

## Math 505, 1/13

Picking up where we left off last time, we ask when a polynomial  $p$  over a field  $K$  is *solvable by radicals*; that is, when the splitting field  $L$  of  $p$  lies inside the last field  $K_n$  of a sequence of extensions  $K = K_0 \subset K_1 \subset \cdots \subset K_n$  such that each  $K_i = K_{i-1}(\alpha_i)$  with  $\alpha_i^{n_i} = \beta_i \in K_{i-1}$  for some positive integer  $n_i$ . (We do not assume that  $K_i$  is Galois over  $K_{i-1}$ , nor do we make any a priori assumption about the degrees  $n_i$ .) Suppose that there is such a chain of fields  $K_i$  for  $p$  and let  $N$  be the product of the integers  $n_i$ . We now extend the field  $L$  slightly, letting  $K'_0$  be the splitting field of  $x^N - 1$  over  $K_0$  and inductively letting  $K'_i$  be the splitting field of  $x^{n_i} - \beta_i$  over  $K'_{i-1}$ . Then  $K'_i$  is Galois over  $K'_{i-1}$  for  $i > 0$  and its Galois group is a subgroup of  $\mathbf{Z}_{n_i}$ , since any  $K'_{i-1}$ -automorphism of  $K'_i$  is determined by what it does to  $\alpha_i$ , and the only choices are to send it to  $\alpha_i$  times some  $n_i$ th root of 1 in  $K'_{i-1}$ . It follows that  $K'_i$  is Galois over  $K'_{i-1}$  with cyclic Galois group if  $i > 0$ , while  $K'_0$  is Galois over  $K_0$  with abelian Galois group. Since a finite abelian group is a direct product of cyclic groups, we may replace the field  $K'_0$  by a chain of fields ending in  $K'_0$  such that each field is Galois over the previous one with cyclic Galois group. The upshot is that some extension  $L'$  of  $L$  is the last field in a chain of fields beginning with  $K_0$ , with each field a cyclic Galois extension of the previous one. Applying the Galois correspondence and recalling that the map from subgroups of the Galois group to intermediate fields is inclusion-reversing, we deduce that there is a decreasing chain of subgroups  $G_0 > G_1 > \cdots > G_n = 1$  with  $G_0$  the Galois group of  $L'$  over  $K$ , each  $G_i$  normal in  $G_{i-1}$ , and each quotient group  $G_{i-1}/G_i$  cyclic. The existence of such a chain for a fixed group  $G_0$  is of course a purely group-theoretic one on  $G_0$ ; amazingly, Galois managed to formulate it and show its equivalence (in his setting) to solvability by radicals \*before\* the notion of an abstract group had been introduced! We express this condition by calling the group  $G_0$  *solvable*; nowadays most students see it for the first time in a group theory course, but Galois introduced it precisely to characterize the conditions under which a polynomial is solvable by radicals over  $\mathbf{Q}$ . An easy formal consequence of the definition is that any quotient of a solvable group is again solvable; applying this observation to the splitting field  $L$  of our original polynomial  $p$  over  $K$ , we see that *if a polynomial over a field is solvable by radicals, then the Galois group of its splitting field must be solvable*. This is half of the famous Galois Criterion.

Over fields  $K$  of characteristic 0, the converse half of the Galois Criterion holds as well: *a polynomial  $p$  over  $K$  is solvable by radicals if and only if the Galois group of its splitting field is solvable*. Before proving this, we take time out to exhibit an example of a quintic polynomial over  $\mathbf{Q}$  that is not solvable by radicals. Take  $p = x^5 - 4x + 2$ . An easy calculus computation shows that  $p$  has exactly three real roots (one negative and two positive). Amazingly enough, this property alone is enough to identify the Galois group  $G$  of (the splitting field  $S$  of)  $p$ : it is the symmetric group  $S_5$ ! To prove this note first that  $S$  is generated over  $\mathbf{Q}$  by the five roots of  $p$  in  $\mathbf{C}$ , so any element of  $G$  permutes these roots and is in turn determined by how it permutes them. Now  $p$  is

irreducible over  $\mathbf{Q}$  (by the Eisenstein Criterion), so the degree of  $S$  over  $\mathbf{Q}$  must be a multiple of the degree 5 of any of the roots of  $p$  over  $\mathbf{Q}$ . It follows that  $G$  contains an element of order 5 in  $S_5$ , which must be a 5-cycle (since 5 is prime). We also know that complex conjugation is an automorphism of  $S$  lying in  $G$ , which fixed 3 of the roots and flips the other two. Taking a suitable power of the 5-cycle, we may label the roots  $r_1, \dots, r_5$  in such a way that two elements of  $S_5$  lying in  $G$  are the 5-cycle  $(r_1, r_2, \dots, r_5)$  and the transposition  $(r_1, r_2)$ . Conjugating the transposition by the 5-cycle we get that the transpositions  $(r_2, r_3), (r_3, r_4), (r_4, r_5)$  all lie in  $G$ . But now a standard fact from a first course on group theory is that transpositions of adjacent indices  $(r_1, r_2), \dots, (r_{n-1}, r_n)$  generate all of  $S_n$  for any  $n$ . We conclude that  $S$  has the maximum possible degree of 120 over  $\mathbf{Q}$  and that  $G$  is all of  $S_5$ , as claimed. Note that it would be essentially impossible to prove this using field theory alone; note also, more generally, that any irreducible polynomial of prime degree  $q$  over  $\mathbf{Q}$  with exactly  $q - 2$  real roots has Galois group  $S_q$  over  $\mathbf{Q}$ .

Since the only normal subgroups of  $S_5$  are 1, the alternating group  $A_5$ , and  $S_5$  itself, we deduce that *no* algebraic expression involving only rational numbers, arithmetic operations, and  $n$ th roots (for any  $n$ ) can represent a root of  $p$ , for if one such expression did represent a root of  $p$ , then all other roots could be gotten from the same expression by making different choices of roots at some step, so that  $p$  would be solvable by radicals over  $\mathbf{Q}$ . It is not difficult (though I will probably not take the time to do it) given any  $n \geq 5$  (prime or not) to write down a polynomial of degree  $n$  over  $\mathbf{Q}$  with Galois group  $S_n$ : no such polynomial is solvable by radicals over  $\mathbf{Q}$ .