Thursday 23rd October 2008 MATH2003 – Group Theory.

Subgroups

$H = \{a^n \mid n \in \mathbb{Z}\}$ G group $a \in G$

Theorem 4.6: G group, $a \in G$. The set $H = \{a^n \mid n \in \mathbb{Z}\}$ is a subgroup.
It is the smallest subgroup of G containing a.
(smallest subgroup: $\forall K \leq G$ s.t. $a \in K \Rightarrow H \leq K$).

Proof: (S1) $a^n \in H$ $a^m \in H \Rightarrow a^n a^m = a^{n+m} \in H$ $(n+m) \in \mathbb{Z}$. (S2) $(a^n)^{-1} = a^{-n} \in H$.
Need to show H smallest subgroup containing a. Let $K \leq G$, $a \in K$
S1 $\Rightarrow aa \in K \Rightarrow a^2 \in K$ ... inductively $\underbrace{a^{n-1}}_{\in K}\underbrace{a}_{\in K} = a^n \in K$ $\forall n > 0$
S2 $a^{-1} \in K$ as above inductively show $a^{-n} \in K$ $\forall n > 0$.
S1 $aa^{-1} \in K$ but $aa^{-1} = a^0 = e$ $\Rightarrow \{a^n \mid n \in \mathbb{Z}\} \leq K$. D

Definition 4.7: Let G be a group and let $a \in G$.
1) The group H of theorem 4.6 is called the cyclic subgroup of G generated by a. Write $H = \langle a \rangle$.
[$D_3 = \{e, r, r^2, s_1, s_2, s_3\}$ $r^{-1} = r^2$, $r^3 = r^0 = e$ $H = \langle r \rangle = \{r^0, r^1, r^2\}$

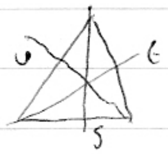
2) An element of G generates G, or is a generator of G, if $\langle a \rangle = G$.
3) If there is an element $a \in G$. s.t. $\langle a \rangle = G$ then we say G is a cyclic group.

Examples 4.8. a) $(\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$. Every element $x \in \mathbb{Z}$ can be written as $x \cdot 1$ $x > 0$ $x = 1 + \dots + 1$ $x < 0$ $x = -(1 + \dots + 1)$.
b). $(\mathbb{Z}_m, +) = \langle [1] \rangle$ e.g. $\mathbb{Z}_4 = \langle [1] \rangle = \langle [3] \rangle$ $\mathbb{Z}_5 = \langle [1] \rangle = \langle [2] \rangle = \dots$
c) $V = \{e, a, b, c \mid a^2 = b^2 = c^2 = e\}$ is NOT cyclic $\langle a \rangle = \{e, a\}$ etc...
d). Dihedral groups NOT cyclic $\langle r \rangle = \{e, r, \dots, r^{n-1}\}$, $\langle s_i \rangle = \{e, s_i\}$

Definition 4.9: Let G be a group and let $a_i \in G$ ($i \in I$, indexing set). The smallest subgroup of G containing $X = \{a_i \mid i \in I\}$ is the subgroup generated by X, written $H = \langle X \rangle$. If $G = \langle X \rangle$, we say G generated by X, or X generates G. a_i are the generators of G.

S1, S2 $a_i^{k_i} \in \langle X \rangle$ $\forall k_i \in \mathbb{Z}$ S2 $a_i^{k_i} a_j^{k_j} \in \langle X \rangle$ $\forall k_i, k_j \in \mathbb{Z}$.
$\langle X \rangle$ consists of all expressions of the form $a_{i_1}^{k_1} a_{i_2}^{k_2} \dots a_{i_m}^{k_m}$
$a_{i_j} \in X$, $k_j \in \mathbb{Z}$ $j = 1, \dots, m$.

Examples: a) D_3 is generated by s, r $t = rs$
$D_3 = \{e, r, r^2, s, rs, r^2 s\}$. $u = r^2 s$



in general $D_n = \{e, r, \dots, r^{n-1}, \underbrace{s, rs, \dots, r^{n-1}s}_{\text{order } 2}\}$.

b) $V=\{e,a,b,c \mid a^2=b^2=c^2\}$ is generated by a, b as $ab=c$
(a, c as $ac=b$, ...).

c) $(\mathbb{Q},+)$ is not finitely generated.

d) Cyclic groups are finitely generated, by 1 element.

G is finitely generated if $\exists\, |X|<\infty$ s.t. $G=\langle X\rangle$

Proposition 4.10: Let H, K be subgroups of G. Then $H\cap K$ is a subgroup.

proof S1) $a,b \in H\cap K \Rightarrow a,b\in H$ and $a,b\in K$

$\xRightarrow{\text{S1) for } H \text{ and } K}$ $ab\in H$ and $ab \in K \Rightarrow ab\in H\cap K$

S2) $a\in H\cap K \Rightarrow a\in H$ and $a\in K$ $\xRightarrow{\text{S2) for } H,K}$ $a^{-1}\in H$ and $a^{-1}\in K$

$\Rightarrow a^{-1}\in H\cap K$ $\square$.

Careful: $H\cup K$ is not necessarily a subgroup.

e.g. $V=\{e,a,b,c \mid a^2=b^2=c^2=e\}$.

$\langle a\rangle = H = \{e,a\}$ $\langle b\rangle = K=\{e,b\}$.

$H\cup K=\{e,a,b\}$ is NOT a subgroup S1) fails $ab=c\notin H\cup K$.

repair by using $\langle H,K\rangle$, the subgroup generated by H and K

$\langle H,K\rangle = \{ x_1^{k_1}x_2^{k_2}\dots x_n^{k_m} \mid x_i\in H \text{ or } x_i\in K \mid k_i\in\mathbb{Z}\}$.

⇝ Subgroup lattice