Quotient spaces

Suppose G is a group and $H \leq G$. It follows from our proof of Lagrange's theorem that the collection of left cosets $\{gH : g \in G\}$ is a partition of G. $(gH = \{gh : h \in H\})$

Def: The (left) <u>quotient space of G modulo H</u> is

$$G/H = \{gH : g \in G\}.$$

Similarly, the right quotient space of G modulo H is

$$H \backslash G = \{Hg : g \in G\}$$

We also define the <u>index of H in G</u>, denoted $|G:H|$, by

$$|G:H| = |G/H|.$$

Note: If $|G| < \infty$ then, again from our proof of Lagrange's theorem, $|G:H| = \frac{|G|}{|H|}$.

Motivating question: Is there a natural way to use the binary operation on G to turn G/H into a group?

Exs:

1) $G=\mathbb{Z}$, $H=n\mathbb{Z}$ $(n\in\mathbb{N})$

$$G/H=\{a+n\mathbb{Z} : a\in\mathbb{Z}\}$$
$$=\{0+n\mathbb{Z},\ 1+n\mathbb{Z},\ \dots,\ (n-1)+n\mathbb{Z}\}$$
$$=\{\bar{0},\bar{1},\dots,\overline{n-1}\}$$ (Ex. 6 from Equivalence relations)

From our video Integers modulo n we saw that the rule

$\bar{a}+\bar{b}=\overline{a+b}$, $a,b\in\mathbb{Z}$, is a binary operation on G/H,

which turns this quotient space into a group.

Key fact in this example: The binary operation above is well-defined.

I.e. it doesn't depend on the choices of representatives for the cosets.

2) $G=S_3$, $H=\langle(1\ 2)\rangle=\{e,(1\ 2)\}$

Scratch work:
$(2\ 3)(1\ 2)=(1\ 3\ 2)$
$(1\ 3)(1\ 2)=(1\ 2\ 3)$

$H_0=eH=\{e,(1\ 2)\}=(1\ 2)H$

$H_1=(2\ 3)H=\{(2\ 3),(1\ 3\ 2)\}=(1\ 3\ 2)H$ $\quad H_2=(1\ 3)H=\{(1\ 3),(1\ 2\ 3)\}=(1\ 2\ 3)H$

$$G/H=\{H_0,H_1,H_2\}$$

What if we try to define multiplication on G/H by the "rule"

$$(g_1H)(g_2H)=(g_1g_2)H\ ?$$

Problem: This "rule" is not well-defined. For example,

$H_0=eH=(1\ 2)H$ and $H_1=(2\ 3)H$, but

$$(e(2\ 3))H=(2\ 3)H=H_1, \text{ and}$$
$$\ne$$
$$((1\ 2)(2\ 3))H=(1\ 2\ 3)H=H_2.$$

Theorem: Suppose G is a group and $H \leq G$. The rule

$$(g_1H)(g_2H) = (g_1g_2)H, \quad \forall g_1H, g_2H \in G/H, \qquad (*)$$

is a well-defined binary operation on G/H if and only if $H \trianglelefteq G$.

When $H \trianglelefteq G$, G/H together with this binary operation is a group, called the <u>quotient group of G modulo H</u>.

Pf: $\Rightarrow$: Suppose $(*)$ is well-defined.

Want to show: $\forall g \in G$, $h \in H$, we have $ghg^{-1} \in H$. $\quad (gHg^{-1} \subseteq H)$

Note that $\forall h \in H$, $hH = H = eH$. Then, $\forall g \in G$, since $(*)$ is well-defined,

$$(hg^{-1})H = (hH)(g^{-1}H) = (eH)(g^{-1}H) = (eg^{-1})H = g^{-1}H.$$

Therefore, $hg^{-1} \in g^{-1}H \Rightarrow \exists h' \in H$ s.t. $hg^{-1} = g^{-1}h' \Rightarrow ghg^{-1} = h' \in H$.

Conclusion: $H \trianglelefteq G$.

$\Leftarrow$: Suppose $H \trianglelefteq G$.

Want to show: If $g_1H = g_1'H$ and $g_2H = g_2'H$ then $(g_1g_2)H = (g_1'g_2')H$.

Note that $g_iH = g_i'H \Rightarrow g_i' \in g_iH \Rightarrow g_i' = g_ih_i$ for some $h_i \in H$.
$(i = 1, 2)$

Then $g_1'g_2' = g_1h_1g_2h_2 = g_1(g_2g_2^{-1})h_1g_2h_2$

$$= (g_1g_2)(g_2^{-1}h_1g_2)h_2 \overset{(H \trianglelefteq G)}{=} (g_1g_2)\underbrace{h'h_2}_{\in H} \quad \text{for some } h' \in H.$$

Therefore $g_1'g_2' \in (g_1g_2)H \Rightarrow (g_1'g_2')H \cap (g_1g_2)H \neq \emptyset \Rightarrow (g_1'g_2')H = g_1g_2H$.

Finally, if $(*)$ is well-defined then it turns G/H into a group:

- associativity:

$\forall\, g_1H, g_2H, g_3H \in G/H$,

$$\big((g_1H)(g_2H)\big)(g_3H) = \big((g_1g_2)H\big)(g_3H) = \big((g_1g_2)g_3\big)H \overset{\text{assoc. in } G}{=} \big(g_1(g_2g_3)\big)H = \cdots = (g_1H)\big((g_2H)(g_3H)\big)$$

- identity $= eH = H$

$$\forall\, gH \in G/H, \quad (eH)(gH) \overset{(g=eg=ge)}{=} gH = (gH)(eH)$$

- inverses: $(gH)^{-1} = (g^{-1})H$

$$(gH)(g^{-1}H) = (g^{-1}H)(gH) = eH. \quad \blacksquare$$

Ex. 2, revisited: $G = S_3$, $H = \langle (1\,2) \rangle = \{e, (1\,2)\}$

Note that $(1\,3)(1\,2)\underbrace{(1\,3)^{-1}}_{=(1\,3)} = (2\,3) \notin H \Rightarrow H \ntrianglelefteq G$.

Therefore by the theorem, multiplication of cosets in G/H, as described there, is not well-defined.

<u>Basic facts</u>

If $H \trianglelefteq G$ then G/H is a group and:

i) $e_{G/H} = eH = H$, ii) $\forall\, gH \in G/H$, $(gH)^{-1} = g^{-1}H$

iii) $gH = g'H \iff g' \in gH$

iv) $\forall\, gH \in G/H$, $n \in \mathbb{Z}$, $(gH)^n = g^nH$.

v) If $g \in G$ has order $k \in \mathbb{N}$ in G, then the order of gH in G/H divides k.

Exs:

3a) $G = C_4 \times C_4 = \langle x \rangle \times \langle y \rangle = \{(x^i, y^j) : 0 \le i, j \le 3\}$

$H = \langle (x^2, e), (e, y^2) \rangle \trianglelefteq G$ (G is Abelian $\Rightarrow$ every subgroup is normal)

$H = \{(x^2, e)^i (e, y^2)^j : i, j \in \mathbb{Z}\} = \{(e,e), (x^2, e), (e, y^2), (x^2, y^2)\}$

$|H| = 4 \Rightarrow |G:H| = |G/H| = \frac{|G|}{|H|} = 4 \Rightarrow G/H \cong C_4$ or V_4.

$G/H = \{(e,e)H, (x,e)H, (e,y)H, (x,y)H\}$

$(e,e)H = \{(e,e), (x^2, e), (e, y^2), (x^2, y^2)\}$

$(x,e)H = \{(x,e), (x^3, e), (x, y^2), (x^3, y^2)\}$

$(e,y)H = \{(e,y), (x^2, y), (e, y^3), (x^2, y^3)\}$

$(x,y)H = \{(x,y), (x^3, y), (x, y^3), (x^3, y^3)\}$

- $C_4 = \langle x \rangle = \{e, x, x^2, x^3\}$
  1 elem of order 1
  1 elem of order 2
  2 elems of order 4

- $V_4 = \langle a, b \mid a^2 = b^2 = e, ab = ba \rangle$
  $= \{e, a, b, ab\}$
  1 elem of order 1
  3 elems. of order 2

Note: $((x,e)H)^2 = (x^2, e)H = (e,e)H$ $((x^2, e) \in (e,e)H)$

$((e,y)H)^2 = (e, y^2)H = (e,e)H$ $((e, y^2) \in (e,e)H)$

$((x,y)H)^2 = (x^2, y^2)H = (e,e)H$ $((x^2, y^2) \in (e,e)H)$

Therefore, all non-identity elements in G/H have order 2,

so $G/H \cong V_4$.

3b) $G = C_4 \times C_4 = \langle x \rangle \times \langle y \rangle = \{ (x^i, y^j) : 0 \le i, j \le 3 \}$

$H = \langle (x, y^3) \rangle \trianglelefteq G$

$H = \{ (x, y^3)^i : i \in \mathbb{Z} \} = \{ (e,e), (x, y^3), (x^2, y^2), (x^3, y) \}$

$|H| = 4 \implies |G : H| = |G/H| = \frac{|G|}{|H|} = 4 \implies G/H \cong C_4$ or V_4.

$G/H = \{ (e,e)H, (x,e)H, (x,y)H, (x,y^2)H \}$

$(e,e)H = \{ (e,e), (x,y^3), (x^2, y^2), (x^3, y) \}$

$(x,e)H = \{ (x,e), (x^2, y^3), (x^3, y^2), (e, y) \}$

$(x,y)H = \{ (x,y), (x^2, e), (x^3, y^3), (e, y^2) \}$

$(x,y^2)H = \{ (x, y^2), (x^2, y), (x^3, e), (e, y^3) \}$

Note: (x,e) has order 4 in G, and $((x,e)H)^2 = (x^2, e)H = (x,y)H \ne (e,e)H$.

Therefore $(x,e)H \in G/H$ has order dividing 4, but it does not have order 2 or 1, so it has order 4.

Conclusion: $G/H \cong C_4$, and $G/H \cong \langle (x,e)H \rangle$.

4) $G = S_n$, $H = A_n$. $(n \geq 2)$

- $H \trianglelefteq G$: ✓

  even — both odd or both even

  $\forall g \in G$ and $h \in H$, ghg^{-1} is even, so $ghg^{-1} \in H$

- $|A_n| = \frac{|S_n|}{2} \Rightarrow |S_n : A_n| = |S_n/A_n| = \frac{|S_n|}{|A_n|} = 2$

  $\Rightarrow S_n/A_n \cong C_2$.

- $S_n/A_n = \{eA_n, (1\,2)A_n\} \Rightarrow S_n/A_n = \langle (1\,2)A_n \rangle$.

  $(1\,2) \notin A_n \Rightarrow eA_n \neq (1\,2)A_n$

5) $G = Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, $H = \langle -1 \rangle = \{\pm 1\}$.

- $H \trianglelefteq G$: ✓

  $\forall h \in H$, $g \in G$, $gh = hg \Rightarrow ghg^{-1} = h \in H$

- $|G:H| = |G|/|H| = 4 \Rightarrow G/H \cong C_4$ or V_4.

- $G/H = \{H, iH, jH, kH\}$

  $H = \{\pm 1\}$, $iH = \{\pm i\}$, $jH = \{\pm j\}$, $kH = \{\pm k\}$

Note: $(iH)^2 = (jH)^2 = (kH)^2 = (-1)H = H$

$\Rightarrow iH$, jH, and kH have order 2 in G/H

$\Rightarrow G/H \cong V_4$.

6) $G = S_4 = \langle (1\,2), (1\,2\,3\,4) \rangle$

$H = \langle (1\,2)(3\,4), (1\,3)(2\,4) \rangle = \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$

$$\big((1\,2)(3\,4)\big)\big((1\,3)(2\,4)\big) = (1\,4)(2\,3) = \big((1\,3)(2\,4)\big)\big((1\,2)(3\,4)\big)$$

- $H \trianglelefteq G$: ✓

$$(1\,2)\big((1\,2)(3\,4)\big)(1\,2)^{-1} = (1\,2)(3\,4) \in H$$

$$(1\,2\,3\,4)\big((1\,2)(3\,4)\big)\overbrace{(1\,2\,3\,4)^{-1}}^{=(4\,3\,2\,1)} = (1\,4)(2\,3) \in H$$

$$(1\,2)\big((1\,3)(2\,4)\big)(1\,2)^{-1} = (1\,4)(2\,3) \in H$$

$$(1\,2\,3\,4)\big((1\,3)(2\,4)\big)\overbrace{(1\,2\,3\,4)^{-1}}^{=(4\,3\,2\,1)} = (1\,3)(2\,4) \in H$$

- $|G:H| = |G/H| = |G|/|H| = 4!/4 = 6 \implies G/H \cong C_6$ or S_3.

- G/H:

Note that

$$\big((1\,2\,3)H\big)\big((1\,2)H\big) = \big((1\,2\,3)(1\,2)\big)H = (1\,3)H$$

$$= \{(1\,3), (1\,3)\big((1\,2)(3\,4)\big), (1\,3)\big((1\,3)(2\,4)\big), (1\,3)\big((1\,4)(2\,3)\big)\}$$

$$= \{(1\,3), (1\,2\,3\,4), (2\,4), (1\,4\,3\,2)\}, \text{ but}$$

$$\big((1\,2)H\big)\big((1\,2\,3)H\big) = \big((1\,2)(1\,2\,3)\big)H = (2\,3)H \neq \big((1\,2\,3)H\big)\big((1\,2)H\big),$$

since $(2\,3) \notin \big((1\,2\,3)H\big)\big((1\,2)H\big)$.

Therefore G/H is non-Abelian, so $G/H \cong S_3$.