Notes for 27 March (Wednesday)

1 The road so far...

1. Proved some generation results for S_n.
2. Defined the sign of a permutation and A_n.
3. Proved that A_n is generated by 3 cycles (when $n \geq 3$).
4. Proved Lagrange's theorem.

2 Back to abstract groups...again

Unfortunately, the quotient set G/H does not always have an obvious group structure. Indeed, suppose we try to define $a.H``*"b.H$ as $a*b.H$, the problem is that if $a_1 * h_1 = a_2 * h_2$, then $a_1 * b * h$ need not be $a_2 * b * \tilde{h} = a_1 * h_1 * h_2^{-1} * b * \tilde{h}$ for some $\tilde{h}$. Here are examples and counterexamples :

1. For $G = \mathbb{Z}, +$ and $H = m\mathbb{Z}$, $G/H = \mathbb{Z}_m$ is a group.
2. More generally, if G is Abelian, then G/H is an Abelian group.
3. Consider $H = \{Id, (12)\}$ in $G = S_3$. Note that $(23)H(23) = \{Id, (13)\} \neq H$. So G/H is not a group.

To make G/H into a group, as discussed earlier, one needs to impose a condition on H : $H \subset G$ is said to be a normal subgroup if $gH = Hg \ \forall \ g \in G$.

Theorem 1. *If $H \subset G$ is a normal subgroup, then G/H is a group with the group operation defined as $a.H * b.H = (a * b).H$.*

Proof. This operation is well-defined (by the earlier calculations). Since $e.H * a.H = a.H * eH = a.H$, there is an identity element. $(a.H * b.H) * c.H = (a * b).H * c.H = (a * (b * c)).H = a.H * (b * c.H) = a.H * (b.H * c.H)$. Also, $a^{-1}.H * a.H = a.H * a^{-1}.H = eH = H$. □

For example, let $G = U_{21}$ the group of units mod 21 of order 12. Let $H = \{[1], [-1], [8], [-8]\}$ be the subgroup consisting of square roots of 1. Then $G/H = \{H, [2]H, [4]H\}$ and is a cyclic group.

The converse to Lagrange's theorem is not true : The group A_4 of size 12 has no subgroup of size 6.

Indeed, A_4 consists of e, cyclic decomposition of two cycles (4 of them forming a subgroup $V \equiv K_4$), and the 8 three cycles. Suppose $H \subset A_4$ is of size 6 and $H' = H \cap V$. By Lagrange's theorem, $|H'| = 1$ or 2. (To be continued...)