wednesday 22^ND October 2008 MATH2003 - Group Theory

Subgroups

§4 Subgroups and Generators

$A_n \subseteq S_n$ Composition of permutations $D_n \subseteq S_n$

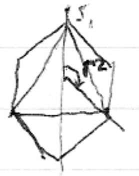
$(\mathbb{Z},+) \subseteq (\mathbb{Q},+) \subseteq (\mathbb{R},+), \ldots$ $[(\mathbb{Z}^*,\cdot) \subseteq]$ $(\mathbb{Q}^*,\cdot) \subseteq (\mathbb{R}^*,\cdot)$

not a group.

Definition 4.1 Let $(G,*)$ be a group and S be a subset. If $\forall a,b \in S$ also $a*b \in S$, then we say S is closed under the group operation of G. The binary operation thus defined on S is called the induced operation.

Example: Addition $\mathbb{Q} \Rightarrow$ addition in $\mathbb{Z}$ is induced.

$2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$ is closed under addition (in general $(m\mathbb{Z},+)$).

$D_3 \subseteq D_6$  $D_6 = \{1, r, \ldots, r^5, s_1, \ldots, s_6\}$ $D_3 = \{1, r^2, r^4, s, s_3, s_5\}$.

D_3 closed under composition on symmetries.

Definition 4.2 Let H be a subset of a group $(G,*)$. If H is closed under the binary operation $*$ and $(H,*)$ is a group. Then we say H is a subgroup of G.

Notation: $H \leqslant G$ $(G \geqslant H)$.

$H < G$ (or $H \lneqq G$) if $H \leqslant G$ and $H \neq G$ Say H is a proper subgroup.

$G \leqslant G$ always $\{e\} \leqslant G$ always $(G2 \Rightarrow ee = e)$

$\{e\}$ is the trivial subgroup.

Examples 4.3 : a) $(\mathbb{Z},+) \lneqq (\mathbb{Q},+) \lneqq (\mathbb{R},+) \lneqq (\mathbb{C},+)$

b) $(\mathbb{Q}^*,\cdot) < (\mathbb{R}^*,\cdot) < (\mathbb{C}^*,\cdot)$

c) $(n\mathbb{Z},+) < (\mathbb{Z},+)$ $[n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$. d) $D_3 \lneqq D_6$.

e) $D_n \leqslant S_n$ [view elements of D_n as permutations of vertices, induced operation is composition]. f) $A_n \lneqq S_n$.

g) $V = \{e, \overset{a}{(12)(34)}, \overset{b}{(13)(24)}, \overset{c}{(14)(23)}\} \lneqq S_4$ $|a| = |b| = |c| = 2$

essentially klein-4-group induced operation. Composition of permutations

$\Rightarrow V \lneqq A_4$ even $\mathrm{sign}(a) = \mathrm{sign}(b) = \mathrm{sign}(c) = 1$.

h) $G = \mathbb{Z}_6 = \{[0]_6, [1]_6, [2]_6, \ldots, [5]_6\}$ and $(\{[0]_6, [2]_6, [4]_6\}, +)$ is a subgroup of $\mathbb{Z}_6$ $[2]+[2]=[4]$ $[2]+[4]=[6]=[0]$ $[4]+[4]=[8]=[2]$ ...

$[2]^{-1} = [4]$ $[4]^{-1} = [2]$ (G3) (G2) $e = [0]_6$ (G1) inherited from $\mathbb{Z}_6$.

Theorem 4.4: A subset H of G is a subgroup of G if and only if the following two conditions hold: (S1) $\forall a,b \in H \Rightarrow ab \in H$ (i.e. H is closed under the induced operation)

(S2) $\forall a \in H \Rightarrow a^{-1} \in H$

"$\Rightarrow$"

Proof: Suppose H is a subgroup of G. Then by definition of subgroup H is closed under induced operation i.e. (S1) holds.

(G3) for $H \Rightarrow \forall a \in H\ \exists a^{-1} \in H$ and this is the same as a's inverse in G as inverses are unique.

"$\Leftarrow$"

Suppose $H \subseteq G$ and (S1) and (S2) hold. (S1) $\Leftrightarrow$ H is closed under the induced operation. Now check G1, G2, G3 for H:

(G1) $a, b, c \in H \Rightarrow a, b, c \in G$ and associativity holds in G, hence holds in H.

(G2) (S2) $\Rightarrow \forall a \in H$ also $a^{-1} \in H \xRightarrow{\text{(S1 and G3 for G)}} aa^{-1} = e_G \in H$.

G2 for $G \Rightarrow \forall a \in H\ ae_G = a = e_G a \Rightarrow$ (G2) holds in H.

(G3) is a restatement of (S2) $\square$

Examples 4.5: a) $G = GL_n(\mathbb{C})$ general linear group, group of invertible matrices over $\mathbb{C}$. Consider $H = \{A \in GL_n(\mathbb{C}) \mid \det A = 1\} \leqslant GL_n(\mathbb{C})$.

(S1) $A, B \in H$ $\det(AB) = \det A \det B = 1 \cdot 1 = 1 \Rightarrow$ (S1)

(S2) $\det A^{-1} = \frac{1}{\det A} = 1$ for $A \in H \Rightarrow A^{-1} \in H \Rightarrow$ (S2)

$H = SL_n(\mathbb{C})$ 'Special linear group'.

b) $D_6 = \{e, r, r^2, \dots, r^5, s_1, \dots, s_6\}$. $H = \{e, r, r^2, \dots, r^5\}$ is a subgroup of D_6:

(S1) $r^i r^j = r^{i+j}$ if $i+j \geqslant 6$ then $r^{i+j} = r^{i+j-6}$ for $i, j \in \{0, \dots, 5\}$.

(S2) $(r^i)^{-1} = r^{6-i}$.

$S = \{e, s_1, s_2, \dots, s_6\}$ is NOT a subgroup.

(S2) holds as $s_i^2 = e$ but (S1) fails e.g. $s_1 s_2 = r^5$

$D_n = \{e, r, \dots, r^{n-1}, s_1, s_2, \dots, s_n\}$ $s_i = r^{i-1}s$ $r^i s = s r^{n-i}$