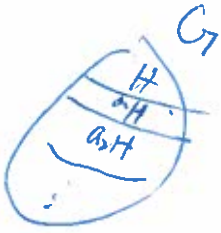
Recall

Suppose G – a group.

$H \leq G$ – a subgroup



If $|G| = n$, if $|H| = m$

then $m \mid n$

$|G:H| = \frac{n}{m}$ is the index of the subgroup H in G

Lagrange Theorem: If $|G| = n$, & $H \leq G$ with $|H| = m$

then $m \mid n$.

In general, for any G, and $H \leq G$

we can define $aH = \{ah : h \in H\}$

for every $a \in G$.

Then aH is an equivalence of the equivalence relation. $(a,b) \in R$ in G.

defined by $a^{-1}b \in H$.

$\therefore$ $G = \bigcup_{a \in G} aH$, i.e., left cosets formed a partition of G.

Next. we study other techniques of getting information of G by counting, or using the

Example 3 If $|G| = 2k$, $H \le G$, $|H| = k$.

then $aH = Ha$ $\forall a \in G$. (e.g. D_n dihedral group.)

Theorem 7.2 Let H, K be finite subgroups of a group. If $HK = \{hk : h \in H, k \in K\}$, then

$$|HK| = |H||K|/|H \cap K|.$$

(a set.) (may not be a subgroup.)

Proof: Note that $(h_1k_1) = (h_2k_2)$ is possible for $(h_1,k_1), (h_2,k_2) \in H \times K$

In general, $(h_1,k_1), (h_2,k_2) \in H \times K$.

$h_1k_1 = h_2k_2 \iff h_2^{-1}h_1 = k_2k_1^{-1} = x \in H \cap K$, i.e., $h_1 = h_2x$, $k_1 = x^{-1}k$ with $x \in H \cap K$

Quick check: If $(h_2,k_1) = (h_2x, x^{-1}k_2)$ then

$$h_1k_1 = (h_2x)(x^{-1}k_2) = h_2k_2.$$

Conversely, if $h_1k_1 = h_2k_2$, then $x = h_1^{-1}h_1 = k_2k^{-1} \in H \cap K$ satisfies $(h_1,k_1) = (h_2x, x^{-1}k_2)$.

∴ Every $(h,k) \in H \times K$ will generate m pairs of elements $(\hat{h}, \hat{k}^{-1})$ so that $hk = \hat{h}\hat{k}^{-1}$, where $m = |H \cap K|$.

∴ The total number of distinct elements in $\{hk : h \in H, k \in K\}$ equals (total number of pairs: (h,k), $|H||K|$ so many of them, divided by $|H \cap K|$.

Theorem 7.3 If G is a group with $|G| = 2p$ for a prime number $p > 2$, then G is isomorphic to the cyclic group $\mathbb{Z}_{2p}$ or the dihedral group D_p.

Proof Let $|G| = 2p$, $p > 2$ is a prime.

Case 1° If $G = \langle a \rangle$ is cyclic then $G \cong \mathbb{Z}_{2p}$

Case 2° Assume no element in G has order $2p$

Then every element in G has order: $1, 2, p$.

∴ It is impossible that all elements have order $1, 2$. i.e.,

"$x \in G \Rightarrow x^2 = e$" is impossible.

Reason: If it does, then for any $x, y \in G$,

$$xyxy = x(yx)y = (xy)^2 = e = x^2y^2 = xxyy$$

$$\therefore \quad yx = xy \text{ for all } x, y \in G.$$

Then $H = \{e, x, y, xy\}$ will be a subgroup of G

But $|H| = 4$ is not a factor of $2p$!!!

∴ There is $a \in G$ such that $|a| = p$.

Claim: There is an element of order 2.

If not, then all non-identity element has order p.

In particular, let $b \notin \langle a \rangle$ has order p.

Then each subgroup $K_1 = \langle a \rangle$, $K_2 = \langle b \rangle$ has p elements

and $K_1 \cap K_2 = \{e\}$

So $|K_1 K_2| = \frac{|K_1||K_2|}{|K_1 \cap K_2|} = \frac{p^2}{1} = p^2 \geq 2p = |G|$

So Thus we have $a, b \in G$, $|a| = p$, $|b| = 2$.

$G = \{e, a, \cdots, a^{p-1}, b, ba, \cdots, ba^{p-1}\}$.

Note $(ba)^2 = e$

$baba = e$

$ab = b^{-1}a^{-1} = ba^{-1}$

Construct the group table.

$*$	e	a	a^2	$\cdots$	a^{p-1}	b	ba	$\cdots$	ba^{p-1}
e									
a									
a^2									
$\vdots$									
a^{p-1}									
b									
ba									
$\vdots$									
ba^{p-1}									

$ba^i \cdot ba^j$

$= b^2 a^{-i} a^j$

$= a^{j-i}$

will be the same as that of D_p. $\therefore G \cong D_p$

Chapter 8 External Direct Products

Idea Decompose a large group into small subgroups, and combine several groups to form a larger group (to get desired or undesired properties).

Definition Let $(G_1, *_1), (G_2, *_2)$ be groups. The external direct product is

$$G_1 \oplus G_2 = \{(g_1, g_2) : g_1 \in G_1, g_2 \in G_2\}$$

under the entry-wise operations $(x_1, x_2) * (y_1, y_2) = (x_1 *_1 y_1, x_2 *_2 y_2)$.

One can extend the definition to $G_1 \oplus \cdots \oplus G_k$.

Examples Many ...

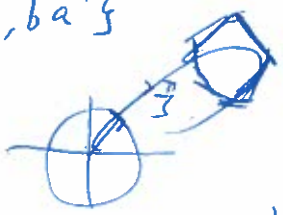
Example $G_1 = (\mathbb{Z}_{12}, +)$, $G_2 = (D_5, \circ)$

$G_1 \oplus G_2 = \{(k, \sigma) : k \in \mathbb{Z}_{12}, \sigma \in D_5\}$

$D_5 = \{e, a, \cdots, a^4, b, ba, ba^2, \cdots, ba^4\}$

$(\bar{3}, ba^4) * (\bar{7}, a^3)$

$= (\bar{10}, ba^5) = (10, b)$



a is the rotation of $\frac{2\pi}{5}$.

b reflection over x

b reflect about x-axis

$ab = ba^{-1}$

Example $G_1 = (\mathbb{Z}_4, +)$, $G_2 = (S_3, \circ)$

Consider $G_1 \oplus G_2$

$(\bar{9}, (2,3)) * (\bar{5}, (3,2,1))$

$= (\bar{2}, (1,2))$.

$\sigma \in S_3$ can be written as $\begin{pmatrix} 1 & 2 & 3 \\ i_1 & i_2 & i_3 \end{pmatrix}$,

or $\sigma = C_1 C_2$ (disjoint cycle)

or $\sigma = \tau_1 \tau_2 \tau_3 \cdots \tau_k$ (product of transposition)

$(2,3) \cdot (3,2,1)$

$= (1,2)$

Fact: $G_1 \oplus G_2$ is a group.

(G0) $\forall (g_1, g_2), (\hat{g}_1, \hat{g}_2) \in G_1 \oplus G_2$

then $(g_1, g_2) * (\hat{g}_1, \hat{g}_2) = (g_1 \hat{g}_1, g_2 \hat{g}_2) \in G_1 \oplus G_2$

(G1) Let $(g_1, g_2), (h_1, h_2), (k_1, k_2) \in G_1 \oplus G_2$

Then $\big((g_1, g_2) * (h_1, h_2)\big) * (k_1, k_2)$

$= \big((g_1 h_1), (g_2 h_2)\big) * (k_1, k_2)$

$= \big((g_1 h_1) k_1, (g_2 h_2) k_2\big)$

$= \big(g_1 (h_1 k_1), g_2 (h_2 k_2)\big)$

$= (g_1, g_2) * (h_1 k_1, h_2 k_2)$

$= (g_1, g_2) * \big((h_1, h_2) * (k_1, k_2)\big)$.

(G2) Let e_1, e_2 be the identities of G_1, G_2, resp.

Then $e = (e_1, e_2)$ satisfies

$e * (h_1, h_2) = (h_1, h_2) = (h_1, h_2) * e$

(G3) Let $(h_1, h_2) \in G_1 \oplus G_2$

Then $(k_1, k_2) = (h_1, h_2)^{-1} = (h_1^{-1}, h_2^{-1})$.

(h_1^{-1} in G_1, h_2^{-1} in G_2; φ inverse in $G_1 \oplus G_2$)

will satisfy $(k_1, k_2) * (h_1, h_2) = (e_1, e_2)$

$= (h_1, h_2) * (k_1, k_2)$.

By induction, $G_1 \oplus \cdots \oplus G_k$ is a group if $G_1, \ldots, G_k$ are.

Some basic results

Theorem 8.1 Let $g = (g_1, \ldots, g_k) \in G_1 \oplus \cdots \oplus G_k$. If $|g_1|, \ldots, |g_k|$ are finite, then $|g| = \text{lcm}(|g_1|, \ldots, |g_k|)$; if one of the $|g_i|$ is infinite, then $|g|$ is infinite.

n_1 $\quad$ n_k

Proof: Suppose $m = \text{lcm}(n_1, \cdots, n_k)$, $n_j = |g_j|$ $j = 1, \cdots, k$.

Then

$$(g_1, \cdots, g_k)^m = (g_1^m, g_2^m, \cdots g_k^m) = (e_1, \cdots, e_k)$$

$\because$ $n_j \mid m$ $\forall j = 1, \cdots, k$.

Assume $(g_1, \cdots, g_k)^d = (e_1, \cdots, e_k)$.

$\therefore$ $g_j^d = e_j$ $\forall j = 1, \cdots, k$

$\therefore$ $|g_j| \mid d$. $\therefore$ d is a common multiple of $n_1, \cdots, n_k$.

So $d \geq m$.

Hence m is the smallest positive integer such that $(g_1, \cdots, g_k)^m = (e_1, \cdots, e_k)$.

i.e., $|(g_1, \cdots, g_k)| = m$.

Theorem 8.2 Let $G_1, \ldots, G_k$ be finite cyclic groups. Then $G_1 \oplus \cdots \oplus G_k$ is cyclic if and only if $\gcd(|G_i|, |G_j|) = 1$ for all $1 \leq i, j \leq k$, equivalently, $\text{lcm}(|G_1|, \ldots, |G_k|) = \prod_{j=1}^{k} |G_j|$.

In particular, $\mathbf{Z}_{n_1 \cdots n_k} = \mathbf{Z}_{n_1} \oplus \cdots \oplus \mathbf{Z}_{n_k}$ if and only if $\gcd(n_i, n_j) = 1$ for all $i \neq j$.

Remark If $k > 1$ and one of the cyclic group G_i is infinite, then $G_1 \oplus \cdots \oplus G_k$ is not cyclic.

If one of g_i has infinite order, then

$$(g_1, \cdots, g_k)^n = (g_1^n, \cdots, g_i^n, \cdots g_k^n) \neq (e_1, \cdots, e_i, \cdots, e_k)$$

$\because$ $g_i^n \neq e_i$.

$\therefore$ $|(g_1, \cdots, g_k)|$ is infinite.