Square Root Constructibility

**Definition 1** A square root tower is a tower of fields

\[ Q = K_0 \subset K_1 \subset \ldots \subset K_r = K \]  

with, for \( 1 \leq i \leq r \), \( K_i = K_{i-1}(\sqrt[2]{\alpha_i}) \) where \( \alpha_i \in K_{i-1} \).

**Definition 2** \( \alpha \) is square root constructible if there exists a square root tower (1) with \( \alpha \in K_r \).

**Theorem 0.1** Given a square root tower (1) there exists another tower with fields \( K_i^+ \), \( 0 \leq i \leq r \) (plus other intermediate fields in the tower) where \( K_i \subset K_i^+ \) and (critically) \( K_i^+ : Q \) is normal.

**Proof:** \( K_0^+ = Q \). Suppose, by induction, that \( K_i^+ \) has been defined and is the splitting field of \( f(x) \in Q[x] \). Let \( \gamma \) be such that \( K_i = K_{i-1}(\sqrt[2]{\gamma}) \). Let \( p(x) \in Q[x] \) be the minimal polynomial for \( \gamma \) and let \( \gamma = \gamma_1, \ldots, \gamma_s \) be the roots of \( p(x) \). Set

\[ K_i^+ K_{i-1}^+ (\sqrt[2]{\gamma_1}, \ldots, \sqrt[2]{\gamma_s}) \]  

We extend the tower from \( K_{i-1}^+ \) to \( K_i^+ \) by

\[ K_{i-1}^+ \subset K_{i-1}^+ (\sqrt[2]{\gamma_1}) \subset K_{i-1}^+ (\sqrt[2]{\gamma_1}, \sqrt[2]{\gamma_2}) \subset \ldots \subset K_{i-1}^+ (\sqrt[2]{\gamma_1}, \sqrt[2]{\gamma_2}, \ldots, \sqrt[2]{\gamma_s}) = K_i^+ \]  

To show \( K_i^+ : Q \) is normal set

\[ g(x) = f(x)p(x^2) \]  

The roots of \( p(x^2) \) are \( \pm \sqrt[2]{\gamma_j} \) and the roots of \( f(x) \) generate \( K_i^+ \) so that \( K_i^+ \) is the splitting field of \( g(x) \).

**Theorem 0.2** Let \( \alpha \) be square root constructible. Let \( \alpha \) have minimal polynomial \( h(x) \in Q[x] \) with \( h(x) \) having roots \( \alpha = \alpha_1, \ldots, \alpha_r \). Let \( L = (\alpha_1, \ldots, \alpha_r) \) be the splitting field of \( h(x) \) over \( Q \). Then \( [L : Q] \) must be a power of two.

**Proof:** There is a square root tower (1) with \( \alpha \in K \) so by Theorem 0.1 there is a square root tower ending in some \( K^+ \) with \( \alpha \in K^+ \) and \( K^+ : Q \) normal. But then all \( \alpha_j \in K^+ \) so that \( L \subset K^+ \). As \( [K^+ : Q] \) is a power of two so is \( [L : Q] \).

**Comment:** Later we will show that Theorem 0.2 gives an if and only if condition for \( \alpha \) to be square root constructible.