85ERP ① 9/1

Order of Group G

$|G| = n$ finite $n \in \mathbb{N}$

$= \infty$ infinite

Order of element $g \in G$

$|g|$ is least $n \cdot \ni \cdot g^n = e_G$

Example $\mathbb{Z}_4$

$|\mathbb{Z}_4| = 4$ $\{0,1,2,3\}$

$2 \in \mathbb{Z}_4$ $2+2 \pmod 4) = 0$ (identity)

so $|2|$ (in $\mathbb{Z}_4$) is 2.

Why does every element in a finite group have its order defined.

Given $\langle G, * \rangle$, to find the order of g

$g * g * \cdots g = g^n$ where n is order of G.

$$g \cdots g^k \cdots g^n * g = g^{\underline{n+1}}$$

Suppose $g^k = g^{n+1}$

$$e_G = g^{n+1-k} = \underbrace{g^{n-k}}_{\text{must be } g^{-1}} \cdot g$$

Subgroup:

Given $\langle G, * \rangle$ and $H \subseteq G$, if $\langle H, * \rangle$ satisfies group axioms, it is called a subgroup of G. $G \geq H$ or $H \leq G$

Note $H \leq G$ means $H = G$ is possible

Then H is called the <u>improper</u> subgroup and $\{0\}$ or more generally $\{e_G\}$ is the trivial subgroup.

If $H \leq G$

Q: Is $e_G = e_H$

Yes: Pf: Pick $h \in H$, h also $\in G$

$\underline{e_H} h = h \quad \underline{e_G} h = h$

So $e_H h = e_G h$.

$e_H \underline{h h^{-1}} = e_G \underline{h h^{-1}}$

$e_H \underline{e_H} = e_G \underline{e_H}$

$e_H = e_G$ ∎

1-step subgroup test:

Let G be a group and $H \neq \emptyset$ with $H \subseteq G$.

If $\underline{ab^{-1}} \in H$ whenever $a, b \in H$, then $H \leq G$.

NB: $\underline{a - b}$ is ab^{-1} if known abelian.

Pf

(i) Establish associativity - inherited

(ii) Establish a & a $\quad aa^{-1} = e \in H < G$

(iii) Establish inverses pick $a = e_G$ &

b arbitrary element in H, then test

says $e_G b^{-1} = b^{-1} \in H$

(iv) Operation is <u>closed</u>. Must show $\forall a, b \in H$

$ab \in H$. We know $b^{-1} \in H$, so $a(b^{-1})^{-1} \in H$

so $\underline{ab} \in H$.

Ex: We know $\langle \mathbb{Z}, + \rangle$ is a group

Is $2\mathbb{Z} < \mathbb{Z}$

Property defining subgroup

① Identify property: evenness

② Verify identity present
yes, $0 \in 2\mathbb{Z}$

→ ③ Assume $a, b \in 2\mathbb{Z}$

$a = 2n$, $b = 2m$

Check 1-step test: is $a - b \in 2\mathbb{Z}$

$2n - 2m = 2(n-m) \in 2\mathbb{Z}$

Automatic subgroups:

If G is a group and $g \in G$

then $\{g^k : k \in \mathbb{N}\} \leq G$

Ex $n\mathbb{Z} \leq \mathbb{Z}$

D_{2n} . .

Zentrum

Center of group G is written $Z(G)$

Centralizer of $g \in G$ is everything that

commutes with it.