Notes for 21 March (Thursday)

1 The road so far...

1. Studied the Dihedral group D_n.
2. Defined and gave examples and non-examples of Dihedral groups.

2 Back to groups...

Note that as a consequence of every element of a finite group having a finite order,

Lemma 2.1. *If G is a finite group, a non-empty subset $H \subset G$ is a subgroup iff it is closed under group multiplication $*$.*

Also, here is another lemma about the existence of non-trivial subgroups.

Lemma 2.2. *If G is a finite Abelian group then G has a non-trivial subgroup unless its size n is 1 or a prime p.*

Proof. If n is not a prime or 1, then $n = rs$ for $r, s > 1$. For each $a \in G$ consider $\langle a \rangle$. If $\langle a \rangle \neq G$ for some a, we are done. If $\langle a \rangle = G$ then $\langle a^r \rangle$ has size s and is hence a proper subgroup. □

We have the following theorem about cyclic groups.

Theorem 1. *1. Every subgroup of $\mathbb{Z}$ is cyclic.*

2. Even better, every subgroup of a cyclic group is cyclic.

Proof. 1. If $H \subset \mathbb{Z}$ is a subgroup, then let n be the smallest positive integer in H (if there is no such n then $H = \{0\} = \langle 0 \rangle$). The claim is that every $a \in H$ is divisible by n. If not, then $a = kn + r$ where $r < n$. But $a - kn \in H$ because H is a subgroup. Therefore we have a contradiction.

2. Suppose $G = \langle x \rangle$ and $K \subset G$ is a subgroup that is not trivial. Every element of K is a power of x. Let $H = \{n \in \mathbb{Z} | x^n \in K\}$. Clearly $H \subset \mathbb{Z}$ is a subgroup and hence cyclic. Suppose it is generated by a. Then $\langle x^a \rangle = H$.

□

Here is a definition : The subgroup $\langle S \rangle \subset G$ generated by a set S is defined to be a subgroup containing S such that any subgroup $H \subset G$ that contains S also contains $\langle S \rangle$. It is easy to see that such a subgroup is unique (indeed if there are two, each is contained within the other). Now define a word in G formed by elements of S as an expression of the form $x_1^{i_1} * x_2^{i_2} * x_3^{i_3} \ldots * x_a^{i_a}$ where $x_u \in S, i_u \in \mathbb{Z}$ (not necessarily distinct). The set of all words from S forms a subgroup W_S of G containing S. In fact,

Lemma 2.3. $W_S = \langle S \rangle$.

Proof. If $S \subset H$, then for any collection $x_1, \ldots, x_a \in S$, by definition of a subgroup, any word formed by them is in H. Hence $W_S \subset H$. Therefore $W_S = \langle S \rangle$. □

A group G is said to be finitely generated if there is a finite set S such that $\langle S \rangle = G$. Here is an important theorem (whose proof we shall omit).

Theorem 2. *Every finitely generated Abelian group is uniquely of the form* $\mathbb{Z}^r \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \mathbb{Z}_{q_3} \ldots \mathbb{Z}_{q_n}$ *where the integers* q_i *satisfy* $q_i | q_{i+1} \ \forall \ i$. *They are called the invariant factors of the group. The integer* r *is called the rank of the group.*

Recalling the fact that the Dihedral group is a subgroup of S_n, it turns out that this observation (due to Cayley) holds for all groups :

Theorem 3. *Let* G *be a group. Then it is isomorphic to a subgroup of* S_G *where* S_G *is the set of all bijections* $f : G \to G$ *made into a group by composition.*

Proof. Given $g \in G$, consider $f_g : G \to G$ as $f_g(a) = g.a$. Clearly f_g is a bijection. Also, e goes to the identity map and $f_{g_1 g_2} = (g_1 g_2).a = g_1.(g_2.a) = f_{g_1} f_{g_2}$ and $g^{-1}.(g.a) = g.(g^{-1}.a) = a$ and hence $f_{g^{-1}} = (f_g)^{-1}$. So $g \to f_g$ is a group homomorphism that is $1-1$. Therefore G is isomorphic to a subgroup of S_G. □

In particular, every finite group of size n is isomorphic to a subgroup of S_n. So in principle it is enough to study subgroups of S_n for finite group theory. (However, concrete that this may be, it is usually useful to forget any particular "embedding" of a finite group into S_n and focus abstractly on the group itself.)

3 S_n in more detail

A 2-cycle is called a transposition. (For ex : (35) interchanges 3 and 5.) Here is an important result.

Theorem 4. *The transpositions in* S_n *generate* S_n.

Proof. It suffices to prove this for a cycle because every permutation is a disjoint union of cycles. Now $(a_1 a_2 \ldots a_k) = (a_1 a_k)(a_1 a_{k-1}) \ldots (a_1 a_2)$. □

Of course this decomposition is not unique. For instance, $(123) = (13)(12) = (21)(23)$.