§3.8 Cosets, Normal Subgroups, and Factor Groups

Shaoyun Yi

MATH 546/701I

University of South Carolina

Summer 2021

Review

$\phi : G_1 \to G_2$ is a **group homomorphism** if $\phi(a * b) = \phi(a) \cdot \phi(b)$.

- $\phi(a^n) = (\phi(a))^n$ for all $a \in G_1$ and all $n \in \mathbf{Z}$. e.g., $n = 0$ & $n = -1$
- If $o(a) = n$ in G_1, then $o\big(\phi(a)\big)$ in G_2 is a divisor of n.
- ϕ is onto: if G_1 is abelian (cyclic), then G_2 is also abelian (cyclic).
- If $G_1 = \langle a \rangle$ is cyclic, then ϕ is completely determined by $\phi(a)$.
- $\ker(\phi) = \{x \in G_1 \mid \phi(x) = e_2\} \subseteq G_1$ & $\mathrm{im}(\phi) = \{\phi(x) \mid x \in G_1\} \subseteq G_2$
- ϕ is one-to-one $\Leftrightarrow$ $\ker(\phi) = \{e_1\}$ & ϕ is onto $\Leftrightarrow$ $\mathrm{im}(\phi) = G_2$
- Homorphisms between cyclic gps: $\mathbf{Z}_n \to \mathbf{Z}_k$, $\mathbf{Z} \to \mathbf{Z}$, $\mathbf{Z} \to \mathbf{Z}_n$, $\mathbf{Z}_n \to \mathbf{Z}$
- **Normal subgroup** H of G: If $ghg^{-1} \in H$ for all $h \in H$ and $g \in G$.
  - i) If H_1 is a subgroup of G_1, then $\phi(H_1)$ is a subgroup of G_2.
  - ii) If ϕ is onto and H_1 is normal in G_1, then $\phi(H_1)$ is normal in G_2.
  - iii) If H_2 is a subgroup of G_2, then $\phi^{-1}(H_2)$ is a subgroup of G_1.
  - iv) If H_2 is normal in G_2, then $\phi^{-1}(H_2)$ is normal in G_1.
- **Fundamental Homomorphism Thm** $G_1/\ker(\phi) = G_1/\phi \cong \mathrm{im}(\phi)$

  $\rightsquigarrow$ Reprove "Every cyclic group G is isomorphic to either $\mathbf{Z}$ or $\mathbf{Z}_n$".

Another Equivalence Relation

Recall the proof of Lagrange's thm: Let H be a subgroup of the group G. For $a, b \in G$ define $a \sim b$ if $ab^{-1} \in H$. Then $\sim$ is an equivalence relation. Moreover, we write the congruence class $[a] = Ha$.

For $a, b \in G$ define $a \sim b$ if $a^{-1}b \in H$. Then $\sim$ is an equivalence relation.

Proof: Reflexive ($a \sim a$): $a^{-1}a \in H$ since $e \in H$.

Symmetric ($a \sim b \rightsquigarrow b \sim a$): $b^{-1}a = (a^{-1}b)^{-1} \in H$ since $a^{-1}b \in H$.

Transitive ($a \sim b$ & $b \sim c \rightsquigarrow a \sim c$): $a^{-1}c = (a^{-1}b)(b^{-1}c) \in H$ [Why?] $\square$

As a consequence, we write the congruence class $[a] = aH$ in this case.

TFAE: 1) $bH = aH$; 2) $bH \subseteq aH$; 3) $b \in aH$; 4) $a^{-1}b \in H$.

Proof: 1) $\Rightarrow$ 2) ✓ 2) $\Rightarrow$ 3) $b = be$ ✓ 3) $\Rightarrow$ 4) $b = ah \rightsquigarrow a^{-1}b = h \in H$

4) $\Rightarrow$ 1) Write $a^{-1}b = h \in H$, then $b = ah$ and $a = bh^{-1}$. $bH \subseteq aH$ ✓ $aH \subseteq bH$ ✓ $\square$

$\rightsquigarrow$ Define $a \sim b$ if $aH = bH$. Then $\sim$ is an equivalence relation on G.

Similarly, **TFAE:** 1) $Hb = Ha$; 2) $Hb \subseteq Ha$; 3) $b \in Ha$; 4) $ba^{-1} \in H$.

Cosets

Let H be a subgroup of the group G, and let $a \in G$.

The **left coset** of H in G determined by a is $aH = \{x \mid x = ah,\ h \in H\}$.

The **right coset** of H in G determined by a is $Ha = \{x \mid x = ha,\ h \in H\}$.

The number of left cosets of H in G is called the index of H in G, and is denoted by $[G : H]$. This index also equals the number of right cosets since

There is a one-to-one correspondence between left cosets and right cosets.

Proof: Let $\mathcal{R} = \{Ha\}, \mathcal{L} = \{aH\}$. Define $\phi : \mathcal{R} \to \mathcal{L}$ by $\phi(Ha) = a^{-1}H$.

well-defined: If $Ha = Hb$, then $ba^{-1} \in H \rightsquigarrow ab^{-1} \in H \rightsquigarrow a^{-1}H = b^{-1}H$

one-to-one: $\phi(Ha) = \phi(Hb) \rightsquigarrow a^{-1}H = b^{-1}H \rightsquigarrow ba^{-1} \in H \rightsquigarrow Ha = Hb$

onto: For any $aH \in \mathcal{L}$, we have $\phi(Ha^{-1}) = (a^{-1})^{-1}H = aH$. $\square$

The left coset aH has the same number of elements as H.

Proof: Define $f : H \to aH$ by $f(h) = ah$ for all $h \in H$. $\rightsquigarrow$ f is 1-to-1 and onto. $\square$

$\rightsquigarrow$ If G is a finite group, then the index $[G : H] = |G|/|H|$.

Example: List the left cosets of a given subgroup H of a finite group.

Algorithm (also works for listing the right cosets of H):

1) If $a \in H$, then $aH = H$. So we begin by choosing any element $a \notin H$.
2) Any element in aH determines the same coset, so for the next coset we choose any element not in H or aH (if possible).
3) Continuing in this process provides a method for listing all left cosets.

Let $G = \mathbf{Z}_{11}^{\times} = \{[1], [2], [3], [4], [5], [6], [7], [8], [9], [10]\}$ & $H = \{[1], [10]\}$.

i) The first coset is H itself, i.e., $[1]H = \{[1], [10]\}$.
ii) Choosing $[2] \notin H$, we obtain $[2]H = \{[2], [9]\}$.
iii) Choosing $[3] \notin H \cup [2]H$, we obtain $[3]H = \{[3], [8]\}$.
iv) Choosing $[4] \notin H \cup [2]H \cup [3]H$, we obtain $[4]H = \{[4], [7]\}$.
v) Choosing $[5] \notin H \cup [2]H \cup [3]H \cup [4]H$, we obtain $[5]H = \{[5], [6]\}$.

Thus the left cosets of H are H, $[2]H$, $[3]H$, $[4]H$, $[5]H$, and $[G : H] = 5$.

Q: what if $N = \langle [3] \rangle = \{[1], [3], [9], [5], [4]\}$? **A:** N, $[2]N$, and $[G : N] = 2$.

Example: Non-abelian Group $G = S_3$

Let $G = S_3 = \{e, a, a^2, b, ab, a^2b\}$, where $a^3 = e, b^2 = e$, and $ba = a^2b$.

Let $H = \{e, b\}$.

The left cosets of H: $H = \{e, b\}$, $aH = \{a, ab\}$, $a^2H = \{a^2, a^2b\}$.

The right cosets of H: $H = \{e, b\}$, $Ha = \{a, a^2b\}$, $Ha^2 = \{a^2, ab\}$.

In this case, the left and right cosets are not the same.

Let $N = \{e, a, a^2\}$.

The left cosets of N: $N = \{e, a, a^2\}$, $bN = \{b, a^2b, ab\}$.

The right cosets of N: $N = \{e, a, a^2\}$, $Nb = \{b, ab, a^2b\}$.

In this case, the left and right cosets are the same.

A natural question: When are the left and right cosets of H in G the same?

Looking ahead: H is normal if and only if its left and right cosets coincide.
In particular, for abelian groups, left cosets and right cosets are the same.

Recall that a subgroup H is normal if $ghg^{-1} \in H$ for all $h \in H$ and $g \in G$.

H is normal if and only if its left and right cosets coincide

Let H be a subgroup of the group G. The following conditions are equivalent:

(1) H is a normal subgroup of G;

(2) $aH = Ha$ for all $a \in G$;

(3) for all $a, b \in G$, abH is the set theoretic product $(aH)(bH)$;

(4) for all $a, b \in G$, $ab^{-1} \in H$ if and only if $a^{-1}b \in H$.

Proof: (1) $\Rightarrow$ (2) Let $a \in G, h \in H$. Then $aha^{-1} \in H$ [Why?] $\rightsquigarrow aH \subseteq Ha$
Similarly, $a^{-1}ha = a^{-1}h(a^{-1})^{-1} \in H \rightsquigarrow Ha \subseteq aH$. Thus $aH = Ha$.

(2) $\Rightarrow$ (3) $abH \subseteq (aH)(bH)$: Let $h \in H$, $abh = (ae)(bh) \in (aH)(bH)$. ✓
$(aH)(bH) \subseteq abH$: Let $(ah_1)(bh_2) \in (aH)(bH)$, for $h_1, h_2 \in H$. Then

$$(ah_1)(bh_2) = a(h_1b)h_2 \overset{(2)}{=} a(bh_3)h_2 = ab(h_3h_2) \in abH \quad \text{for some } h_3 \in H.$$

(3) $\Rightarrow$ (1) For any $a \in G, h \in H$, to show $aha^{-1} \in H$. Take $b = a^{-1}$ in (3), then $(aH)(a^{-1}H) = aa^{-1}H = H$. Thus $aha^{-1} = (ah)(a^{-1}e) \in H$.

(2) $\Leftrightarrow$ (4) The left cosets are the equivalence classes $[a] = \{b \mid a^{-1}b \in H\}$.
The right cosets are the equivalence classes $[a] = \{b \mid ab^{-1} \in H\}$. □

Example: Normal Subgroups of $S_3 = D_3$

Let $G = S_3 = \{e, a, a^2, b, ab, a^2b\}$, where $a^3 = e, b^2 = e$, and $ba = a^2b$.

- The trivial subgroup $\{e\}$ and the improper subgroup G are normal.
- 4 proper nontrivial subgroups of S_3 (each of b, ab, a^2b has order 2):

$$H = \{e, b\}, \quad K = \{e, ab\}, \quad L = \{e, a^2b\}, \quad N = \{e, a, a^2\}.$$

$aH = \{a, ab\} \neq \{a, ba\} = Ha$ since $ba = a^2b$. $\rightsquigarrow$ H is not normal.

$aK = \{a, a^2b\} \neq \{a, aba\} = Ka$ since $aba = b$. $\rightsquigarrow$ K is not normal.

$aL = \{a, b\} \neq \{a, a^2ba\} = La$ since $a^2ba = ab$. $\rightsquigarrow$ L is not normal.

$bN = \{b, ba, ba^2\} \overset{!}{=} \{b, ab, a^2b\} = Nb$. $\rightsquigarrow\rightsquigarrow$ N is normal. [Why?]

In conclusion, N is the only proper nontrivial normal subgroup of S_3.

> Let H be a subgroup of G with $[G : H] = 2$. Then H is normal.

Proof: H has only two left cosets. These must be H and $G - H$. [Why?]
And these must also be the right cosets. [Why?] Thus H is normal. $\square$

e.g., In S_3, the subgroup $N = \{e, a, a^2\}$ has index 2, and so N is normal.

Conversely not true: Easy to find a counterexample from abelian groups.

Example: Normal Subgroups of D_4

$G = D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^{-1}b$.

Refer to the subgroup diagram of D_4 in §3.6, slide #10.

- The trivial subgroup $\{e\}$ and the improper subgroup G are normal.
- The subgroups $\{e, a^2, b, a^2b\}, \{e, a, a^2, a^3\}, \{e, a^2, ab, a^3b\}$ are normal.
- $N = \{e, a^2\}, \quad H = \{e, b\}, \quad K = \{e, a^2b\}, \quad L = \{e, ab\}, \quad M = \{e, a^3b\}$.

Among the subgroups N, H, K, L, M, only the subgroup N is normal.

None of the subgroups H, K, L, M is normal: e.g., by direct computations,

$$aH \neq Ha, \quad aK \neq Ka, \quad aL \neq La, \quad aM \neq Ma.$$

N is normal: Even better, $N = \{e, a^2\}$ commutes with every element of G.
a^2 commutes with b: $ba^2 = (ba)a = (a^{-1}b)a = a^{-1}(ba) = a^{-2}b = a^2b$.
And since a^2 commutes with powers of a, it commutes with every element.
This implies that the left and right cosets of N coincide. $\rightsquigarrow$ N is normal.

Factor Group

If N is a normal subgroup of G, then the set of left cosets of N forms a group under the coset multiplication given by $aNbN = abN$ for $a, b \in G$. This group is called the **factor group** of G determined by N. Write G/N.

Proof: well-defined: For $aN = cN$ and $bN = dN$, to show $abN = cdN$. It suffices to show $(ab)^{-1}cd \in N$. [Why?] Since $a^{-1}c \in N$ and $b^{-1}d \in N$,

$$(ab)^{-1}cd = b^{-1}(a^{-1}c)d = \underbrace{b^{-1}d}_{\in N}\ \underbrace{(d^{-1}(a^{-1}c)d)}_{\in N \text{ [Why?]}} \in N.$$

associativity: Let $a, b, c \in G$. Then $(aNbN)cN = \cdots = aN(bNcN)$.

identity: $eN = N$ is identity element. For $a \in G$, $eNaN = aN, aNeN = aN$.

inverses: The inverse of aN is $a^{-1}N$. $aNa^{-1}N = N, a^{-1}NaN = N$. $\square$

Let N be a normal subgroup of the finite group G. If $a \in G$, then the order of aN is the smallest positive integer n such that $(aN)^n = a^nN = N$. That is, the order of aN is the smallest positive integer n such that $a^n \in N$.

Example

Abelian group $(G, +)$: Any subgroup is normal & "aN" $\rightsquigarrow a + N$.

Let $G = \mathbf{Z}_{12}$, and let $N = \{[0], [3], [6], [9]\} = \langle [3] \rangle$. N is normal.

$\rightsquigarrow$ There are three elements of G/N, i.e., three left cosets of N in G:

i) The first element is $N = [0] + N = \{[0], [3], [6], [9]\}$;

ii) Choose $[1] \notin N$, we obtain $[1] + N = \{[1], [4], [7], [10]\}$;

iii) Choose $[2] \notin N \cup\ [1] + N$, we obtain $[2] + N = \{[2], [5], [8], [11]\}$.

Since the factor group G/N has order 3, we have $G/N \cong \mathbf{Z}_3$. [Why?]

Alternatively, this can also be seen by considering the order of $[1] + N$.

$$2([1] + N) = 2[1] + N = [2] + N, \quad 3([1] + N) = [3] + N = N.$$

I.e., the order of $[1] + N$ is the smallest positive integer n s.t. $n[1] \in N$.

Thus $n = 3$ implies that $[1] + N$ has order 3. $\rightsquigarrow G/N = \langle [1] + N \rangle \cong \mathbf{Z}_3$

Example: $D_4/Z(D_4) \cong \mathbf{Z}_2 \times \mathbf{Z}_2$

$G = D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^{-1}b$.

Let $N = \{e, a^2\}$ be the center $Z(D_4)$ of D_4. (See slide #9)

The factor group G/N consists of the four cosets. More precisely,

$$N = \{e, a^2\}, \quad aN = \{a, a^3\}, \quad bN = \{b, a^2b\}, \quad abN = \{ab, a^3b\}.$$

Recall that the group of order 4 is isomorphic to either $\mathbf{Z}_4$ or $\mathbf{Z}_2 \times \mathbf{Z}_2$.

Since we have

- $(aN)^2 = a^2N = N$
- $(bN)^2 = b^2N = N$
- $(abN)^2 = (ab)^2N = ababN = a(ba)bN = aa^{-1}bbN = N$

This shows that every non-identity element of G/N has order 2. That is,

$$D_4/Z(D_4) \cong \mathbf{Z}_2 \times \mathbf{Z}_2.$$

Another way to show that each of $\{aN, bN, abN\}$ has order 2 in G/N.

$$o(xN) = \min\{n > 0 \mid x^n \in N\} \text{ for any } xN \in G/N.$$

Three Examples from $G = \mathbf{Z}_4 \times \mathbf{Z}_4$

$H = \{([0],[0]),([2],[0]),([0],[2]),([2],[2])\}$: There are four cosets of H

$$H, \quad ([1],[0]) + H, \quad ([0],[1]) + H, \quad ([1],[1]) + H.$$

$$G/H \cong \mathbf{Z}_2 \times \mathbf{Z}_2$$

Proof: Each nontrivial element of the factor group has order 2. □

$K = \{([0],[0]),([1],[0]),([2],[0]),([3],[0])\}$: There are four cosets of K

$$K, \quad ([0],[1]) + K, \quad ([0],[2]) + K, \quad ([0],[3]) + K.$$

$$G/K \cong \mathbf{Z}_4$$

Proof: $o\big(([0],[1]) + K\big) = 4 = |G/K|$. □

$N = \{([0],[0]),([1],[1]),([2],[2]),([3],[3])\}$: There are four cosets of N

$$N, \quad ([1],[0]) + N, \quad ([2],[0]) + N, \quad ([3],[0]) + N.$$

$$G/N \cong \mathbf{Z}_4$$

Proof: $o\big(([1],[0]) + N\big) = 4 = |G/N|$. □

Natural Projection

Let N be a normal subgroup of G. The mapping $\pi : G \to G/N$ defined by

$$\pi(a) = aN, \quad \text{for all } a \in G, \qquad (\star)$$

is called the **natural projection** of G onto G/N.

Recall that the kernel of any group homomorphism is a normal subgroup.

The converse is true: Any normal subgroup is the kernel of some homomorphism.

Let N be a normal subgroup of G. Let $\pi \colon G \to G/N$ be defined as in $(\star)$.

i) Then π is a group homomorphism with $\ker(\pi) = N$. Direct check ✓

ii) There is a one-to-one correspondence between

$$\begin{array}{rcl} \{\text{subgroups } H \text{ of } G \text{ with } H \supseteq N\} & \longleftrightarrow & \{\text{subgroups } K \text{ of } G/N\} \\ H & \longmapsto & \pi(H) \\ \pi^{-1}(K) & \longleftarrow & K \end{array}$$

Under this correspondence, normal subgroups $\leftrightsquigarrow$ normal subgroups.

"$\leftrightsquigarrow$" follows from the fact that π is onto & Slide #12 in § 3.7 ✓.

Proof: $\{\text{subgroups } H \text{ of } G \text{ with } H \supseteq N\} \longleftrightarrow \{\text{subgroups } K \text{ of } G/N\}$

$$\begin{aligned} H &\longmapsto \pi(H) \\ \pi^{-1}(K) &\longleftarrow K \end{aligned}$$

Let N be a normal subgroup of G. The **natural projection** $\pi : G \to G/N$ defined by $\pi(a) = aN$ is an onto group homomorphism with $\ker(\pi) = N$.

Assigning to each subgroup K of G/N its inverse image $\pi^{-1}(K)$ in G is a one-to-one mapping since π is onto. To show that this mapping is onto.

Let H be a subgroup of G with $H \supseteq N$. To show $H = \pi^{-1}(\pi(H))$.

$$\pi^{-1}(\pi(H)) = \{x \in G \mid \pi(x) \in \pi(H)\} \quad \rightsquigarrow H \subseteq \pi^{-1}(\pi(H))$$

To show $\pi^{-1}(\pi(H)) \subseteq H$: Let $a \in \pi^{-1}(\pi(H))$. Then $\pi(a) \in \pi(H)$, and so

$$aN = hN \text{ for some } h \in H. \quad \rightsquigarrow h^{-1}a \in N \subseteq H.$$

Thus $a = h(h^{-1}a) \in H$. $\square$

Fundamental Homomorphism Theorem

If $\phi : G_1 \to G_2$ is a homomorphism with $K = \ker(\phi)$, then $G_1/K \cong \phi(G_1)$.

Proof: Recall that the kernel $K = \ker(\phi)$ is a normal subgroup of G_1.
Define $\overline{\phi} : G_1/K \to \phi(G_1)$ by $\overline{\phi}(aK) = \phi(a)$ for all $aK \in G_1/K$. To show

$\overline{\phi}$ is a group isomorphism.

well-defined: If $aK = bK$, then $a = bk$ for some $k \in \ker(\phi)$. Therefore,

$$\overline{\phi}(aK) = \phi(a) = \phi(bk) = \phi(b)\phi(k) = \phi(b) = \overline{\phi}(bK).$$

$\overline{\phi}$ is a homomorphism: For all $a, b \in G_1$, we have

$$\overline{\phi}(aKbK) = \overline{\phi}(abK) = \phi(ab) = \phi(a)\phi(b) = \overline{\phi}(aK)\overline{\phi}(bK).$$

one-to-one: If $\overline{\phi}(aK) = \overline{\phi}(bK)$, i.e., $\phi(a) = \phi(b)$, then $\phi(b^{-1}a) = \cdots = e_2$
This implies that $b^{-1}a \in K$, and so $aK = bK$.

onto: It is clear by definition of $\overline{\phi}$. $\square$

Examples

Cayley's theorem: Every group G is isomorphic to a permutation group.

Proof: Define $\phi : G \to \mathrm{Sym}(G)$ by $\phi(a) = \lambda_a$, for any $a \in G$, where λ_a is the function defined by $\lambda_a(x) = ax$ for all $x \in G$. ϕ is a homomorphism:

$$\text{For all } a, b \in G,\ \phi(ab) = \lambda_{ab} \overset{!}{=} \lambda_a \lambda_b = \phi(a)\phi(b).$$

$$\text{For all } x \in G,\ \lambda_{ab}(x) = abx = \lambda_a(bx) = \lambda_a\lambda_b(x).$$

one-to-one: λ_a is the identity permutation only if $a = e$. So $\ker(\phi) = \{e\}$.

It follows **Fundamental Homomorphism Theorem** that

$$G/\ker(\phi) = G \cong \phi(G),$$

where $\phi(G)$ is a permutation group since it is a subgroup of $\mathrm{Sym}(G)$. □

$$\mathrm{GL}_n(\mathbf{R})/\mathrm{SL}_n(\mathbf{R}) \cong \mathbf{R}^\times$$

Proof: Define $\phi : \mathrm{GL}_n(\mathbf{R}) \to \mathbf{R}^\times$ by $\phi(A) = \det(A)$ for any $A \in \mathrm{GL}_n(\mathbf{R})$.

ϕ is well-defined. ✓ ϕ is a homomorphism. ✓ ϕ is onto: ✓ [Why?]

$\ker(\phi) = \{A \mid \phi(A) = \det(A) = 1\} = \mathrm{SL}_n(\mathbf{R})$. □

Simple Group

Let $\phi : G_1 \to G_2$ be a group homomorphism. Two special cases:

- ϕ is one-to-one $\Leftrightarrow \ker(\phi) = \{e_1\}$. Thus $G_1 \cong \phi(G_1)$ in this case.
- If $\ker(\phi) = G_1$, then ϕ is the trivial mapping, i.e., $\phi(G_1) = \{e_2\}$.

If G_1 has no proper nontrivial normal subgroups, then ϕ is either 1-to-1 or trivial.

A nontrivial group G is called **simple** if it has no proper nontrivial normal subgps.

e.g., For any prime p, the cyclic group $\mathbf{Z}_p$ is simple, since it has no proper nontrivial subgroups of any kind (every nonzero element is a generator).

An Useful Example: $\mathbf{Z}_n/m\mathbf{Z}_n \cong \mathbf{Z}_m$ if $m|n$

The subgroups of $\mathbf{Z}_n$ correspond to divisors of n, and so to describe all factor groups of $\mathbf{Z}_n$ we only need to describe $\mathbf{Z}_n/m\mathbf{Z}_n$ for all $m|n, m > 0$.

Proof: Since any homomorphic image of a cyclic group is again cyclic, we can define $\phi : \mathbf{Z}_n \to \mathbf{Z}_m$ by $\phi([x]_n) = [x]_m$ for some $m|n$.

well-defined: If $[x]_n = [y]_n$, then $[x]_m = [y]_m$. [Why?]

ϕ is a homomorphism: For any $[x]_n, [y]_n \in \mathbf{Z}_n$, we have

$$\phi([x]_n + [y]_n) = \phi([x+y]_n) = [x+y]_m = [x]_m + [y]_m = \phi([x]_n) + \phi([y_n]).$$

onto: It is clear by definition of ϕ.

$\ker(\phi) = \{[x]_n \mid [x]_m = [0]_m\} = \{[x]_n \mid x \text{ is a multiple of } m\} = m\mathbf{Z}_n$.

It follows from the fundamental homomorphism theorem that

$$\mathbf{Z}_n/m\mathbf{Z}_n \cong \mathbf{Z}_m. \qquad \square$$

Factor Groups of Direct Products

Let $N_1 \subseteq G_1$ and $N_2 \subseteq G_2$ be normal subgroups.

$$N_1 \times N_2 = \{(x_1, x_2) \mid x_1 \in N_1, x_2 \in N_2\} \subseteq G_1 \times G_2.$$

Then $N_1 \times N_2$ is a normal subgroup of the direct product $G_1 \times G_2$. [Why?]

$$(G_1 \times G_2)/(N_1 \times N_2) \cong (G_1/N_1) \times (G_2/N_2). \qquad (\star)$$

Proof: Define $\phi : G_1 \times G_2 \to (G_1/N_1) \times (G_2/N_2)$ by $\phi\big((x_1, x_2)\big) = (x_1 N_1, x_2 N_2)$.

ϕ is well-defined. ✓ ϕ is a homomorphism: For $(x_1, x_2), (y_1, y_2) \in G_1 \times G_2$,

$$\phi\big((x_1, x_2)(y_1, y_2)\big) = \cdots = \phi\big((x_1, x_2)\big)\phi\big((y_1, y_2)\big)$$

ϕ is onto. ✓ $\ker(\phi) = \{(x_1, x_2) \mid \phi\big((x_1, x_2)\big) = (N_1, N_2)\} = N_1 \times N_2$.

The desired $(\star)$ follow from the fundamental homomorphism theorem. □

e.g., the subgroups $H = 2\mathbf{Z}_4 \times 2\mathbf{Z}_4$ and $K = \mathbf{Z}_4 \times \{[0]\}$ in $G = \mathbf{Z}_4 \times \mathbf{Z}_4$.

- $G/H = (\mathbf{Z}_4 \times \mathbf{Z}_4)/(2\mathbf{Z}_4 \times 2\mathbf{Z}_4) \cong (\mathbf{Z}_4/2\mathbf{Z}_4) \times (\mathbf{Z}_4/2\mathbf{Z}_4) \cong \mathbf{Z}_2 \times \mathbf{Z}_2$
- $G/K = (\mathbf{Z}_4 \times \mathbf{Z}_4)/(\mathbf{Z}_4 \times 4\mathbf{Z}_4) \cong (\mathbf{Z}_4/\mathbf{Z}_4) \times (\mathbf{Z}_4/4\mathbf{Z}_4) \cong \mathbf{Z}_1 \times \mathbf{Z}_4 \cong \mathbf{Z}_4$

Internal Direct Product

A group G with subgroups H and K is called the **internal direct product of H and K** if (i) H, K are normal in G (ii) $H \cap K = \{e\}$ (iii) $HK = G$.
Prove that in this case $G \cong H \times K$.

Proof: Define $\phi : H \times K \to G$ by $\phi\big((h,k)\big) = hk$ for all $(h,k) \in H \times K$.

ϕ well-defined. ✓ ϕ is a homomorphism: For all $(h_1,k_1),(h_2,k_2) \in H \times K$,

$$\phi\big((h_1,k_1)(h_2,k_2)\big) = \phi\big((h_1h_2, k_1k_2)\big) = h_1h_2k_1k_2 \overset{!}{=} h_1k_1h_2k_2 = \phi\big((h_1,k_1)\big)\phi\big((h_2,k_2)\big).$$

$\overset{!}{=}$ holds $\Leftrightarrow h_2k_1 = k_1h_2 \Leftrightarrow k_1^{-1}h_2k_1h_2^{-1} = e$. To show $k_1^{-1}h_2k_1h_2^{-1} = e$.

Proof: $k_1^{-1}h_2k_1h_2^{-1} \in H$ since $k_1^{-1}h_2k_1 \in H$ [Why?] and $h_2^{-1} \in H$.

$k_1^{-1}h_2k_1h_2^{-1} \in K$ since $h_2k_1h_2^{-1} \in K, k_1^{-1} \in K$. $\rightsquigarrow k_1^{-1}h_2k_1h_2^{-1} \in H \cap K = \{e\}$ $\square$

ϕ is onto: For any $g \in G$, we have $g \overset{\text{(iii)}}{=} hk$ with $h \in H, k \in K$. ✓

$\ker(\phi) = \{(h,k) \mid \phi((h,k)) = e\} \overset{!}{=} \{(h,k) \mid h,k \in H \cap K\} = \{(e,e)\}$

$\overset{!}{=}$ holds since $hk = e \rightsquigarrow h = k^{-1} \in K \cap H$ & $k = h^{-1} \in H \cap K$ $\square$