Notes for 20 March (Wednesday)

1 The road so far...

1. Discussed quartics and the Abel-Ruffini theorem for quintics.
2. Recalled groups. Groups study symmetry.

2 Back to groups...

Before we go on further, here is a general result whose proof is straightforward.

Lemma 2.1. *If $H, S \subset G$ are two subgroups, then $H \cap S$ is also a subgroup.*

Take a flat square centred at the origin. What distance-preserving operations of $\mathbb{R}^2$ take this square to itself ? Firstly, it can be shown that all distance-preserving maps are combinations of rotations, translations, and reflections about the x-axis. Since the centre is supposed to be preserved, translations are not allowed. Let r be the rotation of $\frac{\pi}{2}$ anticlockwise and s be a reflection about the x-axis. By repeatedly applying these operations one gets a group. Note that $r^4 = 1, s^2 = 1$ and $rs = sr^{-1}$. So this group is actually a finite group having 8 elements $1, r, r^2, r^3, s, rs, r^2s, r^3s$. This group is not Abelian. It is a subgroup of S_4 (obviously, because we are permuting the vertices). It is an example of a "Dihedral group". The general group of symmetries of the n-gon can be proven to be abstractly $1, r, r^2, \ldots, r^{n-1}, s, rs, r^2s, \ldots, r^{n-1}s$ where $r^n = s^2 = 1$ and $rs = sr^{-1}$. This group is quite useful in the study of plane figures and in related fields like crystals in chemistry and physics.

Note that e, r, s, rs unfortunately does not form a subgroup of S_6 (say) because r^2 is not in it (for instance). However, $e, r, r^2, r^3, \ldots, r^5$ is a subgroup of S_6. It generalises as follows : Given a group G and an element $x \in G$, the set $\langle x \rangle = \{e, x, x^{-1}, x^2, (x^{-1})^2, x^3, (x^{-1})^3, \ldots,\}$ is a subgroup and it is said to be "generated by x". Here is a small lemma whose proof is trivial.

Lemma 2.2. *If any subgroup $H \subset G$ contains x, then it contains $\langle x \rangle$.*

The order of x is the smallest positive integer n such that $x^n = 1$. If such an n does not exist, then x is said to have infinite order. (Caution : For fields, a similar property is said to be "characteristic 0".) Note that the order of x is the size of $\langle x \rangle$. We already proved that in a finite group with n elements, every element a has a finite order $\leq n$. If $G = \langle x \rangle$, then G is said to be a cyclic group with generator x. Note that cyclic groups are Abelian.

1. $(\mathbb{Z}, +)$ is cyclic and generated by 1 (as well as by -1).

2. $(\mathbb{Z}_n, +)$ is cyclic and generated by $[1]_n$. In fact, suppose $[a]_n$ is a generator. Then $[1]_n = k[a]_n$ for some k and hence $gcd(a, n) = 1$. This condition is sufficient because if $gcd(a, n) = 1$, there exists a k such that $[k][a] = [1]$ and hence $[n] = nk[a]$. So there are $\phi(n)$ generators.

3. The Dihedral group D_n where $n \geq 3$ is not even Abelian and hence not cyclic.

4. $K_4 = (\mathbb{Z}_2, +) \times (\mathbb{Z}_2, +)$ is not cyclic (a brute-force calculation shows that no element can be a generator). Actually, it can be easily seen that K_4 is isomorphic to D_2.

5. The n^{th} roots of unity form a group under multiplication. This group is in fact cyclic because it is generated by $\omega = e^{2\pi i/n}$. A generator is called a primitive root of unity. Note that if ω^k is a generator, then $(\omega^k)^a = \omega$ and hence $[ka]_n = [1]_n$ which is possible iff $gcd(a, n) = 1$. In fact, if $gcd(a, n) = 1$ then ω^k is a generator.