)\phi(H)\phi(g')\phi(H) \\
=&\psi(gH)\psi(g'H)
\end{aligned}$$

□

Lemma 9.7 (Quotien Group of External Direct Product). *$(H_0 \oplus H_1)/(H_0 \oplus \{e\}) \approx H_1$ and $(H_0 \oplus H_1)/(H_1 \oplus \{e\}) \approx H_0$.*

Proof. We claim the following function is an isomorphism:

$$\boxed{\phi((e,h)(H_0 \oplus \{e\})) = h}$$

But first, we need to show it **is** a function. We need to show that for any $h(H_0 \oplus \{e\}) \in (H_0 \oplus H_1)/(H_0 \oplus \{e\})$ where $h \in H_0 \oplus H_1$, ϕ is defined at $h(H_0 \oplus \{e\})$. Since $h = (h_0, h_1) = (e, h_1)(h_0, e)$, $h(H_0 \oplus \{e\}) = (e, h_1)(h_0, e)(H_0 \oplus \{e\})$ where $(h_0, e) \in (H_0 \oplus \{e\})$. Thus $h(H_0 \oplus \{e\}) = (e, h_1)(H_0 \oplus \{e\})$. Then we need to show that $(e, h_0)(H_0 \oplus \{e\}) = (e, h_1)(H_0 \oplus \{e\}) \implies \phi((e, h_0)(H_0 \oplus \{e\})) = \phi((e, h_1)(H_0 \oplus \{e\}))$. It is clearly that any element in $(e, h_0)(H_0 \oplus \{e\})$ has form (a, h_0). Similarly, in $(e, h_1)(H_0 \oplus \{e\})$ it is (a, h_1). Thus $h_0 = h_1$.

- One-to-one: Trivial.

- Onto: Trivial.

- Structure-Preserve:

$$
\begin{aligned}
&\phi((e,h_0)(H_0 \oplus \{e\})(e,h_1)(H_0 \oplus \{e\})) \\
=&\phi((e,h_0h_1)(H_0 \oplus \{e\})) \\
=&h_0h_1 \\
=&\phi((e,h_0)(H_0 \oplus \{e\}))\phi((e,h_1)(H_0 \oplus \{e\}))
\end{aligned}
$$

For $\{e\} \oplus H_1$, we observe that

$$
\begin{aligned}
&(H_0 \oplus H_1)/(\{e\} \oplus H_1) \\
\approx&(H_1 \oplus H_0)/(H_1 \oplus \{e\}) \\
\approx&H_0
\end{aligned}
$$

□

Lemma 9.8 (Cancellation of Internal Direct Product is False)**.** *The following proposition is False: Let $G = H \times K$ and $G = H' \times K$, then $H = H'$.*

Proof. Consider $Z_2 \oplus Z_2$, we have $(Z_2 \oplus \{e\}) \times (\{e\} \oplus Z_2) = Z_2 \oplus Z_2$, and $\langle(1,1)\rangle \times (\{e\} \oplus Z_2) = Z_2 \oplus Z_2$. But $Z_2 \oplus \{e\} \neq \langle(1,1)\rangle$. □