Math 121. Automorphisms of normal extensions

Let $L/k$ be a normal algebraic extension of fields, and let $K \subset L$ be a subfield containing $k$. In this handout we wish to prove a useful normality criterion for $K/k$ in terms of the effect on $K$ by the action of the group $\text{Aut}_k(L)$ of $k$-automorphisms of $L$.

**Theorem 0.1.** In the above setup, the following three conditions are equivalent:

(i) $K/k$ is normal,
(ii) for all $\sigma \in \text{Aut}_k(L)$, $\sigma(K) = K$,
(iii) for all $\sigma \in \text{Aut}_k(L)$, $\sigma(K) \subset K$.

We will prove this theorem only when $[L:k]$ is finite, as this is the only case we will need. The general case can be reduced to this case by appropriate use of Zorn’s Lemma, etc. In the finite-degree case, certainly $[K:k]$ is finite (it is even a factor of $[L:k]$), so (ii) and (iii) are equivalent since multiplicativity of field degree implies $[K:k] = [K:\sigma(K)][\sigma(K):k]$ yet $[\sigma(K):k] = [K:k]$ since $\sigma : K \cong \sigma(K)$ is a $k$-isomorphism, forcing $[K:\sigma(K)] = 1$ (i.e., $\sigma(K) = K$).

Likewise, if (i) holds then (by finiteness of $k$-degree) we have $K = \text{split}_k(f)$ for some monic non-constant $f \in k[X]$, and hence $K = k(r_1, \ldots, r_d)$ where $f = \prod(X - r_i)$ in $k[X]$. Thus, for any $\sigma \in \text{Aut}_k(L)$ the effect of $\sigma$ on $L$ must permute the $r_i$'s since $\sigma$ preserves $f \in k[X]$. It follows that $\sigma$ carries $K = k(r_1, \ldots, r_d)$ back onto itself, which is to say that (ii) holds.

The main content then is that (iii) (or (ii)) implies (i). Put another way, if $K/k$ is not normal, we seek to construct $\sigma \in \text{Aut}_k(L)$ such that $\sigma(K)$ is not contained in $K$. Failure of normality implies that there is some irreducible $h \in k[X]$ with a root $r \in K$ yet for which $h$ does not split completely over $K$. But $L/k$ is normal and $r \in L$ is a root of $h$, so $h$ does split completely over $L$. Thus, since $h$ does not split completely over $K$, some root $r'$ of $h$ in $L$ must fail to lie in $K$. It therefore suffices to find $\sigma \in \text{Aut}_k(L)$ such that $\sigma(r) = r'$ (as then $\sigma(K)$ contains $\sigma(r) = r' \notin K$, so $\sigma(K)$ is not contained in $K$).

To summarize, it suffices to show that for the finite normal extension $L/k$ and any irreducible $h \in k[X]$ with a root $r \in L$ (so $h$ splits completely over $L$), if $r' \in L$ is a root of $h$ then there exists $\sigma \in \text{Aut}_k(L)$ such that $\sigma(r) = r'$. (Note that this assertion has nothing to do with an intermediate field $K$.) The existence of such a $\sigma$ was already seen in class as part of our proof that splitting fields satisfy the property of being a normal closure, but for the convenience of the reader we now restate the relevant part of the argument.

We may assume $h$ is monic, so $h = \prod_{i=1}^d(X - \rho_i)$ in $L[X]$. Let $F = k(\rho_1, \ldots, \rho_d) \subset L$, so $F$ is a splitting field of $h$ over $k$. Note that $r, r'$ must be among the $\rho_i$'s. We know that $\text{Aut}_k(F)$ acts transitively on the set of roots of $h$ in $F$, so there exists $\sigma_0 \in \text{Aut}_k(F)$ such that $\sigma_0(r) = r'$. It suffices to build an automorphism $\sigma$ of $L$ extending $\sigma_0$ on $F$.

The normality of $L$ over $k$ implies that $L$ is a splitting field of some $\varphi \in k[X]$. Thus, $L$ is generated over $k$ by a set of roots of $\varphi$ (which in turn suffice to completely split $\varphi$ over $L$). Hence, $L$ is generated over $F$ by those roots as well. Consider the given inclusion $j : F \hookrightarrow L$ and the composite inclusion $j \circ \sigma_0 : F \hookrightarrow L$ over $k$. These maps both express $L$ as a splitting field of $\varphi$ over $F$ (the latter because the polynomial $\varphi \in k[X] \subset F[X]$ is unaffected by applying the $k$-automorphism $\sigma_0$ to its coefficients!), so by uniqueness of splitting fields there is an isomorphism $\sigma : L \cong L$ over these two inclusions of $F$ into $L$. This says exactly that $\sigma$ restricts to $\sigma_0$ on the subfield $j : F \hookrightarrow L$. In other words, we have built an automorphism of $L$ which extends $\sigma_0$ on $F$, and we have seen above that this is sufficient for our needs.