MATH 171 : CLASS 3

DAMANIK/ARP

TODAY! SUBGROUPS + CYCLIC GROUPS

RECALL: A SUBSET $H \subseteq G$ OF A GROUP $(G, *)$ IS A SUBGROUP OF G, DENOTED $H \leq G$, IF $(H, *)$ IS ALSO A GROUP.

NOTE! WE REQUIRE THAT H IS A GROUP UNDER THE SAME OPERATION AS G.

EX! $\mathbb{Z}_4 = \{0,1,2,3\}$ $\quad \mathbb{Z}_2 = \{0,1\}$

$\mathbb{Z}_2 \leq \mathbb{Z}_4$

$0+0=0 \quad 0+1=1 \quad 1+1=0$

+	0	1
0	0	1
1	1	0

EX: THE CENTER OF G, $Z(G) \leq G$ FOR ANY GROUP. (PROVED IN HW USING THE FOLLOWING THM)

THM A SUBSET $H \subseteq G$ IS A SUBGROUP

IFF (1) $e \in H$ IDENTITY

(2) $h_1, h_2 \in H \Rightarrow h_1 h_2 \in H$ CLOSURE UNDER MULT.

(3) $h \in H \Rightarrow h^{-1} \in H$ CLOSURE UNDER INVERSES

PF: ($\Rightarrow$) SUPPOSE $H \leq G$. WE SHOW (1), (2), (3) HOLD.

SINCE H IS A GP, IT HAS AN IDENTITY ELEMENT, CALL IT e_H. THEN $e_H \in G$ (AS $H \subseteq G$).

SO
$$e_H \cdot e = e \cdot e_H = e_H$$

ALSO $e_H \cdot e_H = e_H$. THUS
$$e \cdot e_H = e_H \cdot e_H$$
THUS BY RIGHT (OR LEFT) CANCELLATION
$$e = e_H.$$

(2) HOLDS SINCE H IS A GROUP AND HENCE ITS BINARY OPERATION IS CLOSED.

TO SHOW (3), SUPPOSE $h \in H$. WE KNOW $h^{-1} \in G$ AND WANT TO SHOW $h^{-1} \in H$. BUT H IS A GROUP AND $h \in H$, SO h HAS AN INVERSE IN H. CALL IT h'. THEN

$$h \cdot h^{-1} = h^{-1} h = e$$

AND

$$h h' = h' h = e$$

THUS

$$h' = h'e = h' h h^{-1} = e h^{-1} = h^{-1}.$$

THEREFORE $h^{-1} \in H$.

($\Leftarrow$) NOW SUPPOSE (1), (2), (3) HOLD. WE MUST SHOW H IS A GROUP. BUT THE AXIOMS OF A GROUP ARE JUST (1), (2), (3) AND ASSOCIATIVITY. BUT ASSOCIATIVITY HOLDS IN H B/C IT HOLDS IN G.

Q.E.D.

THM: LET $H \subseteq G$ BE A SUBSET. THEN $H \leq G$ IFF $H \neq \emptyset$ AND $a, b \in H \Rightarrow ab^{-1} \in H$.

PF: ($\Rightarrow$) SUPPOSE $H \leq G$. LET $a, b \in H$. THEN $b^{-1} \in H$. THUS $ab^{-1} \in H$ BY CLOSURE.

($\Leftarrow$) WE USE THE PREVIOUS THM.

(1) SUPPOSE $H \neq \emptyset$ AND $a, b \in H \Rightarrow ab^{-1} \in H$.

$H \neq \emptyset$, SO LET $a \in H$. THEN $a \cdot a^{-1} \in H$ SO $e \in H$

(2) LET $a, b \in H$. WE ALSO HAVE $e \in H$.

THUS $e, b \in H \Rightarrow eb^{-1} = b^{-1} \in H$. THUS

$a, b^{-1} \in H \Rightarrow a(b^{-1})^{-1} = ab \in H$.

(3) AS ABOVE, $a \in H \Rightarrow e, a \in H \Rightarrow ea^{-1} = a^{-1} \in H$.

QED

Ex: $G_1 = GL_n(\mathbb{R})$ $\quad G_2 = GL_n(\mathbb{C})$

- $H_1 = \{A \in G_1 \mid AA^T = I\}$ $\quad (O(n)$ ORTH. GP$)$
- $H_2 = \{A \in G_1 \mid |A| = 1\}$ $\quad (SL_n(\mathbb{R})$ SPEC. LIN. GP$)$
- $H_3 = \{A \in G_1 \mid A + A = 0\}$
- $H_4 = \{A \in G_2 \mid |A| = 1\}$ $\quad (SL_n(\mathbb{C}))$
- $H_5 = \{A \in G_2 \mid AA^* = I\}$ $\quad (U(n)$ UNITARY$)$

  CONJUGATE TRANSPOSE
- $H_6 \leq GL_n(\mathbb{H}) = \{A \mid AA^* = I\}$ $\quad (Sp(n)$ SYMPLECTIC GP$)$

$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$

$A^* =$ QUATERNION CONJUGATE TRANSPOSE

$\overline{a + bi + cj + dk} = a - bi - cj - dk$