**Ruler Compass Constructible**

**Definition 1** We say \( \alpha \in C \) is RC-constructible if there exists a tower of fields

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

with all \([K_i : K_{i-1}] = 2\) and \( \alpha \in K \). We also call the field \( K \) at the top of such a tower RC-constructible.

Earlier we showed that if \( \alpha \in C \) is RC-constructible then \([Q(\alpha) : Q] = 2^u\) for some \( u \). This is not a sufficient condition! Here we give necessary and sufficient conditions.

**Theorem 0.1** Let \( \alpha \in C \) have minimal polynomial \( p(x) \) with roots \( \alpha = \alpha_1, \ldots, \alpha_n \) and let \( \Omega \) denote the splitting field \( \Omega = Q(\alpha_1, \ldots, \alpha_n) \). Then \( \alpha \) is RC-constructible if and only if \([\Omega : Q] = 2^u\) for some \( u \).

Suppose \([\Omega : Q] = 2^u\). Let \( G = \Gamma[\Omega : Q] \), the Galois Group. Then \(|G| = 2^u\). By repeated application of the Sylow Theorem we find a reverse tower

\[
G = G_0 \supset G_1 \supset \cdots \supset G_{u-1} \supset G_u = \{e\}
\]

with \(|G_i| = 2^{u-i}\). The Galois Correspondence Theorem then gives a tower

\[
Q = K_0 \subset K_1 \subset \cdots \subset K_{u-1} \subset K_u = \Omega
\]

with each \([K_{i+1} : K_i] = 2\).

Now assume \( \alpha \) is RC constructible with tower (5), \( \alpha = \alpha_1, \ldots, \alpha_n \) the roots of \( p(x) \) above. Let \( \alpha' \) be any of the roots. There is an isomorphism \( \sigma : Q(\alpha) \to Q(\alpha') \) as they both have the same minimal polynomial. By the isomorphism extension theorem we may extend this to \( \sigma^+ : K \to K' \) for some \( K' \). Then, setting \( K'_i = \sigma(K_i) \),

\[
Q = K_0 \subset K'_1 \subset \cdots \subset K'_r = K'
\]

and \( \alpha' \in K' \) so that \( \alpha' \) is RC constructible.

Now we join the towers (5,4) to a single tower. Say \( K'_i = K_{i-1}(\sqrt[4]{\gamma_i}) \). The new tower starts by going to \( K \) and then goes to \( K' \). That is:

\[
Q = K_0 \subset K_1 \subset \cdots K_r \subset K^*_r \subset \cdots K^*_{2r}
\]

with \( K^*_r \subset K^*_r(\sqrt[4]{\gamma_i}) \). (It may happen that \( \sqrt[4]{\gamma_i} \) is already in \( K^*_{r+i-1} \), in which case the tower is even smaller.) We can do this one by one for each
of the roots \( \alpha' \). We end with a tower that contains all \( \alpha_1, \ldots, \alpha_n \) ending at some \( \Lambda \). But then \( [\Lambda : Q] = 2^w \) for some \( w \) and the splitting field \( \Omega \subset \Lambda \) so that, by the Tower Theorem, \( [\Omega : Q] = 2^u \) for some \( u \), completing the proof.

Comment: Suppose \( \alpha \) satisfies an irreducible quartic \( p(x) \) with splitting field \( \Omega \) and Galois Group \( G = \Gamma[\Omega : Q] \cong S_4 \). Then \( \alpha \) is not RC-constructible. The field \( Q(\alpha) \) has \( [Q(\alpha) : Q] = 4 \) but is not RC-constructible which means that it does not have a subfield \( L \) with \( [L : Q] = 2 \). That is: a converse of the Tower Theorem is false – it is not true that when \( [K : F] = s \) and \( d|s \) that there necessarily is an intermediate field \( L \) with \( [L : F] = d \).