—Solvability of algebraic equations by radicals—

General monic polynomials/equations

Let $k$ be any base field, $k[t_0, \ldots, t_{n-1}]$ the polynomial ring in variables $t_1, \ldots, t_n$, and $K = k(t_1, \ldots, t_n)$ its quotients field. The polynomial $P(X) = X^n + t_{n-1}X^{n-1} + \ldots + t_0 \in K[X]$ is called the general (monic) polynomial over $k$. Let further $R = k[X_1, \ldots, X_n]$ be the polynomial ring in the variables $X_1, \ldots, X_n$, and $S = k(X_1, \ldots, X_n)$ be its quotients field. Finally let $s_k$ be the $k^{th}$ elementary symmetric polynomial in $X_1, \ldots, X_n$ for $k = 1, \ldots, n$; and define $\varphi_0 : k[t_0, \ldots, t_{n-1}] \to k[s_n, \ldots, s_1]$ by $t_{n-k} \mapsto s_k$ for $1 \leq k \leq n$.

1) In the above notations, show the following:

a) The symmetric group $S_n$ acts on $R$ and $S$ by $\sigma(X_i) = X_{\sigma^{-1}(i)}$.

b) The fixed ring/field of $S_n$ are $k[s_n, \ldots, s_1]$, resp. $k(s_n, \ldots, s_1)$.

c) Show that $\varphi_0$ is an isomorphism which extends to an isomorphism $\varphi : L \to k(X_1, \ldots, X_n)$.

d) Conclude from this that denoting by $K_{P(X)}|K$ a splitting field extension of the general polynomial $P(X)$, we have: $G_{P(X)} = \operatorname{Aut}(K_{P(X)}|K) \cong S_n$, thus solvable if and only if $n \leq 4$.

$\mathcal{P}$-Solvability of polynomials/equations

Let $K$ be a base field, and $\mathcal{P} \subset K[X]$ be a set of non-constant polynomials.

- We will say that a polynomial $P(X) \in K[X]$ is $\mathcal{P}$-solvable, if $\exists$ a tower of finite field extensions $K = K_0 \subseteq \ldots \subseteq K_1 \subseteq K_{i+1} \subseteq \ldots \subseteq K_n = L$ satisfying the following:
  
  i) $K_{i+1} = K_i(x_i)$ with $x_i$ a zero of some a polynomial of the form $p_i(X) = p_i(X) - a_i$ with $p_i(X) \in \mathcal{P}$ and $a_i \in K_i$.

  ii) All the roots of $P(X)$ lie in $L$, i.e., $L$ contains a splitting field of $P(X)$.

- One says that $P(X)$ is solvable by radicals, if $P(X)$ is $\mathcal{P}_0$-solvable, where $\mathcal{P}_0 = \{X^n \mid n > 0\}$ consists of all the powers of $X$.

- One says that $P(X)$ is solvable by radicals modulo roots of unity, if $P(X)$ is $\mathcal{P}_0$-solvable over $\bar{K}$, where $\bar{K}|K$ is the extension of $K$ obtained by adjoining all the roots of unity to $K$.

Finally, for a polynomial $P(X) \in K[X]$, we denote by $G_{P(X)} = \operatorname{Aut}(K_{P(X)}|K)$ the automorphism group of some splitting field extension $K_{P(X)}|K$ of $K$, and by $\hat{G}_{P(X)} = \operatorname{Aut}(\bar{K}_{P(X)}|\bar{K})$ the automorphism group of a decomposition field of $P(X)$ over $\bar{K}$.

Our aim is to prove the following very famous result by Galois:

**Theorem.** In the above notations one has:

(a) A polynomial $P(X) \in K[X]$ is solvable by radicals modulo roots of unity if and only if $G_{\hat{P}(X)}$ is solvable and $\operatorname{Char}(K)$ does not divide $|G_{\hat{P}(X)}|$.

(b) In particular, the general polynomial of degree $n$ is solvable by radicals modulo roots of unity if and only if $n \leq 4$ and $n < \operatorname{Char}(K)$.

**Supplement:** $X^n - 1$ is solvable by radicals, provided $n < \operatorname{Char}(K)$. In particular, solvability by radicals is equivalent to solvability by radicals modulo roots of unity if $\operatorname{Char}(K) = 0$.

2) First suppose that $P(X)$ is solvable by radicals modulo roots of unity. So let $(K_i)_{i \leq n}$ be a tower of extension such that $K_{i+1} = K_i(x_i)$, where $x_i^{n_i} = a_i$ for some $n_i > 0$, $a_i \in K_i$, and $\bar{K} = K_0$, $L = K_n$. Let $M|\bar{K}$ be a normal closure of $L|\bar{K}$. 

Due: Wed, Feb 15, 2006
a) Show that \( G := \text{Aut}(M|\tilde{K}) \) is solvable, and that \( \text{Char}(K) \) does not divide \( |G| \).
b) Further, show that \( G_{\tilde{P}(X)} \) is a quotient of \( G \), thus it is solvable, and \( \text{Char}(K) \) does not divide \( |G_{\tilde{P}(X)}| \).

**Hint:** Make induction on \( n \), and use Kummer Theory and Artin–Schreier Theory.

3) For the converse, let \( \{1\} = G_r \triangleleft \ldots \triangleleft G_i \triangleleft \ldots \triangleleft G_0 = G_{\tilde{P}(X)} \) be a composition series of \( G_{\tilde{P}(X)} \). Let \( L = \tilde{K}_{\tilde{P}(X)} \) be a splitting field of \( P(X) \) over \( \tilde{K} \). Show the following:
   a) \( L_0 = L^{G_0} \) is pure inseparable over \( \tilde{K} \).
   b) Setting \( L_i = L^{G_i} \), it follows that \( L_{i+1} = L_i(x_i) \), where \( x_i \) satisfies \( x_i^{q_i} = a_i \) for some prime number \( q_i \) and some \( a_i \in L_i \).
   c) Finally deduce from this that \( P(X) \) is solvable by radicals over \( \tilde{K} \).

4) Using Problem 1 above, show that point b) of the Theorem holds.

5) Prove the Supplement of the Theorem.

**Hint:** Suppose that \( P(X) \) is solvable modulo roots of unity, thus \( \tilde{K}_{\tilde{P}(X)}|\tilde{K} \) is a solvable Galois extension (WHY?). Show that if \( m \) is its degree, then setting \( K_m = K[\mu_m] \) we have: \( (K_m)_{\tilde{P}(X)}|K_m \) is a solvable Galois having a tower of sub-extension as at Problem 3b above. Finally, remark \( K_m|K \) is the splitting field of \( X^m - 1 \), etc.

6) Following the proof of the Theorem, indicate how to solve the equations of degree \( \leq 4 \) by radicals. Try to find explicit formulas at least in the case \( n = 3 \).