

**Frank Moore**  
**Algebra 902 Notes**  
**Professor: Tom Marley**

Recall the quadratic formula: The roots of  $f(x) = ax^2 + bx + c \in K[x]$  are  $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$  if the characteristic of  $K$  is not 2, and where  $\sqrt{b^2 - 4ac}$  is a root of  $x^2 - (b^2 - 4ac)$ . Thus, the roots of  $f(x)$  lie in the field  $K(\alpha)$  where  $\alpha$  is a root of  $x^2 - (b^2 - 4ac)$ .

Also, note that Cardano in the 1500s found a formula to solve the general cubic. Indeed, let  $f(x) = x^3 + ax^2 + bx + c \in K[x]$ . Assume that  $\text{Char } K \neq 2, 3$ . Replacing  $x$  by  $x - \frac{1}{3}a$ , we may eliminate the  $x^2$  term, so we may assume that  $f(x) = x^3 + px + q$ . Cardano's formula shows that the roots of  $f(x)$  lie in the field  $K(\omega, \delta, y_1, y_2)$  where  $\omega$  is a primitive  $n$ th root of unity,  $\delta = \sqrt{12pq + 81q^2}$  and  $y_1, y_2 = \sqrt[3]{-\frac{27}{2}q \pm \frac{3}{2}\delta}$ . So we have a tower of fields (called a root tower):

$$\begin{array}{c}
 E = K(\omega, \delta, y_1, y_2) = F_3(y_2) \\
 \left| \begin{array}{c} y_2^3 \in F_3 \end{array} \right. \\
 F_3 = F_2(y_1) \\
 \left| \begin{array}{c} y_1^3 \in F_2 \end{array} \right. \\
 F_2 = F_1(\delta) \\
 \left| \begin{array}{c} \delta^2 \in F_1 \end{array} \right. \\
 F_1 = K(\omega) \\
 \left| \begin{array}{c} \omega^3 \in K \end{array} \right. \\
 F_0 = K
 \end{array}$$

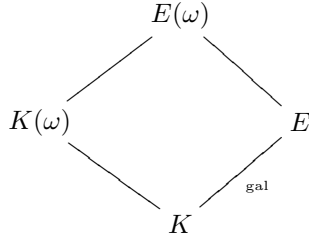
**Definition:** A finite extension  $E/K$  is called a **radical extension** if  $\exists u_1, \dots, u_n$  such that for each  $i$   $\exists n_i$  with  $u_i^{n_i} \in K(u_1, \dots, u_{n-1})$  and  $E = K(u_1, \dots, u_n)$ . The sequence

$$K \subseteq K(u_1) \subseteq K(u_1, u_2) \subseteq \dots \subseteq K(u_1, \dots, u_n) = E$$

is called a **root tower**. A polynomial in  $K[x]$  is said to be **Solvable by Radicals** if  $f(x)$  splits in some radical extension.

**Theorem:** Let  $f(x) \in K[x]$  be a separable polynomial and  $E$  a splitting field for  $f(x)$ . Assume that  $\text{Char } K \nmid [E : K]$ . If  $\text{Gal}_K(f(x))$  is solvable, then  $f(x)$  is solvable by radicals.

*Proof:* Let  $n = [E : K]$  and  $\omega$  a primitive  $n$ th root of unity. Consider the diagram

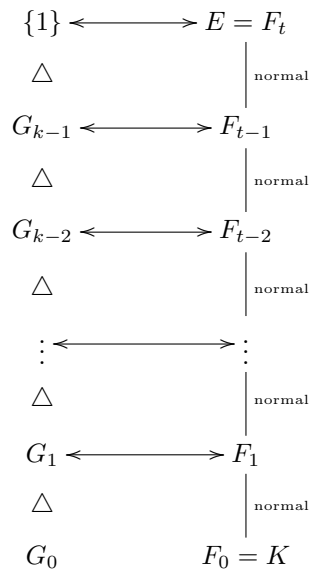


By a homework exercise,  $E(\omega)/K(\omega)$  is Galois. Furthermore, we have that  $\text{Gal}(E(\omega)/K(\omega)) \cong$  a subgroup of  $\text{Gal}(E/K)$ . As subgroups of solvable groups are solvable,  $\text{Gal}(E(\omega)/K(\omega))$  is solvable. If we show that  $E(\omega)/K(\omega)$  is a radical extension, then certainly  $E(\omega)/K$  is a radical extension, since adjoining  $\omega$  is a radical extension. Of course  $f$  splits in  $E(\omega)$  as it splits in  $E$ . Hence without loss of generality, we may replace  $K$  with  $K(\omega)$  and assume  $K$  contains all the  $n$ th roots of unity. Also,  $[E(\omega) : K(\omega)] = |\text{Gal}(E(\omega)/K(\omega))|$  which divides  $|\text{Gal}(E/K)|$  by Lagrange. Hence  $\text{Char } k \nmid [E(\omega) : K(\omega)]$ . So, let  $G = \text{Gal}(E/K)$ . As  $G$  is solvable, there is a normal series

$$\{1\} \triangleleft G_t \triangleleft G_{t-1} \triangleleft \cdots \triangleleft G_1 \triangleleft G_0 = G$$

with  $G_i/G_{i+1} \cong C_{p_i}$  (the cyclic group on  $p_i$  elements). We may assume that we get cyclic groups since any refinement of a solvable series is solvable, and any composition series (i.e. a normal series that all the factor groups are simple) for a solvable group has factor groups that are cyclic of prime order. So we have the correspondence

Group Side                  Field Side



Where the extensions are normal (and hence Galois) because the series of groups on the left are normal. So,  $F_i/F_{i-1}$  is Galois and  $\text{Gal}(F_i/F_{i-1}) \cong G_i/G_{i-1} \cong C_{p_i}$  and  $K$  contains primitive  $p_i$ th roots of unity,  $\omega^{n/p_i}$ . Note that  $p_i \nmid [E : K]$  so  $\text{Char } K \nmid p_i$ . By the theorem on cyclic extensions, we have that  $F_i = F_{i-1}(u)$  where  $u^{p_i} \in F_{i-1}$ . Hence the above is a root tower, and hence  $E/F$  is solvable by radicals.