Lecture 8 : Products

Let G and K be groups. Consider the set $G \times K = \{(g,k) : g \in G \text{ and } k \in K\}$. Consider the operation on $G \times K$, if (g,k) and (g',k') are two elements of $G \times K$ then $(g,k)(g',k') = (gg', kk')$. <u>Claim</u>: $G \times K$ is a group under the operation just defined.

i) (e_G, e_K) is the identity since $(e_G, e_K)(g,k) = (e_G \cdot g, e_K k) = (g,k)$. Similarly. $(g,k)(e_G, e_K) = (g,k)$

ii) Associativity follows from associativity of groups G and K. $((g,k)\cdot(g',k'))\cdot(g'',k'')$
$= (g,k)\cdot((g',k')\cdot(g'',k''))$.

iii) For each $(g,k) \in G \times K$ $(g^{-1}, k^{-1})\cdot(g,k) = (g^{-1}g, k^{-1}k) = (e,e)$

Note the subsets of $G \times K$ given by $\{(g,e) : g \in G\}$ and $\{(e,k) : k \in K\}$ are subgroups that are isomorphic to G and K respectively. Eg $\mathbb{Z}_2 \times \mathbb{Z}_2$ is given by the elements $\{(0,0), (0,1), (1,0), (1,1)\}$. The group multiplication table is

	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)
(1,0)	(1,0)	(1,1)	(0,0)	(0,1)
(1,1)	(1,1)	(1,0)	(0,1)	(0,0)

Notice that this is not a cyclic group. Also this group is isomorphic to the group of symmetries of the chessboard and the group $\{1,3,5,7\}$ under multiplication modulo 8. Now look at the group $\mathbb{Z}_2 \times \mathbb{Z}_3$

	(0,0)	(0,1)	(0,2)	(1,0)	(1,1)	(1,2)
(0,0)	(0,0)	(0,1)	(0,2)	(1,0)	(1,1)	(1,2)
(0,1)	(0,1)	(0,1)	(0,0)	(1,1)	(1,2)	(1,0)
(0,2)	(0,2)	(0,0)	(0,1)	(1,2)	(1,0)	(1,1)
(1,0)	(1,0)	(1,1)	(1,2)	(0,0)	(0,1)	(0,2)
(1,1)	(1,1)	(1,2)	(1,0)	(0,1)	(0,2)	(0,0)
(1,2)	(1,2)	(1,0)	(1,1)	(0,2)	(0,0)	(0,1)

In this group $(1,1)+(1,1) = (0,2)+(1,1) = (1,0) + (1,1) = (0,1)+(1,1) = (1,2)+(1,+1) = (0,0)$
Hence $(1,1)$ is the generator of $\mathbb{Z}_2 \times \mathbb{Z}_3$ and this group is cyclic. This is a group of order 6 an by the previous lecture has to be isomorphic to $\mathbb{Z}_6$. Hence $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$ but $\mathbb{Z}_2 \times \mathbb{Z}_2 \ncong \mathbb{Z}_4$. We have the following thm.

<u>Theorem</u>: $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic iff $\gcd(m,n) = 1$.

<u>Proof</u>: $\Leftarrow$ if $\gcd(m,n) = 1$ then $\operatorname{lcm}(m,n) = mn$ since $\gcd(m,n)\operatorname{lcm}(m,n) = mn$
We claim that the element $(1,1)$ generates $\mathbb{Z}_m \times \mathbb{Z}_n$. Since mn is the $\operatorname{lcm}(m,n)$ mn is the smallest integer k such that $(1,1)+(1,1)+\cdots+(1,1) = (0,0)$. That is mn is smallest positive k such that $(1,1)^k = (0,0)$. Therefore $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic with $\langle(1,1)\rangle = \mathbb{Z}_m \times \mathbb{Z}_n$.

$\Rightarrow$ Since $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic of order mn there must be an element (x,y) such that $(x,y)^{mn} = (0,0)$ and mn is the smallest power that achieves this. But $(x,y)^{\operatorname{lcm}(m,n)} = \left(x^{\operatorname{lcm}(m,n)}, y^{\operatorname{lcm}(m,n)}\right) = \left(x^{k_1 m}, y^{k_2 n}\right)$ for some k_1, k_2. Therefore $(x,y)^{\operatorname{lcm}(m,n)} = \left((x^m)^{k_1}, (y^n)^{k_2}\right) = (e,e)$. Since mn was the smallest such power, this can only happen if $\operatorname{lcm}(m,n) = mn \implies \gcd(m,n) = 1$.