

Definition: order

Let G be a group and let $a \in G$. The **order** of a is the number of elements in $\langle a \rangle$. Alternatively, the **order** of a is the smallest $n > 0$ such that $a^n = e$ or ∞ if no such n exists. We denote the order of a by $|a|$.

1 Cosets and Lagrange's Theorem

See iPad screenshots for what cosets look like. We cut G into pieces and each is the same size as H . This forms a partition of G . None of them are empty, intersection is empty, and union is the whole group. Only one can be a subgroup since identity can only exist in one of them.

Definition

G is a group, $H \leq G$. Define a relation, \sim_L , on G , such that $a \sim_L b \Rightarrow a^{-1}b \in H$ (where the inverse has to be on the left).

WLOG everything below are similar for right cosets.

Theorem

\sim_L is an equivalence relationship.

Proof

- (i) Reflexive: need $a \sim_L a$ for $a \in G$. $a^{-1}a = e \in H$ since H is a subgroup.
- (ii) Symmetric: if $a \sim_L b$, then $b \sim_L a$. Since $a^{-1}b$ and $b^{-1}a$ are inverses. Since H is closed under inverses, hence $b^{-1}a \in H$.
- (iii) transitive: If $a \sim_L b$ and $b \sim_L c$, then $a \sim_L c$. If $a^{-1}b \in H$ and $b^{-1}c \in H$, then $a^{-1}bb^{-1}c = a^{-1}c \in H$ since H is closed under operation.

□

Note. We used all necessary conditions of a subgroup for the above proof.

What is $[a]$, the equivalence class of a ?

$$[a] = \{g \in G : a \sim_L g\}.$$

$a \sim_L g$ means $a^{-1}g \in H \Leftrightarrow a^{-1}g = h \in H \Leftrightarrow g = ah, h \in H$. Then

$$[a] = \{ah : h \in H\} := aH.$$

Definition: cosets

Group G and subgroup $H \leq G$. The **left cosets of H in G** is $aH = \{ah : h \in H\}$. The **right cosets of H in G** is $Ha = \{ha : h \in H\}$.

Property. • Left cosets of H partition G . (Any two left cosets are equal or disjoint).

- $xH = yH$ does **NOT** mean that $x = y$!!!!
- Consider $xH = \{xh : h \in H\}$. Then xH contains x because $e \in H$. So xH is the left coset containing x . No other coset of H does because they form a partition of G .
- $eH\{eh : h \in H\} = H$. So H is one of the left cosets.
- there is a bijection between H and xH . Can always multiply by x^{-1} to undo it. This means that any two left cosets have the same size, and any two right cosets have the same size.
- there is a bijection between left cosets of H and right cosets of H . We can just take inverses of each element in the left coset:

$$\begin{aligned} xH &= \{xh : h \in H\} \\ &= \{h^{-1}x^{-1} : h \in H\} \\ &= \{hx^{-1} : h \in H\} \\ &= Hx^{-1} \end{aligned}$$

This is a bijection. So there are same number of left cosets as right cosets.

Question: What is the condition for x and y to be in the same cosets. Answer: $x \sim y$.

Theorem

$$xH = yH \Leftrightarrow x^{-1}y \in H \text{ and } Hx = Hy \Leftrightarrow xy^{-1} \in H.$$

Theorem: Lagrange's Theorem

Let G be a finite group and let $H \leq G$. Then $|G|$ is equal to $|H|$ times the number of cosets of H in G .

See iPad for picture. Each set has the same size and together they form a partition.

Theorem

$|H|$ divides $|G|$.

$H \leq V_4$: H cannot have size 3 because 3 cannot divide 4.

Note. The converse of Lagrange's Theorem is false.

Example. A_4 is a group of order $4!/2 = 12$. But A_4 has no subgroup of order 6, although Lagrange's Theorem allows it. This is the smallest example for this.

Example. D_6 has order 12 and does have a subgroup of order 6 which are the rotations.

Question: Is D_6 isomorphic to A_4 ? No. Because they have a structural difference described above.

Definition: index

Let G be a group and $H \leq G$. The **index of H in G** is the number of cosets of H in G . We denote this by $|G : H|$ or $\{G : H\}$ or $(G : H)$.

So Lagrange's Theorem implies $|G| = |H| \times \{G : H\}$.

Example (infinite group). $G = \mathbb{Z}$ and $H = 3\mathbb{Z}$.