Solution to problem number 9.5

Problem 1 (9.5). Suppose that \( L : K \) is a finite normal extension and that \( f \) is an irreducible polynomial in \( K[x] \). Suppose that \( g \) and \( h \) are irreducible monic factors of \( f \) in \( L[x] \). Show that there is an automorphism \( \sigma \) of \( L \) which fixes \( K \) such that \( \sigma(g) = h \).

Proof. We may assume that \( f \) is monic without harm, and do so. Now, since \( L : K \) is normal there is \( m_L \in K[x] \) such that \( L \) is the splitting field for \( m_L \) over \( K \) (this by Cor. 1 to Theorem 9.1). Let \( \omega_1, \ldots, \omega_n \) be the roots of \( m_L \), so that \( L = K(\omega_1, \ldots, \omega_n) \) (Theorem 7.1), and let \( \Sigma \) be the splitting field for \( f \) over \( L \). Of course \( \Sigma : K \) and \( f m_L \) splits over \( \Sigma \). Suppose that \( F \) is a subfield of \( \Sigma \) containing \( K \) and that \( f m_L \) splits over \( F \). Then \( \omega_1, \ldots, \omega_n \in F \) so that \( F \) also contains \( L \), and hence \( F = \Sigma \). So \( \Sigma \) is the splitting field for \( f m_L \) over \( K \) and thus is normal over \( K \) (Theorem 9.1).

We may suppose, without loss of generality, that \( \deg g \leq \deg h \) (if in fact \( \deg h \leq \deg g \), the argument below provides an automorphism \( \sigma : L \to L \) which fixes \( K \) and sends \( h \to g \), whence \( \sigma^{-1} \) is an automorphism satisfying the required conditions). Let \( \alpha, \beta \in \Sigma \) be roots of \( g \) and \( h \) respectively. It follows that \( \alpha \) and \( \beta \) are roots of \( f \); in fact, since \( f \) is a monic irreducible in \( K[x] \), it is the unique minimal polynomial of both \( \alpha \) and \( \beta \) over \( K \). So by Cor. 1 to Theorem 7.4 there is a unique isomorphism \( i : K(\alpha) \to K(\beta) \) which extends the identity map on \( K \) and sends \( \alpha \) to \( \beta \).

Certainly \( \Sigma \) is a splitting field for \( f m_L \) over \( K(\alpha) \) (\( f m_L \) obviously splits over \( \Sigma \) and any smaller field \( F \) containing \( K(\alpha) \) over which \( f m_L \) splits necessarily contains \( K \) so that \( \Sigma = F \) as required). Similarly, \( \Sigma \) is a splitting for \( i(f m_L) \) over \( K(\beta) \) because \( i(f m_L) = f m_L \) (recall that \( i \) fixes \( K \)). Thus by Theorem 7.5, there is an automorphism \( j : \Sigma \to \Sigma \) which extends \( i \).

Now we have \( \Sigma : L : K \) with \( \Sigma : K \) and \( L : K \) normal extensions, and conclude, by Theorem 9.2, that \( j(L) = L \). So let \( \sigma = j|_L \), and consider \( \sigma(g) \). Now \( (x-\alpha) \) divides \( g \) (over \( \Sigma[x] \)), so \( j(x-\alpha) = i(x-\alpha) = (x-\beta) \) divides \( j(g) = \sigma(g) \), that is, \( \beta \) is a root of \( \sigma(g) \). But \( h \) is the minimal polynomial for \( \beta \) over \( L \), so \( h \) divides \( \sigma(g) \). On the other hand, \( \sigma(g) \) is monic (since \( g \) is monic) and \( \deg \sigma(g) = \deg g \leq \deg h \), so \( \sigma(g) = h \) as required.

\( \Box \)