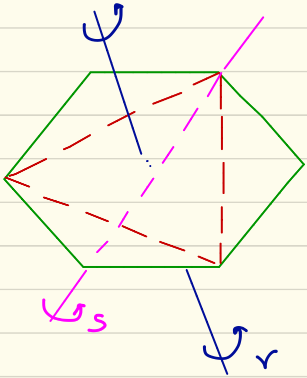
Leture 4 - Subgroups, generators, cyclic groups



Consider the following subset of the group D_6 (the symmetries of a regular hexagon $\{e, r^2, r^4, s, r^2s, r^4s\}$. Then notice that if you multiply any of these elements with each other you get another element within the set. The set is also closed under taking inverses. In other words it is a subset of D_6 which is a group by itself. In fact this group is the group of symmetries of the triangle within the hexagon as shown in the figure. This set is called subgroup of D_6.

Definition (Subgroup)

Let G be a group and $H \subseteq G$, then H is a subgroup of G (denoted by $H < G$) if

(i) $e \in H$

(ii) If $x, y \in H$ then $x * y \in H$

(iii) If $x \in H$ then $x^{-1} \in H$

Examples of subgroups:

1) $\mathbb{Z} < \mathbb{Q} < \mathbb{R}$ under addition
2) $\{e, r, r^2, \dots, r^{n-1}\}$ is a subgroup of D_n
3) The set of diagonal matrices with non-zero entries is a subgroup of $GL_n(\mathbb{R})$
4) In $\mathbb{Z}_6$ the set $\{0, 2, 4\}$ is a subgroup
5) $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ $ac \neq 0$ is a subgroup of $GL_2(\mathbb{R})$

6) Let G be a group and let $x \in G$ then the set $\langle x \rangle = \{x^m : m \in \mathbb{Z}\}$ is a subgroup.

$x^0 = e$, and x^{-m} is inverse of x^m, $x^k \cdot x^p = x^{k+p} \in$

The subgroup $\langle x \rangle$ is called the subgroup generated by x. If $\langle x \rangle$ has infinite order then $\langle x \rangle$ consists of elements $\ldots, x^{-2}, x^{-1}, e, x, x^2, \ldots$ If $\langle x \rangle$ has finite order n then $\langle x \rangle$ has elements $e, x, x^2, \ldots, x^{n-1}$.

If in a group G there exists an element a s.t. $\langle a \rangle = G$ then G is called a cyclic group generated by a.

Examples:

1) $\mathbb{Z}$ is an infinite cyclic group. Its generators are 1 and -1

2) $\mathbb{Z}_6$ is generated by 1 and 5. $\langle 1 \rangle = \langle 5 \rangle = \mathbb{Z}_6$. The subgroup generated by 2 is $\{0, 2, 4\}$.

3) In D_3

$\langle e \rangle = \{e\}$

$\langle r \rangle = \langle r^2 \rangle = \{e, r, r^2\}$

$\langle s \rangle = \{e, s\}$

$\langle rs \rangle = \{e, rs\}$

$\langle r^2 s \rangle = \{e, r^2 s\}$

We see that D_n is not cyclic but each of its elements can be written in terms of r and s, hence r and s together generate D_6.

If X is a subset of a group G then a word in the elements of X is of the form $x_1^{m_1} x_2^{m_2} \cdots x_k^{m_k}$ where each $x_i \in X$. The collection of all words is a subgroup of G. (check!). This subgroup is called the subgroup generated by X. If this is the entire group G then the set X is called the set of generators of G.

The set $\{r, s\}$ is the set of generators of D_6, so is [illegible] set $\{rs, s\}$ (since $rs.s = rs^2 = r$ so any word using [illegible] and s can be converted to a word using rs and s.

Theorem: Let H be a non-empty subset of a group G [illegible]en H is a subgroup of G iff xy^{-1} belongs to H whenever $x, y \in H$

Proof: $\Rightarrow$ Let $x, y \in H$, then since H is a subgroup $y^{-1} \in H$ and hence $xy^{-1} \in H$.

$\Leftarrow$ Since H is non-empty therefore $\exists$ an element $x \in H$ then (i) $e = xx^{-1} \in H$. (ii) If $x \in H$ then $x^{-1} = ex^{-1} \in H$. iii) Let x, $y \in H$ then from ii) $y^{-1} \in H$ and by the assumption $xy = x(y^{-1})^{-1} \in H$.

Theorem: Let H and K be two subgroups of G then $H \cap K$ is a subgroup. In general the intersection of subgroups is a subgroup.

Proof: Exercise

Theorem: Every subgroup of a cyclic group is cyclic.

Proof: Let G be a cyclic group with generator x. Let H be a subgroup of G. Since G is cyclic every element of H is of the form x^j for some $j \in \mathbb{Z}$. Let m be the smallest positive integer such that $x^m \in H$.

Claim: $\langle x^m \rangle = H$

Let x^k be any element of H, then

$$k = qm + r \quad \text{with} \quad 0 \le r < m$$

Then $x^k = x^{qm+r} = x^{qm} . x^r = (x^m)^q . x^r$

$$\underbrace{x^k}_{\in H} = \underbrace{(x^m)^q}_{\in H} \cdot x^r$$

Now $x^k \in H$ and $(x^m)^q \in H$ $\therefore$ $x^r = x^k \cdot (x^m)^{-q} \in H$ since H is a subgroup. But by assumption m is the smallest positive integer s.t. $x^m \in H$. This is a contradiction since $0 \leq r < m$. Therefore r must be zero. Therefore an arbitrary element of H can be written as $(x^m)^q$ for some q. Therefore $\langle x^m \rangle = H$ and H is cyclic.