Math 505, 1/20

Now we digress a bit to give the formulas for solving cubic and quartic equations. As mentioned before, we will step back in time about five centuries, solving these equations using only high-school algebra techniques and avoiding any field or group theory. Given the cubic equation $x^3 + ax^2 + bx + c = 0$, we begin by changing the variable, setting $y = x - (a/3)$. Equating $(y - (a/3))^3 = a(y - (a/3)^2 + b(y - (a - 3)) + c$ to 0 and collecting coefficients of the powers of y, we find that the coefficient of y^2 cancels. Rewrite the resulting equation as $y^3 + py + q = 0$; we call the left side a *reduced cubic*. Now make the substitution $y = z + (k/z)$, where k will be specified in a moment. We get $z^3 + (3k + p)z + (3k^2 + q + pk)z^{-1} + k^{-3}z^{-3} = 0$. Two terms drop out by making the choice $k = -p/3$; with this choice we get $z^3 + q - (p^3/27)z^{-3} = 0$. This last equation becomes quadratic in z^3 if multiplied by z^3 on both sides. Solving it by the quadratic formula and plugging back into y, we get $y = ((-q+S)/2)^{1/3} + ((-q-S)/2)^{1/3}$, where $S = \sqrt{q^2 + (4p^3/27)}$ and the cube roots must be chosen so that their product is $-p/3$ (but otherwise they are unrestricted). This gives us exactly three roots, as desired; note that if p, q are real and $q^2 + (4p^3/27)$ is negative, then the roots are real, but the expressions that lead to them involve complex numbers. This turns out to be unavoidable; it was in fact one of the motivations that led mathematicians to accept complex numbers, since they can be required to express even real solutions to certain equations. (If conversely $q^2 + 4p^3/27$ is positive, then you can check that one root is real while the other two are complex.) If p, q are rational, then the quantity $D = -27q^2 - 4p^3$, a rational multiple of $q^2 + 4p^3/27$, turns out to determine the Galois group of $x^3 + px + q$ over $\mathbf{Q}$; assuming this polynomial has no rational root, or equivalently is irreducible over $\mathbf{Q}$, then its Galois group is A_3 or S_3 according as D is the square of a rational number or not. We call D the *discriminant* of the polynomial; we will see below that any polynomial of degree n has a discriminant which behaves similarly to D in that it determines whether the Galois group is a subgroup of A_n or not.

Turning now to the quartic equation $x^4 + ax^3 + bx^2 + cx + d = 0$, our first step is to get rid of the x^3 term, this time by making the substitution $y = x - a/4$. Combining like powers of y we now get $y^4 + py^2 + qy + r = 0$ fro some p, q, r. Once again we introduce a new parameter, this time called t and add and subtract $t^2/4$, rewriting the resulting equation as $(y^2 + (t/2))^2 - [y^2(t - p) - qy + ((t^2/4) - r)] = 0$. We now choose the parameter t in such a way that the quadratic polynomial in brackets becomes a (constant times a) perfect square, by making its discriminant $q^2 - 4(t - p)((t^2/4) - r)$ equal to 0. This is a cubic equation, called the *resolvent cubic*, which we can solve by the above paragraph. Now we can rewrite our original equation as $A^2 - B^2 = 0$, for suitable expressions A, B; equating A to $\pm B$ and solving, we see that we can find the four roots of our original equation by solving two quadratics. We will not push this through to get explicit expressions for the roots, but note that neither the resulting formula not the cubic formula derived above could have been derived just by analyzing the groups S_3 and S_4; we knew in advance

that some radical formula had to exist, but Galois theory alone does not tell us what it is, though it does correctly predict that expressing the roots of a quartic polynomial requires solving a cubic polynomial along the way, as $\mathbf{Z}_3$ is one of the cyclic subquotients of S_4.

Given a polynomial p of degree n over any field K with roots $r_1, \ldots, r_n$ in its splitting field, we note that the product $D = \Pi_{i<j}(r_i - r_j)$ of all the root differences remains unchanged if an even permutation is applied to the r_i, while it changes by a sign if an odd permutation is applied to the r_i. It follows that D^2 always lies in the basefield K (being fixed by the Galois group, a subgroup of S_n) snd that D lies in K if and only if the Galois group of p is a subgroup of A_n (i.e. consists entirely of even permutations of the $r - I$). By expressing D^2 in terms of the coefficients of p (which in principle can always be done), we thereby derive a criterion for the Galois group of p to be a subgroup of A_n. If p is monic and quadratic, so equal to x^2+bx+c, then D^2 is the familiar expression $b^2 - 4c$ from high-school algebra, which among other things determines whether the roots of p are real or not (if $K = \mathbf{R}$). If p is a monic reduced cubic, then D^2 turns out to equal $-27q^2 - 4p^3$, as mentioned above. There is a similar but more complicated formula for the discriminant of a reduced quartic polynomial.

We conclude by mentioning a purely numerical criterion for solvability of a quintic polynomial p over $\mathbf{Q}$. There is a polynomial in the roots $r_1, \ldots, r_5$ of a such a polynomial (regarded as independent variables) such that the subgroup of S_n fixing this polynomial is the normalizer N of the cyclic subgroup generated by a 5-cycle of the roots r_i (where as above S_5 acts on the r_i by permutations). This polynomial has exactly 6 distinct images $i_1, \ldots, i_6$ under S_5(since N has index 6 in S_5. Taking the product q of the $x - i_j$ we get a polynomial of degree 6 over $\mathbf{Q}$ whose coefficients are polynomials in the coefficients of p. This polynomial has a rational root if and only if the Galois group of p lies in a conjugate of N in S_5; this turns out to be the case if and only if this Galois group is solvable. Thus q has a rational root if and only if p is solvable by radicals over $\mathbf{Q}$. A formula for q is given on p. 639 of the third edition of Dummit and Foote; it takes almost half a page to write out.