29 Aug 2025

Obs $H \leq G$, $K \leq G$ (subgr).

Then $H \cup K$ is not necessarily a subgr. of G.

(*Example*: $2\mathbb{Z} \cup 3\mathbb{Z}$ not a subgr. of $\mathbb{Z}$
$2+3 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$)

$H \vee K := \langle H \cup K \rangle$

Cyclic groups

G group. is called cyclic if there exists $a \in G$ st.

$\langle a \rangle = G$ (so $G = \langle a^n \mid n \in \mathbb{Z} \rangle$)

Ex $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$

Prop G cyclic, $H \leq G \Rightarrow H$ cyclic. (see 420/620)

Prop (a) Every infinite cyclic group is isomorphic to $\mathbb{Z}$.

(b) Every *finite* cyclic group is isom to $\mathbb{Z}_n$, where $n = |G|$ (number of elts of G)

(see 420/620)

Def G group, $x \in G$

$|x|$ or $\operatorname{ord}(x) = |\langle x \rangle|$ (finite or infinite).

Obs If $\operatorname{ord}(x) = n$ (finite), then $\operatorname{ord}(x)$ is the smallest positive integer k st $x^k = e$

$$\langle x \rangle = \{e, x, x^2, x^3, \dots, x^{k-1}\}$$

Prop $k = \operatorname{ord}(x)$, $x^n = e$. Then $k \mid n$

Proof: $n = kq + r$, $0 \le r < k$.

Then $x^r = x^n \cdot (x^{-q})^k = x^n \cdot (x^k)^{-q} = e$

Thus $r = 0$ $\square$

Cosets Set up $H \le G$ (subgr.)

We define equiv. relations:

$\boxed{\equiv_\ell \pmod H}$ $\quad a \equiv_\ell b \iff a^{-1} \cdot b \in H$

- $\boxed{\equiv_r \pmod{H}}$ $\quad a \equiv_r b \Leftrightarrow ab^{-1} \in H$

One can check that <u>both</u> are equiv. rel.

For $\boxed{\equiv_\ell}$, $[a]_\ell = \{ b \in G \mid a \equiv_\ell b \}$

$$= \{ b \in G \mid a^{-1} b \in H \}$$

$$= \{ b \in G \mid b \in aH \} = aH \text{ (left coset)}$$

Similarly, for $\boxed{\equiv_r}$,

$$[a]_r = Ha \text{ (right coset)}$$

Also there exist bijections

$$H \longleftrightarrow aH \longleftrightarrow Ha$$

$$h \longleftrightarrow ah \longleftrightarrow ha$$

$(G/H)_{\equiv_l} = \{aH \mid a \in G\}$

$(G/H)_{\equiv_r} = \{Ha \mid a \in G\}$

There exists a bijection

Notation $[G:H]$ = the common cardinality

$$(G/H)_{\equiv_l} \rightsquigarrow (G/H)_{\equiv_r}$$

$$aH \longrightarrow Ha^{-1} \quad \text{(well defined map)}$$

$$b^{-1}H \longleftarrow Hb$$

<u>Theorem</u> $K \leq H \leq G$. Then

$$[G:K] = [G:H] \cdot [H:K]$$

<u>Proof</u> $G = \underbrace{\bigcup_{i \in I} Ha_i}_{\text{mutually disjoint}}$, $|I| = [G:H]$

$H = \underbrace{\bigcup_{j \in J} Kb_j}_{\text{mutually disjoint}}$, $|J| = [H:K]$

Then $\boxed{G = \bigcup_{(i,j) \in I \times J} K(b_j a_i)}$ mutually disjoint (*)

We prove that these cosets are mutually disjoint.

$Kb_j a_i = Kb_k a_l \Rightarrow b_j a_i = \underset{\in K}{\alpha} b_k a_l$

Then $Ha_i = \underbrace{(Hb_j)}_{= H} a_i = H \underbrace{\alpha b_k}_{\in H} a_l = Ha_l$. So $i = l$

Then $Kb_j a_i = Kb_k a_i \Rightarrow Kb_j = Kb_k$, so $j = k$.

Thm $[G:K] = |I \times J| = |I| \cdot |J| = [G:H] \cdot [H:K]$ $\boxtimes$

Corollary $H \leq G$. Then

$$|G| = [G:H] \cdot |H|$$

Proof Take $K = \{e\}$ in prev. theorem.

Cor $H \leq G$. Then $|H|$ divides $|G|$.

Corollary $x \in G$. Then $\text{ord}(x)$ divides $|G|$.

Proof Take $H = \langle x \rangle$

Theorem $H, K \leq G$, $\underbrace{HK}_{\text{not necessarily a subgroup of } G} = \{hk \mid h \in H, k \in K\}$

Assume H, K are finite.

Then $|HK| = \dfrac{|H|\cdot|K|}{|H\cap K|}$

<u>Proof</u> $L = H\cap K \leq G$, $L \leq K$

$K = \bigcup_{i=1}^{n} L k_i$ (mutually disj.) where $n = [K:L]$

Then $HK = \bigcup_{i=1}^{n} \underbrace{HL}_{\substack{\| \leftarrow L\subseteq H \\ H}} k_i = \bigcup_{i=1}^{n} H k_i$ disjoint union

because

$H k_i = H k_j \Rightarrow k_i \cdot k_j^{-1} \in H \Rightarrow k_i \cdot k_j^{-1} \in H\cap K = L$

$\Rightarrow L k_i = L k_j$, so $i = j$.

Thus $|HK| = |H|\cdot n = |H|\cdot[K:L] = |H|\cdot\dfrac{|K|}{|L|}$

$= \dfrac{|H|\cdot|K|}{|H\cap K|}$ ☒