

Factor Groups

Definition: Let G be a group and H be a normal subgroup. Let G/H be the set of left cosets of H in G . Introduce a multiplication on left cosets by the rule

$$(aH)(bH) = abH.$$

$\uparrow \quad \uparrow$

$$\# G/H = \frac{\# G}{\# H}$$

Lagrange's Theorem

$$G = S_3$$

$$H = \{e, r, r^2\}$$

$$G/H = \left\{ \begin{array}{l} H \\ sH \end{array} \right. \quad 2 \text{ sets}$$

$$H \cdot H = H$$

$$sH \cdot sH = s^2 H = eH$$

$$eH \cdot sH = sH = sH \cdot eH.$$

$$(H = eH)$$

$$(eH)(eH) = eH$$

G/H	eH	eH	sH	$\cong \mathbb{Z}_2$
	sH	sH	eH	

Proposition: If G is a group and H is a normal subgroup, the operation on cosets given by $(aH)(bH) = (ab)H$ is well-defined and makes the set

$$\boxed{G/H}$$

of cosets into a group. The identity element is H and the inverse of aH is $a^{-1}H$.

$$(aH)(eH) = eH \cdot aH = eaH = aH$$

$$(aH)(a^{-1}H) = eH \quad a^{-1}H \text{ looks like inverse.}$$

$$H = eH = hH \text{ for any } h \in H.$$

$$xH = yH \Rightarrow x = yh$$

$$\Leftrightarrow xH \cap yH \neq \emptyset$$

$$G = S_3 \quad H = \{e, r, r^2\}$$

$$sH = rsH$$

$$sH \cap rsH = \{rs\}$$

$$rs = sr^{-1} \quad r^{-1} \in H$$

$$rs \in sH \quad sr^{-1} \in sH$$

$$e \in rsH$$

$$(sH)(rsH) = srsH$$

$$srsH = H$$

$$r^{-1}H = H$$

$$rsH = sH$$

$$(sH)(rsH) = sH \cdot sH = s^2H = H$$

well-defined

$$\begin{bmatrix} aH = bH \\ cH = dH \end{bmatrix}$$

$$(aH)(cH) = acH \stackrel{?}{=} bdH$$

$$cH = bH \text{ means } c = bh_1, \quad h_1, h_2 \in H.$$

$$cH = dH \text{ means } c = dh_2$$

$$acH = \underbrace{bh_1, dh_2}_{H}H = bh_1dH = bh_1(Hd)$$

$$= \underbrace{bh_1H}_d$$

$$= \underbrace{bd}_H$$

$$= bdH$$

$$Hd = dH$$

since H normal

Basic Examples

- $G = \underline{\mathbb{Z}}$ and $H = \underline{n\mathbb{Z}}$. $n > 1$

G abelian, H is normal.

cosets of H are $a+n\mathbb{Z}$ $0 \leq a \leq n-1$

$$\underline{a+n\mathbb{Z}} \cap \underline{a'+n\mathbb{Z}} = \emptyset \quad \text{if } a \not\equiv a' \pmod{n} \quad [\text{division algorithm}]$$

$$\underline{a+n\mathbb{Z}} = \underline{a'+n\mathbb{Z}} \quad \text{if } a \equiv a' \pmod{n}.$$

So G/H has n cosets $n\mathbb{Z}, 1+n\mathbb{Z}, \dots, n-1+n\mathbb{Z}$

$$(a+n\mathbb{Z}) + (b+n\mathbb{Z}) = (a+b) + n\mathbb{Z}.$$

$n = 7$

$$\begin{aligned} (5+n\mathbb{Z}) + (6+n\mathbb{Z}) &= 11+n\mathbb{Z} = 11+7\mathbb{Z} \\ &= 4+7\mathbb{Z} \\ (5+7\mathbb{Z}) + (6+7\mathbb{Z}) &= 4+7\mathbb{Z}. \end{aligned}$$

$$(a+n\mathbb{Z}) + (b+n\mathbb{Z}) = (a+b) + n\mathbb{Z}$$

where $a+b \equiv a+b \pmod{n}$.

$$[a] = a+n\mathbb{Z}$$

$$[b] = b+n\mathbb{Z}$$

$$[c] = [c] \Leftrightarrow a \equiv c \pmod{n}$$

$$[b] = [d] \Leftrightarrow b \equiv d \pmod{n}$$

$$[c] = c+n\mathbb{Z}$$

$$[d] = d+n\mathbb{Z}$$

$$[a+c] = [b+d]$$

if $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$ then $a+b \equiv c+d \pmod{n}$.

- $G = \mathbb{Z}_n$ and $H = d\mathbb{Z}_n$ where d is a divisor of n .

$$G = \mathbb{Z}_n \quad d \text{ is a divisor of } n. \quad n \geq 2$$

$$\langle d \rangle = \{0, d, 2d, \dots\} \subseteq \mathbb{Z}_n \quad d\mathbb{Z}_n$$

what is G/H .

$$G = \mathbb{Z}_6 \quad d = 2 \quad \langle d \rangle = \{0, 2, 4\} = H$$

$$|G| = 6 \quad |\langle d \rangle| = 3$$

$$\langle d \rangle = H$$

$$1+H = 1+\langle d \rangle = \{1, 3, 5\}.$$

$$\langle d \rangle \cong \mathbb{Z}_3 \subseteq \mathbb{Z}_6$$

$$\mathbb{Z}_6 / \langle d \rangle = \mathbb{Z}_2.$$

$$G = \mathbb{Z}_n \quad \langle d \rangle = \{0, d, 2d, \dots, (\frac{n}{d}-1)d = nd-d\}$$

$\langle d \rangle$ has n/d elements

$G/\langle d \rangle$ must have d elements.

$$\left. \begin{array}{l} \langle d \rangle \\ 1+\langle d \rangle \\ \vdots \\ (d-1)+\langle d \rangle \end{array} \right\} d \text{ cosets}$$

they are all different.

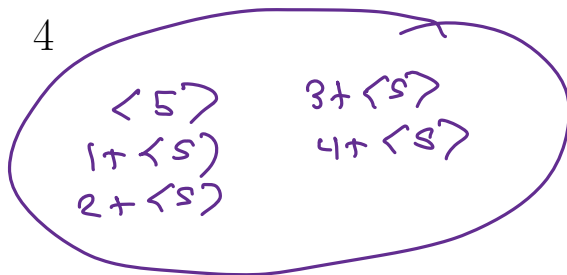
$$(i+\langle d \rangle) + (j+\langle d \rangle) \quad i, j \in \mathbb{Z}_n$$

$$= i+j + \langle d \rangle$$

$$\mathbb{Z}_n / \langle d \rangle = \mathbb{Z}_d$$

\uparrow
 n/d elts.

$$\mathbb{Z}_{20} / \langle 5 \rangle = \mathbb{Z}_5$$



- $G = D_n$, for $n \geq 3$, and H is the subgroup of rotations.

G has $2n$ elements H has n elts.

G/H has 2 elements.

$$H = \{e, r, \dots, r^{n-1}\}$$

$$sH = \{s, sr, \dots, sr^{n-1}\}$$

$$H \cdot H = H, \quad H \cdot sH = sH \cdot H = sH; \quad sH \cdot sH = H.$$