Notes for 19 March (Tuesday)

1 The road so far...

1. Proved the fundamental theorem of symmetric polynomials.
2. Discussed an "algorithm" to solve the cubic.

2 Cubics, Quartics, Quintics, etc

For the quartic $x^4 + bx^3 + cx^2 + dx + e = 0$, in principle one can reduce the "Resolvent" equation for 24 values of t to a sixth order equation for t^4 which can further be reduced to a quadratic. But let us use a slightly different set of variables $s_0 = x_0 + x_1 + x_2 + x_3$, $s_1 = x_0 - x_1 + x_2 - x_3$, $s_2 = x_0 + x_1 - x_2 - x_3$, and $s_3 = x_0 - x_1 - x_2 + x_3$. Note that s_0 is determined whereas s_1^2, s_2^2, s_3^2 are roots of $(x - s_1^2)(x - s_2^2)(x - s_3^2) = 0$. The coefficients are symmetric polynomials in x_i and hence determined. This is a cubic and hence can be solved.

If we apply these ideas to the quintic, the usual resolvent equation for t has degree 120 but can be reduced to degree 24 in t^5. Unfortunately, no trick like the one for the quartic works because all the fifth roots of unity are primitive. This already suggested to Lagrange that it might be impossible to solve the equation.

In fact, the Abel-Ruffini theorem states that there is no formula involving a finite sequence of operations from $+, -, x, /, ()^{1/n}$ applied on the coefficients that can work for all polynomials of degree 5. Clearly, the permutations of the roots play a role. A simple way to prove this (due to Arnold) is in a youtube video called "Short proof of Abel's theorem that 5th degree polynomial equations cannot be solved". Here is a brief sketch of the proof. To make it fully rigorous would require some knowledge of either topology (covering spaces) or complex analysis (winding numbers).

1. Firstly, observe that $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ is not a continuous function if a, b, c are complex numbers !! In fact, $\sqrt{z}$ itself cannot be defined as continuous function on the complex plane. The obvious definition $r^{1/2} e^{i\theta/2}$ is problematic on the positive x-axis where θ abruptly jumps from 0 to 2π. Using this fact and the fact that $y^2 = z$ has at most two solutions, one can prove that there is no continuous square root defined on any ball containing the origin. The same kind of a proof works for n^{th} roots.
2. Secondly, if you travel around the origin k times, $\sqrt{z}$ picks up a sign of $(-1)^k$. Likewise, for higher roots.

3. Thirdly, assume that the quintic has distinct roots and that they are given by a formula involving a finite sequence of arithmetic operations $+, \times, /, -$ and the n^{th} root $()^{1/n}$ on the coefficients. If you change the coefficients of the quintic in the complex plane continuously, going through quintics having distinct roots and come back to the original quintinc at time $t = 1$, then the set of roots comes back to the original set. However, the ordering might change, i.e., the roots will get permuted.

4. In fact, any permutation of the roots can be realised this way by simply considering $a_5(z-z_1(t))(z-z_2(t))\ldots$ where $z_i(t)$ are all distinct for $0 \leq t \leq 1$ and are continuous functions of t.

5. Suppose the formula for the roots is $(arithmetic\ operations\ on\ the\ coefficients)^{1/n}$ (or an arithmetic combination of such "1-nested radicals") for the sake of argument. Then a loop of coefficients $\gamma_1(t)$ may not preserve such an expression. However, an expression of the form $\gamma_1(t)\gamma_2(t)\gamma_1^{-1}\gamma_2^{-1}$ will preserve it !! (In fact any finite sequence of such "commutator" loops will preserve the hypothetical formula.) So if there is a non-trivial commutator that permutes the roots, then we have a contradiction because the formula for the roots is left unchanged.

6. Suppose instead that the formula for the roots involves N-nested radicals, then a commutator of a commutator of a commutator.... (N times) will preserve such an expression.

7. It turns out that for every N, there is a finite multiplication of commutator of a commutator of ... (N times)-type expressions of permutations in S_5 that is non-trivial, i.e., it permutes the roots non-trivially. However, this means that no finite nesting of radicals works.

3 Back to groups...

We saw the definition of a group G, subgroups $H \subset G$, cartesian product $G \times H$, the definition of group homomorphisms $f : G \to H$, examples of Abelian (like $\mathbb{Z}_n$ under addition) and non-Abelian (like S_n, invertible matrices, etc) groups, and a generalisation of Fermat's little theorem theorem for Abelian groups. The image of a group homomorphism can be easily proven to be a subgroup of the target. By the way, $\mathbb{Z}_2 \times \mathbb{Z}_2$ is sometimes called Klein's four group. The points were largely to produce convenient language to study questions regarding permutations (cyclic decomposition), to define rings, and to give a proof of $\phi(ab) = \phi(a)\phi(b)$. However, subgroups of S_n (called "permutation groups of substitutions" originally by Galois) arose out of the study of polynomials and whether the quintic can be solved. Another source of groups is through "symmetries" (whether geometric ones or otherwise).