Lemma 11.1. [Kummer's theory]. Let K be a field of characteristic zero, $n > 1$ a number such that K contains all the roots of order n of 1 and $L \supset K$ be a Galois extension with the Galois group $Gal(L/K)$ equal to $\mathbb{Z}_n$. Then there exists $\alpha \in L$ such that $L = K(\alpha)$ and $\alpha^n \in K$.

Proof. Fix $\zeta \in K$ such that $\zeta^n = 1, \zeta^m \neq 1$ for $1 < m < n$ and choose a generator σ of the group $Gal(L/K)$. By Dedekind's lemma the K-linear maps $\sigma^i : L \to L, 0 \leq i < n$ are linearly independent. Therefore there exists $x \in L$ such that $\alpha := \sum_{i=0}^{n-1} \zeta^{-i}\sigma^i(x) \neq 0$. Then

$$\sigma(\alpha) = \sum_{i=0}^{n-1} \zeta^{-i}\sigma^{i+1}(x) = \zeta \sum_{i=0}^{n-1} \zeta^{-(i+1)}\sigma^{i+1}(x) = \zeta\alpha$$

Therefore $\sigma(\alpha^n) = \alpha^n$. So $\alpha^n \in K$.

I claim that $K(\alpha) = L$. Since $K(\alpha) \subset L$ it is sufficient to show that $dim_K(K(\alpha)) \geq n$. But is is clear that the elements $\alpha^i \in L, 0 \leq i < n$ are eigenvectors of σ with distinct eigenvalues ζ^i. Therefore elements $\alpha^i \in L, 0 \leq i < n$ are linearly independent over K. So $dim_K(K(\alpha)) \geq n$.$\square$

Definition 11.1. Let K be a field and $p(t) \in K[t]$ an irreducible polynomial of positive degree and $L \supset K$ the splitting field of of $p(t)$. We say that the group $Gal(L/K)$ is *the Galois group of* $p(t)$.

b) If $L \subset \bar{K}$ is a finite extension of K we say that L is *obtainable from K by adding radicals* if there exists a finite extension $F_n \supset L$ and an increasing sequence of fields $K = F_0 \subset F_1 ... \subset F_n$ such that for any $i, 0 \leq i < n$ we have $F_{i+1} = F_i(\alpha_i)$ where $\alpha_i^{r_i} \in F_i$ for some $r_i > 0$,

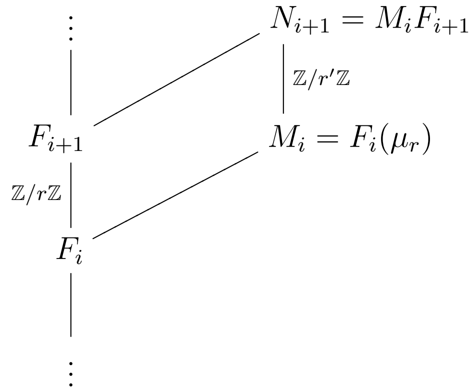
c) if $p(t) \in K[t]$ is an irreducible polynomial of positive degree we say that an equation $p(t) = 0$ is *solvable in radicals* if the extension $L := K[t]/(p(t))$ of K is obtainable from K by adding radicals.

Theorem 11.1. Let K be a field of characteristic 0 and $L \supset K$ a normal extension. Then L is obtainable from K by adding radicals iff the Galois group $Gal(L/K)$ is solvable.

Proof. a) Assume that the Galois group $Gal(L/K)$ is solvable. Then there exists a sequence of subgroups $(e) = H_0 \subset H_1 ... \subset H_m = G$ such that $H_i \triangle H_{i+1}$ and the quotient group $H_{i+1}/H_i, 0 \leq i < m$ are cyclic.

Define $F_i := L^{H_{n-i}}$. Then we have a sequence of subfields $K = F_0 \subset F_1 \subset ... \subset F_n = L$ such that extensions F_{i+1}/F_i are normal and the Galois groups $Gal(F_{i+1}/F_i)$ are cyclic. It is sufficient to show that for any $i, 0 \leq i < m$ one can obtain the field F_{i+1} from F_i by adding radicals.

Assume that $Gal(F_{i+1}/F_i) = \mathbb{Z}_r$. Let M_i be the splitting field of $t^r - 1$ over F_i. It is clear that we can obtain the field M_i from F_i by adding radicals. Let $N_{i+1} = F_{i+1}M_i$.



Then it is easy to see (?) that N_{i+1}/M_i is a Galois extension and $Gal(N_{i+1}/M_i)$ is a subgroup of $Gal(F_{i+1}/F_i) = \mathbb{Z}_r$.

So $Gal(N_{i+1}/M_i) = \mathbb{Z}_{r'}$ where $r'|r$. Since M_i contains all all the roots of order r' of 1 and $L \supset K$ is a Galois extension with the Galois group $Gal(L/K)$ equal to $\mathbb{Z}_{r'}$ it follows from Lemma 11.1 that one can obtain the field F_{i+1} from M_i by adding radicals. □

b) Assume that L is obtainable from K by adding radicals. We want to show that the Galois group $Gal(L/K)$ is solvable. Using the induction it is sufficient to prove the following result which I'll leave for you to prove.

Claim. Let K be a field, L is a splitting field of a polynomial $t^n - a$. Then the Galois group $Gal(L/K)$ is solvable.

Definition 11.2. a) The symmetric groups S_n is the group of permutations of the set $(1, ..., n)$.

b) For any sequence $\bar{i} = (i_1, i_2, ..., i_r)$ of distinct elements of $(1, ..., n)$ we denote by $[i_1, i_2, ..., i_r] \in S_n$ the permutation such that

$$[i_1, i_2, ..., i_r](i_k) = i_{k+1}, 1 \leq k < r, [i_1, i_2, ..., i_r](i_r) = i_1, [i_1, i_2, ..., i_r](i) = i, i \notin \bar{i}$$

The element $[i_1, i_2, ..., i_r] \in S_n$ is called the *cycle* corresponding to the sequence $\bar{i} = (i_1, i_2, ..., i_r)$,

c) we call the cycle $s_i := [i, i+1], 1 \leq i < n$ an *elementary permutation.*

Given any $\sigma \in S_n$ and $i \in (1, ..., n)$ we may form an orbit $\bar{i} \subset (1, ..., n)$ of i under the action of the cyclic group generated by σ. Then $(1, ..., n)$ may be decomposed in a disjoint union of orbits of the cyclic group generated by σ. Then σ is equal to the product of commuting cycles corresponding to this decomposition.

Lemma 11.3. a) The elementary permutations $s_i, 1 \leq i < n$ generate S_n,

b) if n is a prime number, $\sigma \in S_n$ is an n-cycle and $\tau \in S_n$ an elementary permutation then (σ, τ) generate S_n,

c) two elements of S_n are conjugate iff they are products of cycles of the same length,

d) if n is prime and $\sigma \in S_n$ is an element of order n then σ is an n-cycle.

Proof. a),c) and d) are easy and I'll only outline the proof of b).

By renumbering the elements we can assume that $\tau = (1, 2)$. We can find $r, 0 < r < n$ such that $\sigma^r(1) = 2$. Since n is prime we see that σ^r is also an n-cycle. Therefore by another renumbering the elements we can assume that $\sigma^r = (1, 2, ..., n)$. But then we have $\sigma^{-ir} \circ \tau \circ \sigma^{ir} = s_i, 1 \leq i < n$. So the subgroup of S_n generated by (σ, τ) contains $s_i, 1 \leq i < n$.□

Theorem 11.2. The groups S_n are not solvable if $n > 4$.

Proof. Theorem 11.2 is an immediate corollary of the following result.

Theorem 11.2'. Let $H \subset S_n, n > 4$ be a subgroup containing all 3-cycles and $H' \lhd H$ be a normal subgroup such that the quotient group H/H' is abelian. Then H' also contains all 3-cycles.

Proof of Theorem 11.2'. Let $[rki] \in S_n$ be a 3-cycle. We want to show that $[rki] \in H'$. Choose numbers $j, s \in (1, ..., n)$ distinct from r, k, i and consider $\sigma := [ijk], \tau := [krs]$. By the condition on H we have $\sigma, \tau \in H$. I claim that $\sigma\tau\sigma^{-1}\tau^{-1} \in H'$. Really since the group H/H' is abelian we have $q(\sigma\tau\sigma^{-1}\tau^{-1}) = q(\sigma)q(\tau)q(\sigma)^{-1}q(\tau)^{-1}) = e_{H/H'}$ whre $q : H \to H/H'$ is the natural projection and $e_{H/H'}$ is the unit in H/H'.

On the other hand $\sigma\tau\sigma^{-1}\tau^{-1} = [rki]$. So $[rki] \in H'$.□

Let $s(t) \in K[t]$ be an irreducible polynomial of degree n. Then the Galois group G of $s(t)$ acts on the set $R \subset \bar{\mathbb{Q}}$ of roots of $s(t)$ in $\bar{\mathbb{Q}}$. In other words we have an imbedding of the group G into the symmetric group S_n. In particular we can talk about the decomposition of $\sigma \in G$ in the product of cycles.

Theorem 11.3. Let $s(t) \in K[t]$ be an irreducible polynomial of a prime degree p. Suppose that there exists $\sigma \in G$ which acts on R as an elementary transposition. Then $G = S_n$.

Proof. Let $F := K[t]/(s(t)), L$ be the normal closure of F over K and $G = Gal(L/K)$. We want to show that $G = S_n$.

Since $|G| = [L : K] = [L : F][F : K]$ we see that p divides $|G|$. Therefore it follows from the Cauchy's theorem that there exists $\tau \in G$ of order p. Consider the imbedding of the group G into the symmetric group S_p coming from the action on roots of $s(t)$). Since p is a prime number it follows from Lemma 11.2 d) that $\tau \in S_n$ is an n-cycle. Theorem 11.3 follows now from Lemma 11.2 b).□

Corollary 1. Let $s(t) \in \mathbb{Q}[t]$ be a polynomial of a prime degree p which have exactly two non-real roots in $\mathbb{C}$. Then the Galois group of $s(t)$ is equal to S_p.

Proof. We have to show that the image of the Galois group $Gal(L/K)$ in S_p contains an elementary transposition. By the complex conjugation acts on the set of roots of $s(t)$ as an elementary transposition.

Corollary 2. The Galois group of $s(t) = t^5 - 6t + 3$ is equal to S_5.

Proof. The Eisenstein's criterion shows the irreducibility of $s(t)$.

Since

$p(-3) < 0, p(-1) > 0, p(-1) < 0, p(2) > 0$ we see that $s(t)$ has at least 3 real roots. On the other hand $p'(t)$ has only 2 zeros. So it follows from the Rolle's theorem that $s(t)$ has at most 3 real roots. We see that $s(t)$ has exactly three real roots. Therefore $s(t)$ has exactly two complex roots and the result follows from Corollary 1.