Finitely Generated Abelian Groups

23/9/2024

- The **Cartesian product of sets** $S_1, S_2, \cdots, S_n$ is the set of all ordered n-tuples $(a_1, a_2, \cdots, a_n)$, where $a_i \in S_i$ for $i = 1, 2, \cdots, n$. The Cartesian product is denoted by either

$$S_1 \times S_2 \times \cdots \times S_n$$

or by

$$\prod_{i=1}^{n} S_i. \qquad \blacksquare$$

- Let $G_1, G_2, \cdots, G_n$ be groups. For $(a_1, a_2, \cdots, a_n)$ and $(b_1, b_2, \cdots, b_n)$ in $\prod_{i=1}^{n} G_i$, define $(a_1, a_2, \cdots, a_n)(b_1, b_2, \cdots, b_n)$ to be the element $(a_1b_1, a_2b_2, \cdots, a_nb_n)$. Then $\prod_{i=1}^{n} G_i$ is a group, the **direct product of the groups** G_i, under this binary operation.

ie., If $G_1, G_2, \cdots, G_n$ are groups then $\prod_{i=1}^{n} G_i$ is a group with binary operation consisting of componentwise multiplication

$$(a_1, a_2 \cdots, a_n)(b_1, b_2, \cdots, b_n) = (a_1b_1, a_2b_2, \cdots, a_nb_n)$$

Proof : $a_i \in G_i$, $b_i \in G_i$ and G_i is a group $\Rightarrow a_i b_i \in G_i$

$\therefore \prod_{i=1}^{n} G_i$ is closed under componentwise multiplication (binary operation)

$$(a_1, a_2, \cdots, a_n)\left[(b_1, b_2 \cdots, b_n)(c_1, c_2, \cdots, c_n)\right] = (a_1, a_2, \cdots, a_n)\left[(b_1c_1, b_2c_2, \cdots, b_nc_n)\right]$$

$$= (a_1, a_2, \cdots, a_n)(b_1c_1, b_2c_2, \cdots, b_nc_n)$$

$$= (a_1(b_1c_1), a_2(b_2c_2), \cdots, a_n(b_nc_n))$$

$$= ((a_1b_1)c_1, (a_2b_2)c_2, \cdots, (a_nb_n)c_n)$$

$$= (a_1b_1, a_2b_2, \cdots, a_nb_n)(c_1, c_2, \cdots, c_n)$$

$$= \left[(a_1, a_2, \cdots, a_n)(b_1, b_2, \cdots, b_n)\right](c_1, c_2, \cdots, c_n)$$

$\Rightarrow$ associative

identity : $(e_1, e_2, \ldots, e_n)$

Inverse : $(a_1, a_2, \ldots, a_n)^{-1} = (a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1})$

11.5 Theorem The group $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic and is isomorphic to $\mathbb{Z}_{mn}$ if and only if m and n are relatively prime, that is, the gcd of m and n is 1.

Proof. $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$

Consider $(1,1) \in \mathbb{Z}_m \times \mathbb{Z}_n$

The 1st component cycles back to the identity after m operations, and the 2nd after n operations.

∴ To yield $(0,0)$, the # of summands must be a multiple of m and n.

$|(1,1)| = \text{lcm}(m,n)$ and $\gcd(m,n)\,\text{lcm}(m,n) = mn$

– If $d = \gcd(m,n) = 1$ then $mn = \text{lcm}(m,n)$

$|(1,1)| = mn$ } $(1,1)$ generates a cyclic subgroup $\mathbb{Z}_m \times \mathbb{Z}_n$ of order mn, which is the order of the whole group.

6.10 Theorem Let G be a cyclic group with generator a. If the order of G is infinite, then G is isomorphic to $\langle \mathbb{Z}, + \rangle$. If G has finite order n, then G is isomorphic to $\langle \mathbb{Z}_n, +_n \rangle$.

$\Rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_{mn}$ if $\gcd(m,n) = 1$

– If $d = \gcd(m,n) > 1$ then $\text{lcm}(m,n) = \frac{mn}{d}$

$\Rightarrow m \mid \frac{mn}{d}$ and $n \mid \frac{mn}{d}$

For any $(r,s) \in \mathbb{Z}_m \times \mathbb{Z}_n$,

$$\underbrace{(r,s)+(r,s)+\cdots+(r,s)}_{k} = k(r,s) = (kr \bmod m,\ ks \bmod n)$$

$$\underbrace{(r,s)+(r,s)+\cdots+(r,s)}_{\frac{mn}{d}} = \frac{mn}{d}(r,s) = (0,0)$$

$\frac{mn}{d}$ is divisible by both m & n

$$|(r,s)| = \frac{mn}{d} < mn \implies$$ no element (r,s) in $\mathbb{Z}_m \times \mathbb{Z}_n$ can generate the entire group

$\therefore$ $\mathbb{Z}_m \times \mathbb{Z}_n$ is not cyclic, and therefore not isomorphic to $\mathbb{Z}_{mn}$

$\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$

The group $\prod_{i=1}^{n} \mathbb{Z}_{m_i}$ is cyclic and isomorphic to $\mathbb{Z}_{m_1 m_2 \cdots m_n}$ if and only if the numbers m_i for $i = 1, \cdots, n$ are such that the gcd of any two of them is 1.

* If $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ where p_i is prime for $i = 1, 2, \cdots, k$, then

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \mathbb{Z}/p_2^{\alpha_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}$$

11.12 Theorem **(Fundamental Theorem of Finitely Generated Abelian Groups)** Every finitely generated abelian group G is isomorphic to a direct product of cyclic groups in the form

$$\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \cdots \times \mathbb{Z}_{(p_n)^{r_n}} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z},$$

where the p_i are primes, not necessarily distinct, and the r_i are positive integers. The direct product is unique except for possible rearrangement of the factors; that is, the number (**Betti number** of G) of factors $\mathbb{Z}$ is unique and the prime powers $(p_i)^{r_i}$ are unique.

30/9/2024

13 Homomorphisms

13.1 Definition A map ϕ of a group G into a group G' is a **homomorphism** if the homomorphism property

$$\phi(ab) = \phi(a)\phi(b) \tag{1}$$

holds for all $a, b \in G$. ■

Examples.

(1) Evaluation Homomorphism:

$\mathcal{F}$ – additive group of all functions mapping from $\mathbb{R}$ to $\mathbb{R}$

$\mathbb{R}$ – additive group of real # & c is any real #

$\phi_c : \mathcal{F} \to \mathbb{R}$ such that $\phi_c(f) = f(c)$ for $f \in \mathcal{F}$ is the evaluation homomorphism.

$$\phi_c(f+g) = (f+g)(c) = f(c) + g(c) = \phi_c(f) + \phi_c(g)$$

(2) Linear Transformation:

$\mathbb{R}^n$: additive group of column vectors with n real # components

A: an $m \times n$ matrix of real numbers

$T : \mathbb{R}^n \to \mathbb{R}^m$ such that $T(v) = Av$ for each $v \in \mathbb{R}^n$ is a homomorphism.

$$T(v+w) = A(v+w) = Av + Aw = T(v) + T(w)$$

(3) Determinant:

$GL(n,\mathbb{R})$ – multiplicative group of all invertible $n \times n$ matrices

$A \in GL(n,\mathbb{R})$ iff $\det(A) \neq 0$

$\mathbb{R}^*$ – multiplicative group of non-zero real numbers

For $A, B \in GL(n,\mathbb{R})$,

$$\det(AB) = \det(A)\det(B)$$

$\therefore$ $\det : GL(n,\mathbb{R}) \to \mathbb{R}^*$ is a homomorphism

(4) Projection mappings:

$G = G_1 \times G_2 \times \cdots \times G_i \times \cdots \times G_n$ – direct product of groups

The projection map $\pi_i : G \to G_i$ where $\pi_i(g_1, g_2, \cdots, g_i, \cdots, g_n) = g_i$ is a homomorphism for each $i = 1, 2, \ldots, n$

the binary operation of G coincides in the ith component with the binary operation in G_i.

$$\begin{aligned}\pi_i(a_1 + a_2) &= \pi_i\big((g_1, g_2, \cdots, g_n) + (h_1, h_2, \cdots, h_n)\big) \\ &= \pi_i(g_1 + h_1, g_2 + h_2, \cdots, g_n + h_n) \\ &= g_i + h_i = \pi_i(a_1) + \pi_i(b_1)\end{aligned}$$

13.11 Definition Let ϕ be a mapping of a set X into a set Y, and let $A \subseteq X$ and $B \subseteq Y$. The **image** $\phi[A]$ **of** A **in** Y **under** ϕ is $\{\phi(a) \mid a \in A\}$. The set $\phi[X]$ is the **range of** ϕ. The **inverse image** $\phi^{-1}[B]$ **of** B **in** X is $\{x \in X \mid \phi(x) \in B\}$. ■

13.12 Theorem Let ϕ be a homomorphism of a group G into a group G'.

1. If e is the identity element in G, then $\phi(e)$ is the identity element e' in G'.
2. If $a \in G$, then $\phi(a^{-1}) = \phi(a)^{-1}$.
3. If H is a subgroup of G, then $\phi[H]$ is a subgroup of G'.
4. If K' is a subgroup of $G' \cap \phi[G]$, then $\phi^{-1}[K']$ is a subgroup of G.

If $H' \leq G'$, then $\phi^{-1}(H') \leq G$

$\Rightarrow \phi$ preserves the identity element, inverses, and subgroups.

Proof

(1) For $a \in G$, $\phi(a) = \phi(ae) = \phi(a)\,\phi(e)$

$\phi(a) \in G' \Rightarrow \phi(a)^{-1} \in G'$

$\therefore e' = \phi(e)$

(2) $e' = \phi(e) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1}) \Rightarrow \phi(a^{-1}) = \phi(a)^{-1}$

A subset H of a group G is a subgroup of G if and only if

1. H is closed under the binary operation of G,
2. the identity element e of G is in H,
3. for all $a \in H$ it is true that $a^{-1} \in H$ also.

(3) Let $H \leq G$ then,

- $e \in H \Rightarrow \phi(e) = e' \in \phi(H)$ $\therefore$ identity
- $a \in H \Rightarrow a^{-1} \in H \Rightarrow \phi(a^{-1}) = \phi(a)^{-1} \in H$
- Let $\phi(a), \phi(b) \in \phi(H)$ then $\phi(a)\phi(b) = \phi(ab) \in \phi(H) \Rightarrow \phi(H)$ is closed under the binary operation of G'.

$\therefore \phi(H) \leq G'$

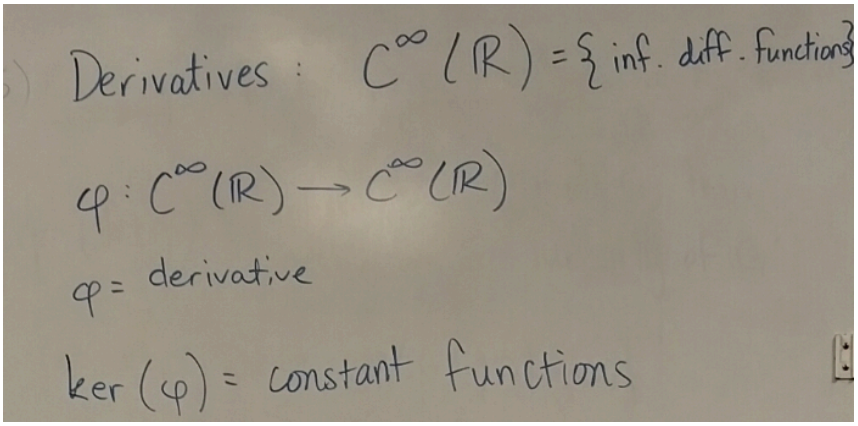
(4) $H' \leq G'$ then

- $e' = \phi(e) \in H' \Rightarrow \phi^{-1}(e') = \phi^{-1}(\phi(e)) = e \in \phi^{-1}(H')$
- If $a \in \phi^{-1}(H')$ then $\phi(a) \in H' \Rightarrow \phi(a)^{-1} \in H'$

  $\phi(a^{-1}) = \phi(a)^{-1} \Rightarrow \phi(a^{-1}) \in H' \Rightarrow a^{-1} \in \phi^{-1}(H')$
- Let $a', b' \in \phi^{-1}(H')$ then $\phi(a'), \phi(b') \in H' \Rightarrow \phi(a')\,\phi(b') \in H'$

  $\phi(a'b') \in H' \Rightarrow a'b' \in \phi^{-1}(H')$

13.13 Definition Let $\phi : G \to G'$ be a homomorphism of groups. The subgroup $\phi^{-1}[\{e'\}] = \{x \in G \mid \phi(x) = e'\}$ is the **kernel of** ϕ, denoted by $\mathrm{Ker}(\phi)$. ■



13.15 Theorem Let $\phi : G \to G'$ be a group homomorphism, and let $H = \mathrm{Ker}(\phi)$. Let $a \in G$. Then the set

$$\phi^{-1}[\{\phi(a)\}] = \{x \in G \mid \phi(x) = \phi(a)\} = aH$$

is the left coset aH of H, and is also the right coset Ha of H. Consequently, the two partitions of G into left cosets and into right cosets of H are the same.

- If $\phi : G \to G'$ be a group homomorphism with $H = \ker(\phi)$, then $H \trianglelefteq G$
  - ⇒ The kernel of a group homomorphism is always a normal subgroup of the domain.

Proof

($\Rightarrow$) Let $y \in \{x \in G \mid \phi(x) = \phi(a)\}$ then,

$$\phi(y) = \phi(a)$$

$$H = \ker(\phi) = \{x \in G \mid \phi(x) = e'\}$$

$$[\phi(y)]^{-1}\phi(y) = e'$$

$$[\phi(a)]^{-1}\phi(y) = \phi(a^{-1})\,\phi(y) = \phi(a^{-1}y) = e'$$

$$\Rightarrow a^{-1}y \in H = \ker(\phi)$$

$$\Rightarrow y = ah \text{ for some } h \in H$$

$$\Rightarrow y = ah \in aH$$

$$\therefore \{x \in G \mid \phi(x) = \phi(a)\} \subseteq aH$$

($\Leftarrow$) Let $y \in aH$ then,

$y = ah$ for some $h \in H = \ker(\phi)$

$\phi(y) = \phi(ah) = \phi(a)\phi(h)$

$\lceil \phi(h) = e' \rceil$

$\therefore\ y \in \{x \in G \mid \phi(x) = \phi(a)\}$.

Q.E.D

13.18 Corollary A group homomorphism $\phi : G \to G'$ is a one-to-one map if and only if $\mathrm{Ker}(\phi) = \{e\}$.

Proof.

($\Rightarrow$) If $\phi : G \to G'$ is one-to-one, then

$\phi(x) = \phi(e) \Rightarrow x = e$ for any $x \in G$

$\Rightarrow$ e is the only element in G satisfying $\phi(x) = e'$

$\therefore \ker(\phi) = \{e\}$

($\Leftarrow$) Let $\ker(\phi) = \{e\}$,

Assume $\phi(x) = \phi(y)$ for some $x, y \in G$ then

$\phi(y)^{-1}\phi(x) = \phi(y)^{-1}\phi(y) = e'$

$\phi(y^{-1})\phi(x) = e'$

$\phi(y^{-1}x) = e'$

$y^{-1}x = e$ $\quad [\ker(\phi) = \{e\}]$

To Show $\phi : G \to G'$ Is an Isomorphism

Step 1 Show ϕ is a homomorphism.

Step 2 Show $\text{Ker}(\phi) = \{e\}$.

Step 3 Show ϕ maps G onto G'.

13.19 Definition A subgroup H of a group G is **normal** if its left and right cosets coincide, that is, if $gH = Hg$ for all $g \in G$. ■

Note that all subgroups of abelian groups are normal.

14 Factor Groups

14.1 Theorem Let $\phi : G \to G'$ be a group homomorphism with kernel H. Then the cosets of H form a **factor group**, G/H, where $(aH)(bH) = (ab)H$. Also, the map $\mu : G/H \to \phi[G]$ defined by $\mu(aH) = \phi(a)$ is an isomorphism. Both coset multiplication and μ are well defined, independent of the choices a and b from the cosets.

$\phi : G \to G'$ is a group homomorphism with $H = \ker(\phi)$

Factor group, G/H = Set of cosets of H

= "G mod H"

= $\{aH \mid a \in G\}$ where

(or) Quotient group

$(aH)(bH) = (ab)H$: coset multiplication

$\mu : G/H \to \phi[G]$ defined by $\mu(aH) = \phi(a)$ is an isomorphism

$$|G/H| = (G:H) = \frac{|G|}{|H|}$$

- Let G be a finite group & S a set with the same cardinality as G, ie., $|S| = |G|$

$\Rightarrow$ one-to-one correspondence b/w S and G

We can define a binary operation on S, making S into a group isomorphic to G.

if $x \leftrightarrow g_1$ & $y \leftrightarrow g_2$ and $z \leftrightarrow g_1 g_2$ then $xy = z$ where $x, y \in S$

This gives us a one-to-one function μ mapping S onto G_1.

if $\mu(x)=g_1$ & $\mu(y)=g_2$ and $\mu(z)=g_1g_2$, then $xy=z$

$\Rightarrow \mu: S \to G_1$ is an isomorphism, mapping the group S onto the group G_1.

- Let G_1 and G_1' be groups, and let $\phi: G_1 \to G_1'$ be a homomorphism and let $H = \ker(\phi)$.

13.15 Theorem Let $\phi : G \to G'$ be a group homomorphism, and let $H = \text{Ker}(\phi)$. Let $a \in G$. Then the set

$$\phi^{-1}[\{\phi(a)\}] = \{x \in G \mid \phi(x) = \phi(a)\} = aH = Ha$$

is the left coset aH of H, and is also the right coset Ha of H. Consequently, the two partitions of G into left cosets and into right cosets of H are the same.

$\Longrightarrow$ one-to-one correspondence $aH \longleftrightarrow \phi(a)$ b/w cosets of H in G_1 and elements of the subgroup $\phi(G_1)$ of G_1'.

Theorem 13.12: $H \leq G_1 \Rightarrow \phi(H) \leq G_1'$

The set of all cosets of H : G_1/H

"G_1 over H" (or)
"G_1 modulo H" (or)
"G_1 mod H"

- Replacing S by G_1/H & G_1 by $\phi[G_1]$

$\Longrightarrow G_1/H$ is a group isomorphic to $\phi(G_1)$ with isomorphism μ

For $xH, yH \in G_1/H$,

if $\mu(xH) = \phi(x)$ & $\mu(yH) = \phi(y)$ and $\mu(zH) = \phi(x)\phi(y)$

then $(xH)(yH) = zH$

What is $z \in G$ such that $\mu(zH) = \phi(x)\phi(y)$?

ϕ is a homomorphism $\Rightarrow$ $\phi(xy) = \phi(x)\phi(y)$

Take $z = xy \in G$,

$$\mu(zH) = \mu(xyH) = \phi(xy) = \phi(x)\phi(y) = \mu(xH)\mu(yH)$$

$$\Rightarrow \mu(xH)\mu(yH) = \mu(xyH)$$

$\mu : G/H \to \phi(G)$ is an isomorphism

$$\Rightarrow (xH)(yH) = xyH$$

- If $h_1, h_2 \in H$ so that $xh_1 \in xH$ & $yh_2 \in yH$

13.15 Theorem Let $\phi : G \to G'$ be a group homomorphism, and let $H = \text{Ker}(\phi)$. Let $a \in G$. Then the set

$$\phi^{-1}[\{\phi(a)\}] = \{x \in G \mid \phi(x) = \phi(a)\} = aH = Ha$$

is the left coset aH of H, and is also the right coset Ha of H. Consequently, the two partitions of G into left cosets and into right cosets of H are the same.

$\Rightarrow$ there exists $h_3 \in H$ such that $h_1 y = y h_3$

$$(xh_1)(yh_2) = x(h_1 y)h_2 = x(yh_3)h_2 = (xy)h_3 h_2 \in (xy)H$$

4/10/2024

14.4 Theorem Let H be a subgroup of a group G. Then left coset multiplication is well defined by the equation

$$(aH)(bH) = (ab)H$$

if and only if H is a normal subgroup of G.

13.19 Definition A subgroup H of a group G is **normal** if its left and right cosets coincide, that is, if $gH = Hg$ for all $g \in G$. ■

Note that all subgroups of abelian groups are normal.

Proof

($\Rightarrow$) Suppose that $(aH)(bH)=(abH)$ give a well defined binary operation on left cosets.

Let $x \in aH$ and $a^{-1} \in a^{-1}H$ since $e \in H$ & $a^{-1} = a^{-1}e \in a^{-1}H$

$(xH)(a^{-1}H) = (xa^{-1})H$

and $a \in aH$ and $a^{-1} \in a^{-1}H$

$(aH)(a^{-1}H) = (aa^{-1})H = eH = H$

left coset multiplication is well defined $\Rightarrow$ the result of multiplying a cosets should be a specific coset, independent of the representatives we pick from each coset.

$x \in aH$ & $y \in bH$ $\Rightarrow xy \in abH$ $\Leftarrow$

$\therefore$ $xa^{-1}H = (aH)(a^{-1}H) = H \Rightarrow xa^{-1}h_1 = h_2 \Rightarrow xa^{-1} = h_2h_1^{-1} = h$ (say)

$\therefore$ $xa^{-1} = h \in H$

$x = ha \in Ha$

$\Rightarrow aH \subseteq Ha$

Similarly, $Ha \subseteq aH$

$\therefore$ $Ha = aH$ $\Rightarrow$ H is a normal subgroup

$(H \trianglelefteq G)$

($\Leftarrow$) Assume $aH = Ha \ \forall\, a \in G$

$H \trianglelefteq G$

Let $x \in aH$ and $y \in bH$ then

$x = ah_1$ and $y = bh_2$ for some $h_1, h_2 \in H$

$$(ah_1)(bh_2) = a(h_1 b)h_2$$
$$= a(bh_3)h_2$$
$$= (ab)(h_3 h_2) \in (ab)H$$

$h_1 b \in Hb = bH$

$\Rightarrow h_1 b = bh_2$ for some $h_3 \in H$

Q.E.D

14.5 Corollary Let H be a normal subgroup of G. Then the cosets of H form a group G/H under the binary operation $(aH)(bH) = (ab)H$. ▲

Let $H \trianglelefteq G$, then G/H is a group using left coset multiplication

Proof

$H \trianglelefteq G \Rightarrow (aH)(bH) = (ab)H$ is well defined & $aH = Ha \ \forall\, a \in G$

- $(aH)[(bH)(cH)] = (aH)[(bc)H] = [a(bc)]H$, and similarly, we have $[(aH)(bH)](cH) = [(ab)c]H$, so associativity in G/H follows from associativity in G.

Associativity in $G \Rightarrow$ Associativity in G/H

- $(aH)(eH) = (ae)H = aH = (ea)H = (eH)(aH)$

$\therefore$ $eH = H$ is the identity element in G/H

- $(a^{-1}H)(aH) = (a^{-1}a)H = eH = (aa^{-1})H = (aH)(a^{-1}H)$

$\therefore$ $(aH)^{-1} = a^{-1}H$

We have seen that every homomorphism $\phi : G \to G'$ gives rise to a natural factor group (Theorem 14.1), namely, $G/\text{Ker}(\phi)$. We now show that each factor group G/H gives rise to a natural homomorphism having H as kernel.

14.9 Theorem Let H be a normal subgroup of G. Then $\gamma : G \to G/H$ given by $\gamma(x) = xH$ is a homomorphism with kernel H.

"canonical homomorphism"

Proof.

14.4 Theorem Let H be a subgroup of a group G. Then left coset multiplication is well defined by the equation

$$(aH)(bH) = (ab)H$$

if and only if H is a normal subgroup of G.

Let $x, y \in G$ then,

$\gamma(xy) = (xy)H = (xH)(yH) = \gamma(x)\gamma(y)$

$\Rightarrow$ γ is a homomorphism

$eH = H$ is the identity element in G/H.

$x \in \ker(\gamma)$ iff $\gamma(x) = xH = H$ and

$xH = H$ if and only if $x \in H$

$\Rightarrow$ $\ker(\gamma) = H$.

Fundamental Homomorphism Theorem

14.1 Theorem Let $\phi : G \to G'$ be a group homomorphism with kernel H. Then the cosets of H form a **factor group**, G/H, where $(aH)(bH) = (ab)H$. Also, the map $\mu : G/H \to \phi[G]$ defined by $\mu(aH) = \phi(a)$ is an isomorphism. Both coset multiplication and μ are well defined, independent of the choices a and b from the cosets.

if $\phi : G \to G'$ be a group homomorphism with kernel $H \Rightarrow \mu : G/H \to \phi(G)$ where $\mu(gH) = \phi(g)$ is an isomorphism

14.9 Theorem Let H be a normal subgroup of G. Then $\gamma : G \to G/H$ given by $\gamma(x) = xH$ is a homomorphism with kernel H.

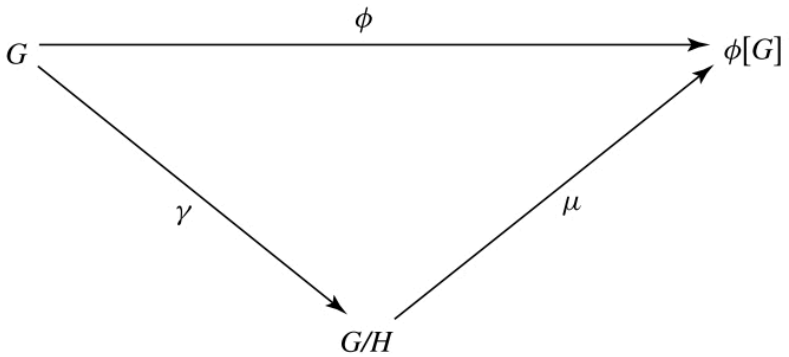
"canonical homomorphism"

$\gamma : G \to G/H$ defined by $\gamma(g) = gH$ is a homomorphism

$\therefore \quad \phi(g) = \mu(gH) = \mu(\gamma(g))$

$\Rightarrow$ homomorphism ϕ can be factored

$\phi = \mu\gamma$ where γ is a homomorphism & μ is an isomorphism of G/H with $\phi(G)$



14.11 Theorem **(The Fundamental Homomorphism Theorem)** Let $\phi : G \to G'$ be a group homomorphism with kernel H. Then $\phi[G]$ is a group, and $\mu : G/H \to \phi[G]$ given by $\mu(gH) = \phi(g)$ is an isomorphism. If $\gamma : G \to G/H$ is the homomorphism given by $\gamma(g) = gH$, then $\phi(g) = \mu\gamma(g)$ for each $g \in G$.

μ : canonical or natural isomorphism

γ : " homomorphism.

In summary, every homomorphism with domain G gives rise to a factor group G/H, and every factor group G/H gives rise to a homomorphism mapping G into G/H. Homomorphisms and factor groups are closely related. We give an example indicating how useful this relationship can be.

Example : Classify the group $(\mathbb{Z}_4 \times \mathbb{Z}_2)/(\{0\} \times \mathbb{Z}_2)$ according to the fundamental theorem of finitely generated abelian groups (Theorem 11.12).

Ans: The projection map $\pi_1 : \mathbb{Z}_4 \times \mathbb{Z}_2 \to \mathbb{Z}_4$ given by $\pi_1(x,y) = x$

$$\pi_1\big((x_1,y_1)+(x_2,y_2)\big) = \pi_1(x_1+x_2, y_1+y_2) = x_1+x_2 = \pi_1(x_1,y_1) + \pi_1(x_2,y_2)$$

$\Rightarrow$ homomorphism of $\mathbb{Z}_4 \times \mathbb{Z}_2$ onto $\mathbb{Z}_4$

$$\ker(\pi_1) = \{(x,y) \in \mathbb{Z}_4 \times \mathbb{Z}_2 \mid \pi_1(x,y) = 0\}$$
$$= \{(0,y) \mid y \in \mathbb{Z}_2\}$$
$$= \{0\} \times \mathbb{Z}_2$$

Theorem 14.11 $\Rightarrow (\mathbb{Z}_4 \times \mathbb{Z}_2)/(\{0\} \times \mathbb{Z}_2) = G/H \cong \pi_1(G) = \mathbb{Z}_4$

14.13 Theorem The following are three equivalent conditions for a subgroup H of a group G to be a *normal* subgroup of G.

1. $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$.
2. $gHg^{-1} = H$ for all $g \in G$.
3. $gH = Hg$ for all $g \in G$.

Condition (2) of Theorem 14.13 is often taken as the definition of a normal subgroup H of a group G.

Proof.

1 → 2

(⊆) Let $y \in gHg^{-1}$ then,

$\exists\ h \in H$ s.t $y = ghg^{-1} \in H$ ——— (1)

$\therefore gHg^{-1} \subseteq H$

(⊇) Let $h \in H$ then,

$ghg^{-1} \in H$ ——— (1)

?

2 - 3

Let $gHg^{-1} = H$ for all $g \in G$,

Take any $gh \in gH$ where $h \in H$

$gh = (ghg^{-1})g = h'g$ for some $h' \in H$ since $gHg^{-1} = H$

$\therefore gh \in Hg \Rightarrow gH \subseteq Hg$

and similarly $Hg \subseteq gH$

$\therefore \quad gH = Hg$ Q.E.D

3 → 1

Let $gH = Hg \ \forall \ g \in G$

$gh \in gH = Hg \Rightarrow gh = h'g$ for some $h' \in H$

$\therefore \quad ghg^{-1} = h'gg^{-1} = h' \in H$ Q.E.D

14.15 Definition An isomorphism $\phi : G \to G$ of a group G with itself is an **automorphism** of G. The automorphism $i_g : G \to G$, where $i_g(x) = gxg^{-1}$ for all $x \in G$, is the **inner automorphism of G by g**. Performing i_g on x is called **conjugation of x by g**. ■

The equivalence of conditions (1) and (2) in Theorem 14.13 shows that $gH = Hg$ for all $g \in G$ if and only if $i_g[H] = H$ for all $g \in G$, that is, if and only if H is **invariant** under all inner automorphisms of G. It is important to realize that $i_g[H] = H$ is an equation in *sets;* we need not have $i_g(h) = h$ for all $h \in H$. That is i_g may perform a nontrivial *permutation* of the set H. We see that the normal subgroups of a group G are precisely those that are invariant under all inner automorphisms. A subgroup K of G is a **conjugate subgroup** of H if $K = i_g[H]$ for some $g \in G$.

$= gHg^{-1}$ for some $g \in G$

Q. Prove that an inner automorphism is an isomorphism

Proof Let G be a group, and let $g \in G$

The inner automorphism induced by g is defined as:

$$i_g(x) = gxg^{-1} \quad \forall\, x \in G$$

- $i_g(x_1 x_2) = g(x_1 x_2)g^{-1} = gx_1 g^{-1} g x_2 g^{-1} = (gx_1 g^{-1})(gx_2 g^{-1})$
  $= i_g(x_1)\, i_g(x_2)$

  $\Rightarrow$ homomorphism

- Assume $i_g(x_1) = i_g(x_2)$ then

  $gx_1 g^{-1} = gx_2 g^{-1} \Rightarrow g^{-1}(gx_1 g^{-1})g = g^{-1}(gx_2 g^{-1})g$

  $\Rightarrow x_1 = x_2$

  $\therefore$ i_g is one-to-one

- Let $y \in G$,

  $y = i_g(x) = gxg^{-1} \Rightarrow x = g^{-1}yg$

  For any $y \in G$, there exists $x \in G$ such that $i_g(x) = y$.

  $\therefore$ i_g is onto

* If $H \leq G$, then $i_g[H] \leq G$ [Theorem 13.12
* If $H \trianglelefteq G$, then $i_g[H] = H$ [Theorem 14.13
  ie., H is invariant under conjugation

$i_g[H]$: conjugate subgroup of H

Corollary: If a finite group G has exactly one subgroup H of a given order, then $H \trianglelefteq G$.

Proof

Let G be a finite group, and let $H \subseteq G$ be the unique subgroup of G with a specific order $|H|$.

For any $g \in G$, the conjugate of H by g is the set

$$gHg^{-1} = \{ghg^{-1} / h \in H\}$$

Part 1

- Let $a, b \in gHg^{-1}$ then

  $a = gh_1g^{-1}$ and $b = gh_2g^{-1}$ for some $h_1, h_2 \in H$

  $ab = (gh_1g^{-1})(gh_2g^{-1}) = gh_1(g^{-1}g)h_2g^{-1} = gh_1h_2g^{-1} \in gHg^{-1}$

  since $h_1h_2 \in H \implies$ closure

- $geg^{-1} = gg^{-1} = e \in gHg^{-1}$ since $e \in H$

  $\implies$ existance of identity

- If $a = ghg^{-1}$ for some $h \in H$ then

  $a^{-1} = (ghg^{-1})^{-1} = (g^{-1})^{-1}h^{-1}g^{-1} = gh^{-1}g^{-1}$ such that

  $aa^{-1} = ghg^{-1}gh^{-1}g^{-1} = e$

  $\implies$ existance of inverse element

$\therefore \quad gHg^{-1} \leq H$ ——— 5.1

Part 2 → Let's define $\phi : H \to gHg^{-1}$

- If $\phi(h_1) = \phi(h_2) \Rightarrow gh_1g^{-1} = gh_2g^{-1}$

$\Rightarrow g^{-1}(gh_1g^{-1})\,g = g^{-1}(gh_2g^{-1})\,g \Rightarrow h_1 = h_2$

$\therefore \phi$ is one-to-one

- Let $y = \phi(h)$ then

$y = ghg^{-1} \Rightarrow h = g^{-1}yg$

$\therefore$ For any $y \in gHg^{-1}$ there exists $h \in H$ such that $y = ghg^{-1}$.

$\therefore \phi$ is on-to

$\Rightarrow \phi : H \to gHg^{-1}$ is a bijective function.

$\therefore \quad |gHg^{-1}| = |H|$ ——— 5.2

From eq^n: 5.1 and 5.2,

$gHg^{-1} \leq H$ and $|gHg^{-1}| = |H|$

$\Rightarrow gHg^{-1} = H \quad \forall\, g \in G$

$\Rightarrow H$ is a normal subgroup of G

ie., $H \trianglelefteq G$

15

The Converse of Lagrange's theorem is false

(Falsity of the Converse of the Theorem of Lagrange) The theorem of Lagrange states if H is a subgroup of a finite group G, then the order of H divides the order of G. We show that it is false that if d divides the order of G, then there must exist a subgroup H of G having order d. Namely, we show that A_4, which has order 12, contains no subgroup of order 6.

S_4: set of permutations of 4 elements

A_4: subgroup of S_4 consisting of only the even permutations

$|S_4| = 4! = 24 \Longrightarrow |A_4| = 12$

Claim: $6 \mid 12 \Rightarrow \nexists\, H \leq A_4$ s.t $|H| = 6$

* A subgroup of index 2 is always normal

$H \leq G$ & $[G:H] = 2 \Longrightarrow H \trianglelefteq G$

Proof Suppose $H \leq G$ s.t $[G:H] = 2$

$\therefore$ H has 2 left cosets (and 2 right cosets) in G

If $g \in H$ then $gH = H = Hg$

If $g \notin H$ then $gH = G \setminus H = G - H$ as there are only 2 cosets partition G

For the same reason, $g \notin H \Rightarrow Hg = G \setminus H = G - H$

$\therefore$ $gH = Hg \Rightarrow H \trianglelefteq G$

Proof (by contradiction)

Suppose $H \leq A_4$ s.t $|H| = 6$

$$(A_4 : H) = \frac{|A_4|}{|H|} = \frac{12}{6} = 2 \Longrightarrow H \text{ is normal}$$
ie; $H \trianglelefteq A_4$

$A_4/H = \{H, \sigma H\}$ for some $\sigma \in A_4$ but $\sigma \notin H$

In a group of order 2, the square of each element is the identity.

$|A_4/H| = 2 \Longrightarrow (H)(H) = H$ & $(\sigma H)(\sigma H) = H$

$\therefore$ For $\alpha \in H$, $\alpha^2 \in H$ & For each $\beta \in \sigma H$, $\beta^2 \in H$

$\therefore$ For each $\tau \in A_4$, $\tau^2 \in H$

$(123) = (132)^2 \in H$, $(132) = (123)^2 \in H$, $(124) = (142)^2 \in H$, $(142) = (124)^2 \in H$

$(134) = (143)^2 \in H$, $(143) = (134)^2 \in H$, $(234) = (243)^2 \in H$, $(243) = (234)^2 \in H$

$\Longrightarrow |H| > 6$ which is a contradiction.

$\therefore \not\exists\ H \leq A_4$ s.t $|H| = 6$

---

* If G is abelian, then the converse of Lagrange's theorem is true

$$G \cong \mathbb{Z}_{p_1^{\alpha_1}}/\mathbb{Z} \times \mathbb{Z}_{p_2^{\alpha_2}}/\mathbb{Z} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}/\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$$

15.8 Theorem Let $G = H \times K$ be the direct product of groups H and K. Then $\overline{H} = \{(h, e) \mid h \in H\}$ is a normal subgroup of G. Also $G/\overline{H}$ is isomorphic to K in a natural way. Similarly, $G/\overline{K} \simeq H$ in a natural way.

Proof Consider $\pi_2 : H \times K \to K$ where $\pi_2(h,k) = k$

$$\pi_2\left((h_1,k_1)(h_2,k_2)\right) = \pi_2(h_1h_2, k_1k_2) = k_1k_2 = \pi_2(h_1,k_1)\,\pi_2(h_2,k_2)$$

$\Rightarrow \pi_2 : H \times K \to K$ is a homomorphism

$$\ker(\pi_2) = \{(h, e_K) : h \in H\} = \overline{H}$$

14.11 Theorem **(The Fundamental Homomorphism Theorem)** Let $\phi : G \to G'$ be a group homomorphism with kernel H. Then $\phi[G]$ is a group, and $\mu : G/H \to \phi[G]$ given by $\mu(gH) = \phi(g)$ is an isomorphism. If $\gamma : G \to G/H$ is the homomorphism given by $\gamma(g) = gH$, then $\phi(g) = \mu\gamma(g)$ for each $g \in G$.

$\pi_2 : G \to K$ is a group homomorphism with kernel $\overline{H}$.

$\pi_2[G] = K$ is a group

$$\Rightarrow G/\ker(\pi_2) \cong \pi_2(G)$$

$$\Rightarrow G/\overline{H} \cong K$$

15.9 Theorem A factor group of a cyclic group is cyclic.

Proof Let $G = \langle a \rangle$ be a cyclic group

Every cyclic group is abelian & a subgroup of a cyclic group is cyclic

All subgroups of abelian groups are normal.

$\Rightarrow$ Any subgroup $H \leq G = \langle a \rangle$ is normal

- coset multiplication is well defined iff $H \trianglelefteq G$.

$\Longrightarrow$ G/H is a group on the left cosets

aH is a left coset $\in G/H$ where $a \in G$

$(aH)^k = a^k H \Longrightarrow$ we produce every possible left coset

$\Longrightarrow$ aH generates G/H

Ex: 15.11 $\quad (\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle(2,3)\rangle$

$\mathbb{Z}_4 = \{0,1,2,3\}$ & $\mathbb{Z}_6 = \{0,1,2,3,4,5\}$

$\langle(2,3)\rangle = \{(0,0),(2,3)\}$

cosets of $\langle(2,3)\rangle = (a,b) + \langle(2,3)\rangle$ where $(a,b) \in \mathbb{Z}_4 \times \mathbb{Z}_6$

$= \{(a,b), (a+2 \bmod 4, b+3 \bmod 6)\}$

□ Simple Groups

15.14 Definition A group is **simple** if it is nontrivial and has no proper nontrivial normal subgroups.

G is nontrivial $\Rightarrow G \neq \{e\}$

Non trivial subgroup $\Rightarrow H \leq G$ s.t $H \neq \{e\}$

Proper subgroup $\Rightarrow H \leq G$ s.t $H < G$ & $H \neq G$

Ex:

(1) Cyclic groups of prime order

— $G = \mathbb{Z}_p$ where p is a prime # is simple

(2) The alternating group A_n is simple for $n \geq 5$.

15.16 Theorem Let $\phi : G \to G'$ be a group homomorphism. If N is a normal subgroup of G, then $\phi[N]$ is a normal subgroup of $\phi[G]$. Also, if N' is a normal subgroup of $\phi[G]$, then $\phi^{-1}[N']$ is a normal subgroup of G.

ie; If $\phi : G \to G'$ is a group homomorphism. Then,

$$N \trianglelefteq G \implies \phi(N) \trianglelefteq \phi[G]$$

$$N' \trianglelefteq \phi(G) \implies \phi^{-1}[N'] \trianglelefteq G$$

A homomorphism $\phi : G \to G'$ preserves normal subgroups b/w G and $\phi[G]$.

15.17 Definition A **maximal normal subgroup of a group** G is a normal subgroup M not equal to G such that there is no proper normal subgroup N of G properly containing M. ■

15.18 Theorem M is a maximal normal subgroup of G if and only if G/M is simple.

The Center and Commutator Subgroups

Every nonabelian group G has two important normal subgroups, the *center* $Z(G)$ of G and the *commutator subgroup* C of G. (The letter Z comes from the German word *zentrum,* meaning center.) The center $Z(G)$ is defined by

$$Z(G) = \{z \in G \mid zg = gz \text{ for all } g \in G\}.$$

Exercise 52 of Section 5 shows that $Z(G)$ is an abelian subgroup of G. Since for each $g \in G$ and $z \in Z(G)$ we have $gzg^{-1} = zgg^{-1} = ze = z$, we see at once that $Z(G)$ is a normal subgroup of G. If G is abelian, then $Z(G) = G$; in this case, the center is not useful.

The center of a group G always contains the identity element e. It may be that $Z(G) = \{e\}$, in which case we say that **the center of G is trivial**. For example, examination of Table 8.8 for the group S_3 shows us that $Z(S_3) = \{\rho_0\}$, so the center of S_3 is trivial. (This is a special case of Exercise 38, which shows that the center of every nonabelian group of order pq for primes p and q is trivial.) Consequently, the center of $S_3 \times \mathbb{Z}_5$ must be $\{\rho_0\} \times \mathbb{Z}_5$, which is isomorphic to $\mathbb{Z}_5$. ▲

Since Theorem 11.12 gives complete information about the structure of all sufficiently small abelian groups, it might be of interest to try to form an abelian group as much like G as possible, an *abelianized version* of G, by starting with G and then requiring that $ab = ba$ for all a and b in our new group structure. To require that $ab = ba$ is to say that $aba^{-1}b^{-1} = e$ in our new group. An element $aba^{-1}b^{-1}$ in a group is a **commutator of the group.** Thus we wish to attempt to form an abelianized version of G by replacing every commutator of G by e. By the first observation of this paragraph, we should then attempt to form the factor group of G modulo the smallest normal subgroup we can find that contains all commutators of G.

15.20 Theorem Let G be a group. The set of all commutators $aba^{-1}b^{-1}$ for $a, b \in G$ generates a subgroup C (the **commutator subgroup**) of G. This subgroup C is a normal subgroup of G. Furthermore, if N is a normal subgroup of G, then G/N is abelian if and only if $C \leq N$.

Proof

$(aba^{-1}b^{-1})^{-1} = bab^{-1}a^{-1}$ is again a commutator

$e = eee^{-1}e^{-1}$ is a commutator

$\Rightarrow$ The commutators generates a subgroup C.

For any commutator $cdc^{-1}d^{-1}$,

$$\begin{aligned} g^{-1}(cdc^{-1}d^{-1})g &= (g^{-1}cdc^{-1})e(d^{-1}g) \\ &= (g^{-1}cdc^{-1})(gd^{-1}dg^{-1})(d^{-1}g) \\ &= [(g^{-1}c)d(g^{-1}c)^{-1}d^{-1}][dg^{-1}d^{-1}g] \in C \end{aligned}$$

$\Rightarrow$ C is normal in G

16 Group Action on a Set

The Notion of a Group Action

a binary operation $*$ on a set S to be a function mapping $S \times S$ into S. The function $*$ gives us a rule for "multiplying" an element s_1 in S and an element s_2 in S to yield an element $s_1 * s_2$ in S.

More generally, for any sets A, B, and C, we can view a map $* : A \times B \to C$ as defining a "multiplication," where any element a of A times any element b of B has as value some element c of C. Of course, we write $a * b = c$, or simply $ab = c$. In this section, we will be concerned with the case where X is a set, G is a group, and we have a map $* : G \times X \to X$. We shall write $*(g, x)$ as $g * x$ or gx.

16.1 Definition Let X be a set and G a group. An **action of G on X** is a map $* : G \times X \to X$ such that ■

1. $ex = x$ for all $x \in X$,
2. $(g_1 g_2)(x) = g_1(g_2 x)$ for all $x \in X$ and all $g_1, g_2 \in G$.

Under these conditions, X is a **G-set.**

16.3 Theorem Let X be a G-set. For each $g \in G$, the function $\sigma_g : X \to X$ defined by $\sigma_g(x) = gx$ for $x \in X$ is a permutation of X. Also, the map $\phi : G \to S_X$ defined by $\phi(g) = \sigma_g$ is a homomorphism with the property that $\phi(g)(x) = gx$.

D X is a G-set. For each $g \in G$,

$\sigma_g : X \to X$ defined by $\sigma_g(x) = gx$ $\forall\, x \in X$

is a permutation of X

$\Rightarrow$ $\sigma_g : X \to X$ is a bijective function

Proof Let $\sigma_g(x_1) = \sigma_g(x_2)$ for $x_1, x_2 \in X$

$$gx_1 = gx_2 \Rightarrow g^{-1}(gx_1) = g^{-1}(gx_2)$$

$$ex_1 = ex_2 \Rightarrow x_1 = x_2$$

$\therefore \sigma_g$ is one-to-one

$$\sigma_g(x) = gx = y \text{ (say)}$$

$$g^{-1}y = g^{-1}(gx) = ex = x$$

For every $y \in X$, $\exists\, x = g^{-1}y$ such that $\sigma_g(x) = \sigma_g(g^{-1}y) = y$

$\therefore \sigma_g$ is onto

$\Rightarrow \sigma_g : X \to X$ is a bijective function

$\Rightarrow \sigma_g$ is a permutation

(2) S_X : the symmetric group of all permutations of X

The map $\phi : G_1 \to S_X$ is defined by $\phi(g) = \sigma_g$

where σ_g : permutation corresp. to $g \in G_1$.

For any $g_1, g_2 \in G_1$,

$$\phi(g_1g_2)(x) = \sigma_{g_1g_2}(x) = (g_1g_2)(x) = g_1(g_2x) = g_1\,\sigma_{g_2}(x)$$

$$= \sigma_{g_1}(\sigma_{g_2}(x)) = (\sigma_{g_1} \circ \sigma_{g_2})(x) = (\phi(g_1)\,\phi(g_2))(x)$$

$\therefore \phi(g_1g_2) = \phi(g_1)\,\phi(g_2) \quad \forall\ g_1, g_2 \in G_1$

$\Rightarrow \phi$ is a homomorphism

Isotropy Subgroups

Let X be a G-set. Let $x \in X$ and $g \in G$. It will be important to know when $gx = x$. We let

$$X_g = \{x \in X \mid gx = x\} \qquad \text{and} \qquad G_x = \{g \in G \mid gx = x\}.$$

16.12 Theorem Let X be a G-set. Then G_x is a subgroup of G for each $x \in X$.

G_x: isotropy subgroup of x

Proof X is a G-set & $G_x = \{g \in G \mid gx = x\}$

- Let $x \in X$ and let $g_1, g_2 \in G_x$ then $g_1 x = x$ and $g_2 x = x$

  $(g_1 g_2)x = g_1(g_2 x) = g_1 x = x \implies g_1 g_2 \in G_x$

  $\therefore$ G_x is closed under the induced operation of G

- $ex = x$ since X is a G-set $\implies e \in G_x$

- If $g \in G_x$ then $gx = x$

  $g^{-1}x = g^{-1}(gx) = (g^{-1}g)x = ex = x \implies g^{-1} \in G_x$

$\therefore$ G_x is a subgroup of G.

16.13 Definition Let X be a G-set and let $x \in X$. The subgroup G_x is the **isotropy subgroup of** x.

16.14 Theorem Let X be a G-set. For $x_1, x_2 \in X$, let $x_1 \sim x_2$ if and only if there exists $g \in G$ such that $gx_1 = x_2$. Then $\sim$ is an equivalence relation on X.

Proof

- For each $x \in X$, $ex = x \implies x \sim x$
  $\therefore$ $\sim$ is reflexive
- Suppose $x_1 \sim x_2 \implies gx_1 = x_2$ for some $g \in G$
  Then, $g^{-1}x_2 = g^{-1}(gx_1) = (g^{-1}g)x_1 = ex_1 = x_1 \implies x_2 \sim x_1$
  $\therefore$ $\sim$ is symmetric
- If $x_1 \sim x_2$ and $x_2 \sim x_3$ then $g_1x_1 = x_2$ and $g_2x_2 = x_3$ for some $g_1, g_2 \in G$. Then,
  $(g_2g_1)x_1 = g_2(g_1x_1) = g_2(x_2) = x_3 \implies x_1 \sim x_3$
  $\therefore$ $\sim$ is transitive

16.15 Definition Let X be a G-set. Each cell in the partition of the equivalence relation described in Theorem 16.14 is an **orbit in** X **under** G. If $x \in X$, the cell containing x is the **orbit of** x. We let this cell be Gx. ■

$$Gx = \{gx \mid g \in G\}$$

16.16 Theorem Let X be a G-set and let $x \in X$. Then $|Gx| = (G : G_x)$. If $|G|$ is finite, then $|Gx|$ is a divisor of $|G|$.

$(G : G_x)$ – index of G_x in G

– # of left cosets of G_x in G

Proof

Let X be a set and G a group. An **action of G on X** is a map $* : G \times X \to X$ such that ■

1. $ex = x$ for all $x \in X$,
2. $(g_1 g_2)(x) = g_1(g_2 x)$ for all $x \in X$ and all $g_1, g_2 \in G$.

Under these conditions, X is a **G-set.**

$$G_x = \{g \in G \mid gx = x\}.$$

$$X_g = \{x \in X \mid gx = x\}$$

Let X be a G-set. For $x_1, x_2 \in X$, let $x_1 \sim x_2$ if and only if there exists $g \in G$ such that $gx_1 = x_2$. Then $\sim$ is an equivalence relation on X.

If $x \in X$, the cell containing x is the **orbit of** x.

$Gx = \{gx : g \in G\}$

Let X be a G-set and fix $x \in X$.

Define $\psi : Gx \longrightarrow G/G_x$

Let $x_1, x_2 \in Gx$ then $\exists\ g_1 \in G$ s.t $g_1 x = x_1$

$\exists\ g_2 \in G$ s.t $g_2 x = x_2$

Let's define $\psi(x_1) = g_1 G_x$, the left coset of G_x in G corresponding to g_1.

14.9 Theorem Let H be a normal subgroup of G. Then $\gamma : G \to G/H$ given by $\gamma(x) = xH$ is a homomorphism with kernel H.

"canonical homomorphism"

Suppose that $g_1 x = x_1$ and $g_1' x = x_1$ for some other $g_1' \in G$

ie.,
$$g_1 x = g_1' x \implies g_1^{-1}(g_1 x) = g_1^{-1}(g_1' x)$$

$$x = (g_1^{-1} g_1') x$$

$$\therefore \; g_1^{-1} g_1' \in G_x \implies g_1^{-1} g_1' = g \in G_x$$

$$\therefore \; g_1' = g_1 g \text{ for some } g \in G_x$$

Then,
$$g_1' G_x = (g_1 g) G_x = g_1 G_x \qquad \left[g G_x = G_x \text{ for } g \in G_x \right]$$

$\implies$ The map ψ is well defined, independent of the choice of $g_1 \in G$ such that $g_1 x = x_1$.

1-1 :

Suppose $x_1, x_2 \in Gx$ and $\psi(x_1) = \psi(x_2)$ then $\exists\, g_1, g_2 \in G$ such that $x_1 = g_1 x$, $x_2 = g_2 x$ and

$g_1 G_x = g_2 G_x$.

$G_x \leq G \implies e \in G_x \implies g_2 \in g_2 G_x \implies g_2 \in g_1 G_x$

$\therefore \; g_2 = g_1 g$ for some $g \in G_x$

$\therefore \; x_2 = g_2 x = g_1 (g x) = g_1 x = x_1$ $\qquad \left[g \in G_x \implies g x = x \right]$

$\implies \psi$ is one-to-one

Onto : Let $y \in G/G_x$ then $y = g_1 G_x$ for some $g_1 \in G$

we can choose $x_1 = g_1 x$ such that $\psi(x_1) = g_1 G_x = y$

$\therefore$ For all $y \in G/G_x$ there exists $x_1 \in Gx$ s.t $\psi(x_1) = y$.

$\Rightarrow \psi$ is on-to

$\therefore$ There exists a bijective map ψ from $G_{\mathcal{O}x}$ to the collection of left cosets of G_x in G.

$$\Rightarrow |G_{\mathcal{O}x}| = |G/G_x| = (G : G_x)$$

---

17 Applications of G-sets to Counting

The # of ways to mark the six faces of a cube with numbers from 1 to 6, such that markings can be made identical through rotations of the cube?

Let us distinguish between the faces of the cube for the moment and call them the bottom, top, left, right, front, and back. Then the bottom can have any one of six marks from one dot to six dots, the top any one of the five remaining marks, and so on.

# of ways to mark the cube faces = $6! = 720$

There are 6 different faces to choose from, to be the top face of the cube. Each choice gives a different orientation of the cube. For each top face, there are 4 possible rotations ($0°, 90°, 180°, 270°$) around the vertical axis that goes through the center of the top face.
ie.: for each 6 possible to face, there are 4 possible different rotations which give different orientations of the cube.

6 (top faces) $\times$ 4 (rotations per top face) $= 24$ total rotational symmetries

$\therefore$

There are $\frac{720}{24} = 30$ distinguishable dice.

The 24 rotations of the die form a group G_1, which is isomorphic to a subgroup of S_8.

Let X be the 720 possible ways of marking the cube and let G_1 act on X by rotation of the cube.

Two markings in X give the same die if one can be carried into the other under action by an element of G_1.
ie., By rotating the cube.

ie.,

Each orbit in X under G_1 correspond to a single die, and different orbits to give a different dice.

$\Rightarrow \#\{\text{distinguishable dice}\} = \#$ of orbits under G_1 in a G_1-set X.

Let X be a set and G a group. An **action of G on X** is a map $* : G \times X \to X$ such that ■

1. $ex = x$ for all $x \in X$,
2. $(g_1 g_2)(x) = g_1(g_2 x)$ for all $x \in X$ and all $g_1, g_2 \in G$.

Under these conditions, X is a **G-set.**

$$G_x = \{g \in G \mid gx = x\}.$$

Let X be a G-set. For $x_1, x_2 \in X$, let $x_1 \sim x_2$ if and only if there exists $g \in G$ such that $gx_1 = x_2$. Then $\sim$ is an equivalence relation on X.

If $x \in X$, the cell containing x is the **orbit of x.**

$G_1 x = \{gx : g \in G_1\}$

The following theorem gives a tool for determining the number of orbits in a G-set X under G. Recall that for each $g \in G$ we let X_g be the set of elements of X left fixed by g, so that $X_g = \{x \in X \mid gx = x\}$. Recall also that for each $x \in X$, we let $G_x = \{g \in G \mid gx = x\}$, and Gx is the orbit of x under G.

17.1 Theorem (**Burnside's Formula**) Let G be a finite group and X a finite G-set. If r is the number of orbits in X under G, then

$$r \cdot |G| = \sum_{g \in G} |X_g|. \tag{1}$$

Proof Consider all pairs (g, x) where $gx = x$ & let N be the # of such pairs.

$X_g = \{x \in X \mid gx = x\} \Rightarrow |X_g|$: for any $g \in G$, how many $x \in X$ does g fix?

$\therefore \quad N = \sum_{g \in G} |X_g|$

$G_x = \{g \in G \mid gx = x\} \Rightarrow |G_x|$: for any $x \in X$, how many elements $g \in G$ that leave x unchanged?

$\therefore \quad N = \sum_{x \in X} |G_x|$

Theorem 16.16 $\Rightarrow |G_x| = (G : G_x) = |G/G_x|$

$$(G : G_x) = \frac{|G|}{|G_x|} \Rightarrow |G_x| = \frac{|G|}{|Gx|}$$

$$\therefore N = \sum_{x \in X} |G_x| = \sum_{x \in X} \frac{|G|}{|Gx|} = |G| \left(\sum_{x \in X} \frac{1}{|Gx|} \right)$$

$Gx = \{ gx \mid g \in G \}$ is the orbit of x under g.

$\therefore \frac{1}{|Gx|}$ has the same value for all x in the same orbit.

Let $\mathcal{O}$ be any orbit, then

$$\sum_{x \in \mathcal{O}} \frac{1}{|Gx|} = \sum_{x \in \mathcal{O}} \frac{1}{|\mathcal{O}|} = \frac{1}{|\mathcal{O}|} \sum_{x \in \mathcal{O}} 1 = 1$$

$\therefore$

$$N = |G| \sum_{x \in X} \frac{1}{|Gx|} = |G| \times \underbrace{\sum_{x \in \mathcal{O}} \frac{1}{|Gx|}}_{1} \times \{ \# \text{ of orbits in } X \text{ under } G \}$$

$$= |G| \times (\# \text{ of orbits in } X \text{ under } G)$$

$$= |G| \cdot r$$

$$\therefore r|G| = N = \sum_{g = G} |X_g| = \sum_{x \in X} |G_x|$$

17.2 Corollary If G is a finite group and X is a finite G-set, then

$$(\text{number of orbits in } X \text{ under } G) = \frac{1}{|G|} \cdot \sum_{g \in G} |X_g|.$$

Ex 17.3 → Let, X: the set of 720 different markings of faces of a cube using 1 to 6.

G: the group of 24 rotations of the cube

# of distinguishable dice = # of orbits in X under G

$|G| = 24$, $X_g = \{x \in X \mid gx = x\}$

$|X_g|$: for any $g \in G$, how many $x \in X$ does g fix

For $g \in G$ where $g \neq e$, $|X_g| = 0$ [any rotation other than the identity element changes any one of the 720 markings into a different one.]

$|X_e| = 720$ [identity element leaves all 720 markings fixed]

$$\# \text{ of orbits} = \frac{1}{|G|} \sum_{g \in G} |X_g| = \frac{1}{24} \times 720 = 30$$

∴ There are 30 distinguishable dice.

Combinatorics: Assume that one face of the die is fixed. Say, the face marked '1' is fixed, to be on the bottom.
Next, the face opposite to the fixed face have 5 possible options.
The remaining 4 numbers are arranged in $(4-1)! = 3 \times 2 \times 1 = 6$ ways.

∴ Total # of possibilities $= 5 \times 3 \times 2 \times 1 = 30$.

17.4 Example How many distinguishable ways can seven people be seated at a round table, where there is no distinguishable "head" to the table?

Ans. X : $7!$ ways to assign people to the different chairs

Rotation generates a cyclic group G_1 of order 7.

G_1 act on X.

Only the identity $e \in G_1$ leaves any arrangement fixed.

$\Rightarrow$ e leaves all $7!$ arrangements fixed.

$$\therefore \#\text{ of orbits in } X \text{ under } G_1 = \frac{1}{|G_1|}\sum_{g\in G_1}|X_g| = \frac{1}{7}\times 7! = 6! = \underline{720}.$$

The n^{th} dihedral group D_n is the group of symmetries of the regular n-gon. It consists of:

i) n rotations of the n-gon around its center by multiples of $\frac{360^\circ}{n}$

ii) n reflections of the n-gon across specific axis of symmetry, passing through opposite vertices or midpoints of opposite sides.

17.5 Example How many distinguishable necklaces (with no clasp) can be made using seven different-colored beads of the same size?

Ans: Unlike the table, the necklace can be turned over as well as rotated $\Rightarrow$ dihedral group D_7 of order $2 \cdot 7 = 14$ acting on the set X of $7!$ possibilities.

$\therefore$ The # of distinguishable necklaces is,

$$\#\text{ of orbits in } X \text{ under } G = \frac{1}{|G|}\sum_{g \in G} |X_g| = \frac{1}{14} \cdot 7! = \underline{\underline{360}}.$$

17.6 Example Let us find the number of distinguishable ways the edges of an equilateral triangle can be painted if four different colors of paint are available, assuming only one color is used on each edge, and the same color may be used on different edges.

Ans: Each of 3 edges may be any one of the 4 colors

$\Rightarrow 4^3 = 64$ ways of painting the edges in all.

X: the set of these 64 possible painted triangles.

The group G acting on X is the group of symmetries of the triangle, D_3 of order $3+3=6$. $\quad G \simeq S_3$

$|X_{\rho_0}| = 64$ [every painted Δ is left fixed by ρ_0]

$|X_{\rho_1}| = 4$

$|X_{\rho_2}| = 4$

[To be invariant under ρ_1, ρ_2, all edges must be the same color]

$|X_{\mu_1}| = 4 \times 4 = 16$

$|X_{\mu_2}| = |X_{\mu_3}| = 16$

The edges that are interchanged by reflection must be the same color (4 possibilities) and the other edge may also be any of the colors (times 4 possibilities)

$\therefore$

$$\#\text{ of orbits in } X \text{ under } G = \frac{1}{|G|}\sum_{g \in G} |X_g|$$

$$= \frac{1}{6}\left[64 + 4 + 4 + 16 + 16 + 16\right] = \frac{1}{6} \times 120 = \underline{\underline{20}}.$$

17.7 Example We repeat Example 17.6 with the assumption that a different color is used on each edge.

Ans: # of possible ways of painting the edges $= 4 \times 3 \times 2 = 24$

$\therefore$ X : the set of 24 possible painted triangles

Group acting on X is D_3.

$|X_{\rho_0}| = 24$, $|X_{\rho_1}| = 0 = |X_{\rho_2}|$, $|X_{\mu_1}| = |X_{\mu_2}| = |X_{\mu_3}| = 0$

$$\#\text{ of orbits} = \frac{1}{|G|}\sum_{g \in G} |X_g|$$

$$= \frac{1}{6} \times 24 = \underline{\underline{4}}.$$