Notes for 26 March (Tuesday)

1 The road so far...

1. Proved that subgroups of cyclic groups are cyclic.
2. Stated the structure theorem for finitely generated Abelian groups.
3. Cayley's theorem.
4. Proved that transpositions generate S_n.

2 S_n in more detail

Furthermore,

Theorem 1. *1. The transpositions* $(12), (13), (14), \dots (1n)$ *generate* S_n.

2. So do $(12)(23)\dots(n-1n)$.

Proof. 1. Indeed, $(ij) = (1i)(1j)(1i)$.

2. Now $(1k) = (k-1k)\dots(34)(23)(12)(23)(34)\dots(k-1k)$ (Basically, inductively assume that $(1k-1)$ can be expressed using $(12), (23), \dots (k-2k-1)$. Now interchange $k-1, k$, apply the induction hypothesis and then interchange them again.

□

If σ is a permutation and $\alpha = (a_1 \dots a_s)$ is a cycle, then $\beta := \sigma \circ \alpha \circ \sigma^{-1}$ is called the conjugate of α by σ. Note that we used conjugates above. Here is an important theorem about conjugates (proof as HW).

Theorem 2. *Let* $\alpha = (a_1 \dots a_s)$ *and* $\beta = (b_1 \dots b_s)$ *be two cycles. Then*

1. *There exists a permutation* σ *such that* $\sigma(a_i) = b_i \ \forall \ 1 \leq i \leq s$.
2. *If* σ *is any permutation such that* $\sigma(a_i) = b_i \ \forall \ 1 \leq i \leq s$, *then* $\beta = \sigma\alpha\sigma^{-1}$.

Now we prove an important generation result.

Theorem 3. (12) *and* $(12\dots n)$ *generate* S_n.

Proof. we need to show that $(kk+1)$ can be expressed in terms of these two. Suppose this is true for $1, 2\dots, k-1$. Then, $(kk+1) = (12\dots n)(k-1k)(12\dots n)^{-1}$ by the above result on conjugates. □

While every element of S_n can be written in terms of transpositions in many ways,

Lemma 2.1. *The parity of the number of transpositions required for writing a $\sigma \in S_n$ is uniquely determined by σ.*

Proof. Let $P(x_1, \ldots, x_n) = \Pi_{i<j}(x_i - x_j)$. If $\alpha \in S_n$ define $\alpha P = \Pi_{i<j}(x_{\alpha(i)} - x_{\alpha(j)})$. Note that $\alpha P = \pm P$ and the sign is determined purely by α. If $\alpha, \beta \in S_n$ then $sgn(\alpha\beta) = sgn(\alpha)sgn(\beta)$. Therefore, $sgn(\sigma\alpha\sigma^{-1}) = sgn(\alpha)$. Since $sgn(12) = -1$, $sgn(1a) = -1$ and hence $sgn(ab) = -1$. Thus the parity of the number of transpositions is well-defined. □

The set of even permutations $A_n \subset S_n$ is very important.

Theorem 4. *A_n is a subgroup of size $\frac{n!}{2}$ (called the Alternating group).*

Proof. Of course identity is an even permutation. If $\alpha, \beta \in A_n$, since sgn is multiplicative, $\alpha\beta \in A_n$. Likewise, $sgn(\alpha^{-1})sgn(\alpha) = 1$ and hence $sgn(\alpha^{-1}) = sgn(\alpha)$. Thus A_n is a subgroup. The map $\alpha \to (12)\alpha$ is a bijection from even permutations to odd permutations (by multiplicativity of the sign). Hence $|A_n| = \frac{n!}{2}$. □

Here is the last generation result.

Theorem 5. *For $n \geq 3$, A_n is generated by 3-cycles.*

Proof. Every 3-cycle is even. Every element of A_n can be written using an even number of transpositions of the form $(1a)$. Pairing them and noting that $(1a)(1b) = (1ba)$ we are done. □

3 Back to abstract groups...again

We proved that for Abelian groups, the order of any element divides the order of the group. For that we have to use the group multiplication table. Unfortunately, $x_1.a.x_2.a \neq x_1.x_2.a^2$ for non-Abelian groups. Despite this problem, there is a wonderful theorem due to Lagrange :

Theorem 6. *If $H \subset G$ is a subgroup of a finite group, then $|H|$ divides $|G|$.*

If $H = \langle a \rangle$ and G is Abelian, we get the generalisation of Fermat's theorem to Abelian groups. The strategy to prove Lagrange's theorem is somewhat different from the one for Fermat. It seems crucial to know what $x_1.a, x_1.a^2, \ldots$ look like (in the sense that if $x_2.a = x_1.a^2$ for instance, then we can try to do some manipulations). More generally, we define a relation : $x \sim y$ iff $x.h_1 = y.h_2$ for some $h_1, h_2 \in H$. This relation is an equivalence relation. The equivalence classes are denoted as $x.H$ and are called left cosets of H. This relation generalises the notion of congruence. Now $x.H$ and $y.H$ have the same number of elements for all $x, y \in G$. Indeed, here is a bijection : $z \in x.H \to y.x^{-1}z \in y.H$. In particular, the cardinality of $x.H$ is the same as $e.H = H$. Hence if G is finite, $|G| = |H||G/H|$.